UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Moša Maržun
Tjaša Karničar

Načrtovanje zaščite ınformacıjsko-komunıkacıjske ınfrastrukture v gospodarskih družbah, zavodih in drugih organizacijah posebnega pomena za obrambo države

Magistrsko delo

Ljubljana, 2015

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Moša Maržun
Tjaša Karničar

Mentor: doc. dr. Uroš Svete

Načrtovanje zaščite ınformacıjsko-komunıkacıjske ınfrastrukture v gospodarskih družbah, zavodih in drugih organizacijah posebnega pomena za obrambo države

Magistrsko delo

Ljubljana, 2015

Zahvala

Najlepše se zahvaljujeva svojima družinama za podporo in razumevanje pri raziskovanju in pisanju magistrskega dela.

Še posebej se zahvaljujeva mentorju doc. dr. Svetetu, ki nama je s kritičnimi a konstruktivnimi nasveti utiral pot, ko je bila le ta nejasna.

Najiskrenejša zahvala pa gre nekaterim sodelujočim v raziskavi ge. Alenki Čarni in g. Romeu Palčiču z Ministrstva za obrambo Republike Slovenije in g. Alojzu Cestniku iz Univerzitetnega kliničnega centra Ljubljana, ki so nama s svojimi odgovori in pripravljenostjo na sodelovanje stali ob strani od samega začetka do konca.

Vedno na koncu sta dve poti, izbereš pa tisto, ki je ni.

POVZETEK: Načrtovanje zaščite ınformacıjsko-komunıkacıjske ınfrastrukture v gospodarskih družbah, zavodih in drugih organizacijah posebnega pomena za obrambo države

Sodobna družba je vedno bolj vpeta v globalizacijske tokove, povezanost različnih držav in družb se krepi tudi z uporabo informacijsko-komunikacijske tehnologije. Omenjena tehnologija pridobiva na pomenu, s tem je tudi tarča sodobnih groženj varnosti in različnih virov ogrožanja.

Republika Slovenija je za potrebe obrambe izpopolnila sistem civilne obrambe, ki je bil koncipiran še v prejšnjem družbeno-političnem sistemu, in določila gospodarske družbe, zavode in druge organizacije, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji. Te organizacije imajo odgovornost stalnega zagotavljanja storitev, proizvodov in dejavnosti ter družbeno dolžnost oblikovanja obrambnih načrtov za primere kriz in vojne. Tudi omenjene organizacije se v današnjih časih vedno bolj zanašajo na uporabo informacijsko-komunikacijske tehnologije, ki je lahko podvržena morebitnemu ogrožanju s strani različnih akterjev. Zato je načrtovanje zaščite te infrastrukture v okviru mednarodno sprejetih smernic in zavez ter nacionalne zakonodaje bistvena naloga organizacij. Poleg tega se v Republiki Sloveniji pospešeno razvija koncept kritične infrastrukture, ki narekuje določitev elementov kritične infrastrukture ter načrtovanje zaščite le teh, zajema pa tudi informacijsko komunikacijsko infrastrukturo.

Cilj magistrske naloge je izpostaviti pomen načrtovanja zaščite elementov informacijsko-komunikacijske infrastrukture in preučiti sistemske rešitve, ter pripravljenost informacijsko-komunikacijske infrastrukture v gospodarskih družbah, zavodih in drugih organizacijah, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji tudi v povezavi s konceptom zaščite kritične infrastrukture in obrambnega planiranja.

V delu avtorja skozi opredelitev groženj varnosti informacijsko komunikacijski infrastrukturi v organizacijah, katerih dejavnost je posebnega pomena za obrambo države, pristopiva k preučevanju koncepta obrambnega načrtovanja v Republiki Sloveniji in na koncu določanju sektorjev in elementov kritične infrastrukture v Republiki Sloveniji. To doseževa s poglobljeno analizo normativnih aktov s področja načrtovanja zaščite informacijsko komunikacijske infrastrukture v omenjenih organizacijah ter z neposrednim anketiranjem odgovornih za varnost in zaščito informacijsko komunikacijske infrastrukture v organizacijah, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji. Pri tem se osredotočiva na nacionalno zakonodajo ter smernice EU in NATO. Poseben poudarek dajeva preučevanju obrambnega planiranja in načrtovanju zaščite informacijsko komunikacijske infrastrukture v gospodarskih družbah, zavodih in drugih organizacijah, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji. Končni produkt se odraža v poglobljenem spoznanju o horizontalnih in vertikalnih povezavah, odgovornostih, nadzoru in pogledih pri obrambnem planiranju in načrtovanju zaščite informacijsko komunikacijske infrastrukture med omenjenimi organizacijami in sistemskimi odločevalci na ravni države. Pri tem prideva do praktičnih spoznanj o načinih zaščite informacijsko komunikacijske infrastrukture, komunikacijskih povezavah med organizacijami in sistemskimi odločevalci ter o vključevanju različnih varnostnih akterjev v zaščito informacijsko komunikacijske infrastrukture v Republiki Sloveniji.

Ključne besede: informacijsko-komunikacijska infrastruktura, obrambno planiranje, načrtovanje zaščite, organizacije

ABSTRACT: Planning the protection of information-communication tehnology in business companies, institutions and other organizations of special importance for the defence of the Republic of Slovenia

Modern society is becoming more and more integrated into globalization flows and the connection between countries and societies is strengthened through the use of information-communication technology. This technology is gaining importance which leads to it being a target of modern-day security risks and different sources of threat.
For defence needs, the Republic of Slovenia has improved the system of civil defence that had been designed in the previous socio-political system. The country has also selected business companies, institutions and other organizations that are of special importance for the defence of the Republic of Slovenia. These organizations have the responsibility to provide permanent service, products and activities, and the social duty to design defence plans for the cases of crises and war. Nowadays, these organizations also increasingly rely on the use of information-communication technology that could be subject to threats by different agents. Therefore, planning the protection of this infrastructure in the framework of internationally accepted guidelines and obligations as well as the national regulations is the key task of these organizations. Moreover, in the Republic of Slovenia, there is a fast development of the concept of critical infrastructure that dictates specification of the elements of critical infrastructure and planning of its protection and also includes information-communication infrastructure.
The aim of the master's thesis is to emphasize the meaning of protection planning of information-communication infrastructure elements and to study the system solutions and the readiness of information-communication infrastructure in business companies, institutions and other organizations, the activities of which are of special importance for the defence in the Republic of Slovenia, in connection to the concept of protection of critical infrastructure and defence planning.
In the thesis, the authors study the concept of defence planning in the Republic of Slovenia through defining the threats to security of information-communication infrastructure in organizations, the activities of which are of special importance for the defence of the country. Finally, we specify sectors and elements of critical infrastructure in the Republic of Slovenia. We achieve that through detailed analysis of regulations from the field of information-communication infrastructure defence planning in the aforementioned organizations and with surveying the people who are responsible for security and protection of information-communication infrastructure in organizations, the activities of which are of special importance for the defence in the Republic of Slovenia. We focus on the national legislation and the EU and NATO guidelines. There is a special emphasis on studying defence planning and information-communication infrastructure defence planning in business companies, institutions and other organizations that are of special importance for the defence of the Republic of Slovenia. The thesis presents thorough findings about horizontal and vertical connections, responsibilities, control and views on defence planning and information-communication infrastructure protection planning among the aforementioned organizations and national policy-makers. We have gained practical findings about the ways of information-communication infrastructure protection, communication connections between organizations and policy-makers and about including different security agents into the information-communication infrastructure protection in the Republic of Slovenia.

Key words: information-communication infrastructure, defence planning, protection planning, organizations

KAZALO

KAZALO SLIK

KAZALO TABEL

Seznam uporabljenih kratic

CIIP	zaščita kritične informacijske infrastrukture (ang. *Critical Information Infrastructure Protection*)
CIWIN	informacijsko omrežje za opozarjanje o ključni infrastrukturi (ang. *Critical Infrastructure Warning Information Network*)
EK	evropska komisija
EKI	evropska ključna infrastruktura
ENISA	Evropska agencija za omrežno in informacijsko varnost (ang. *European Network and Information Security Agency*)
EPCIP	Evropski program zaščite kritične infrastrukture (ang. *European Programm for Critical Infrastructure Protection*)
EU	Evropska unija
IK	informacijsko-komunikacijski
IKI	informacijsko-komunikacijska infrastruktura
IKT	informacijsko-komunikacijska tehnologija
JRKB	jedrsko, radiološko, kemično in biološko
KI	ključna oz. kritična oz. vitalna infrastruktura
KIKI	kritična informacijsko-komunikacijska infrastrukture
MORS	Ministrstvo za obrambo Republike Slovenije
NATO	Organizacija severnoatlantskega sporazuma (ang. *North-Atlantic Treaty Organization*)
NCKU	Nacionalni center za krizno upravljanje
OVS	Obveščevalno-varnostna služba (MORS)
ReSNV	Resolucija o strategiji nacionalne varnosti Republike Slovenije
RS	Republika Slovenija
SOVA	Slovenska obveščevalno-varnostna agencija
VOI	varnost omrežij in informacij
VRS	Vlada Republike Slovenije
ZDA	Združene države Amerike
ZKI	zaščita kritične infrastrukture
ZTP	Zakon o tajnih podatkih
ZKIKI	zaščita kritične informacijske-komunikacijske infrastrukture

1 UVOD

Republika Slovenija (RS) se je v letih svojega obstoja znašla v mnogih kriznih situacijah, s katerimi se je bolj ali manj uspešno spopadala. V zadnjih letih so se spremenile tako grožnje (oz. njihovo pojmovanje in vrednotenje) kot tudi odzivanje nanje. Države se namreč soočajo s hkratnim obstojem groženj iz različnih dimenzij (večdimenzionalnost), ki so visoko (ne)linearno povezane in transnacionalne (Prezelj 2002, 59–64). RS je članica Evropske Unije (EU) in Severnoatlantskega zavezništva (NATO). Ti dve mednarodni organizaciji vplivata na oblikovanje smernic in zmogljivosti odzivanja na grožnje.

Krize so postale del našega sveta, del našega načina življenja (Rosenthal in drugi 2001). Sodobne družbe so postale tehnološko napredne in s tem tudi vedno bolj odvisne od informacijsko-komunikacijskih sistemov. Fizično obvladovanje prostora kot elementa tradicionalne geopolitike še vedno prevladuje, pojavlja pa se tudi razprava o strateški vlogi in pomenu IKT (informacijsko-komunikacijske tehnologije), ki je splošno družbeno prisotna, razširjena in služi kot temelj za delovanje (državnih) institucij, industrije ter gospodarstva. Od telekomunikacij in omrežij so odvisni tudi infrastrukturni podsistemi, kot so: promet, energetski sistem, bančne in finančne institucije, zdravstvo ter sistem zaščite in reševanja in javna uprava (Svete 2010, 43).

V letu 2014 je bilo na svetu 2,89 milijarde uporabnikov interneta, kar je že več kot dva od petih ljudi na svetu. Spletna javnost bo v letu 2015 presegla 3 milijarde, kar pomeni kar 6,2 odstotno povečanje števila uporabnikov. Slednji podatki kažejo, da bo v letu 2015 internet uporabljalo že 42,4 odstotka svetovnega prebivalstva. Do leta 2018 bo internet uporabljala skoraj polovica svetovnega prebivalstva ali 3,6 milijarde ljudi. Analitiki pri eMarketerju pravijo, da poceni mobilni telefoni in mobilne širokopasovne povezave spodbujajo dostop in uporabo interneta v državah, kjer je bil fiksni internet zunaj dosega potrošnikov, bodisi zaradi pomanjkanja infrastrukture bodisi dostopnosti (eMarketer 2014).

V prvem četrtletju 2014 je imelo v Sloveniji dostop do interneta 77 % gospodinjstev, med temi so bila skoraj vsa gospodinjstva z otroki (97 %) (Statistični urad Republike Slovenije: Uporaba interneta v gospodinjstvih in pri posameznikih, Slovenija, 2014 - končni podatki) Med gospodinjstvi z dostopom do interneta je čedalje več tudi takih, ki dostopajo do interneta prek mobilnih širokopasovnih internetnih povezav. V prvem četrtletju 2013 je bilo takih gospodinjstev 42 odstotkov, v prvem četrtletju 2014 pa že 49 odstotkov (prav tam).

Naj omeniva, da se je število kibernetskih napadov na svetovni ravni v primerjavi z letom 2012 v letu 2013 povečalo za kar 350 odstotkov. Ocenjena vrednost škode zaradi kibernetskih napadov tako znaša 445 milijard dolarjev na leto (Pišlar 2014, 9).

To pomeni, da se potencialni napadalci zavedajo pomena IKT, čeprav gre v tem primeru za kibernetske napade. Ta podatek ne zajema fizičnih napadov na sisteme IKT, ki je "eden od sektorjev kritične infrastrukture" (Svete v Prezelj 2010, 43). Kot vidimo je sektor IKT podvržen tako fizičnim kot tudi kibernetskim grožnjam, nikakor pa ne smemo zanemariti tudi okoljskih groženj varnosti in človeškega dejavnika ogrožanja varnosti. Grožnjam IKT ni podvržen samo IKT sektor ampak tudi ostali tradicionalni sektorji. Ti sektorji zajemajo tudi subjekte nacionalne varnosti, kot so gospodarske družbe, zavodi in druge organizacije, ki imajo zaradi opravljanja svoje dejavnosti z zakonom opredeljene posebne naloge pri obrambi države (ZObr-UPB1, 73. člen). Gospodarski idr. subjekti, ki so v RS opredeljeni kot subjekti posebnega pomena za obrambo države, so (MORS 2014a, Sklep št. 80101-1/2014/5):

- Aerodrom Ljubljana d.d.,
- Eles - Elektro Slovenija d.o.o.,
- Univerzitetni klinični center Ljubljana,
- Luka Koper d.d.,
- Petrol d.d.,
- Javni zavod Radiotelevizija Slovenija,
- Slovenske železnice d.o.o.,
- Telekom Slovenije d.d.,
- Zavod RS za blagovne rezerve,
- Zavod RS za transfuzijsko medicino,
- Nacionalni inštitut za javno zdravje,
- Kontrola zračnega prometa Slovenije d.o.o.,
- Univerzitetni klinični center Maribor.

Do leta 2014, ko je bil sprejet nov sklep, je veljal Sklep iz leta 1996 (MORS 1996), ki je vključeval tudi Pošto Slovenije. Leta 2014 so z novim Sklepom Pošto Slovenije izvzeli, dodali pa so UKC Maribor, Nacionalni inštitut za javno zdravje ter Kontrolo zračnega prometa (MORS 2014).

Pomen infrastrukture se je skozi čas spreminjal. Uničenje pomembne infrastrukture je bila vedno prednostna naloga vojaških enot v posameznih vojnah. Vendar se je pojmovanje in pomen ključne infrastrukture spremenil in je postala pomemben sestavni del nacionalne varnosti. To se je zgodilo med hladno vojno oziroma kasneje po 11.9.2001. Termin kritična

infrastruktura je po drugi strani v veljavi od sredine 90-ih let 20. stoletja, ko ga je v uporabo vpeljala Clintonova administracija (Aradau 2010).

Literatura, ki sva jo predelala, se v zadnjem času osredotoča predvsem na kibernetske grožnje varnosti. Področje načrtovanja zaščite IKI (informacijsko-komunikacijske infrastrukture) je široko in ne zajema samo spletnih storitev, pač pa je v to potrebno vključiti tudi zagotavljanje fiksnih telekomunikacij in mobilnih telekomunikacij, radijske komunikacije, satelitske komunikacije in oddajnike, s katerimi se bova tudi ukvarjala v magistrskem delu.

Glede na naraščajoče podatke o številu priključkov (tako fiksnih kot mobilnih) lahko zaključimo, da smo vedno bolj odvisni od IKI, kar posledično pomeni, da smo tudi bolj dovzetni za grožnje. Kot primer navajava potek sklicne liste v primeru alarmiranja sil Slovenske vojske, ki poteka preko mobilnih ali stacionarnih telefonov. Drugi primer je primer zdravnikov – kirurgov, ki uporabljajo sistem na klic (Prezelj 2008). Slednje nakazuje, da nedelovanje IKI lahko privede do posrednih posledic, tudi žrtev. Tudi Coward (2009) poudarja pomen informacijsko-komunikacijske infrastrukture, saj jo uvrša med eno izmed treh pomembnejših elementov (informacijsko-komunikacijski sektor, transportni sektor in elektroenergetski sektor) v razpravah o kritični infrastrukturi.

Stroški sesutja omrežja IKI so nedoločljivi, saj bi nedelovanje sektorja IKT imelo posledice v vseh drugih sektorjih. Svete (v Prezelj 2010, 59) trdi, da je IKT sektor neposredno najbolj povezan s finančnim, energetskim in prometnim sektorjem. V kolikor bi se zgodila nepredstavljiva kriza, katere posledice bi najbolj občutil sektor IKT, bi se kriza prenesla tudi vsaj v preostale tri omenjene sektorje.

V letu 2008 je projektna skupina na Fakulteti za družbene vede pod vodstvom doc. dr. Prezlja zaključila raziskovalni projekt "Definicija in zaščita kritične infrastrukture Republike Slovenije" in pripravila končno poročilo. V poročilu so prišli do spoznanja, da bi morali IKT z vidika kritične infrastrukture preučevati znotrajsektorsko in ne samostojno (Prezelj 2008, 475). Zaradi slednje ugotovitve sva se odločila, da k najini problematiki pristopiva na tak način.

2 METODOLOŠKI OKVIR

2.1 Opredelitev predmeta in ciljev preučevanja

Osnovni namen naloge je, na podlagi preučitve normativnih aktov in akterjev podati predloge za bodoče urejanje področja načrtovanja zaščite IKI v Republiki Sloveniji. Preučila bova vpletenost (nacionalno) varnostnih akterjev v načrtovanje zaščite glede na intenziteto groženj s katerimi so se do sedaj oz. se bodo v prihodnosti soočali gospodarski idr. subjekti posebnega pomena za obrambo države. Zanima naju tudi, na kakšen način v RS izvajajo načrtovanje zaščite IKI in stopnja vključenosti države v oblikovanje načrtovanja zaščite le-te.

Cilj magistrskega dela je preučiti pomembnost IKI in možnost opredelitve informacijsko-komunikacijske infrastrukture kot KIKI (kritično informacijsko-komunikacijsko infrastrukturo) ter preučiti izvajanje načrtovanja zaščite IKI v RS na primeru vseh zgoraj omenjenih gospodarskih subjektov ključnega pomena za obrambo države. Skozi nalogo bova skušala preučiti kako so sistemi IKI, znotraj omenjenih gospodarskih družb in zavodov, zaščiteni pred raznimi viri ogrožanja. Cilj je tudi preučiti, do katere mere so upoštevane normativne usmeritve in dobre prakse na nadnacionalni ravni, kjer se bova osredotočila predvsem na EU in NATO.

2.2 Metodološki pristop

Najina raziskava bo kvalitativna, zato sva se odločila za uporabo naslednjih tehnik.

§ ***Analiza in interpretacija sekundarnih virov*.**

Analizirala bova uradne dokumente (EU, NATO in Slovenije), monografske publikacije in članke, ki se ukvarjajo s področjem zaščite IKI in sva jih navedla v literaturi. S tem bova ugotovila, kakšno bi moralo biti stanje zaščite IKI znotraj gospodarskih družb, zavodov in drugih organizacij posebnega pomena za obrambo Slovenije.

§ **Študija primera** "je podrobna raziskava, pogosto s podatki, ki jih zbiramo daljše obdobje, ene ali več organizacij ali skupin v organizacijah, ki skuša analizirati kontekst in procese, ki jih vključuje pojav, ki je predmet preučevanja. Pojava ne preučujemo izolirano od konteksta ampak nas zanima natanko zato, ker je v odnosu do konteksta" (Cassell in Symon 1994, 208 v Mesec 2011, 2). "Metodo študije primera se izvede tako, da se o primeru zbere podatke iz

različnih virov in z različnimi metodami, primer se opiše in analizira ter na tej osnovi oblikuje posplošitve primerov, njihovega razvoja in procesov" (Mesec 2011, 2).

Najine študije primera bodo gospodarske družbe, zavodi in druge organizacije, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji (v nalogi imenovane tudi organizacije posebnega pomena za obrambo države). Bolj podrobno naju bo znotraj teh podjetij zanimala zaščita IKI. Ker podjetja zaradi opravljanja svoje dejavnosti spadajo pod različne sektorje bo šlo za medsektorski horizontalni pogled, kjer bova spremljala zaščito IKI po različnih sektorjih oz. po različnih organizacijah, ki so posebnega pomena za obrambo države. S to metodo bova poskušala prikazati tudi kako veliko vlogo ima IKT sektor znotraj ostalih sektorjev in zakaj je njegova zaščita tako pomembna. Pri vsem tem je potrebno opozoriti, da se bova soočala z omejenim dostopom do informacij zaradi samega značaja družb, zavodov in organizacij ter primarne dejavnosti, ki jo opravljajo.

S pomočjo študije primerov bova ugotovila kakšno je dejansko stanje zaščite IKI v gospodarskih družbah, zavodih in drugih organizacijah posebnega pomena za obrambo Slovenije ter kateri varnostni akterji so vključeni v zaščito.

§ *Metoda delphi (delfi)*

Metodo delfi sestavljata tako kvalitativni kot kvantitativni proces, njen temelj pa so mnenja skupine strokovnjakov (Bourgeois in sodelavci v Urbanc, Perko in Petek 2008, 144). Metodo delfi lahko uporabimo tudi takrat, ko o nekem problemu nimamo zadostnega znanja, torej v primeru pomanjkanja podatkov (Adler in Ziglio; Delbeq in sodelavci v Urbanc, Perko in Petek, 2008, 144). S pomočjo metode delfi lahko pridobivamo in usklajujemo mnenja izvedencev, iščemo med mnenji podobnosti in razlike. Strokovnjaki vprašanja dobijo večkrat zapored in na njih odgovarjajo individualno, saj mora biti zagotovljena anonimnost. Ker metoda defi poteka v večih krogih imajo strokovnjaki priložnost, da svoja mnanja nadgradijo na podlagi rezultatov iz prejšnjih krogov, z izjemo prvega. Metoda je posebna, ker kljub raznolikosti mnenj in brez neposrednega stika z strokovnjaki in med njimi omogoča zanesljivost (Urbanc, Perko in Petek 2008, 144–145). Pri metodi je pomembno, da vključimo v raziskavo visoko usposobljene izvedence različnih področij, ki so povezani z raziskovalnim problemom (prav tam).

Metoda je bila izbrana zaradi ocenjevanja področja dejavnosti, ki so odvisna od tehnološkega razvoja ter s tem podvržena tudi subjektivni oceni posameznikov o pomembnosti IKI za opravljanje primarne dejavnosti podjetij, zavodov in drugih organizacij,

katerih dejavnost je posebnega pomena za obrambo v RS, s čimer bi rada to subjektivnost ocene izničila.

Metodo delfi izvedemo v večih krogih anketiranja:

1. **krog**: Skušamo dobiti bolj splošne informacije. Prvi vprašalnik zato vsebuje odprta vprašanja, povezana z raziskovalnim problemom. Strokovnjaki podajo mnenja in vrnejo prašalnike (Urbanc, Perko in Petek 2008, 145).
2. **krog**:. Raziskovalci obdelajo odgovore in na njihovi podlagi izdelajo drugi vprašalnik.strokovnjaki ocenjujejo in razvrščajo teme, ki so bile oblikovane v prvem krogu. Poleg starih tem so v vprašalniku tudi nova vprašanja. V tem krogu lahko izvedenci tako podajo mnenja kot utemeljitve odgovore (prav tam).
3. **krog**: Rezultati analize drugega kroga so temelj oblikovanja vprašalnika za tretji krog. Na začetku vprašalnika se nahaja povzetek odgovorov iz prvih dveh krogov, skupaj z nekaterimi statističnimi podatki, kar omogoča strokovnjakom, da svoje odgovore primerjajo z drugimi. V tem krogu imajo tudi možnost, da popravijo ali dopolnijo katerikoli prejšnji odgovor. Raziskovalci ponovno obdelajo odgovore in se odločijo ali bodo izpeljali nadaljnje kroge in ponavljajo opisano, dokler eksperti ne dosežejo konsenza o določeni problematiki (prav tam).

V najinem primeru to pomeni uporabo prirejene metode z izvedbo le dveh krogov anketiranja, zaradi slabega odziva anketirancev. Anketiranje in vprašalniki so prilagojeni raziskavi z močnim poudarkom na prvi krog anketiranja s poglobljeno analizo predmeta preučevanja. Raziskava bo zajemala:

§ *Individualni poglobljeni intervjuju*

Zaradi malega števila gospodarskih družb, zavodov in drugih organizacij posebnega pomena za obrambo Slovenije, bova uporabila nestrukturirane vprašalnike. Intervjuvala bova strokovnjake, ki so v teh podjetjih odgovorni za zaščito njihove IKI. Intervju bova opravila tudi v Nacionalnem centru za krizno upravljanje, na Uradu vlade Republike Slovenije za varovanje tajnih podatkov ter na Ministrstvu za visoko šolstvo, znanost in tehnologijo. Zanimalo pa naju bo tudi mnenje odločevalcev, zato bova opravila intervjuje še z generalnim direktorjem Direktorata za obrambne zadeve Ronaldom Želom ter z Rajkom Najzerjem iz Sektorja za zaščito. V okviru raziskave si puščava odprta vrata za dodajanje intervjuvancev, v kolikor bi se v toku raziskave to izkazalo za potrebno.

§ *Posredovanje zaprtega/polzaprtega vprašalnika*

V vprašalniku bodo istim anketirancem ponujene alternative na odgovore pridobljene pri prvem anketiranju. S tem jih bova že postavila v situacijo, da podrobneje razmislijo o danih odgovorih na prvem srečanju ter jim dala možnost, da si premislijo. Poleg tega jim bo dopuščena možnost dopisovanja lastnih ugotovitev in prepričanj, s čimer lahko anketiranci vplivajo na raziskavo z odpiranjem novih pogledov raziskovalcev na raziskovano tematiko.

§ *Vprašalnik s statističnimi vrednostmi in časovnimi intervali*

S tretjim krogom bi raziskovalca preverila točnost odgovorov v drugem krogu in ocenila njihovo vrednost v napovedanem času. V najinem primeru se je to izkazalo kot nemogoče, zaradi slabega odziva preučevanih organizacij na prva dva kroga.

2.3 Hipoteze

V nalogi sva si zastavila naslednji hipotezi, ki jih bova v sklepu poskušala bodisi potrditi ali zavrniti.

Hipoteza 1: Nadnacionalne organizacije (EU, NATO) vse bolj v ospredje postavljajo predvsem kibernetske grožnje varnosti, čemur se gospodarske družbe, zavodi in druge organizacije posebnega pomena za obrambo prilagajajo.

Hipoteza 2: Primarna dejavnost gospodarskih družb, zavodov in drugih organizacij posebnega pomena za obrambo Republike Slovenije je v veliki meri odvisna od IKI, zato lahko slednjo opredelimo kot ključno/kritično IKI (KIKI).

2.4 Temeljni pojmi

Opredelitev pojmov (po Uredba o evropski kritični infrastrukturi 2011):

(a) „*kritična infrastruktura državnega pomena*“ obsega tiste zmogljivosti, ki so ključnega pomena za državo in bi prekinitev njihovega delovanja ali njihovo uničenje pomembno vplivalo oziroma imelo resne posledice na nacionalno varnost, gospodarstvo, temeljne družbene funkcije, zdravje, varnost in zaščito ter družbeno blaginjo, ocenjene po merilih, ki jih določi Vlada Republike Slovenije;

(b) „*evropska kritična infrastruktura*“ ali „EKI“ obsega kritično infrastrukturo, ki se nahaja v državah članicah in katere okvara ali uničenje bi imelo resne posledice, ocenjene po medsektorskih merilih v vsaj dveh državah članicah;

(c) „*analiza tveganja*“ pomeni obravnavo ustreznih scenarijev nevarnosti, da se ocenijo šibke točke in morebitne posledice okvare ali uničenja kritične infrastrukture;
(d) „*občutljive informacije, povezane z zaščito kritične infrastrukture*“ pomeni dejstva o kritični infrastrukturi, katerih razkritje bi se lahko uporabilo za načrtovanje in delovanje z namenom povzročitve okvare ali uničenja objektov kritične infrastrukture;
(e) „*zaščita*“ pomeni vse dejavnosti, katerih namen je zagotavljati funkcionalnost, kontinuiteto in integriteto kritične infrastrukture, da se preprečijo, ublažijo in nevtralizirajo nevarnosti, tveganja in šibke točke;
(f) „*lastniki/upravljavci EKI*“ pomeni subjekte, odgovorne za naložbe v posamezno infrastrukturno zmogljivost, sistem ali njegov del, ki je v skladu s to direktivo določen kot EKI in/ali njihovo vsakodnevno delovanje.

3 TEORETIČNI OKVIR

3.1 Sodobno razumevanje varnosti in varnostne teorije

Konec hladne vojne in posledično spremenjeno varnostno okolje sta prinesla premik od tradicionalnih groženj k ne-tradicionalnim virom ogrožanja varnosti. Kar naenkrat ni bila več v ospredju samo nacionalna varnost ampak tudi varnost posameznika in mednarodne skupnosti. V preteklosti je imelo varnostno okolje predvsem vojaško-politične razsežnosti, danes pa vključuje tudi druge socialne in kulturno-civilizacijske dimenzije. Družbeno in naravno okolje je postalo bolj kompleksno. Proces globalizacije in decentralizacija moči otežujejo delitev groženj varnosti na notranje in zunanje.

Sodobno varnostno razpravo definirajo predvsem trije referenčni objekti: na koga se varnost nanaša, kdo ali kaj to varnost ogroža in preko katerih varnostnih mehanizmov se varnost zagotavlja. S pomočjo teh referenčnih objektov lahko razlikujemo med tradicionalno zaščito nacionalnega teritorija in konceptom človekove varnosti. “Sestavine človekove varnosti so med seboj soodvisne, kar pomeni, da je med indikatorji posameznih dimenzij varnosti cela vrsta povezav” (Human Development Report 1994 v Prezelj 2007, 9). Prišlo je torej do spremembe referenčnega objekta varnosti. Namesto države, so v ospredju družba, posamezniki, okolje in vse bolj tudi kritična infrastruktura (Prezelj 2007, 14–16).

Literatura razlikuje med tremi varnostnimi paradigmami: tradicionalnimi, kritičnimi in alternativnimi. Pod tradicionalne paradigme štejemo realizem, liberalizem in kopenhagensko šolo. H kritični paradigmi štejemo kritično teorijo, kritične varnostne študije in kritično teorijo

varnosti. Pod alternativne paradigme spadajo konstruktivizem, koncept človekove varnosti in (neo)marksizem.

Utemeljitelji več-razsežnostnega znanstvenega raziskovanja varnosti so predstavniki kopenhagenske šole, ki so v svojih ključnih delih razdelili varnost sodobne družbe na različne dimenzije v katerih je moč identificirati različne grožnje varnosti: vojaško, okoljsko, gospodarsko, politično in družbeno. S tem so v analizo varnosti vključili prej zanemarjena vprašanja. Buzan, Wæver in Wilde, ki so predstavniki kopenhagenske šole opredeljujejo povezave med varnostnimi dimenzijami kot medsektorsko varnost. Pri tem gre za to, da varnostna vprašanja enega področja obarvajo varnostna vprašanja drugega oziroma varnostne zaznave na enem področju vplivajo na varnostne zaznave na drugem področju (Buzan, Wæver in Wilde 1998 v Prezelj 2007, 8–9). Terriff, Croft, James in Morgan (v Prezelj 2007, 8–9). opredeljujejo meddimenzionalne odnose kot dopolnjevalne, kar pomeni, da imajo učinki na enem področju, če niso odpravljeni pravilno, učinek na več drugih področjih. Določeni nevojaški pojavi lahko na primer ustvarijo problem na vojaškem področju ali na drugih nevojaških področjih Tako ima lahko informacijska dimenzija zaradi svoje razširjenosti v sodobnem svetu vpliv na različne druge dimenzije. Buzan že posveča določeno mero pozornosti varnosti posameznika, čeprav ohranja državo kot osrednji objekt varnosti. To se kaže v tezi, da lahko posameznik doseže potrebno raven varnosti samo v močni državi, delujoči v zreli anarhiji mednarodnega sistema (Grošelj 2007, 29–30).

Korak naprej pri razumevanju varnosti naredi Wæver s konceptom zaznavanja procesa opredeljevanja nekega vprašanja kot varnostnega vprašanja (sekuritizacija). Pri tem gre za posebno ekstremno obliko politizacije. V teoriji lahko katero koli javno vprašanje najdemo na lestvici od nepolitiziranega do politiziranega in sekuritiziranega vprašanja. Nepolitizirana vprašanja so tista, s katerimi se država ne ukvarja in niso del javne debate ali na dnevnem redu odločevalcev. Politizirana vprašanja so tista, ki so del javne politike in zahtevajo odločitve vlade ter prerazporeditev sredstev. Neko vprašanje oziroma zadeva lahko postane varnostno vprašanje (sekuritizirano) brez obstoja realne varnostne grožnje, saj je lahko samo vprašanje predstavljeno kot eksistencialna grožnja. Varnost je v tem primeru govorno dejanje. Ko nekaj označimo kot varnostno vprašanje, s tem ustvarimo občutek pomembnosti in opravičimo uporabo posebnih ukrepov, ki so izven ustaljenih političnih procesov. Neko vprašanje postane varnostno vprašanje šele, ko je kot tako prepoznano s strani javnosti (Buzan, Wæver in Wilde 1998, 23–25). Objekt ali vprašanje samo sebe ne more opredeliti kot varnostno vprašanje. Pri tem je pomembno kdo proces sekuritizacije izvaja, glede katerih

vprašanj, za koga in zakaj, s kakšnimi učinki, pod kakšnimi pogoji in kaj naredi ta proces uspešen (Grošelj 2007, 30).

3.2 Ogrožanje varnosti

3.2.1 Grožnje varnosti

Sodobno varnostno okolje je v zadnjih letih izoblikovalo eno samo stalnico, ki se kaže skozi različne kazalce – hitro spremenljivost, nepredvidljivost, kompleksnost, transnacionalnost kriz in groženj varnosti. Varnost je predvsem kompleksna in relativna, odvisna od dojemanja posameznika, skupin, enot, organizacij. Varnost lahko kot komponento izboljšamo z uporabo tehnoloških rešitev, ki služijo kot pomoč pri napovedovanju, preprečevanju in predvidevanju varnostno ogrožajočih dogodkov, a kot trdi Prezelj (2007, 7) stoodstotne varnosti ni mogoče doseči niti pri delovanju tehnoloških sistemov, kaj šele v zvezi z družbenimi sistemi, ki so podrejeni delovanju bistveno večjega števila zunanjih in notranjih ogrožajočih vplivov. Trdi še (prav tam), da so in bodo grožnje varnosti vedno prisotne v bolj ali manj latentni obliki.

"Grožnje varnosti lahko na splošno opredelimo kot vse družbene ali naravne pojave, ki zmanjšujejo varnost oz. njene definicijske prvine" (Prezelj 2007, 7).

Grožnje varnosti se lahko netradicionalistično opredelijo kot večdimenzionalne, saj se sodobne države soočajo s hkratnim obstojem groženj iz različnih dimenzij; kot transnacionalne, ker se širijo ne glede na umetno vzpostavljene meje držav in vzajemno povezane, kar lahko označimo kot kompleksnost ogrožanja (nacionalne) varnosti.

Torej se grožnje nacionalni varnosti v eni države lahko preko meja prenesejo v druge države in tam začnejo ogrožati nacionalno varnost, ki tako preraste v ogrožanje mednarodne varnosti. Širjenje oboroženih spopadov spada med klasične oblika transnacionalnega ogrožanja varnosti, medtem ko med »netipične« spadajo tudi informacijske motnje, ki ogrožajo klasične in neklasične informacijske strukture, na primer kibernetski terorizem in kibernetski kriminal (Prezelj 2007, 10). Predvsem informacijske motnje lahko kaj kmalu postanejo tipične transnacionalne, predvsem zaradi vedno večje »informatizacije« družbe, kar je seveda relevantno iz vidika magistrske naloge.

Glede na to, da so grožnje večdimenzionalne, jih torej delimo na dimenzije oziroma sektorje, pri tem pa je potrebno poudariti, da je to netradicionalistični pristop in da je večina groženj v današnjem svetu nevojaških. Temeljne dimenzije in ključne grožnje so (Prezelj 2007, 8):

- ➔ vojaška dimenzija (grožnja = oboroženi napad na državo);
- ➔ gospodarska dimenzija (grožnja = izrazito poslabšanje gospodarskih razmer ne glede na razlog);
- ➔ policijsko-kriminalistična dimenzija (grožnja = organizirani kriminal);
- ➔ ekološka oziroma okoljevarstvena dimenzija (grožnja = onesnaževanje človekovega okolja);
- ➔ zaščitno-reševalna dimenzija (grožnja = naravne in antropogene nesreče);
- ➔ teroristična dimenzija (grožnja = teroristični napadi terorističnih skupin);
- ➔ zdravstvena dimenzija (grožnja = širjenje nalezljivih bolezni);
- ➔ **informacijska dimenzija** (grožnja = namerni posegi v delovanje pomembnih nacionalnih informacijskih sistemov);
- ➔ obveščevalna dimenzija (grožnja = sovražno delovanje obveščevalnih služb drugih držav);
- ➔ migracijska dimenzija (grožnja = visoka stopnja ilegalnih migracij).

Kot smo že ugotovili, so različne dimenzije varnosti povezane. "Predstavniki kopenhagenske šole (Buzan, Wæver in Wilde 1998) opredeljujejo povezave med varnostnimi sektorji kot medsektorsko varnost. Pri tem gre za to, da varnostne zaznave na enem področju vplivajo na varnostne zaznave na drugem področju" (Prezelj 2007, 8–9).

Za najino nalogo je najpomembnejša informacijska dimenzija ogrožanja (nacionalne) varnosti in jo zato bolj podrobno predstavljava, čeprav niso druge nič manj pomembne. Informacijska dimenzija ali sektor varnosti opredeljuje grožnje varnosti, kjer so ključna grožnja namerni posegi v delovanje pomembnih nacionalnih informacijskih sistemov. V povezavi z najino nalogo, bi lahko kot pomembne nacionalne informacijske sisteme imenovali sisteme, ki jih za upravljanje in komunikacijo uporabljajo v gospodarskih družbah, zavodih in drugih organizacijah posebnega pomena za obrambo države. Kateri so ti sistemi avtorja ugotavljava tudi v tej nalogi.

3.2.2 Kriza: kompleksna kriza, vzroki kriz

Rosenthal in drugi (2001, 6–7) krizo razumejo kot resno grožnjo osnovnim strukturam ali temeljnim vrednotam in normam sistema, za katero je pod časovnim pritiskom in v visoko negotovih okoliščinah nujno potrebno sprejeti kritične odločitve.

Krize od prizadetih in odgovornih zahtevajo, da v čim krejšem času vzpostavijo stanje, ki je bilo pred krizo, pri čemer je treba obvladovati vire nastajanja kriznih razmer in njihove posledice. V kolikor se odgovorni ne odzovejo primerno, so posledice krize lahko še hujše

(več žrtev in materialne škode ter poslabšanje varnostnih razmer) (Prezelj 2005, 16). Pripravljenost na krize bodisi na lokalni, regionalni ali nacionalni ravni se lahko kaže kot popolna improvizacija na eni strani, do vnaprej pripravljene politike in sistemskih mehanizmov na drugi strani (Prezelj 2007, 6).

Krize, ki ogrožajo življenja, materialne dobrine in velike tehnične sisteme so postale neizogibno dejstvo v sodobnem svetu in posledično smo kot družba, zaradi razvoja informacijske in drugih tehnologij ter odvisnosti od le teh vedno bolj ranljivi (Prezelj 2007, 6). Krize so namreč postale del našega sveta, del našega načina življenja, del življenja, ki ga želimo živeti (Rosenthal in drugi 2001, 5–6). Razvoj poleg pozitivnih lastnosti prinaša tudi negativne (Prezelj 2005, 14–15). Krize bi morali razumeti kot obdobja preloma in kolektivnega stresa, ki ovirajo vsakodnevne vzorce in ogrožajo temeljne vrednote in strukture družbenih sistemov na nepričakovan, pogosto nepojmljiv način. Današnje krize niso ločeni dogodki ampak procesi razširjenih in mnogovrstnih sil, ki so v interakciji na nepričakovan in vznemirljiv način. Moderne krize vedno bolj zaznamujejo kompleksnost, medsebojna odvisnost in politizacija. V tem smislu bodo jutrišnje krize videti drugače od današnjih in včerajšnjih kriz (Rosenthal in drugi 2001, 6).

V zadnjem obdobju se soočamo s krizami, ki jih povzročajo teroristični napadi, naravne nesreče, vojne ipd.. 11. september, napadi v Madridu in Londonu so v celotnem spektru ogrožanja varnosti prispevali k prioritiziranju terorizma kot ključne grožnje. Slednje ima vpliv na oblikovanje zaščite kritične infrastrukture. Vendar se je treba zavedati, da obstajajo tudi številne druge krize, ki s svojim nastankom in obsegom, ki presega nacionalne meje opozarjajo, da terorizem nikakor ni nujno glavna grožnja varnosti ter da je potrebno pri izgradnji nacionalnega sistema kriznega upravljanja upoštevati vse vidike ogrožanja (Prezelj 2007, 6).

3.2.3 Vzroki kriz

Na mikro ravni je pri raziskovanju vzrokov kriz fokus na vlogi posameznikov. Večina kriz se zgodi zaradi primerov, ko gre za napačne odločitve ob napačnem času, nepazljivost, spodrsljaje in sabotaže. Človeške napake se ne pripisuje samo navadnim delavcem ampak jih zagrešijo tudi upravitelji in izvršilni direktorji. Raziskovalci se ukvarjajo tudi s tem, zakaj so določeni posamezniki storili določeno napako, saj želijo odkriti motive za njihova dejanja. Raziskave na tem področju kažejo tudi, da so človeške napake neizogibne in se dogajajo v vsakem normalnem okolju (Rosenthal in drugi 2001, 8).

Na mezo ravni se fokus premakne na organizacijske dejavnike in procese, ki lahko igrajo vlogo pri povzročanju kriz. Ključno vprašanje je, ali organizacije lahko kompenzirajo s človeškimi omejitvami in okoljskimi dejavniki, ki vodijo do krize. Na eni strani imamo skupino raziskovalcev, ki trdijo, da je večina organizacij nezmožna preprečiti človeške napake ali lajšati posledice le teh. Na drugi strani pa trdijo, da organizacije same prinašajo v ospredje procese, ki povečujejo možnost nastanka krize. Ekstremno plat pri tej debati predstavljajo raziskovalci, ki konceptualizirajo organizacijo kot sredstvo za močne ampak odklonske ali celo preprosto neumne voditelje (Perrow, Whicker in Pitcher v Rosenthal in drugi 2001, 8–9).

Na makro ravni analize teoretiki vključijo še druge vzroke, ki naredijo krize bolj ali manj neizbežne in neizogibne pojave moderne družbe. Eden od najbolj prepričljivih avtorjev na tem področju Charles Perrow trdi, da bodo veliki tehnični sistemi prej ali slej proizvedli nesrečo, kot kombiniran rezultat zaradi samega potenciala, tehnične kompleksnosti in same narave napak. Spet druga skupina raziskovalcev trdi, da okoljski pritiski silijo organizacije k povečevanju učinkovitosti in outputa, pri tem pa se zanemarja varnostne ukrepe (Sagan in Heimann v Rosenthal in drugi 2001, 9).

»Najbolj kritičen člen v verigi zagotavljanja učinkovite informacijske varnosti je še vedno človek. Upoštevaje Parotov princip 80/20 je za 80 % vseh neljubih dogodkov v povezavi z informacijsko varnostjo odgovoren človek, bodisi z namerno (finančni motiv, vohunjenje, maščevanje, objestnost, vandalizem, terorizem) ali nenamerno (nepazljivost, neznanje, malomarnost, slaba varnostna kultura) dejavnostjo. V svetu je bilo opravljenih veliko število analiz, raziskav in proučevanj človekovega vedenja, vendar splošne metode za zagotavljanje zanesljivosti človeka preprosto še ni. Pri teh raziskavah in analizah vedenja človeka se po drugi strani ponavljajo enaki ali podobni vzorci na osnovi katerih lahko ugotovimo, da so ključni elementi za zagotavljanje zanesljivosti človeka znanje, usposobljenost, izkušnje, obremenitev in nadzor (Hudoklin 1996 v Rolih 2001, 26).

Glede na visok odstotek neljubih dogodkov, za katere je odgovoren človek, je temu problemu potrebno posvetiti tudi sorazmerno več pozornosti. Nabor kadrovskih ukrepov se prične z izbiro ustreznega kadra, ki mora najprej skozi sito varnostnega preverjanja, čemur sledi selektivno izbiranje glede na znanje in izkušnje. Izrednega pomena je stalno izobraževanje, saj nobena tehnologija nima uporabne vrednosti, poleg tega predstavlja varnostno grožnjo, če je ne znamo uporabljati ali jo uporabljamo nepravilno. Pri usposabljanju je potrebno omeniti tudi skrb za razvijanje varnostne kulture, kajti le ustrezna ozaveščenost ustvarja trdne temelje varnega okolja. Za preprečevanje nenamernih a tudi namernih napak človeka sta pomembna dejavnika še obremenjenost in izkušnje. Ustrezna

raven obremenjenosti spodbuja ustvarjalnost, prevelika ali premajhna obremenitev pa imata nasprotno negativen učinek. Na zmanjšanje predvsem nenamernih napak, ki imajo prav tako lahko katastrofalne posledice, imajo velik vpliv poleg znanja tudi izkušnje. Na področju informacijske varnosti si namreč ne smemo privoščiti, da bi svoje znanje in izkušnje razvijali in bogatili na osnovi storjenih napak. Nikakor ne smemo tiščati glave v pesek in trditi, da se to ne dogaja. V primeru, da pride do odtekanja podatkov, poti nazaj namreč ni. Kot zadnjega od dejavnikov zagotavljanja informacijske varnosti, je potrebno omeniti tudi nadzor, kar pomeni, da je potrebno spremljati tako strokovni razvoj kadrov kot tudi njihovo delo. Na morebitne incidente se je potrebno odzvati z ustreznimi sankcijami, česar se morajo zaposleni zelo dobro zavedati (Rolih 2011, 26).

3.2.4 Ogrožanje nacionalne varnosti RS

Po Ullmanu "med grožnje nacionalni varnosti spadajo tisti dogodki ali nizi dogodkov, ki grozijo, da bodo v kratkem času drastično znižali kakovost življenja prebivalcev države ali zožili izbiro možnih političnih reakcij, ki so na voljo državi in zasebnim nevladnim subjektom (posameznikom, skupinam, korporacijam) znotraj države" (Ullman 1983, 133 v Prezelj 2007, 7). Torej gre pri ogrožanju nacionalne varnosti bodisi za "onemogočanje fizičnega obstoja prebivalstva; motenje ali onemogočanje normalnega delovanja temeljnih družbenih in državnih struktur oziroma infrastruktur; onemogočanje izvajanja politične suverenosti ali za preprečevanje relativno nemotenega družbenega razvoja" (Prezelj 2007, 7).

Obstajajo različni kriteriji delitve virov ogrožanja. Tradicionalna delitev razvršča vire ogrožanja na vojaške in nevojaške, na zunanje in notranje, na naravne in antropogene ali pa glede na vsebino groženj na vojaške, politične, družbene, ekonomske, okoljske in druge. Zaznavanje, analiziranje in realno ocenjevanje virov ogrožanja ni preprosto saj obstajajo vsaj tri različne ravni zaznave. Poznamo deklarativne, zaznane in dejanske vire ogrožanja. Deklarativni viri ogrožanja so zapisani v strateških dokumentih s področja varnosti, ki so jih sprejeli odločevalci. Zaznani viri ogrožanja so prepoznani med prebivalci določene države. Dejanski viri ogrožanja pa se dejansko uresničijo in so statistično dokumentirani (Sotlar, Tičar in Tominc 2012 v Sotlar in Tominc 2014, 233).

"Viri ogrožanja so ključni dejavniki, ki determinirajo varnostno politiko in v okviru nje tudi interese in cilje, ki si jih država zastavlja na področju varnosti" (Sotlar 2008 v Sotlar in Tominc 2014, 233). Obstoj in razvoj družbe sta pomembna atributa varnosti, zato je izrednega pomena, da države vnaprej določijo grožnje, za katere domnevajo, da bodo v bližnji

prihodnosti predstavljale največjo nevarnost (Grizold 1992 in Sotlar 2001 v Sotlar in Tominc 2014, 233).

Na zgoraj opisan način je tudi Slovenija na področju državne varnosti sprejela tri temeljne strateško - usmerjevalne dokumente v katerih je opredelila svoje varnostne interese, cilje in politike, strukturo nacionalno-varnostnega sistema ter grožnje, ki so za Slovenijo najbolj nevarne (Sotlar in Tominc 2014, 233–234). "Gre za naslednje dokumente: Resolucija o izhodiščih zasnove nacionalne varnosti Republike Slovenije (1993, 1994), Resolucija o strategiji nacionalne varnosti Republike Slovenije (2001) in Resolucija o strategiji nacionalne varnosti Republike Slovenije (2010)" (Sotlar in Tominc 2014, 234).

Najpomembnejši viri ogrožanja so v Resoluciji iz leta 2010 v primerjavi s starejšimi dokumenti drugače opredeljeni, prav tako je določen njihov izvor (globalen, nadnacionalen ali nacionalen).

Med globalne vire ogrožanja nacionalne varnosti spadajo podnebne spremembe, globalna finančna, gospodarska in socialna tveganja ter krizna žarišča. Ti viri imajo globalno poreklo, lokalne posledice in multiplikatorski značaj, ki vpliva na nastanek drugih varnostnih groženj ter hkrati povečujejo njihove učinke in posledice (ReSNV-1 2010 v Sotlar in Tominc 2014, 240).

Med nadnacionalne vire ogrožanja spadajo morebitne vojaške grožnje, organiziran kriminal, terorizem, nedovoljene dejavnosti na področju konvencionalnega orožja, orožij za množično uničevanje in jedrske tehnologije, kibernetske grožnje in zloraba informacijskih tehnologij in sistemov ter dejavnosti tujih obveščevalnih služb. Ti viri imajo transnacionalno poreklo in čezmejne razsežnosti (prav tam).

Nacionalni viri ogrožanja spadajo v ožje življenjsko okolje družbe in obsegajo ogrožanje javne varnosti, naravne in druge nesreče, omejenost naravnih virov ter degradacijo življenjskega okolja, zdravstveno-epidemiološke grožnje ter določene dejavnike negotovosti. Ti viri ogrožanja so povezani z dogajanjem v nacionalnem okolju, čeprav določene grožnje, kot so naravne in druge nesreče in zdravstveno-epidemiološke grožnje ne poznajo državnih meja (prav tam).

Zgoraj omenjeni trije viri spadajo med deklarativne vire ogrožanja. Da bi bilo izvajanje varnostne politike kredibilno je pomembno tudi zaznavanje virov ogrožanja pri prebivalcih, ki groženj bodisi ne zaznavajo ali podcenjujejo. Slednje je lahko nevarno, ko se dejanska grožnja pojavi in se je potrebno z njo spopasti. Dejavniki ogrožanja imajo izvor (globalna, nadnacionalna ali nacionalna raven) lahko različen, medtem ko so posledice takšnih dogodkov najizrazitejše prav na lokalni ravni (Sotlar in Tominc 2014, 234)

3.2.5 Ocenjevanje ogrožanja nacionalne varnosti

"Grožnje varnosti kot družbeni in naravni pojavi so neke vrste procesi, ki jih je mogoče bolj ali manj natančno spremljati, zaradi njihove potencialne destruktivnosti pa je to nujno početi. Pri spremljanju groženj nacionalni varnosti je potrebno upoštevati tudi temeljno stalnico v sodobnem varnostnem okolju, to je, da se grožnje varnosti nenehno spreminjajo." (Prezelj 2007, 11–12).

Ocenjevanje ogrožanja nacionalne varnosti mora biti proces spremljanja groženj varnosti, ki obsega (Prezelj 2007, 12):

- ➔ identificiranje pojavov, ki ogrožajo nacionalno varnost oziroma bi jo lahko ogrozili;
- ➔ utemeljevanje razlogov, zakaj identificirani pojavi ogrožajo nacionalno varnost;
- ➔ analiziranje njihovih splošnih in konkretnih pojavnih značilnosti;
- ➔ analiziranje in opredelitve tipičnih povezav z drugimi grožnjami,
- ➔ ocenjevanje oziroma merjenje intenzivnosti identificiranih pojavov oziroma groženj, kar lahko temelji na indikatorjih;
- ➔ posredovanje ocen relevantnim odločevalcem in
- ➔ posredovanje obvestil javnosti.

3.3 Ogrožanje omrežne in informacijske varnosti

"Številni empirični indikatorji[1] kot so: število uporabnikov interneta, rast informacijskega sektorja sodobnih družb, razvoj novih družbenih infrastruktur na osnovi uporabe IKT ter sprememba starih, kažejo na pomen, ki ga ima IKT v sodobnih (informacijskih) družbah" (Svete 2007, 27). Ključne storitve, ki jih uporablja naša družba temeljijo na informacijskih sistemih. Ti sistemi za svoje nemoteno delovanje potrebujejo različna omrežja, zato je njihova varnost in zaščita ključnega pomena. Informacijske sisteme Odbor za nacionalno varnost informacijskih sistemov in telekomunikacij ZDA definira kot celotno infrastrukturo, organizacijo, osebje in komponente namenjene zbiranju, obdelavi, hranjenju, oddajanju, prikazovanju in širjenju informacij. Zanimivo je, da definicija vključuje zaposleno osebje oziroma administratorje kot del informacijskega sistema (National Information Security (INFOSEC) glossary v Šuligoj 2011, 42).

[1] Predstavljeni v sledečih poglavjih.

Schneier (v Šuligoj 2011, 43) pripisuje informacijskim sistemom značilnosti, kot so: kompleksnost, interaktivnost in nepredvidljivost. Informacijski sistem je kompleksen, ker ima že preprost osebni namizni računalnik operacijski sistem, ki ga sestavlja več tisoč vrstic dolga koda, povezovanje večjega števila takih računalnikov lahko sestavlja računalniške mreže. Sistemi so interaktivni zato, ker so med seboj kompatibilni in se posledično medsebojno povezujejo. Primer slednjega je internet. Sistemi so tudi nepredvidljivi, ker se lahko razvijejo drugače, kot so si sprva predstavljali razvijalci in programerji.

"Posledično zaradi vse večjega pomena IKT v sodobnih družbah, so omrežja sama referenčni objekt, na katerega se varnost nanaša. Na tej točki govorimo torej o omrežni varnosti oziroma širše o informacijski varnosti, ki se v skladu z varnostno teorijo nanaša na uravnotežen, stabilen razvoj in delovanje" (Svete 2007, 30).

Revolucionarni razmah razvoja informacijsko-komunikacijske tehnologije v sodobnih družbah je v zadnjem desetletju povzročil pospešeno zavedanje o možnem ogrožanju informacijsko-komunikacijske ter omrežne varnosti. Svet je postal prepletena zmes in postaja vedno enotnejša celota. Državne meje ne predstavljajo več tolikšnih fizičnih ovir za komunikacijo, kot so jih predstavljale še pred dobrima dvema desetletjema. V tem času se je politična slika močno spremenila, spremenile pa so se tudi obrambno-varnostne razmere, ki od nas zahtevajo vedno večjo povezanost družbe, gospodarstva, politike in drugih elementov na eni strani ter zagotavljanje vedno večje varnosti informacijsko-komunikacijskih sistemov na drugi strani. Uporaba IKT je namreč že pred časom prešla raziskovalne, vojaške in druge okvirje in se je zakoreninila kot neobhodni pogoj delovanja sodobnih družb. Svete (2005, 10) "trdi, da so telekomunikacije, satelitske povezave in računalniška omrežja velik del sveta povezala v prepleteno celoto – informacijsko družbo, ki je danes že splošno sprejet aksiom tako v znanstveni kot tudi javni in politični sferi." Sodobne družbe so postale v veliki meri odvisne od delovanja IK sistemov. Sami IKT, in preko tega celotni IKI, lahko zaradi tega pripišemo strateško vlogo in pomen v sodobnih družbah. To pa ravno zaradi razširjenosti IKT in njene uporabe v (državnih) institucijah, industriji ipd. ter za zagotavljanje (že samoumevnih) storitev državne in zasebne sfere. Zaradi vedno večje odvisnosti družbe od nemotenega delovanja IKI lahko govorimo o sodobnih družbah kot o informacijskih (prav tam).

Ravno zato, ker lahko govorimo o informacijski družbi, se je nujno zavedati potencialnih groženj omrežni oz. informacijski varnosti. IKT je korenito spremenila delovanje posameznika, družbenih skupin in ustanov ter kot taka postala cilj in sredstvo za doseganje njihovih interesov (prav tam). Tega so se v zadnjem času začele zavedati tudi države, ki si

večinoma lastijo monopol nad uporabo represivnih, zaščitnih in obrambnih ukrepov proti (pravnim) osebam in dejanjem, ki bi škodile njihovi (nacionalni) varnosti. Čeprav se akterji trudijo držati korak z razvojem ukrepov zaščite IKT, prihaja do zaostankov pri načrtovanju zaščite. Pomanjkljiva (včasih pa preobsežna in nerazumljiva) dokumentacija, nedorečenost postopkov, dolžnosti ter omrežnih politik, povzroča dodatne ranljivosti v sistemih, tudi KI (Markulec 2008). Nekatere države so se tega dejstva začele zavedati prej, saj so na tem področju razvitejše, druge kasneje, mednje žal sodi tudi Republika Slovenija.

3.3.1 Akterji varnostne problematike IKT

Akterjev, ki lahko ogrožajo omrežno varnost oz. ki lahko ogrozijo celotno informacijsko infrastrukturo, poznamo več vrst. Schneier (2000, 43) jih deli na:

- Hekerje – eksperimentira z omejitvami sistemov zaradi radovednosti, lastnega ega, uporništva ali užitka in nikakor ne zaradi političnih ipd. ciljev;
- Osamljene zločince ali organizirane kriminalne združbe – prvi povzročijo največ računalniškega zločina. Motivira jih pohlep, večinoma napadajo poslovne sisteme, zaradi denarja. Ne predstavljajo grožnje delovanju informacijskega sistema, problem se pojavlja, ker ga včasih zmorejo premostiti, zato se pojavi varnostna dilema informacijskega sistema; drugi uporabljajo tehnologijo na dva načina: pri prvem uporabljajo orodja za vdiranje v računalniške sisteme (npr. bank), pri drugem pa uporabijo tehnologijo za vodenje in organizacijo drugih poslov (primer zlorabe bančnih kartic). V drugo skupino lahko uvrstimo tudi teroristične skupine, čeprav je njihov motiv večinoma vojaško-političen;
- Škodoželjni zaposleni – zlorabljajo svoj položaj znotraj organizacije, saj je veliko varnostnih sistemov naravnanih na grožnje »od zunaj«. Škodoželjni zaposleni velikokrat poznajo delovanje varnostnih sistemov in jih tako lažje zlorabijo.
- Industrijski vohuni – cilj je pridobiti prednost pred konkurenco oz. kraja tehnologije. Stroški vohunjenja so po navadi desetkrat nižji od lastnega razvoja. Industrijsko vohunjenje predstavlja velikansko tveganje in je v večini držav opredeljeno kot nacionalno-varnostno tveganje oz. grožnja;
- Mediji – gre za obliko pridobivanja informacij, včasih vohunjenja, z namenom dokopati se do atraktivne zgodbe;
- Obveščevalno-varnostne službe – obveščevalne, varnostne ali obveščevalno-varnostne službe so lahko javne ali zasebne. Pri prvih gre za zakonsko določene

naloge izvajanja zaščite informacijskih sistemov pred viri ogrožanja omrežne varnosti, pri drugih pa za poslovni motiv, katerih primarno vodilo je dobiček;

- Informacijski bojevniki – opredeljeni kot vojaški nasprotniki, ki napadajo omrežno oz. informacijsko infrastrukturo, s ciljem oslabitve nasprotnika na različnih področjih.

Ko govorimo o akterjih in sami omrežni varnosti je potrebno opozoriti, da se je zaradi uporabe vedno bolj prefinjene (sofisticirane) IKT opreme, samostojno ali kot sestavni del večjega sistema, spremenilo tudi oblikovanje politik v mednarodni skupnosti, ki se predvsem trudijo držati tempo z razvojem tehnologije. Poleg omenjenih akterjev ogrožanja omrežne varnosti lahko omenimo še (tradicionalne) akterje ogrožanja IKT, ki lahko ogrozijo IKI na tradicionalen, konvencionalen način, s fizičnim uničenjem IKI, kar ima za posledico nedelovanje celotnega sektorja IKT. EU na prvo mesto postavlja teroriste oz. teroristične grožnje IK varnosti, ki so lahko tradicionalno konvencionalne ali kibernetske.

Kibernetska kriminaliteta se na splošno nanaša na vrsto različnih kriminalnih dejavnosti, pri katerih so računalniki in informacijski sistemi osnovno orodje ali glavna tarča. Kibernetska kriminaliteta obsega običajna kazniva dejanja (goljufija, ponarejanje in kraja identitete), kazniva dejanja v zvezi z vsebino (širjenje otroške pornografije na spletu ali spodbujanje k rasnemu sovraštvu na spletu) in kazniva dejanja, tipična za računalnike in informacijske sisteme (napadi na informacijske sisteme, ohromitev storitev in zlonamerna programska oprema (Strategija za kibernetsko varnost 2013, 3).

Kibernetski napadi postajajo vse pogostejši, uspešnejši, bolj predrzni, tehnično dovršeni in uničujoči. Kljub naštetemu si nekateri še vedno zatiskajo oči pred omenjenimi napadi iz kibernetskega prostora. Poleg tega ni nujno, da so vsi napadi registrirani in da javnost izve za vse napade. Slednje namreč v primeru uničujočega vdora v informacijski sistem lahko ogrozi ugled podjetij in zaupanje zvestih strank (Rolih 2011, 10).

Nacionalne zakonodaje in mednarodna zakonodaja, za boj proti globalnim informacijskim grožnjam so v veliko primerih neuspešne. Do sedaj še niso dosegli skupnega dogovora o tem, kaj je kibernetsko vojskovanje, kako ga prepoznati, dokazati in sankcionirati, kljub temu, da se mednarodna skupnost zaveda resnosti problematike. (Bosworth in Kabay 2002 v Čaleta in Rolih 2011, 14).

Razlogi za to so predvsem v tem, da (Čaleta in Rolih 2011, 14):

→ mednarodna zakonodaja kibernetsko vojskovanje priznava le v primeru smrtnih žrtev ali znatne materialne škode;

→ zakonodaja posameznih držav zunaj njenih meja nima vedno učinka;

→ ne obstaja celovit in centraliziran nadzor nad internetom ter komunikacijskimi in informacijskimi sistemi;
→ vse države informacijskih groženj ne obravnavajo enako;
→ je identifikacija napadalcev izredno zahtevna ali celo nemogoča;
→ je motiv napadalca težko dokazljiv ali celo nemogoč;
→ so nove tehnologije vedno korak pred zakonodajo.

Kot problem se je za politične akterje v državah pojavila vsesplošna dostopnost tehnologije in s tem postavila dogajanja na oči svetovne javnosti. Po drugi strani sta razvoj in uporaba IKT dala družbi moč vplivanja na politične odločitve in tudi sprožilne mehanizme pri doseganju ciljev, kot se je izkazalo pri Arabski pomladi leta 2011. Vendar so se države začele zavedati moči IKT že mnogo prej, preden so se v zadnjih letih zgodili ti dogodki.

Vidik ogrožanja omrežne varnosti je v zadnjem času prerasel tudi v vidik ogrožanja omrežne posameznikove varnosti, saj smo posamezniki kot uporabniki informacijske tehnologije vedno bolj odvisni od njenega nemotenega delovanja in opravljamo vse več storitev s pomočjo informacijske tehnologije. S tem smo postali tudi dovzetnejši za grožnje omrežni varnosti in tudi bolj odprti za načrtovanje zaščite IKI, kar nam je predvsem v lastnem interesu, v čemer se odraža tudi sebična posameznikova nrav.

3.3.2 Omrežna in informacijska varnost v Republiki Sloveniji

Informacijska varnost oz. vidik je po opredelitvi Urada Vlade RS za varovanje tajnih podatkov naslednja (Urad vlade RS za varovanje tajnih podatkov: *Varnost KIS* 2014): "Informacijska varnost obsega določanje in uporabo ukrepov za zaščito tajnih (idr.)[2] podatkov, ki se obdelujejo, shranjujejo in prenašajo s pomočjo komunikacijskih, informacijskih in drugih elektronskih sistemov pred naključno ali namerno izgubo tajnosti, celovitosti ali razpoložljivosti ter ukrepov za preprečevanje izgube celovitosti in razpoložljivosti samih sistemov."

"Informacijsko varnost (INFOSEC) predstavljajo ukrepi in postopki, ki jih je treba opraviti, da obdelava, uporaba in prenos tajnih podatkov s pomočjo informacijske tehnologije ne bi ogrozila njihove vsebine. Vsa programska in strojna oprema za obdelavo tajnih podatkov mora biti ustrezno atestirana in preverjena, njeno uporabo pa lahko odobri samo pristojni akreditacijski organ" (Čaleta 2004 v Svete 2007, 39).

[2] Opomba avtorja

Informacijska varnost je varstvo podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, spremembo ali uničenjem (Detektivska agencija Satja: *Informacijska varnost 2014*). Pri zagotavljanju informacijske varnosti sledimo (vsaj) trem načelom in sicer zaupnosti, neokrnjenosti oz. nedotakljivosti in razpoložljivosti (ang. *confidentiality, integrity, availability*). Izrazi informacijska varnost, varovanje računalniških sistemov, varstvo informacij se pogosto uporabljajo kot sopomenke in se jih včasih zamenjuje. Kljub temu, da so ta področja v medsebojnem odnosu in si delijo skupne cilje varstva zaupnosti, neokrnjenosti in razpoložljivosti informacij, obstajajo med njimi komaj opazne razlike (Wikipedia 2014).

Po drugi strani ima omrežna varnost ožji pomen in se nanaša na varnost na spletu oz. na varnost naprav, ki imajo povezavo s svetovnim spletom. Za nadzor nad dogodki na področju omrežne varnosti v RS skrbi Arnesov SI–CERT (ang. *Slovenian Computer Emergency Response Team*), ki je nacionalni center za obravnavo omrežnih incidentov. V letu 2012 je izdal Poročilo o omrežni varnosti za leto 2011 v Sloveniji, v katerem lahko zasledimo glavne zaznane grožnje omrežni varnosti v Sloveniji (v nadaljevanju Poročilo 2011). Omenimo, da so zaznane grožnje s strani SI–CERT naslednje: preiskave zlonamerne kode, vprašanja in svetovanja, vdor v računalnik, goljufija, »phishing«, poskus vdora, kraja omrežne identitete, interno, zloraba omrežne storitve, »DOS«, »Spam«, »Botnet«, odredba sodišča, kršitev avtorske pravice. Na tem mestu je potrebno omeniti, da je omrežna varnost lahko razumljena kot most med varnostjo informacijskih sistemov, zato je potrebno nameniti veliko pozornosti načrtovanju zaščite le teh. Po navadi je smotrno načrtovati zaščito informacijske infrastrukture, predvsem take, ki je neposredno povezana s spletom, preko katerega lahko vešči uporabniki izkoriščajo globalno dostopnost sistemov, povezanih v mrežo.

Kibernetska varnost se na splošno nanaša na zaščitne in druge ukrepe, ki se lahko tako na civilnem kot vojaškem področju uporabljajo za zaščito kibernetskega prostora pred grožnjami, ki so povezane z njegovimi soodvisnimi omrežji in informacijsko infrastrukturo oziroma jih lahko ogrozijo. Pri kibernetski varnosti gre za ohranjanje razpoložljivosti in celovitosti omrežij in infrastrukture ter zaupnosti informacij, ki jih ta omrežja in infrastruktura vsebujejo (Strategija za kibernetsko varnost Evropske unije 2013, 3).

Kibernetsko varnost težje razumemo kot sopomenko omrežne varnosti, saj prva opisuje dogodke in ukrepe varnosti v odprtem kibernetskem svetu svetovnega spleta, medtem ko se omrežna varnost nanaša tudi na zaprta omrežja (LAN, WAN). V zadnjem času se je število kibernetskih napadov povečalo. Omenimo, da se je stopnja kibernetskih napadov v zadnjih šestih letih povečala za 4-krat, na 6 tisoč napadov dnevno (Carr 2009, 6). To pomeni, da se

potencialni napadalci zavedajo pomena in uporabnosti IKT. To se kaže skozi različne akcije različnih interesnih skupin na svetovnem spletu.

Za zagotavljanje višje stopnje omrežne varnosti je potrebno zagotoviti različne ravni načrtovanja zaščite IKI. S tem imamo v mislih tako (nad)nacionalno raven, načrtovanje zaščite na ravni gospodarskih in drugih organizacij ter načrtovanje zaščite posameznih elementov IKT.

3.3.3 Ogrožanje omrežne in informacijske varnosti v Republiki Sloveniji

Kritičnost IKT sektorja v slovenski družbi se vidi predvsem v zagotavljanju oziroma omogočanju vse številčnejših elektronskih storitev in procesov, tako v njenem zasebnem kot javnem sektorju. Tako gospodarski kot upravni in drugi procesi so odvisni od telekomunikacijskih povezav oziroma prenosov. Brez elektronskega načina delovanja država in družba ne moreta več delovati oziroma bi potrebovali izjemno veliko časa, da bi vse procese in postopke ponovno »analogizirali« (Prezelj 2008, 354).

Ključna grožnja je pomanjkanje usposobljenih kadrov, ki razumejo in vzdržujejo IKT. Drugače so grožnje bolj fizične, obstajajo pa tudi nenamerne grožnje- kot rezultat proizvodov. Pri IKT je problem testiranja in vse krajših razvojnih ciklov novih tehnologij. Ciklusi razvoja se zelo krajšajo. Testna faza se krči, celo preskakuje, kriteriji se nižajo zaradi pritiska trgov, uporabniki so se sprijaznili z razmeroma veliko nezanesljivostjo informacijskih in komunikacijskih sistemov. Tudi simulacije v laboratorijih ne odražajo vedno realnega časa. Grožnja pa je seveda tudi namerna. Vsak, ki je priključen na omrežje, je že s tem ogrožen. Rešitev je samo v popolnoma ločenem omrežju oziroma celo v analognih oblikah podatkov, kajti po nekaterih informacijah naj bi bilo mogoče prestreči vse elektronske oziroma električne signale, naj so povezani v omrežja ali ne. Tudi Microsoft v svoje osnovne programe vgrajuje kode, ki jih uporabniki ne poznajo in jih je preko tega mogoče nadzorovati (Prezelj 2008, 343).

Kar zadeva telekomunikacijske operaterje, so najbolj ogroženi njihovi telekomunikacijski objekti in omrežja. Predvsem so občutljivi na fizične oblike ogrožanja, kot so terorizem, sabotaže ali naravne nesreče. Seveda so popolnoma soodvisni tudi od električnega omrežja, kajti ob njegovem izpadu je onemogočeno delovanje telekomunikacijske infrastrukture. Občutljivi so na vdore, tako fizične kot programske oziroma virtualne. Sicer Telekom v primeru naravnih nesreč lahko zagotovi obhodne poti oziroma nadomestne povezave. Veliko težavo bi pomenili simultani teroristični napadi na več točkah hkrati. Če bi prišlo do napada tako direktnih kot obhodnih poti, ni nobenega operaterja, ki bi to lahko zaščitil. Velika

grožnja je seveda uničenje komunikacijskega centra oziroma obeh glavnih central. Ogrožanje je lahko posledica tako izpada drugega (pod)sektorja, od katerega so telekomunikacije soodvisne, na drugi strani pa imamo neposredno ogrožanje podsektorja z namernimi ali nenamernimi grožnjami. Seveda lahko pomembni del ogrožanja predstavljajo tudi notranji dejavniki (zaposleni). Zato na primer pri Telekomu razvijajo načrt varnega poslovanja, ki predvideva zaščito notranjih informacij, tako v odnosu do konkurence kot seveda vseh drugih že omenjenih virov ogrožanja (Prezelj 2008, 354).

Neposredna škoda pri IKT je predvsem vpliv na ljudi, ki lahko privede do panike. Vendar že na posledice panike lahko gledamo kot na posredno škodo. Bolnišnice, lekarne (ipd.), vse deluje na osnovi informatike, kar ima lahko hude posledice. Vendar na tej točki govorimo o posredni škodi. Vse posledice so dejansko posredne. Kaj če odpove mobilna tehnologija za tri dni? Klici na 112 in 113? Zlasti tam, kjer imamo samo mobilno tehnologijo. IKT ne povzroči mrtvih, lahko pa pride do žrtev zaradi nedelovanja le te. Program te ne more ubiti ali resno poškodovati. Dejstvo pa je, da imajo tudi kirurgi sistem na klic. Če mobilna telefonija ne deluje, potem lahko tudi ta izpad pomeni žrtve (Prezelj 2008, 344).

Tudi škoda v gospodarstvu lahko hitro naraste nad 500 milijonov evrov, če pride do sesutja borze, bankomatov, finančnih transakcij, poslovanja med podjetji, saj je danes vse bolj ali manj virtualno in digitalizirano. Gospodarska kriza v Sloveniji je pomenila izjemno veliko škodo slovenskemu gospodarstvu, ko so številke in biti krojili usodo države, podjetij in je bilo v gospodarstvo vloženih več milijard evrov.

Naslednja dimenzija varnosti informacijsko komunikacijske sfere je dimenzija interneta reči (ang. *İnternet of things*). Internet reči je računalniški oz. informacijski koncept, ki opisuje, kako bodo (so) v prihodnosti vsakodnevne stvari kot so televizija, centralno ogrevanje, vodovod, pospeševalniki utripa povezani s spletom in jim bo tako omogočeno povezovanje z drugimi stvarmi, ki imajo dostop do svetovnega spleta (Techopedia 2014). Internet reči lahko opišemo kot informacijsko komunikacijsko tehologijo, čeprav je mnogo več, saj vključuje med drugim tudi tehnologijo senzorjev in brezžično tehnologijo. Lahko ga opišemo kot razvijajočo se informacijsko infrastrukturo oz. sistem, ki temelji na svetovnem spletu. Internet reči je predvsem pomemben za posamezne sisteme, ki tako s povezavo s svetovnim spletom presežejo lastno namembmnost. S pridobitvijo t. i. digitalne sposobnosti te vsakodnevne stvari tako omogoči sistemu, da postane mnogo več in mnogo bolj povezljiv, uporaben in varnostno sporen, kot je bil do sedaj (Weber 2010).

Kot primere varnostnega ogrožanja lahko navedemo par primerov. Internet reči se je razširil na mnoga do nedavnega nepojmljiva področja. Pametni telefoni, hladilniki z zasloni,

pametni TV ekrani, nadzor nad centralnim ogravanjem, daljinski nadzor nad železniškimi povezavami, pametni avtomobili, digitalni vzpodbujevalci srčnega utripa, digitalni slušni aparati, digitalni respiratorji... (DeLoach 2014). Smo kdaj pomislili na varnostne zadržke ob uporabi te napredne tehnologije. Najbrž ne, dokler nismo sami žrtev nepravilnega delovanja omenjene tehnologije ali celo kibernetskega napada. Digitalna tehnologija namreč za seboj pušča digitalne podpise, s katerimi se lahko povezuje v svetovna omrežja. Tako ima lahko internet reči neposredne varnostne posledice ob uporabi digitalnih srčnih spodbujevalnikov, do katerih lahko oddaljeno dostopamo na podlagi povezave v svetovna omrežja. Pametni avtomobili z vrsto senzorjev za nadzor parkiranja, nadzor oddaljenost med avtomobili, pomoč pri zaviranju. V kolikor pride do varnostnega dogodka z vdorom v omrežje pametnega avtomobila, bolnišnične sisteme in manipulacijo s senzorji, lahko internet reči povzroči neposredne varnostno sporne posledice tudi v ogrožanju človeških življenj.

Da bi bil internet reči sposoben odzivanja na grožnje je v Evropski uniji zaslediti trend sledenja predvsem štirim varnostnim zahtevam (Weber 2010):

- Odpornost na napade (ang. *Resilience to attacks*),
- Sposobnost preverjanja podatkov (ang. *Data authentication*),
- Nadzor dostopa (ang. *Access control*),
- Zasebnost (ang. *Client privacy*).

Trenutno v Republiki Sloveniji primera, da bi bil sektor IKT resno moten ni bilo. Pade na primer samo mobilna telefonija recimo ob novem letu, vendar le za nekaj minut. Občasne motnje na primer elektronske pošte ali katere od ostalih internetnih storitev so sicer precej pogoste, vendar so napake večinoma odpravljene v nekaj urah, kar pomeni, da slednje ne moremo šteti k resnim grožnjam (Prezelj 2008, 346).

Zanesljivost sistemov in programske opreme, je v veliki meri prepuščena trgu. Prav tako je programska oprema prepletena s strojno. Državne institucije, ki bi to preverjala ni. Edini način preverjanja so javna naročila. Torej, kar je zanesljivo in uporabniku prijazno ima prednost. Slovenija sama ne more razvijati programske opreme za splošno uporabo. Dokler je bil CVI, je bil ta urad tovrstna institucija. Drugače je državna uprava naročena na Sophos, ki se redno posodablja in zaenkrat dobro deluje (Prezelj 2008, 347).

3.4 Koncept (zaščite) kritične infrastrukture

3.4.1 Razumevanje kritičnosti

Schulman in Roe (Prezelj 2009, 467) v pojmovanje kritičnosti prinašata razumevanje, ki izpostavlja kritičnost posameznega sektorja, ravno zaradi posledic njegovega nedelovanja na druge družbene dejavnosti in zmogljivosti. Nedelovanje oziroma omejeno delovanje kritične infrastrukture prinaša posledice varnostnih razsežnosti. Neučinkovita preskrba s hrano, vodo in temeljnimi energenti (nafta, plin, elektrika), nedelovanje finančnih sistemov plačevanja ter sistemov zdravstvene oskrbe bi prinesli specifično družbeno krizo. V kolikor te krize ne bi uspešno obvladovali, bi prišlo do varnostnih situacij, v katerih bi bil ogrožen fizični obstoj posameznikov.

Eden od ključnih problemov v zvezi z določanjem kritičnosti je v tem, da se njena opredelitev skozi čas spreminja (prav tam), razlog za to pa je, da gre za subjektivni proces označevanja nečesa kot kritičnega (Prezelj 2008, 10).

Johnson (2006, 6) ugotavlja, da soodvisnost med sektorji povratno otežuje natančno definiranje, kaj spada in kaj ne pod kritično infrastrukturo. Na tej točki Hellstrom (2006, 5) poudarja, da obstaja tveganje, da vse kar je pomembno za delovanje družbe postane kritična infrastruktura, pri tem se ne osredotočimo na nič specifičnega pri njeni zaščiti, zato se je tudi po Lewisovem mnenju potrebno osredotočiti na ožje elemente (Prezelj 2009, 468).

V želji po zmanjševanju širine kritične infrastrukture so nastali trije povezani pristopi, ki imajo za izhodišče, da seveda ni vse kritično temveč le nekateri procesi (pristop A), nekatere točke (pristop B) ali nekateri elementi (pristop C). Hellstrom (2006, 12 v Prezelj 2008, 11) ugotavlja, da kritične infrastrukture niso kritične samo zato, ker so na splošno pomembne, temveč ker s svojo strateško povezanostjo odražajo popolno družbeno ranljivost na samo nekaj ključnih točkah v sistemu. Zato predlaga, da se analiza začne z opredelitvijo sistemske maksimalne referenčne točke in se tako oceni, kje je tehnološki in družbeni sistem najbolj ranljiv in kako je ta ranljivost povezana (Hellstrom 2006, 5 v Prezelj 2008, 11). Reinermann in Weber (2003v Prezelj 2008, 10–11), ki spadata pod pristop A, ločita med več nivoji kritičnosti. Kritični procesi za družbo, kritični procesi za sektor ter poslovno kritični procesi, katerih motenje bi lahko ogrozilo preživetje podjetja. V primeru, da so onemogočeni procesi v enem podjetju, slednje verjetno ne bo imelo velikega učinka na družbo. Popolnoma drugače je, če ima takšno podjetje velik tržni delež v sektorju ali celo monopol. Lewis (2006, 16 v Prezelj 2008, 11) sektorje kritične infrastrukture vidi kot mreže, zato uporabi mrežno analizo, s katero lahko določi kritične točke in njihove vzajemne povezave. Kritične točke so po

njegovem mnenju najpomembnejše točke razdora. Gre namreč za točko v sektorju, kjer napad, nesreča ali druga motnja lahko povzroči največ škode. Kritičnost točke temelji na številu povezav z drugimi točkami, torej je kritičnost največja tam, kjer je največje število povezav. Hkrati je tam tudi največja ranljivost celotnega sistema (Lewis 2006, 73 v Prezelj 2008, 11). Lewis opozarja tudi, da je pri zaščiti kritične infrastrukture pomembno razumevanje (neenakomernosti) porazdelitve kritične infrastrukture. Kritične točke so pogosto geografsko zgoščene, najpogosteje jih najdemo na bolj urbanih področjih (Prezelj 2010, 13).

3.4.2 Kritična infrastruktura in njena konceptualna opredelitev

V novem tisočletju se je vedno bolj začel uveljavljati pristop, ki se osredotoča na ogroženost in zaščito temeljnih družbenih infrastrukturnih objektov in sistemov. Še vedno je v ospredju proučevanje potencialno ogrožajočih vplivov na človeka, vendar se je fokus preučevanja usmeril na same infrastrukturne sisteme od katerih je velikokrat odvisen človekov obstoj (Prezelj 2008, 7).

Pojmovanje kritične infrastrukture se je sčasoma zaradi razvoja tehnologije in vzpona terorizma spremenilo. Nekoč se je med kritično infrastrukturo uvrščalo tiste infrastrukture, katerih daljše motenje bi lahko povzročilo večje vojaške in ekonomske posledice (Dunn 2005, 264 in Moteff v Hellstrom 2006, 5 v Prezelj 2008, 7). Danes je kritična infrastruktura izjemno široka kategorija. Kljub vsemu je opaziti, da se raziskave in praksa osredotočajo na nekatere kritične infrastrukture. Torej različni avtorji različno opredeljujejo kritično infrastrukturo. Tako Schulman in Roe (2006 v Prezelj 2008, 7) opredeljujeta kritično infrastrukturo kot temeljne zmogljivosti, tehnične sisteme in organizacije, ki zagotavljajo zmogljivosti. Vse omenjeno omogoča zagotavljanje velikega spektra družbenih aktivnosti, dobrin in storitev. Ellison, Boin, Lagadec, Michel-Kerjan in Overdijk, Lewis, Nozickova in Turnquist, Schulman in Roe in drugi (v Prezelj 2008, 8) pojmujejo kritične infrastrukture kot mreže, ki zagotavljajo prometne, finančne, komunikacijske, preskrbne, elektroenergetske in podobne transakcije. Michel-Kerjan (2003, 134 v Prezelj 2008, 8) pa pojmuje kritično infrastrukturo kot kompleksni sistem med seboj vedno bolj povezanih elementov. Tako v kritično infrastrukturo uvršča industrije, institucije in distribucijske mreže ter sisteme, ki zagotavljajo kontinuiran tok dobrim in storitev, ki so nujne za varnost in blagostanje prebivalstva.

Glede na zgoraj zapisano lahko ugotovimo, da v opredelitve kritične infrastrukture štejejo predvsem (Prezelj 2008, 8):

- ➔ transportne sisteme (cestni, zračni, pomorski, železniški),
- ➔ telekomunikacijske in informacijske sisteme,

- elektroenergetske sisteme (elektrika, nafta, plin),
- finančne in bančne sisteme,
- sisteme preskrbe z vodo in
- sisteme preskrbe s hrano.

Nekateri avtorji ali države pod kritično infrastrukturo uvrščajo tudi državne institucije, reševalne službe, vključno z javnim zdravstvom, kemično industrijo in podobno. Prezelj (2008, 8) ugotavlja tudi, da avtorji večinoma previdno ohranjajo odprte opredelitve kritične infrastrukture. Kljub temu je potrebna sektorizacija celotne kritične infrastrukture, saj se le tako lahko zagotovi njeno zaščito. Na tej točki je potrebno poudariti tudi, da ne obstaja univerzalno mednarodno soglasje o opredelitvi kritične infrastrukture, saj je to področje relativno mlado. Že v preteklosti so se opredelitve spreminjale, tako da je to mogoče pričakovati tudi v prihodnosti. Le Grand, Springsfield in Riguidel so leta 2003 navedli nekatere splošne značilnosti kritične infrastrukture, ki bi jih bilo treba poznati in razumeti, še preden se vzpostavijo mehanizmi njihove zaščite (Prezelj 2008, 8–9). Te splošne značilnosti so:

- močna vzajemna povezanost infrastrukturnih sektorjev,
- visok delež privatne lastnine v sektorjih kritične infrastrukture,
- naraščajoča odvisnost sektorjev od informacijske tehnologije,
- naraščajoč mednarodni pomen sektorjev kritične infrastrukture,
- naraščajoče zahteve do infrastrukturnih sektorjev, ki povečujejo vpliv kakršnihkoli napak.

3.4.3 Kritična IKI v Sloveniji in EU, odvisnost in načini ogrožanja IKT sektorja

IKT je postala nepogrešljiv del zagotavljanja delovanja procesov v skorajda vseh družbenih podsistemih. Posledično je sektor informacijske in komunikacijske tehnologije mogoče obravnavati samostojno tako kot v okviru analize ostalih sektorjev. Najbolj logična je obravnava IKT sektorja znotraj vseh ostalih sektorjev ter še dodatna delitev v dva podsektorja IKT-informatika pod katerega lahko štejemo programsko opremo oziroma programje ter IKT komunikacije in strojna oprema, ki predstavlja prenos podatkov preko javnih in zasebnih mrež ter strojno opremo, ki tak prenos omogoča (Prezelj 2008, 476).

Ogrožanje sektorja IKT[3] lahko razdelimo na naravna ogrožanja, kamor spadajo naravne in antropogene nesreče, ki ne izhajajo iz same IK tehnologije, lahko pa jo poškodujejo oziroma

[3] V času pisanja v RS še ni bilo določenih sektorjev kritične infrastrukture in sva se avtorja dela za potrebe naloge naslonila na obstoječe opredelitve in delitve sektorjev kritične infrastrukture. Ob zaključevanju dela je v RS Vlada RS sprejela in določila sektorje kritične infrastrukture, kamor spada tudi sektor informacijsko

ogrožajo; namerna ogrožanja, kamor štejemo terorizem, vojne, informacijske napade in zlonamerna delovanja zunanjih ali notranjih akterjev ter nenamerna-tehnološka ogrožanja, kamor uvrščamo človeške napake in samo obratovanje naprav, predvsem v primeru avtomatiziranih procesov (Prezelj 2008, 477).

Podsektor IKT-informatika najbolj ogrožajo odpoved strojne opreme oziroma grožnje fizične narave, pomanjkanje usposobljenih kadrov, ki razumejo delovanje IKT in ga vzdržujejo, vse krajši razvojni cikli novih tehnologij, nezadostna testiranja, nižanja kriterijev zaradi pritiska trgov. Pojavljajo pa se tudi namerne grožnje. V današnjih časih je mogoče prestreči skoraj vse digitalne in elektronske signale, velike korporacije (Microsoft, Google) pa domnevno v svoje osnovne programe vgrajujejo kode, preko katerih je možno izvajati nadzor nad uporabniki (prav tam).

Drugi podsektor IKT komunikacije in strojna oprema vključuje različne vrste prenosov podatkov, zato so tudi načini ogrožanja različni. V primeru telekomunikacijskih operaterjev so najbolj ogroženi telekomunikacijski objekti in omrežja.

V EU se vseh 6 podsektorjev nanaša na komunikacije oziroma različne vidike in načine prenosa podatkov. Delitev na dva podsektorja IKT ravno nasprotno izpostavlja pomen zbiranja, obdelave ter prikaza podatkov, ki se ne prenašajo vedno po javnih ali privatnih omrežjih. Pomembna je torej logistika ter čim boljša kvaliteta programja, ki omogoča najboljši možni izkoristek poti, obremenitev ter čim boj optimalno prenašanje podatkov na relaciji vstop-izstop. Vsi ti podatki in programje so izrednega pomena zato, ker iz teh zajetih podatkov, njihovega prenosa in izhodnega prikaza sledijo človeške odločitve, ki so v nasprotju z vso digitalno tehnologijo še vedno analogne narave. Trend gre v smer avtomatizacije odločitev s hkratnim zoževanjem števila kadrov, ki razumejo oziroma izvajajo procese na področju IKT. Slednje pomeni kritičnost tako na področju zaščite kot tudi kadrov, ki zagotavljajo delovanje.

Pomembnost podsektorja IKT komunikacije in strojna oprema, ki predstavlja fizični del informacijsko komunikacijske infrastrukture, se kaže predvsem v zagotavljanju vse bolj dostopnih ter številčnih elektronskih storitev in procesov slovenskemu javnemu ter zasebnemu delu družbe. Vse vrste procesov, vključno z gospodarskimi in upravnimi, so odvisne od telekomunikacijskih povezav, kar pomeni, da bi družba in država potrebovali zelo veliko časa, da bi procese in postopke spravili v prvotno »analogno« stanje (Prezelj 2008, 476–477)

komunikacijske podpore (Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji, sklep Vlade RS št. 80200-1/2012/5, z dne 17. 10. 2012).

Odvisnost drugih sektorjev od IKT sektorja (obeh podsektorjev) je velika, ker je v današnji informacijski družbi velika večina družbenih podsektorjev, njihovih procesov in storitev ter outputov tako ali drugače sloni na uporabi IKT-ja (Prezelj 2008, 493–495).

Odvisnost od podsektorja IKT informatika:

V popolni odvisnosti (4) od podsektorja IKT informatika so:

- proizvodnja, rafiniranje, predelava, skladiščenje in distribucija nafte ter plina,
- proizvodnja in distribucija električne energije,
- nadzor kakovosti voda,
- zdravila, cepiva in farmacevtski proizvodi,
- laboratoriji z biološkimi materiali in reagenti (biolaboratoriji in bioagensi),
- infrastruktura za trgovanje, plačila, kliring in poravnave ter sistemi finančnih instrumentov,
- zračni promet,
- vesolje,
- znanstvenoraziskovalne zmogljivosti.

V visoki stopnji odvisnosti (3) so:

- proizvodnja, predelava in skladiščenje jedrskih snovi,
- zagotavljanje pitne vode,
- zajezitev in nadzor nad količino vode,
- zagotavljanje hrane in njene neoporečnosti,
- zdravniška in bolnišnična oskrba,
- cestni promet,
- pomorski promet.

V srednji stopnji odvisnosti (2) so:

- železniški promet,
- proizvodnja, shranjevanje in predelava kemičnih snovi.

Odvisnost od podsektorja IKT komunikacije in strojna oprema:

V popolni stopnji odvisnosti (4) so:

- znanstvenoraziskovalne zmogljivosti,
- zračni promet.

V visoki stopnji odvisnosti (3) so:

- proizvodnja in distribucija električne energije,
- zdravniška in bolnišnična oskrba,
- zdravila, cepiva in farmacevtski proizvodi,

- laboratoriji z biološkimi materiali in reagenti,
- infrastruktura za trgovanje, plačila, kliring in poravnave ter sistemi finančnih instrumentov,
- železniški promet,
- proizvodnja, shranjevanje in predelava kemičnih snovi.

V srednji stopnji odvisnosti (2) so:

- proizvodnja, rafiniranje, predelava, skladiščenje in distribucija nafte ter plina,
- zagotavljanje pitne vode,
- nadzor kakovosti vode,
- zajezitev in nadzor nad količino vode,
- zagotavljanje hrane in njene neoporečnosti,
- pomorski promet.

V majhni stopnji odvisnosti (1) so:

- proizvodnja, predelava in skladiščenje jedrskih snovi,
- cestni promet.

Družbeni ključni infrastrukturni sistemi niso nikakršen novodoben pojav, le pojmovani so bili v drugačnem časovnem kontekstu družbenega pomena. V preteklosti so jih pojmovali kot fizično in logično ločene sisteme z malo medsebojne povezanosti (Radvanovsky 2006, 5 v Prezelj 2008). S pojavitvijo in napredkom informacijske tehnologije so postali omenjeni sistemi večinoma avtomatizirani in vedno bolj medsebojno povezani. Govorimo lahko o mrežnem oz. procesnem pristopu proučevanja kritične infrastrukture.

Koncept (zaščite) kritične infrastrukture se je razvijal že od 60-ih let 20. stoletja, čeprav se je strokovni izraz »kritična infrastruktura« pojavil sredi 90. let 20. stoletja, ko so se, predvsem v ZDA, začeli zavedati pomena objektov, procesov, storitev, dejavnosti in sistemov, ključnih za nacionalno in državno varnost ter za nemoteno delovanje družbe ter jih imenovali kritična infrastruktura. Izraz kritična infrastruktura je tako v strokovnih krogih pogosteje prisoten od sredine 90-ih let, ko ga je v uporabo vpeljala Clintonova administracija. Če pomislimo, ni kritična infrastruktura popolnoma nič novega, samo dojemanje njenega pomena za delovanje družbe se je spremenilo oz. poostrilo. Slednje se je zgodilo s pojavom določenih kritičnih dogodkov, ki so vplivali na ogroženost elementov infrastrukture ključnega pomena za nacionalno in državno varnost ter za nemoteno delovanje družbe. S pojavom teh dogodkov so vidni odločevalci (npr. že prej omenjeni Clinton) ali strokovnjaki ovarnostili (sekuritizirali) to infrastrukturo kot ključno oz. kritično, ker so jo kot tako sprejeli tudi strokovni krogi.

V strokovnih krogih se pojavlja dilema poimenovanja kritične infrastrukture, ki v slovenskem jeziku pride še toliko bolj do izraza, zaradi včasih preveč enostavnega in prehitrega poslovenjenja tujih izrazov, brez posvetovanja s slovenisti. Za poimenovanje infrastrukture, ki je posebnega pomena tako za gospodarstva držav, družbo in nacionalno varnost, se v znanstvenih krogih uporabljata poleg termina »kritična infrastruktura« še »vitalna« oz. »ključna infrastruktura«. Lewis (2006, 3 v Prezelj 2008) govori o infrastrukturi »…,ki je tako vitalna oziroma ključna, da bi njena onesposobitev ali uničenje izredno oslabila državno obrambo ter ogrozila nacionalno varnost.« Po opredelitvah Slovarja slovenskega knjižnega jezika pomenijo pridevniki:

- *ključen*: od katerega je odvisen nadaljnji potek, razjasnitev, rešitev česa; ki je po pomembnosti na prvem mestu; glaven
- *kritičen*: nanašajoče se na krizo, težaven (npr. položaj);
- *vitalen*: ki je bistven za ohranjanje življenja; ki je bistven za obstoj, nadaljnji potek česa; ključen, osnoven (povzeto po Slovar slovenskega knjižnega jezika).

Kot vidimo so prav vsi trije pridevniki primerni za opisovanje omenjene infrastrukture, pomembne za nacionalno varnost, družbeno blaginjo in gospodarski razvoj. Vsakič, ko govorimo o grožnjah kritični infrastrukturi, jo povezujemo s krizo in je zato primerna uporaba pridevnika kritičen. Ko govorimo o infrastrukturi, ki je tako bistvena za obrambo, nacionalno varnost, družbo in gospodarstvo, da si brez nje ne znamo predstavljati nadaljnjega razvoj oz. delovanja, uporabljamo pridevnik vitalen, v kolikor pa govorimo o infrastrukturi, od katere je odvisen nadaljnji razvoj in delovanje ter zagotavljanje nacionalne varnosti, družbe, gospodarstva, pa uporabimo pridevnik ključen. V našem primeru bi uporabljali edini popolnoma slovenski pridevnik tj. ključen, kakršen je uporabljen tudi v dokumentu Zelena knjiga o evropskem programu za varovanje ključne infrastrukture (Evropska komisija 2005). Radvanovsky (2006, 5) trdi, da se pojem ključne infrastrukture torej navezuje na sredstva fizičnih ali računalniško in informacijsko podprtih sistemov, ki so bistveni (ključni[4]) za osnovo delovanje gospodarstva in vlade.

S slednjim poimenovanjem infrastrukture kot ključne se ne strinjajo na Ministrstvu za obrambo Republike Slovenije, na kar so naju prijazno opozorili preko elektronske pošte v sklopu sodelovanja ob izdelavi magistrske naloge, saj je bilo v letu 2014 sprejetih več

[4] Opomba avtorja.

dokumentov[5], ki ključno/vitalno/kritično infrastrukturo v RS poimenujejo izključno kot kritično. Iz tega razloga bova pisca dela v nalogi uporabljala izraz kritična infrastruktura.

Pri mrežnem pojmovanju tako sedaj kritične infrastrukture moramo biti pozorni na (so)odvisnost posameznih sektorjev. Le Grand, Springinsfeld in Riguidel (2003, 3 v Prezelj 2008, 15) poudarjajo razliko med odvisnostjo in soodvisnostjo. Po njihovem mnenju odvisnost pomeni, da stanje ene infrastrukture vpliva na stanje druge, medtem ko soodvisnost pomeni odvisnost v obe smeri.

Kritično infrastrukturo lahko povežemo s konceptom totalne vojne in še prej strateškega bombardiranja. Kot prvega teoretika, ki je jasno in sistematično izrazil tezo o strateškem bombardiranju, omenjamo italijanskega teoretika o zračnih silah in moči Giulia Douheta. Njegovo teorijo so pred 2. svetovno vojno dopolnili nemški in ameriški teoretiki. Douhet je že v začetku 20. stoletja verjel, da se vojne ne bijejo več samo med vojskami, pač pa med celotnimi ljudstvi. Trdil je, da je narod (oz. nacijo) potrebno najprej izčrpati, preden je ta pripravljen priznati poraz (v Collier in Lakoff v Dunn Cavelty in Kristensen 2008, 20). Slednje je logično povezano z razvojem industrijske družbe, ki je bila sposobna v velikih količinah proizvajati sredstva in dobrine za vodenje vojne. Industrializacija in razvoj sta družbo pripeljali do točke, da se je, kot trdi Aron (154, 88), vojska industrializirala, industrija militarizirala, vojska je posrkala narod (oz. nacijo)[6], narod in nacija pa se preslikata na vojsko.[7] Ker sta bila narod (nacija) in vojaška moč v obliki vojske tako tesno povezani, je bilo potrebno veliko potrpežljivosti in sistematičnosti pri doseganju vojaških ciljev s pomočjo strateškega bombardiranja ključne vojaško pomembne infrastrukture. Za dosego tega je bilo najprej potrebno zagotoviti zračno prevlado, ko je bilo to doseženo, so lahko bombniki dosegli najvitalnejše, najbolj ranljive in najslabše zavarovane točke sovražnikovega zalednega ozemlja. Douhet je določil pet (5) ključnih točk države ki so bile ključne tarče strateškega bombardiranja: industrija, transportna infrastruktura, komunikacijska vozlišča, vladne stavbe in »volja ljudstva« (Meilinger 1997 v Collier in Lakoff v Dunn Cavelty in Kristensen 2008, 20). V preteklosti je bilo že mnogokrat v vojaški strategiji določeno, katera infrastruktura je ključna za doseganje vojaških idr. ciljev. Kot primer navedimo samo strateška bombardiranja Porurja v Nemčiji v času 2. svetovne vojne ali pa oviranje železniškega prometa s strani partizanskih vojsk in odporniških gibanj po celi Evropi v istem času.

[5] Veljavni kriterji kritičnosti za določanje kritične infrastrukture državnega pomena; Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji; Spremembe in dopolnitve osnovnih in sektorskih kriterijev kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji; Sklep o določitvi kritične infrastrukture državnega pomena v RS idr.

[6] Opomba avtorja.

[7] Prevod je avtorjev.

V preteklosti je bila kritična infrastruktura res rezervirana za vojaške kroge. Šele v 60. letih 20. stoletja, dokončno pa leta 1996 se je ta del pojmovanja varnostne dimenzije premaknil iz vojaških v civilno-varnostne kroge, ko je bila v ZDA ustanovljena komisija za zaščito kritične infrastrukture. Leta 1997 je izdala poročilo, ki je določalo osnovo in smernice pojmovanja pomena KI kot ključnega pomena za gospodarsko-ekonomsko blaginjo, vojaško moč in politično vitalnost. Takrat se je namreč začelo infrastrukturo dojemati drugače kot do tedaj, kar je tudi posledica hladne vojne. Prvič se jo je namreč ovarnostilo (sekuritiziralo) na podlagi prepričanj, da je infrastruktura temelj družbe in razvoja (v Aradau 2010). Takrat so se začeli tudi drugi nacionalnovarnostni akterji (poleg vojske) zanimati za vlogo in pomen kritične infrastrukture (Coward 2009 in Aradau 2010).

V strokovni literaturi je moč zaslediti številne opredelitve kritične infrastrukture, vendar je njihov pomen močno povezan s prostorsko lokacijo in časom opredelitve. Schulman in Roe (2006 v Prezelj 2008, 7) opredeljujeta kritično infrastrukturo kot temeljne zmogljivosti, tehnične sisteme in organizacije, ki zagotavljajo zmogljivosti. Vse navedene stvari omogočajo zagotavljanje večine družbenih aktivnosti, dobrin in storitev. V splošnem pomenu so kot kritična infrastruktura opredeljeni sistemi, ki so posebnega pomena za posamezno lokalno ali regionalno skupnost (Lukman in Bernik 2009). Slednja trditev nas lahko naveže že na v nalogi obravnavani Sklep o določitvi gospodarskih družb, zavodov in drugih organizacij, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji.

V ZDA kot začetnici koncepta kritične infrastrukture so jo opredelili kot infrastrukture, ki »…so tako vitalnega pomena, da bi njihova onesposobitev ali uničenje imelo uničujoč učinek na obrambo in ekonomsko varnost.« (Collier in Lakoff v Dunn Cavelty in Kristensen 2008, 17). Sledimo lahko tudi opredelitvi, ki je navedena v Priročniku o ZKII iz leta 2004 (CIIP Handbook 2004), in jo razumemo kot infrastrukturo oz. sredstvo, katerega onesposobitev ali uničenje bi imelo oslabitveni učinek na nacionalno varnost in ekonomsko ter socialno blagostanje nacije oz. naroda[8]. Iz tega izhaja tudi dejstvo, da je zaščita strateško pomembne infrastrukture ter njeno načrtovanje že desetletja vodilni koncept pri načrtovanju ZKI. Pri tem je potrebno opozoriti, da se stopnje pomembnosti zaščite infrastruktur različnih sektorjev spreminjajo glede na njihov trenuten pomen za nacionalno varnost. To ponazorimo s primerom, da je bila infrastruktura za transport in predelavo nafte v moderni dobi vedno objekt kritične infrastrukture, v zadnjem času pa v ospredje stopa infrastruktura IKT, ki praktično nadzoruje, povezuje in upravlja vse ostale sektorje. Do spoznanja o vse večjem

[8] Prevod avtorja.

pomenu IKT, povezane v IKI, je prišlo na podlagi informacijske revolucije, ki je naša življenja naredila v večji meri odvisna od IKT. S tem se je začel povečevati obseg možnih virov ogrožanja, pojavile so se tudi nove oblike groženj, ki jih do tedaj nismo poznali, to so predvsem informacijski oz. kibernetski napadi in dejanja kibernetskega terorizma.

3.4.4 Evropska kritična (informacijska) infrastruktura

Teroristični napadi znotraj EU, v Londonu in Madridu so med drugim onemogočili tudi delovanje kritične infrastrukture. Slednje in nekatere nesreče ter dogodki, ki so imeli evropske razsežnosti, so spodbudili k razmišljanju o določitvi evropske kritične infrastrukture. Dejstvo je, da v današnjem globalnem svetu okvara ali uničenje dela infrastrukture v eni državi lahko vpliva na dve ali več držav članic, kar ima posledično negativen vpliv na celotno evropsko gospodarstvo. Vse to je mogoče zaradi novih tehnologij ter liberalizacije trga, kar pomeni, da je velik del infrastrukture del večjega omrežja, zato je z varnostnimi ukrepi potrebno zaščititi najšibkejše člene v tej verigi. V EU obstajajo nekatere KI, katerih okvara ali uničenje bi imelo resne čezmejne posledice. To lahko vključuje čezmejne med-sektorske vplive, ki izhajajo iz soodvisnosti medsebojno povezanih infrastruktur. Takšne EKI je zato potrebno ugotoviti in določiti (Direktiva 2008). Določitev evropske kritične infrastrukture (EKI) je po mnenju Evropske Komisije (EK) mogoča le s skupnim postopkom ugotavljanja EKI in oceno za izboljšanje zaščite in varovanja teh infrastruktur. Integrirani pristop na ravni EU bi smiselno pripomogel pri ugotavljanju slabosti, šibkih točk in pomanjkljivosti varnostnih ukrepov na nacionalni ravni ter dodal vrednost nacionalnim programom zaščite in omogočil normalno delovanje evropskega notranjega trga (Prezelj 2010, 18–19).

Zavedanje o pomenu kritične infrastrukture je v Evropi začelo naraščati po napadih na Svetovni trgovinski center v New Yorku septembra leta 2001. Največkrat se zaščita kritične infrastrukture v evropskih državah povezuje s protiteroristično dejavnostjo in je dandanes enako pomembna kot je zaščita meja in državljanov. Pri ZKI se tako največkrat govori o dveh pristopih zaščite in sicer fizičnem in kibernetskem. Pri prvem pristopu gre za fizično zaščito ključne infrastrukture s pomočjo človeškega nadzora osebno, na mestu oz. preko množice senzorjev, brezpilotnih zrakoplovov in daljinsko vodenih bojnih postaj, ki dopolnjujejo pasivno zaščito kakovostnih standardiziranih konstrukcijskih elementov. Pri drugem pristopu pa gre za omrežni oz. kibernetski oddaljen nadzor predvsem informacijskih sistemov, ki upravljajo z elementi kritične infrastrukture (npr. nadzorni sistem za upravljanje prometa na železnicah) in brez katerih ni možno daljinsko upravljati teh sistemov. Kot vidimo je tudi

fizična zaščita delno že odvisna od kibernetske, saj se vedno bolj zanašamo na precizno tehnologijo, ki nam omogoča zgodnejše zaznavanje groženj ter s tem pravočasno ukrepanje. Ugotovimo lahko, da je omrežna (oz. kibernetska) dimenzija prodrla tudi v »pore« načrtovanja zaščite kritične infrastrukture. Tudi v tem primeru lahko govorimo o razmahu interneta reči.

Postopek določanja (evropske) ključne informacijsko-komunikacijske infrastrukture sledi določanju evropske kritične infrastrukture in poteka v naslednjem zaporedju (COM (2008), 114):

»Evropski svet je junija 2004 zaprosil za pripravo splošne strategije za zaščito kritičnih infrastruktur. Komisija je v odgovor na to 20. oktobra 2004 sprejela sporočilo z naslovom „Varovanje kritične infrastrukture v boju proti terorizmu“, v katerem je predstavila predloge o tem, kaj bi okrepilo preprečevanje terorističnih napadov na kritično infrastrukturo ter pripravljenost in odziv nanje v Evropi. Slednje je jasno pokazalo, da EU kot največjo grožnjo dojema terorizem in teroristične napade. Razvoj načrtovanja zaščite se je nadaljeval z ustanovitvijo ENISE. Organizirali so seminarje, katerih so se udeležile vse države članice, industrijska združenja, kot tudi strokovnjaki s področja informacijske varnosti. Komisija je nato 17. novembra 2005 sprejela Zeleno knjigo o evropskem programu za varovanje ključne infrastrukture, v kateri so bile navedene politične možnosti za oblikovanje Evropskega programa za zaščito kritične infrastrukture (EPCIP) in informacijskega omrežja za opozarjanje o kritični infrastrukturi (CIWIN). CIWIN je steber EPCIP, katerega namen je izboljšati zaščito kritične infrastrukture v Evropi, v vseh državah članicah EU in v vseh relevantnih sektorjih ekonomske aktivnosti. CIWIN je zaščiten internetni portal, na katerem so objavljene raziskave, analize in študije ter omogoča izmenjavo informacij in mnenj strokovne javnosti s področja KI. Objavljajo tudi primere dobrih praks kot priporočila za njihovo implementacijo na različnih področjih (MORS, Omrežje za opozarjanje o ogroženosti kritične infrastrukture, 2015).

V odzivih na Zeleno knjigo je bila poudarjena dodana vrednost okvira Skupnosti glede zaščite kritične infrastrukture. Pomenila je dodano vrednost glede povezovanja aktivnosti za zaščito, povečanja zmogljivosti zaščite ter pomoč pri zmanjšanju števila šibkih točk glede kritičnih infrastruktur. Cilj je bil poenotiti kriterije za določanje, zagotoviti ustrezno in poenoteno stopnjo zaščite, zagotoviti čim manj nezavarovanih točk ter vzpostaviti hitre in preverjene ukrepe za odpravo posledic. Definirali so enajst sektorjev kritične infrastrukture; energetika, informacijska in komunikacijska tehnologija, voda, hrana, zdravje, finance, javni

red in mir, javna uprava prevozni sektor, kemična in jedrska industrija ter vesolje in raziskave (Čaleta in Rolih 2011, 46).

Priznana je bila potreba po povečanju zmogljivosti zaščite kritične infrastrukture v Evropi in po pomoči pri zmanjšanju števila šibkih točk glede kritičnih infrastruktur. Poudarjen je bil pomen ključnih načel subsidiarnosti, sorazmernosti in dopolnjevanja pa tudi dialoga med zainteresiranimi stranmi. Svet za pravosodje in notranje zadeve je decembra 2005 pozval Komisijo, naj pripravi predlog EPCIP, ki naj bi temeljil na pristopu upoštevanja vseh nevarnosti, pri čemer naj bi bil boj proti grožnjam terorizma njegova prednostna naloga. V skladu s tem pristopom bi bilo treba v postopku zaščite kritične infrastrukture upoštevati človeške in tehnološke grožnje ter naravne nesreče, vendar bi morale biti grožnje terorizma prednostno obravnavane. Leta 2006 je bila sprejeta Strategija o varni informacijski družbi, ki je okrepila vlogo ENISE. Svet je aprila 2007 sprejel sklepe o EPCIP, v katerih je ponovno navedel, da so predvsem države članice odgovorne za to, da poskrbijo za ureditev zaščite kritične infrastrukture znotraj nacionalnih meja, obenem pa je pozdravil prizadevanja Komisije, da oblikuje evropski postopek za ugotavljanje in določanje evropske kritične infrastrukture (EKI) ter za oceno potrebe po izboljšanju njene zaščite. Leta 2008 je bila sprejeta Direktiva o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite (v nadaljevanju Direktiva), ki predstavlja prvi korak v postopnem pristopu za ugotavljanje in določanje EKI ter ocenjevanja potrebe za izboljšanje njene zaščite. Pot, ki je vodila do sprejetja direktive v EU kontekstu je bila zelo težka. Na neformalnem srečanju v Luksemburgu leta 2008 so namreč ministri za notranje zadeve podpirali idejo, da namesto direktive pripravijo le dokument, ki bo vključeval le minimalne skupne imenovalce povezane s tem področjem. Kljub temu so maja 2008 sprejeli odločitev, da sprejmejo direktivo, ki ji je še vedno nasprotovala Švedska. Zaradi številnih različnih mnenj, pristopov in pogledov držav članic glede obravnavane tematike, je bila leta 2008 izdana okrnjena direktiva, ki označuje začetek postopne identifikacije in definiranja EKI, kot tudi implementacijo potreb za izboljšanje zaščite. Namesto prvotno načrtovanih enajstih sektorjev so kompromisno omejili direktivo na dva sektorja, in sicer energetski in prometni, ostalih sektorjev se direktiva le blago dotika (Čaleta in Rolih 2011, 46–47).

Kot lahko opazimo se je normativna ureditev na ravni EU že dodobra razvila, vendar sta v Direktivi kot edina dva sektorja EKI določena energetski in prevozni (poimenovan tudi transportni) sektor. Že v času sprejetja Direktive je bilo opozorjeno, da obstaja potreba po vključitvi dodatnega sektorja med sektorje EKI, to je sektorja IKT, ki je kot vseprisoten sektor nedvomno pomemben. Omenjena direktiva tudi poudarja oblikovanje skupnega pristopa in

postopkov določanja EKI, katerih naj bi se določevalci držali. V tem primeru predvidevava, da je pri oblikovanju kriterijev določitve nacionalne ključne infrastrukture potrebno le-te postopke, v kolikor obstajajo, upoštevati. Odgovornost zaščite (E)KI leži na državah članicah in lastnikih oz. upravljavcih infrastruktur.

Določanje evropske kritične infrastrukture še ni zaključen proces, zato tudi ni oblikovanih enotnih kriterijev za določitev. Strinjamo se lahko, da tudi ko bo določena EKI in kriteriji, se bodo infrastrukture in njihov pomen spreminjale, s tem pa se bo spreminjal tudi njihov status kot element (E)KI. Trenutno velja, da bi lahko evropska kritična infrastruktura obsegala tiste materialne vire, storitve, infrastrukturo informacijske tehnologije, omrežja in infrastrukturne zmogljivosti, katerih okvara ali uničenje bi resno vplivala na zdravje, varnost, gospodarsko ali družbeno blaginjo (Evropska komisija 2005, 6):

(a) dveh ali več držav članic – to vključuje določeno dvostransko kritično infrastrukturo (kjer pride v poštev);

(b) bi zadevalo tri ali več držav članic – to izključuje določeno dvostransko kritično infrastrukturo.

Tako je zapisano v Zeleni knjigi iz leta 2005. Za učinkovito varovanja ključne infrastrukture so pomembni "… komunikacija, koordinacija in sodelovanje na ravni države in EU med vsemi zainteresiranimi stranmi – lastniki in upravljavci infrastrukture, zakonodajalci, strokovnimi telesi in gospodarskimi združenji v sodelovanju z vsemi upravnimi ravnmi in javnostjo." (Evropska komisija 2005, 2).

Najpomembnejši dokument s področja informacijske varnosti je bil sprejet 30. marca 2009 in sicer t.i. Communication (COM (2009), 149) on Critical Information Infrastructure protection (CIIP), ki se osredotoča na varnost EU pred kibernetskimi napadi in motnjami ter spodbuja pripravljenost, varnost in odpornost pred njimi. Pred tem je bilo v ospredju še sprejetje Evropskega programa za zaščito kritične infrastrukture (EPCIP), ki je bil sprejet 12. decembra leta 2006 z namenom izboljšanja zaščite KI in oblikovanja evropskega okvirja za ZKI. CIIP dokument je bil osnova za akcijski načrt petih stebrov: pripravljenost in preprečevanje, zaznavanje in odgovor, omilitev in obnova, mednarodno sodelovanje ter določitev kriterijev IKT sektorja. Napori za povečanje stopnje IK varnosti so se odrazili v Resoluciji Evropske komisije o skupnem evropskem pristopu k omrežni in informacijski varnosti, ki je bila sprejeta 18. decembra 2009. Slednja sledi skupnemu evropskemu cilju, ki teži k zagotavljanju zaščite evropske kritične infrastrukture. Trenutno v EU potekajo napori za sprejetje Evropske strategije spletne varnosti, ki je bila v času pisanja te naloge napovedana za tretje četrtletje leta 2012 in bi bila odlična osnova za nadaljevanje razvoja načrtovanja zaščite

(K)IKI. Dejansko sprejetje strategije se je zavleklo v začetek leta 2013, ko je bila sprejeta Strategija za kibernetsko varnost Evropske unije „Odprt, varen in zanesljiv kibernetski prostor“ (z dne 7. februar 2013).

Na državni ravni, natančneje v Republiki Sloveniji, se trenutno razpravlja o nacionalni kritični infrastrukturi, kar izhaja tudi iz usmeritev Zelene knjige. Rezultat je sprejetje sektorjev kritične infrastrukture v RS v letu 2014 in določitev kritične infrastrukture državnega pomena v RS, prav tako v letu 2014[9].

Začetki oblikovanja sektorjev in elementov kritične infrastrukture v RS segajo v prva leta 21. stoletja. Leta 2008 je raziskovalna skupina pod vodstvom dr. Iztoka Prezlja iz Fakultete za družbene vede predstavila zaključno poročilo o stanju kritične infrastrukture v RS ter določila 9 osnovnih sektorjev:

- sektor energetika,
- jedrski sektor,
- sektor voda,
- sektor hrana,
- sektor zdravje,
- sektor finance,
- sektor promet,
- sektor kemične industrije,
- sektor informacijsko-komunikacijske tehnologije

(Definicija in zaščita kritične infrastrukture Republike Slovenije 2008).

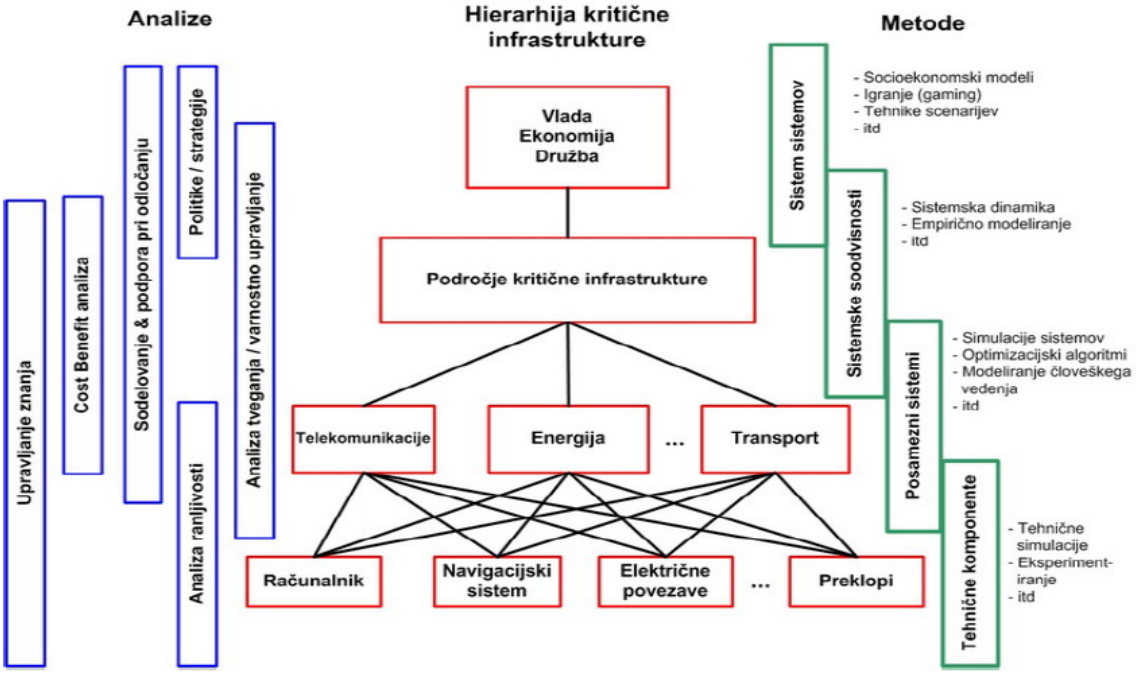
Zavzetost in želja po oblikovanju nacionalne kritične infrastrukture je rezultiralo v oblikovanju končnega dokumenta Sklep o določitvi kritične infrastrukture državnega pomena v RS, sprejetega pri Vladi RS aprila 2014. Sklep je označen z oznako tajnosti INTERNO in zato ni dostopen širši javnosti ter tudi ne more biti predmet raziskave v tej, javni, magistrski nalogi.

[9] V nadaljevanju naštevam pomembne zakonodajne akte, ki se navezujejo na določanje elementov kritične infrastrukture v RS:
- Definicija kritične infrastrukture, sklep Vlade RS št. 80000-2/2010/3, z dne 19. 4. 2010;
- Veljavni kriterji kritičnosti za določanje kritične infrastrukture državnega pomena;
- Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji, sklep Vlade RS št. 80200-1/2012/5, z dne 17. 10. 2012;
- Spremembe in dopolnitve osnovnih in sektorskih kriterijev kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji - sklep Vlade RS št. 80200-2/2013/3, z dne 9. 1. 2014;
- Sklep o določitvi kritične infrastrukture državnega pomena v RS, VRS, št. 80200-2/2014/8, z dne 10. 4. 2014 (op. a. – sklep je označen s stopnjo tajnosti INTERNO in zato ni dostopen javnosti).

3.4.5 Pristopi k zaščiti kritične infrastrukture v Sloveniji in po svetu

K zaščiti kritične infrastrukture je potrebno pristopati interdisciplinarno. To si lahko razložimo tako, da je za popolno razumevanje in načrtovanje zaščite kritične infrastrukture potrebno posedovati tako tehnična, računalniška, pravna kot tudi družboslovna znanja. Naravoslovna znanja nam lahko ponudijo neposredno obvladovanje elementa infrastrukture, družboslovna znanja pa poskušajo predvidevati vplive na celotno družbo v primeru nedelovanja elementov kritične infrastrukture. Za proučitev tveganj in ranljivosti je dodatno treba vključiti še strokovnjake s področja obvladovanja tveganja (ang. risk management) ali kriznega upravljanja (Perenboom 2001). Slednja dognanja so se v obramboslovni znanosti o zaščiti kritične infrastrukture pojavila v zadnjih dvajsetih letih, prej je namreč veljalo, da so se s kritično infrastrukturo ukvarjale predvsem naravoslovne in tehnične vede, večinoma vojaških krogov. Dunn (2005, 265) trdi, da v sedanjosti narašča nujnost vključitve tudi družboslovnih pristopov. Mednje lahko nedvomno vključimo tudi prispevke obramboslovja in varstvoslovja. Kljub vsemu naj poudariva, da so, kot meni Dunn (prav tam) trenutne metodologije za analizo kritične infrastrukture absolutno nezadostno razvite. Pogrešamo lahko predvsem interdisciplinarne metode, ki bi povezovale družboslovne in naravoslovne pristope.

Slika 3.1: Hierarhija infrastruktur v povezavi z analitičnimi metodami in perspektivami



Vir: Le Grand, Springsfield in Riguidel (2003).

Zaščita ključne infrastrukture zajema »…koncepte, politike, strategije, pripravljenost v smeri preprečevanja destabiliziranja in odzivanje na destabilizacijske pojave pri delovanju mrež in sistemov kritičnih infrastruktur (motnje, nesreče, napade ipd.)« (Definicija in zaščita kritične infrastrukture Republike Slovenije 2008, 17–18). V istem poročilu avtorji prav tako poudarjajo, da lahko zaščito kritične infrastrukture opazujemo na več nivojih:

- v okviru tehničnega sistema,
- v okviru institucije (npr. podjetja),
- v okviru infrastrukturnega sektorja,
- na nacionalni ravni (vsi sektorji skupaj s perspektive sistema sistemov)
- in na mednarodni ravni (npr. v EU).

V zadnjem času se krepi predvsem pomen zadnjih dveh nivojev, v nalogi bi rada uporabila nivo pregleda ustanove, natančneje podjetja in še to v okviru enega določenega sektorja – sektorja IKT; oziroma bi pregledala nivo infrastrukturnega sektorja (IK) v gospodarskih družbah, zavodih in drugih organizacijah, katerih dejavnost je posebnega pomena za obrambo države.

Zaradi množice potencialnih kritičnih infrastruktur je potrebno izločiti tiste, ki so »ključnejše« od ostalih. Lewis (2006, 7) trdi, da je najboljši način zaščite kritične infrastrukture v vsakem sektorju izbrati t. i. ključna vozlišča (ang. nodes – vozli, grče) oz. objekte, predmete, strukture in jih določiti ter zaščititi[10]. V primeru RS to pomeni določitev struktur, ki so najvitalnejše za njeno nacionalno varnost ter blaginjo prebivalcev in gospodarstva.

Koncept zaščite kritične infrastrukture je predvsem reaktivnega značaja, manj pa preventivnega, kot ugotavlja Radvanovsky (2006, 6). Da bi prevladoval slednji in bi bil dosežen primarni cilj zaščite kritične infrastrukture (preprečitev nastanka motenj ali njihova odprava, ko se pojavijo), bi bilo toliko bolj potrebno usmeriti znanstvene in gospodarske napore k znanstvenem preučevanju in načrtovanju zaščite KI, izdelavi ocen ogroženosti, nenehnemu posodabljanju sistemov zaščite, izdelavi modelov in simuliranja dogodkov Radvanovsky (2006, 6) imenuje ocenjevanje ranljivosti, načrte, postopke, politike, usposabljanja in potrebno opremo kot proaktivne ukrepe v smeri zmanjševanja groženj, tveganj in ranljivosti kritične infrastrukture – pripravljenost kritične infrastrukture (ang. critical infrastructure preparedness). Vse to je predvsem proces, ki ne prinaša takojšnjih vidnih uspehov in je predvsem naložba v prihodnost, ki se je slovensko gospodarstvo

[10] Prevod avtorja.

nemalokrat otepa[11]. Nekateri (Auerswald, Branscomb, La Port in Michel-Kerjan 2005, 79) trdijo, da cilj zaščite kritične infrastrukture ni v zaščiti infrastrukturnih objektov, ampak temeljnih storitev, proizvodov, dejavnosti ipd. Slednje je sicer v rahlem protislovju, saj kako neka organizacija lahko zaščiti (pro)izvajanje dejavnosti, storitev, proizvodov (ipd.), če ne skozi fizično zaščito objektov (kritične) infrastrukture.

Za učinkovito zaščito kritične infrastrukture je potrebno sledenje dvema potrebnima konceptoma: sposobnost preživetja (ang. survivability) in zanesljivost (ang reliability) ključne infrastrukture.

Prvi koncept opisuje sistemsko sposobnost za nadaljevanje delovanja, ko mu različni dogodki iz okolja povzročijo večjo škodo (Definicija in zaščita kritične infrastrukture Republike Slovenije 2008, 18). Sistem naj bi bil potemtakem sposoben (morda v zmanjšanem obsegu) nadaljevati z zagotavljanjem storitev, proizvodov, dejavnosti ipd. v danem operativnem okolju, ko razni dogodki škodujejo njemu ali okolju okoli njega. Prezelj (2005) imenuje ta koncept »robustnost« sistema.

Zanesljivost se za razliko od sposobnosti preživetja oz. robustnosti nanaša na dostopnost storitev oziroma zmožnost povezanih infrastruktur, da zagotovijo svojim strankam pričakovane storitve (Nozickova in Turnquist 2005 v Definicija in zaščita kritične infrastrukture Republike Slovenije 2008, 18). Ravno zanesljivost sistema je v konceptu kritične infrastrukture v času krize najbolj na preizkušnji, ko se med uporabniki odrazi povečana potreba po uporabi storitev, proizvodov, dejavnosti elementov ključne infrastrukture.

3.4.5.1 Medresorska koordinacijska skupina za usklajevanje priprav za zaščito kritične infrastrukture

Medresorsko koordinacijsko skupino za usklajevanje priprav za zaščito kritične infrastrukture je imenovala Vlada Republike Slovenije septembra 2012, spremembe so bile dodane septembra 2014. V njeni sestavi so predstavniki ministrstev, pristojnih za notranje zadeve, obrambo, finance, gospodarski razvoj in tehnologijo, infrastrukturo in prostor, kmetijstvo in okolje, zdravje, izobraževanje, znanost in šport, Obveščevalno-varnostne agencije ter Banke Slovenije (MORS, Medresorska koordinacijska skupina za usklajevanje priprav za zaščito kritične infrastrukture, 2014).

[11] Med intervjujem na Petrolu z g. Biščakom decembra 2011 je sogovornik poudaril, da je včasih njegovo delovno mesto razumljeno kot nujno zlo zaradi zakonodajne ureditve v državi.

Naloge skupine so usklajevanje in koordinacija priprav in nalog za zaščito evropske kritične infrastrukture v Republiki Sloveniji; določitev kritične infrastrukture državnega pomena za Republiko Slovenijo; oblikovanje predlogov ukrepov in postopkov za zaščito kritične infrastrukture z upoštevanjem usmeritev in stališč v zvezi Nato in EU; priprava predloga organov in organizacij, ki bi morale načrtovati ukrepe za zaščito kritične infrastrukture državnega pomena za Republiko Slovenijo (prav tam).

Predlogi ministrstev za določitev kritične infrastrukture so se zelo razlikovali, pokazala se je potreba po popravkih kriterijev kritičnosti. Slednje je vodilo do oblikovanja ožje delovne skupine pod vodstvom Ministrstva za obrambo, ki je predloge za določitev kritične infrastrukture državnega pomena uravnotežila in spremenila tudi kriterije. Spremenili in dopolnili so osnovne in sektorske kriterije ter določitev medsektorskih vplivov na občutljivost delovanja kritične infrastrukture ter določitev prioritet kritičnosti.

Skupina je oblikovala definicijo kritične infrastrukture državnega pomena v RS, na podlagi katere so določili sektorje kritične infrastrukture, ki zagotavljajo energetsko podporo, prometne povezave, preskrbo s hrano in pitno vodo, zdravstveno oskrbo, finance, varstvo okolja ter informacijsko in komunikacijsko podporo. Določili so tudi osnovne kriterije za določanje kritične infrastrukture RS, ob upoštevanju posledic nedelovanja zmogljivosti in dejavnosti, ki so ključnega pomena za državo (Informacijski portal energetika 2012).

3.4.5.2 NCKU

Nacionalni center za krizno upravljanje (NCKU) ima v primeru vojnega, izrednega ali stanja kriz posebno vlogo, ki se odraža tudi v zagotavljanju IK podpore subjektom nacionalne varnosti. V 2. odstavku 2. člena je določeno, da NCKU zagotavlja prostorske, tehnične, informacijske in telekomunikacijske pogoje za delo Vlade RS 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 (Ur. l. RS št. 9/2006). Za potrebe dela Vlade RS je v 1. odstavku 3. Člena določeno, da NCKU zagotavlja informacijske in komunikacijske povezave za izmenjavo podatkov in informacij med drugim[12] tudi z gospodarskimi družbami, zavodi in drugimi organizacijami, ki so po sklepu vlade posebnega pomena za obrambo (Ur. l. RS št. 9/2006).

[12] NCKU zagotavlja omenjene pogoje tudi z Uradom Predsednika Republike Slovenije, Generalnim sekretariatom Državnega zbora Republike Slovenije, Generalnim sekretariatom Vlade Republike Slovenije, Svetom za nacionalno varnost, ministrstvi, vladnimi službami, Operativno komunikacijskim centrom Generalne policijske uprave, Centrom za obveščanje Republike Slovenije, Poveljniškim centrom Slovenske vojske ter operativnimi centri in dežurnimi službami drugih državnih organov.

3. odstavek 9. člena določa, da podatki in informacije NCKU praviloma posredujejo v elektronski obliki preko zaščitenega komunikacijskega in informacijskega sistema centra oziroma drugih razpoložljivih zaščitenih elektronskih komunikacij tako, da je zagotovljeno varstvo posredovanih podatkov v skladu s predpisi, ki urejajo varstvo tajnih podatkov (Ur. l. RS št. 9/2006).

Iz tega sledi, da se vsi podatki in informacije, ki so označeni z določeno stopnjo tajnosti oziroma kot posebnega pomena za obrambo države in s katerimi razpolagajo organizacije posebnega pomena za obrambo države, opredeljeni kot tajni podatki in je treba z njimi ravnati v skladu z ZTP. Zatorej mora biti tudi načrtovanje zaščite opreme IKI v omenjenih organizacijah v skladu z ZTP in njegovimi podzakonskimi predpisi.

3.4.6 Kritična infrastruktura: javna, zasebna in/ali javno-zasebna

Teoretiki se na področju kritične infrastrukture osredotočajo na nekatera osnovna področja preučevanja in sicer na[13]: teorijo in koncepte kritične infrastrukture ter njene zaščite; varnostna tveganja in grožnje kritični infrastrukturi ter razvoj metodologije za ocenjevanje le-teh; organizacijo nacionalnih in zasebnih sistemov regulacije zaščite ključne infrastrukture v okviru nacionalnih sistemov kriznega upravljanja oziroma sistemov nacionalne varnosti; krizno upravljanje ob ogrožanju ali prekinitvi delovanja ključne infrastrukture; aplikacijo teorije kompleksnosti in mrežne teorije na sisteme ključne infrastrukture; sposobnost preživetja (ang. survivability) sistemov ključne infrastrukture in značilnosti takšnih sistemov. To so le nekatera osnovna področja preučevanja kritične infrastrukture v svetovnem merilu.

Pri zaščiti kritične infrastrukture je potrebno biti pozoren na »nove« smernice, ki se pojavljajo in sicer o povezovanju javnega in zasebnega. Javno zasebno partnerstvo se je razvilo iz potreb po večji varnosti določenih infrastruktur, varnosti katerih država ni hotela ali zmogla zagotavljati. Iz tega so nastale razne zasebne varnostne organizacije, ki ponujajo storitve zagotavljanja varnosti z glavnim vodilom dobička, katere usmerja predvsem ekonomska logika in so prisotne tudi pri zagotavljanju varnosti in načrtovanju zaščite v organizacijah z elementi kritične infrastrukture.

3.4.7 Koncept (K)IKI v RS

O kritični informacijsko-komunikacijski infrastrukturi v javnosti ni veliko govora, medtem ko se strokovni izraz kritična informacijsko komunikacijska infrastruktura v strokovni

[13] Glej Definicija in zaščita kritične infrastrukture Republike Slovenije 2008, 21.

javnosti pojavlja dokaj pogosto, čeprav na državni ravni do nedavnega[14] ni bilo uradno sprejete enotne opredelitve, kar je posebej oteževalo načrtovanje zaščite le-te. Vendar pojdimo lepo po vrsti. Vsekakor je potrebno natančno razmejiti kritično infrastrukturo (ang. Critical Infrastructure) in jo ločiti od ključne informacijske infrastrukture (ang. Critical Information Infrastructure). Pojem kritična infrastruktura je širši od pojma informacijska kritična infrastruktura.

Procesi, storitve in sistemi so del kritične infrastrukture, njihovo (ne)delovanje ali uničenje pa ima lahko vpliv na nacionalno varnost, gospodarsko in družbeno blaginjo. Kritični sektorji v tem smislu so: promet, energetski sistem, bančne in finančne institucije, zdravstvo ter sistem zaščite in reševanja, dodamo pa lahko še sistem javne preskrbe z vodo, hrano in strateškimi surovinami in namensko (obrambno) industrijo (Svete 2007, 160).

Informacijska kritična infrastruktura pa vsebuje komponente, kot so telekomunikacije, strojne in programska računalniške opreme, internet, satelitske komunikacije, optična vlakna ipd. (Dunn in Wigrt 2004, 20 v Simčič 2007, 13). Informacijska infrastruktura so tudi računalniki povezani med seboj v mrežo (Svete 2007, 160).

Kot izhodišče za izpeljavo opredelitev in predstavitev pomena KIKI, sva si s kolegico izbrala zaključno poročilo o stanju KI v Republiki Sloveniji Definicija in zaščita kritične infrastrukture Republike Slovenije in Priročnik o zaščiti kritične informacijske infrastrukture iz leta 2004 (v nadaljevanju Priročnik) švicarskega Zveznega tehnološkega inštituta iz Züricha ter opredelitev sektorja informacijsko-komunikacijske podpore v Sklepu Vlade RS z dne 17. 10. 2012 z naslovom: Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji.

Kljub vsemu izhajava iz opredelitve Vlade RS, ki je kritično infrastrukturo državnega pomena opredelila kot »…tiste zmogljivosti in storitve, ki so ključnega pomena za državo in bi prekinitev njihovega delovanja ali njihovo uničenje pomembno vplivalo in imelo resne posledice na nacionalno varnost, gospodarstvo, ključne družbene funkcije, zdravje, varnost in zaščito ter družbeno blaginjo.« (Sklep Vlade RS z dne 19. aprila 2010). Ta opredelitev je izhodišče za oblikovanje opredelitve KIKI.

V Priročniku o zaščiti kritične informacijske infrastrukture (2004, 17) je zapisano, da se KIKI dojema kot ključni del nacionalne varnosti v številnih državah. Zato jo lahko štejemo kot dejstvo in kot termin, ki opredeljuje ožje področje kritične infrastrukture, ki je omejeno le na IKT. Prvi, ki so uvedli v uporabo termin KIKI so bili člani Predsedniške komisije za

[14] Natančneje do oktobra 2012, ko je bil v sklopu oblikovanja sektorjev kritične infrastrukture v RS na MORS sprejet sektor informacijsko-komunikacijske podpore.

zaščito kritične infrastrukture, ki so v poročilu leta 1997 zapisali, da so varnost, gospodarstvo, način življenja in celo preživetje industrializiranega sveta odvisni od medsebojno povezanega trojčka: električne energije, komunikacij in računalnikov (CIIP Handbook 2004, 18). Iz vsega tega je razvidno, da je večina sektorjev kritične infrastrukture nadzorovana ali pa deluje s pomočjo izredno ranljive IKT. Zaradi tega so t. i. »kibernetične« infrastrukture postale težišča varnostne politike držav. Ta del narodne, nacionalne, regionalne oz. globalne informacijske infrastrukture, ki je ključen za stalnost izvajanja dejavnosti in storitev kritičnih infrastruktur, se imenuje kritična informacijska infrastruktura (ang. critical information infrastructure – CII) (CIIP Handbook 2004, 19).

V Sklepu Vlade RS iz oktobra 2012 je jasno zapisano, da je sektor informacijsko-komunikacijske podpore pomemben in kritičen v primeru: »…nedelovanja elektronsko komunikacijske opreme, omrežja in storitev, ki podpirajo ključne funkcije v državi, ki se nanašajo na zagotavljanje delovanje enega od sektorjev kritične infrastrukture nacionalno varnostnega sistema, energetskega sistema in financ, ki povzroči izpad podpore za več kot 6 oziroma 24 ur.« (Sklep Vlade RS, št. 802-15/2011-67 z dne 17. 10. 2012). Tako v slovenskem in evropskem prostoru nedvomno ločimo informacijsko in komunikacijsko komponento sektorja informacijsko komunikacijske podpore in jo lahko preslikamo tudi na ožje pojmovanje informacijsko-komunikacijske kritične infrastrukture.

In ker je v slovenskih in evropskih strokovnih krogih že močno zakoreninjen izraz informacijske in komunikacijske tehnologije in ker je komunikacijska tehnologija vedno bolj povezana z informacijsko, je znanstveno, terminološko in strokovno pravilno, da ne govorimo izključno o kritični informacijski infrastrukturi, pač pa o kritični informacijsko-komunikacijski infrastrukturi (KIKI).

V praksi lahko prihaja do zamenjevanja terminov KI in KIKI oz. ZKI in ZKIKI, vendar tukaj po navadi ne prihaja do napak zaradi nenatančnosti ali zamenjave konceptov, pač pa različnih stopenj razvitosti koncepta ZKI, ki v kasnejši fazi večinoma razvijejo (pod)koncept ZKIKI. Razlike med konceptoma so ogromne. Priročnik dojema ZKI višje na lestvici kot ZKII, vendar ga opredeljujejo kot ključen del ZKI. KI oz. ZKI obsega vse ključne sektorje narodne (nacionalne) infrastrukture, KIKI oz. ZKIKI pa je podkoncept širšega koncepta, saj se osredotoča zgolj na IKI[15] (CIIP Handbook 2004, 20).

[15] IKT in zaradi tega IKI pa je prisotna v večini, če ne že v vseh, sektorjev.

4 NORMATIVNI AKTI NA PODROČJU KIBERNETSKE VARNOSTI

4.1 Evropska unija

EU je v času pisanja te magistrske naloge načrtovala sprejetje Strategije o evropski spletni varnosti (ang. European Internet Security Strategy) v tretjem četrtletju leta 2012. Tako je takrat napovedala takratna evropska komisarka za evropski digitalni program – agendo Neelie Kroes. Potreba po skupni evropski strategiji na področju spletne varnosti narašča zaradi povečevanja zavedanja o pomenu spleta v gospodarstvu in pri vsakdanjem delovanju družbe. Svetovna banka namreč ocenjuje, da 10% povečanje hitrih spletnih povezav prinese 1,3% gospodarsko rast.[16] Potrebno je še omeniti, da Svetovni gospodarski forum (ang. World Economic Forum) ocenjuje, da obstaja 10% verjetnost sesutja KIKI, kot jo imenuje, in s tem škodo okoli 250 milijard evrov.[17]

Dejansko sprejetje strategije se je zavleklo v začetek leta 2013, ko je bila sprejeta Strategija za kibernetsko varnost Evropske unije »Odprt, varen in zanesljiv kibernetski prostor«.

Omenjeno strategijo sta predložila Komisija in visoka predstavnica Unije za zunanje zadeve in varnostno politiko (v nadaljevanju: visoka predstavnica) in predstavlja celostno vizijo EU na tem področju, pojasnjuje vloge in odgovornosti ter določa potrebne ukrepe.

Vizija EU za kibernetsko varnost se v strategiji osredotoča na pet prednostnih nalog:

- pridobivanje kibernetske odpornosti;
- znatno zmanjšanje kibernetskega kriminala;
- razvoj politike in zmožnosti za kibernetsko obrambo, povezanih s skupno varnostno in obrambno politiko;
- razvoj industrijskih in tehnoloških virov za kibernetsko varnost;
- določitev usklajene mednarodne politike Evropske unije za kibernetski prostor in spodbujanje temeljnih vrednot EU

Temeljni cilj strategije je dobra in učinkovita zaščita v spletnem okolju EU (Strategija za kibernetsko varnost 2013, 3). Temeljne pravice, demokracijo in pravno državo je potrebno varovati tudi v kibernetskem prostoru. Da pa bi slednji lahko ostal odprt in svoboden, bi morali na spletu veljati isti predpisi, načela in vrednote, ki jih EU promovira v ne-spletnem okolju in so zapisani v Listini o temeljnih pravicah Evropske unije ter temeljnih vrednotah EU. Pri zagotavljanju svobodnega in varnega kibernetskega prostora imajo pomembno vlogo

[16] Proposal in a European Strategy for Internet Security.
[17] Prav tam.

vlade. Slednje morajo izpolnjevati več nalog, kot so: varovanje dostopa in odprtosti, spoštovanje in varovanje temeljnih pravic na spletu ter ohranjanje zanesljivosti in interoperabilnosti interneta. Ne smemo pa zanemariti tudi pomembne vloge zasebnega sektorja saj je precejšen del kibernetskega prostora v lasti zasebnih podjetij (Strategija za kibernetsko varnost 2013, 2). EU podpira pristop upravljanja interneta, ki vključuje več zainteresiranih strani. Vsi zadevani akterji, tako javni kot zasebni sektor in posamezni državljani, se morajo za povečanje kibernetske varnosti zavedati skupne odgovornosti. Komisija se zaveda, da je spopadanje z varnostnimi izzivi v kibernetskem prostoru predvsem naloga držav članic vendar v Strategiji predlaga ukrepe za povečevanje skupne uspešnosti EU, ki vključujejo raznovrstna orodja politike in različne akterje (institucije EU, države članice, industrijski sektorji) (Strategija za kibernetsko varnost 2013, 3–4).

Število namernih ali naključnih kibernetskih napadov se zaskrbljujoče hitro povečuje, slednje lahko prekine zagotavljanje bistvenih storitev, ki jih imamo za samoumevne (voda, zdravstveno varstvo, elektrika, mobilne storitve). Če si Evropa ne bo močno prizadevala za izboljšanje javnih in zasebnih zmogljivosti, virov in postopkov za preprečevanje, odkrivanje in obravnavanje kibernetskih incidentov, bo ostala ranljiva. Kljub napredku, ki so ga prinesle prostovoljne zveze, v EU še vedno ostajajo vrzeli, zlasti na področju nacionalnih zmogljivosti, usklajevanja v primeru čezmejnih incidentov ter vključenosti in pripravljenosti zasebnega sektorja. Zato je Komisija razvila politiko na področju varnosti omrežij in informacij (VOI), v okviru Evropske agencije za varnost omrežij in informacij (ENISA) (Strategija za kibernetsko varnost 2013, 5).

Zgoraj omenjeni zakonodajni predlog vsebuje spodaj zapisane cilje. Eden od ciljev je določitev skupnih minimalnih zahtev za VOI na nacionalni ravni, ki vključujejo imenovanje nacionalnih organov, pristojnih za VOI, vzpostavitev dobro delujočih CERT-ov, sprejetje nacionalne strategije za VOI in pripravo nacionalnega načrta za sodelovanje na področju VOI. Ker pa je gradnja zmogljivosti in usklajevanje tudi v domeni EU so leta 2012 ustanovili stalni CERT-EU za odzivanje na računalniške grožnje, ki je odgovoren za varnost sistemov IT v institucijah, agencijah in organih EU. Za cilj so si postavili tudi vzpostavitev mehanizmov za usklajeno preprečevanje, odkrivanje, ublažitev in odzivanje. Slednji mehanizmi bodo omogočali izmenjavo informacij in medsebojno pomoč med nacionalnimi organi pristojnimi za VOI. Pomemben cilj je tudi izboljšanje pripravljenosti in vključenosti zasebnega sektorja, ki bi moral z zadostnim vlaganjem razviti lastno tehnično zmogljivost za kibernetsko odpornost in si izmenjati najboljše prakse med sektorji. Orodja za odzivanje na incidente

(ugotavljanje vzrokov, opravljanje forenzičnih preiskav), ki jih je razvila industrija pa bi moral izkoristiti tudi javni sektor (Strategija za kibernetsko varnost 2013, 5–6).

Potrebno je vzpostaviti kulturo kibernetske varnosti, ki bi okrepila poslovne priložnosti in konkurenčnost v zasebnem sektorju, hkrati pa bi kibernetsko varnost lahko izkoristili za promoviranje izdelkov in storitev. Subjekti v zasebnem sektorju bi morali nacionalne organe pristojne za VOI obvestiti o incidentih, ki lahko privedejo do prekinjenega delovanja ključnih storitev in dobave blaga zaradi odvisnosti od omrežij in informacijskih sistemov. Organi pristojni za VOI bi morali organe kazenskega pregona obvestiti o incidentih, za katere sumijo, da so resne kriminalne narave. Na ravni EU bi bilo potrebno še naprej razvijati evropsko javno-zasebno partnerstvo (EP3R), omogočiti finančno podporo za ključno infrastrukturo, preiskovanje kibernetske kriminalitete in boj proti njej. Pomembne so tudi vaje na področju kibernetskih incidentov na ravni EU, ki so bistvene za simulacijo sodelovanja med državami članicami in zasebnim sektorjem (Strategija za kibernetsko varnost 2013, 6–7). Zanemariti pa ne smemo tudi povezovanja raziskovalnega in akademskega sveta ter strokovnjakov.

Do interneta in neoviranega pretoka informacij bi moral imeti dostop vsak, pomembno je tudi, da je ta dostop varen za vse. Za doseganje varnega dostopa je potrebno ozaveščanje končnih uporabnikov o tveganjih, s katerimi se soočajo na spletu in jim dati možnost, da sprejmejo preproste ukrepe za obrambo (Strategija za kibernetsko varnost 2013, 8). Vse večja digitalizacija sveta pomeni več možnosti za kibernetske kriminalce. Kibernetska kriminaliteta, ki ne pozna meja, je ena od najhitreje rastočih oblik kriminala in vsak dan prizadene več kot milijon ljudi po svetu. Kibernetski kriminalci uporabljajo vse naprednejše tehnike in imajo zelo dobro razvite mreže, izkoriščajo tudi anonimnost spletnih domen, kar jim prinaša visoke dobičke ob nizkem tveganju. Metode kibernetske kriminalitete se zelo hitro razvijajo, zato organi kazenskega pregona potrebujejo primerne zmogljivosti za odzivanje, saj se proti njej ne morejo boriti z zastarelimi operativnimi orodji (Strategija za kibernetsko varnost 2013, 8–9). Nedavno je bil zato ustanovljen Evropski center za boj proti kibernetski kriminaliteti (EC3), ki bo zagotavljal analize in podatke, opravljal visokokakovostno forenzično delo, spodbujal sodelovanje in omogočal izmenjavo informacij med vsemi zainteresiranimi stranmi.

Prizadevanja za kibernetsko varnost v EU vključujejo tudi kibernetsko obrambo, ki se bo osredotočala na odkrivanje naprednih kibernetskih groženj, odzivala nanje in zagotavljala obnovo po njihovi odpravi. Glede na to, da so grožnje večplastne je pomembna sinergija med civilnimi in vojaškimi pristopi. Na tem področju bi se EU in NATO lahko dopolnjevala v

svojih prizadevanjih, da ne bi prihajalo do nepotrebnih podvajanj (Strategija za kibernetsko varnost 2013, 11–12).

Kibernetska kriminaliteta, uperjena proti zasebnemu sektorju in posameznikom že zdaj vpliva na gospodarstvo EU. Evropa ima odlične zmogljivosti za raziskave in razvoj, vendar imajo številni vodilni svetovni ponudniki inovativnih izdelkov in storitev IKT sedež izven EU. Obstaja tveganje za preveliko odvisnost od IKT in varnostnih rešitev razvitih zunaj meja Evrope. Ključnega pomena je, da so elementi strojne in programske opreme, ki se uporabljajo v kritičnih storitvah, infrastrukturi in mobilnih napravah proizvedeni v EU, zaradi zanesljivosti in varnosti ter zagotavljanja varstva osebnih podatkov. Predvsem bi se bilo treba osredotočiti na varnost dobavne verige v ključnih gospodarskih sektorjih (industrijski kontrolni sistemi, energetska in prometna infrastruktura). Na žalost številni akterji varnost vidijo kot dodatno breme, zato je potrebo uveljaviti zahteve glede kibernetske varnosti. Ena od možnih opcij je, da bi podjetja na svoje izdelke prilepila varnostne oznake oziroma oznake kakovosti, ki bi dokazovale zagotavljanje visoke kibernetske varnosti. Slednje bi jim pomagalo pri promociji njihovih izdelkov in storitev in zagotovilo večjo konkurenčno prednost, hkrati bi potrošniki imeli boljši pregled nad trgom (Strategija za kibernetsko varnost 2013, 12–14).

4.2 NATO

NATO se je s prvimi resnimi kibernetskimi napadi soočil med kosovsko krizo. Takrat so bili zaznani vdori na NATO spletno stran, za več dni so tudi blokirali račun elektronske pošte zavezništva za zunanje obiskovalce. Za tisti čas je bilo značilno, da so na kibernetske razsežnosti spora gledali kot na oviranje NATO informacijske kampanje. Kibernetski napadi, ki so imeli omejen obseg in škodo so sicer veljali za tveganje ampak so zahtevali le omejeno tehnično odzivanje. Tematika je postala zaradi vse večjega ogrožanja javne varnosti in stabilnosti države aktualna šele po 11. septembru in dobila dokončno politično pozornost z tritedenskimi vali množičnih kibernetskih napadov v Estoniji leta 2007. K večjemu zavedanju so prispevali tudi incidenti v naslednjih letih. Leta 2008 so bili resno ogroženi ameriški vojaški računalniški sistemi preko vohunske programske opreme. V enem od ameriških vojaških oporišč na Bližnjem vzhodu so s pomočjo USB ključka prenesli na tisoče datotek na strežnike pod tujim nadzorom. Od takrat naprej je kibernetsko vohunjenje postalo skoraj stalna grožnja varnosti, saj s tem močno varovane skrivnosti prehajajo v anonimne in po vsej verjetnosti zlonamerne roke. Pomemben incident se je zgodil tudi leta 2010, ko je zlonamerna programska oprema »Stuxnet« z motnjami kritičnih računalniških sistemov za

upravljanje oskrbe z energijo napadla iranski jedrski program. S tem napadom so se za resnična izkazala opozorila strokovnjakov iz leta 2001, ki so opozarjali, da bo kibernetska razsežnost prej ali slej uporabljena za resne napade s smrtonosnim izidom v fizičnem svetu. Kibernetsko razsežnost je imel tudi spor med Gruzijo in Rusijo. Gruzija je bila namreč tarča napadov na vladne spletne strani in strežnike. Omenjeni napadi niso imeli smrtonosnega izida, so pa oslabili gruzijsko vlado v ključni fazi spora (Theiler, 2011).

Ti incidenti jasno nakazujejo, da so trenutno nacionalne države najnevarnejši akterji na kibernetskem področju, saj visoko sofisticirano vohunstvo in sabotiranje še vedno potrebuje zmogljivosti, odločenost ter ustrezno razmerje stroškov in koristi. Zmogljivosti za napad so vedno bolj dostopne tudi kriminalnim mrežam, zato lahko v prihodnosti pričakujemo tudi napade nedržavnih akterjev, kot so teroristi. Težava je v tem, da pri kibernetskem bojevanju praktično ni učinkovitega odvračanja, saj je ob spoštovanju mednarodnega prava skoraj nemogoče ugotoviti kdo je napadalec (prav tam).

NATO se ves čas prilagaja tej novi vrsti varnostnih izzivov. Že leta 2002 (po napadih 11. Septembra) je NATO kot del praških zavez za zmogljivosti objavil pomemben poziv k izboljšanju zmogljivosti za obrambo pred kibernetskimi napadi vendar so se sprva osredotočali le na izvajanje pasivnih zaščitnih ukrepov. Leta 2008 (po napadih v Estoniji) je NATO prvič uradno pripravil Politiko za kibernetsko obrambo, ki je vzpostavila tri osrednje stebre politike Nata v kibernetskem okolju: subsidiarnost, nepodvajanje in varnost. Subsidiarnost pomeni, da se pomoč zagotovi na prošnjo držav članic. Nepodvajanje pomeni, izogibanje podvajanju struktur in zmogljivosti na mednarodni, regionalni in nacionalni ravni. Pri tretjem stebru (varnost) gre za sodelovanje na podlagi zaupanja (prav tam).

NATO se za razliko od EU ukvarja z ogrožanjem omrežne varnosti predvsem na vojaško-politični ravni. V zadnjem času je zaslediti veliko pomislekov v smeri, da bi bilo dobro sprejeti dva krovna dokumenta, saj število kibernetskih napadov narašča na 6 tisoč napadov dnevno (Carr, 2009, 6). Organizacija je določila, da največjo grožnjo predstavljajo napadi, ki pridejo z območja Kitajske in tudi Ruske federacije (NATO Requests Cyber Security Cooperation From India). V Natu tako opozarjajo na odsotnost krovnih dokumentov kot sta mednarodna sporazuma o kibernetskem kriminalu in kibernetski varnosti.

Nov strateški koncept Nata opozarja, da so kibernetski napadi vse pogostejši, bolj organizirani in dražji, kar se tiče odpravljanja njihovih posledic. Predvsem se kibernetske grožnje nanašajo na ogrožanje varnosti in vpliv na vladne ustanove, gospodarstvo, posledično lahko prizadenejo tudi transportne in oskrbovalne mreže ter tudi kritično infrastrukturo. Tovrstni napadi ogrožajo evro-atlantsko blaginjo, rast, varnost in stabilnost. V konceptu je

tudi opredeljeno, da lahko napadi izvirajo tudi od tujih vojaških, obveščevalnih struktur, organiziranega kriminala, terorističnih in ekstremističnih skupin (*Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization 2010*).

S tem namenom je potrebno razvijati zmožnosti preprečevanja, zaznavanja in zaščite ter obrambe pred tovrstnimi napadi ter nenazadnje tudi zmožnosti obnove po napadih. Ravno načrtovanje zaščite lahko največ doprinese k povečevanju varnosti, saj obsega tako spremljanje trendov, preteklih napadov in napovedovanje ter razvijanje zmožnosti zaščite pred njimi.

NATO želi biti koordinator in vodilni partner sodelujočih nacionalnih centrov zmožnosti zaščite pred kibernetskimi napadi ter poskuša centralizirati zaščito NATO ustanov pred njimi. Organizacija se zaveda pomena načrtovanja zaščite IKI pred različnimi vrstami groženj in predlaga uporabo NATO procesa načrtovanja zaščite pred le-temi.

Kot trenutno največjo oz. najaktivnejšo grožnjo NATO zaznava terorizem, ki je lahko v tradicionalni – konvencionalni obliki, lahko pa se pojavi tudi v obliki omrežnega terorizma. Terorizem predstavlja neposredno grožnjo državljanom držav članic NATO ter širši mednarodni stabilnosti in blaginji. Ekstremistične skupine se še naprej širijo na in v območja, strateškega pomena za Zavezništvo[18], sodobna tehnologija pa le še povečuje grožnje in morebitni vpliv terorističnih napadov.

Vse države so vedno bolj odvisne od ključnih komunikacij, transporta in tranzitnih poti, od katerih je odvisno mednarodno trgovanje, energetska varnost in blaginja. Odpornost pred napadi in motenjem zahteva vedno več mednarodnega truda, saj so/bodo nekatere države Nata vedno bolj odvisne od tujih dobaviteljev energentov. Predvsem pošiljke energentov so vedno bolj izpostavljene različnim »motnjam«. Ključne okoljske omejitve in omejenost virov, zdravstvena tveganja, podnebne spremembe, omejenost vodnih virov in povečevanje energetskih potreb bodo tudi v bodoče oblikovale varnostno okolje pomembno za NATO, kar bo morebiti tudi vplivalo na Natovo načrtovanje in operacije.[19]

NATO je kibernetske grožnje prvič omenil v svojem strateškem konceptu leta 2002 in nato še leta 2006. V Strateškem konceptu iz leta 2008 je NATO priznal, da je šele kibernetski napad na Estonijo, ki se je zgodil leta 2007, povzročil vsesplošno in resno zavedanje o tovrstnih pojavih. V zadnjem Strateškem konceptu, ki ga je NATO sprejel leta 2010 na vrhu v Lizboni, so kibernetske grožnje prepoznali kot zelo resne, vse pogostejše, dobro organizirane in vse bolj uničujoče glede na cilje napada, ki so lahko vladne, poslovne, gospodarske ali

[18] Pri tej trditvi lahko potegnemo vzporednice tudi z Bližnjim vzhodom in ISIS-om.
[19] Povzeto po NATO Strategic Concept.

druge organizacije. NATO pa se zaveda tudi potencialne nevarnosti v napadih na kritično infrastrukturo, katere nedelovanje bi lahko prizadelo tako nacionalne interese, kot tudi interese, blaginjo, varnost in stabilnost zavezništva. Možni napadalci bi lahko bile obveščevalne službe, teroristične in ekstremistične skupine, ter skupine, ki so že sedaj vpletene v organiziran kriminal. Zaradi novih trendov, bo NATO v procese načrtovanja in bodoče operacije vključil najnovejšo tehnologijo (*Strategic Concept For the Defence and Security of the Members of the Nato* 2010, 4). Korak bližje tem uresničitvam je NATO storil, ko je ustanovil Center odličnosti v Estoniji (CCDCOE – *Cooperative Cyber Defence Centre of Excellence*).

NATO bo skladno s svojim novim strateškim konceptom (2010, 5) razvijal svoje zmogljivosti in sicer, sisteme za preprečevanje, zaznavo, obrambo in okrevanje pred kibernetskimi napadi. Razvijal bo tudi procese načrtovanja za povečanje in koordinacijo nacionalnih zmogljivosti ter centralizirano zaščito, zavedanje, opozarjanje in odzivanje vseh članic. Poskušali bodo razviti tudi kapacitete za zaščito energetskih virov in pripadajoče energetske infrastrukture, ki bi lahko bila tarča terorističnih napadov.

V primeru kibernetskih napadov ameriška zunanja politika zagovarja uporabo 5. člena Severnoatlantske pogodbe, ki pravi, da bo oborožen napad na eno državo zavezništva razumljen kot napad na vse članice. Menijo namreč, da napadi ne bodo prihajali več iz zraka in topov, ampak preko optičnih kablov in da je na take napade potrebno odločno odgovoriti, še posebej, če bo tarča napadov kritična infrastruktura (Amies 2010 v Čaleta in Rolih 2011, 10).

Natov kibernetični center odličnosti (v nadaljevanju Center) v Talinu v Estoniji je koncem marca 2012 organiziral mednarodno vajo zagotavljanja kibernetske obrambe in omrežne varnosti, na kateri so preverjali sposobnost zaščite in zavarovanja IKT sistemov v manjših telekomunikacijskih podjetjih širom Evrope. Na vaji žal niso sodelovali predstavniki iz Slovenije. Glavni namen vaje je bil krepitev obrambnih sposobnosti, načrtovanja zaščite, usposabljanje predstavnikov in specialistov NATO držav pred kibernetskimi napadi, kar je tudi glavni cilj Centra.

Republika Slovenija se kot polnopravna članica zavezništva zaveda pravic in dolžnosti do te vojaško-politične organizacije ter pomena načrtovanja zaščite tudi v informacijski (kibernetski) dimenziji. S tem namenom je Republika Slovenija v strateškem dokumentu Resolucija o splošnem dolgoročnem programu opremljanja in razvoja slovenske vojske do leta 2025 (ReDPRSV25), ki je bila sprejeta novembra 2010 spoznala, da bo bojišče prihodnosti poleg kopnega, morja in zraka obsegalo tudi kibernetski prostor in vesolje.

Poseben poudarek bo SV posvetila razvoju (med drugimi zmogljivostmi) zmogljivosti računalniških in komunikacijskih sistemov za zaščito pred kibernetskimi napadi. Kot multiplikatorje bojne moči bo med drugim razvila tudi zmogljivosti kibernetskega bojevanja. Vzpostavljena bo varna in prilagodljiva komunikacijska in informacijska omrežna infrastruktura, skladna z zahtevami NATO zmogljivosti omrežnega delovanja. Vzpostavljeni bodo ukrepi in zmogljivosti informacijske varnosti z namenom preprečevanja nenadzorovanega dostopa in vključevanja v omrežje (Čaleta in Rolih 2011, 54–55).

Kibernetska varnost je bila tudi ena izmed tem Strateškega foruma 2014 na Bledu. V razpravi so sodelovali strokovnjaki iz EU, Nata, mednarodnih ustanov ter nacionalnih organov. Tam so izpostavili, da večina držav ne kaže zadostnega interesa, da bi upravljanje interneta prevzela neka krovna mednarodna organizacija. Slednje onemogoča vzpostavitev mednarodno sprejetega pravnega reda, ki bi urejal kibernetski prostor in reševal morebitne spore (Pišlar 2014, 8).

Področje kibernetske varnosti postaja eden izmed glavnih izzivov Nata, saj so obrambni ministri članic zavezništva junija 2014 sprejeli okrepljeno politiko kibernetske obrambne. Njen osnovni element so določila, ki se nanašajo na pomoč zavezništva ob kibernetskem napadu in pri razvoju zmogljivosti za zagotavljanje kibernetske varnosti (prav tam).

Na Natovem vrhu v Walesu so predsedniki vlad in držav članic potrdili prednostne cilje razvoja zmogljivosti zavezništva v prihodnosti. V to kategorijo spadajo tudi zmogljivosti na področju kibernetske obrambe. Kibernetska obramba je prvič predstavljena kot del kolektivne obrambe, kar obsega tudi možnost delovanja po 5. členu Severnoatlantske pogodbe. Izpostavili so tudi dejstvo, da v kibernetskem prostoru velja mednarodno pravo. Skladno z novo okrepljeno politiko kibernetske obrambe NATO pomoč zaveznicam obravnava na podlagi dveh temeljnih načel, in sicer da se NATO omejuje na oblikovanje kibernetskih zmogljivosti v okviru svojih komunikacijsko-informacijskih sistemov, za razvoj nacionalnih obrambnih zmogljivosti pa so odgovorne države članice same. Vlaganje v kibernetsko obrambo ni več priporočilo ampak obveznost. Del Natovih zmogljivosti je tudi tako imenovani *cyber range* oz. omrežje, ki je namenjeno usposabljanju in vajam ter vzpostavitvi partnerstva med Natom in industrijo na kibernetskem področju ter krepitvi sodelovanja pri izmenjavi informacij med zaveznicami in s tem tudi zaupanja (Pišlar 2014, 9).

NATO ponuja pomoč državam članicam pri ozaveščanju, usposabljanju, šolanju in na vajah s področja zagotavljanja kibernetske varnosti. Ena od takih vaj je tudi vaja *Locked Shields*.

4.2.1 NATO Vaja Locked Shields

Obrambne vaje NATO Locked Shields se odvijajo vsako leto že od leta 2012 naprej. Gre za obrambno vajo, ki poteka v realnem času. Leta 2014 jo je izvedel NATO Center odličnosti, ki je stacioniran v Talinu v Estoniji, vključevala pa je okrog 300 udeležencev iz 17 držav. Pri organizaciji so sodelovali tudi: Estonski organ za informacijske sisteme, Enota za kibernetsko obrambo Estonske obrambne lige, estonske in finske obrambne sile ter še mnogi drugi. Vaja se je odvijala dva dneva, pri čemer je vključevala 12 obrambnih ekip in eno napadalno. Sodelovale so naslednje ekipe: Estonija, Finska, Italija, Španija, Nemčija in Nizozemska, Turčija, Latvija in Češka, Madžarska, Francija, Poljska, Avstrija in Litva, NATO CIRC (*Computer Incident Response Capability*). Ekipe so tekmovale iz svojih matičnih držav, sedež nadzora je bil v Talinu. Zmagovalka vaje, ki predstavlja edinstveno priložnost za usposabljanje in sodelovanje, je bila tokrat (leta 2014) Poljska (CCDCOE 2014).

Vaja je zastavljena kot tekmovanje v katerem se ekipe v obrambi točkuje glede na njihovo uspešnost. Čeprav ekipe v obrambi med seboj tekmujejo, je vaja zastavljena tako, da spodbuja ekipe k izmenjavi informacij in sodelovanju, kolikor je to le mogoče (prav tam).

Tokratni scenarij je ekipe postavil v fiktivno državo Berylio, katere industrija je bila tarča kibernetskih napadov. Vaja se je začela z hektivističnimi napadi, nadaljevala pa z vohunjenjem in sabotažami ter napadom na omrežje. Poleg tehnične obrambe je dogodek vključeval številne dodatne naloge pravne narave in forenzične izzive, katerih cilj je vajo narediti čim bolj realistično. 12 obrambnih modrih ekip je sestavljalo največ 16 članov, njihova naloga je bila zaščita omrežja fiktivne organizacije pred napadi rdeče napadalne ekipe. Prav tako je bila njihova naloga obvladovanje incidenta, delitev ugotovitev z ostalimi ekipami, odzivanje na pravne in medijske dileme iz scenarija ter razrešiti forenzične izzive. Omrežje, ki so ga morale braniti modre ekipe je bilo večje kot prejšnja leta in je bilo sestavljeno iz približno 50 računalnikov na ekipo. Ta vaja je bila prva, kjer je tehnično okolje imelo popolno podporo IPv6. Vaja je vključevala tehnologijo, ki je večina udeležencev modrih ekip ni poznala. Na podlagi izkušenj iz vaje Locked Shields 2013 je bila rdeča ekipa znatno okrepljena. Na splošno so bili napadalci spet zelo uspešni, vendar je potrebno upoštevati, da je vaja vedno zastavljena v korist napadalne ekipe, saj ta ekipa ni sestavljena iz udeležencev, ki so se udeležili usposabljanja. Napadalna ekipa ima ločene izobraževalne delavnice, popolno znanje o sistemih in njihovih ranljivostih, lahko pa tudi uporabi že vnaprej pripravljeno zlonamerno kodo (prav tam).

4.3 Republika Slovenija

Slovenija se je na grožnje informacijski varnosti v zadnjem času »privadila« in razvila določene mehanizme, s pomočjo katerih se bo zoperstavila vedno večjemu ogrožanju v informacijskem okolju. Kot takega lahko izpostavimo sprejetje Resolucije o strategiji nacionalne varnosti leta 2010, ki je že opredelila tudi informacijske oz. kibernetske grožnje kot dejavnike ogrožanja nacionalne varnosti Republike Slovenije (ReSNV-1).

V najinem delu se ukvarjava izključno z grožnjami, ki se dotikajo IKI, zatorej so izmed pomembnejših dokumentov, katere moramo spoznati, poleg ReSNV in Obrambne strategije tudi Zakon o tajnih podatkih (ZTP), Zakon o elektronskih komunikacijah, Kazenski zakonik, Uredba o varovanju tajnih podatkov in Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih ter Priporočila informacijske varnostne politike javne uprave. Predvsem pa je pri obravnavi tematike potrebno ločevati med tajnimi in javnimi podatki. V času pisanja najine naloge je Slovenija sprejela Strategijo kibernetske varnosti, zato bova vključila tudi slednjo.

4.3.1 Resolucija o strategiji nacionalne varnosti

ReSNV je najvišji normativni dokument, v katerem je zaslediti omembo informacijskih groženj oz. groženj informacijskim sistemom in infrastrukturi. Resolucija o strategiji nacionalne varnosti iz leta 2010 opredeljuje tudi informacijske oz. kibernetske grožnje kot dejavnike ogrožanja nacionalne varnosti Republike Slovenije in sicer kot nadnacionalne vire ogrožanja in tveganja nacionalni varnosti (ReSNV-1 2010). Že samo poimenovanje omenjenih groženj kaže na resnost groženj, saj zaradi svoje nadnacionalne narave tovrstni viri ogrožanja kažejo na težavno določljivost izvora ter njihovo pomembnost.

Slovenija je v Resoluciji o strategiji nacionalne varnosti (ReSNV-1 2010) opredelila vire tveganja nacionalni varnosti, kot so: terorizem, nedovoljene dejavnosti na področju konvencionalnega orožja, orožje za množično uničevanje in jedrske tehnologije, organiziran kriminal ter nezakonite migracije in tudi kibernetske grožnje. V dokumentu je zapisano: »Zaradi razvejanosti informacijskih in komunikacijskih sistemov, neomejenosti kibernetskega prostora in težav pri nadzoru nad tem prostorom, lahko tudi v Republiki Sloveniji pričakujemo širitev različnih oblik računalniške kriminalitete, zlasti kibernetskih vdorov in napadov državnih in nedržavnih subjektov, ki jih prostorsko in časovno ne bo mogoče omejiti« (ReSNV-1 2010 v Čalet in Rolih 2011, 11). Resolucija grožnje asimetrične narave prepoznava kot vse bolj verjetne, k bojiščem prihodnosti pa poleg kopnega, morja in zraka prišteva tudi kibernetski prostor. Kot odziv na kibernetske grožnje in zlorabo informacijskih

tehnologij in sistemov je v dokumentu zapisano: » Republika Slovenija bo na področju kibernetske varnosti izdelala nacionalno strategijo za odzivanje na kibernetske grožnje in zlorabo informacijskih tehnologij ter sprejela potrebne ukrepe za zagotovitev učinkovite kibernetske obrambe, v katero bosta v največji možni meri vključena javni in zasebni sektor. Ena od prioritetnih nalog na področju zagotavljanja kibernetske varnosti bo tudi ustanovitev nacionalnega koordinacijskega organa za kibernetsko varnost« (ReSNV-1 2010 v Čaleta in Rolih 2011, 11).

V tem delu je jasno zapisano, da se država podaja na pot javno-zasebnega partnerstva, ki ga je v praksi še potrebno udejaniti. To je pomembno predvsem pri načrtovanju zaščite IKI, kjer državne ustanove in organizacije ne morejo zagotavljati zaščite brez vključevanja zasebnega sektorja. V naših primerih je to najbolj očitno pri varovanju objektov s strani zasebnih varnostnih služb oz. uporabi protivirusnih idr. računalniških zaščitnih programov, ki jih razvijajo predvsem zasebne družbe.

Dejavnost zagotavljanja ukrepov za zaščito pred kibernetskimi grožnjami mora biti usklajena na vseh ravneh. Pri tem je pomembno, da vsi odgovorni delujejo uigrano, upoštevajo etična in zakonska določila, se ustrezno odzivajo na dogodke, spremljajo področje kibernetskih groženj ter se ustrezno prilagajajo spremembam. Za zaščito pred kibernetskimi grožnjami mora z ustreznimi zaščitnimi ukrepi najprej poskrbeti vsak posameznik sam, kot tudi podjetja ter civilne ali javne organizacije. Kadar govorimo o zaščiti kritične infrastrukture, ko je potrebno zaščititi nacionalni interes, pa se je potrebno problema lotiti bolj sistemsko (Rolih 2011, 21).

ReSNV ločuje informacijske in kibernetske vire ogrožanja, vendar v dokumentu samem ni nikjer obrazloženo, kaj so informacijski viri ogrožanja in kaj kibernetski. Poleg tega se ne osredotočajo na splošne vire ogrožanja omrežne varnosti. V nadaljevanju dokumenta je predstavljen načrt za odzivanje na kibernetske grožnje in zlorabo informacijskih tehnologij, v katerem je opredeljeno, da bo Republika Slovenija na področju kibernetske varnosti izdelala nacionalno strategijo za odzivanje na kibernetske grožnje in zlorabo informacijskih tehnologij ter sprejela potrebne ukrepe za zagotovitev učinkovite kibernetske obrambe, v katero bosta v največji možni meri vključena javni in zasebni sektor. Ena od prioritetnih nalog na področju zagotavljanja kibernetske varnosti bo tudi ustanovitev nacionalnega koordinacijskega organa za kibernetsko varnost. Med prioritetami zagotavljanja kibernetske varnosti je preprečevanje poveličevanja, opravičevanja in vzpodbujanja terorizma (ReSNV-1 2010, poglvje 5.3.5).

4.3.2 Obrambna strategija

Obrambna strategija je temeljni razvojno-usmerjevalni dokument države na obrambnem področju in izhaja iz Resolucije o strategiji nacionalne varnosti RS. Obrambna strategija govori o kompleksnem, dinamičnem, soodvisnem mednarodnem varnostnem okolju, ki je podvrženo nepredvidljivim spremembam in različnim sodobnim virom ogrožanja, ki imajo lahko globalne razsežnosti. Med drugim poudarja, da se je povečala ranljivost držav na asimetrične grožnje, praviloma zaradi nedržavnih subjektov, ki so po naravi kompleksni, soodvisni, spremenljivi in pogosto težko predvidljivi. Ti subjekti imajo multiplikativen značaj in zaradi čezmejnih učinkov lahko vplivajo na nastanek in intenzivnost drugih varnostnih groženj in tveganj.

Opisano dinamično spreminjanje mednarodnega varnostnega okolja od obrambnega sistema RS zahteva nenehno dejavnost ter ustrezno prilagodljivost in odzivnost (Obrambna strategija 2012, 1–2).

Obrambna strategija na podlagi Resolucije o strategiji nacionalne varnosti navaja poleg drugih groženj tudi kibernetske grožnje in zlorabo informacijskih tehnologij in sistemov ter ogrožanje kritične infrastrukture. Poudarja, da je za zagotavljanje ustrezne obrambne sposobnosti države potrebno razumeti naravo sodobnih varnostnih groženj in tveganj ter jih pravočasno prepoznati. Posledično bosta razvoj in transformacija obrambnih zmogljivosti usmerjena v njihovo prožnost, sposobnost za združevanje in souporabo, hitro prilagajanje nastalim razmeram ter doseganje ustrezne stopnje povezljivosti, uporabnosti in pripravljenosti (Obrambna strategija 2012, 3–4).

Razvoj organiziranosti, opremljenosti in usposobljenosti Slovenske vojske kot nosilke vojaške obrambe države bo usmerjen v pripravljenost in uporabnost njenih zmogljivosti tako ob konvencionalnih kot tudi asimetričnih in hibridnih oblikah bojnega delovanja (Obrambna strategija 2012, 4).

Skladno z nacionalno strategijo za odzivanje na kibernetske grožnje in zlorabo informacijskih tehnologij, se bodo tudi na obrambnem področju izvajali ukrepi za zagotovitev učinkovitih zmogljivosti kibernetske varnosti, pri čemer bo posebna pozornost namenjena celovitosti in usklajenosti ukrepov za zaščito informacijsko-komunikacijskih sistemov in druge takšne infrastrukture v državi (Obrambna strategija 2012, 5).

Obrambna strategija govori tudi o obrambnem načrtovanju, s pomočjo katerega naj bi se zagotavljalo izvajanje nacionalnih ukrepov za pripravljenost in Natovih ukrepov za odzivanje na krize ter ukrepov kriznega odzivanja EU. Obrambno načrtovanje zajema tudi materialno-zdravstveno oskrbo, izvajanje ukrepov zaščite kritične infrastrukture ter ocenjevanje virov ogrožanja in tveganja za nacionalno varnost, komunikacijsko-informacijsko podporo

obrambnemu sistemu ter druge zmogljivosti obrambnega sistema. Za informacijsko-komunikacijsko in drugo tehnično podporo pri izvajanju nalog kriznega upravljanja na obrambnem področju bo z ustrezno racionaliziranim in posodobljenim sistemom upravnih zvez ter povezavami z Natom in EU še naprej skrbel Nacionalni center za krizno upravljanje (NCKU) (Obrambna strategija 2012, 9–11).

Obseg infrastrukture na obrambnem področju Obrambna strategija prilagaja potrebam države. Selektivno se bodo opuščali infrastrukturni objekti na neperspektivnih lokacijah. Ohranili bodo le takšen obseg infrastrukture, ki bo zadosten za miroljubno obrambno zmogljivost države, za njene vojaške strateške rezerve in za izvajanje podpore države gostiteljice. Nepremičnine, ki imajo status objekta ali okoliša posebnega pomena za obrambo države, bodo dolgoročno ostale v upravljanju Ministrstva za obrambo (Obrambna strategija 2012, 13).

Razvoj komunikacijsko-informacijskih zmogljivosti na obrambnem področju bo omogočal varno izmenjavo informacij ter učinkovito odzivanje na sodobne vire ogrožanja in tveganja v kibernetskem prostoru. Komunikacijsko-informacijska infrastruktura bo omogočala učinkovito sodelovanje med vsemi subjekti obrambnega sistema, ter tudi sodelovanje obrambnega sistema z drugimi podsistemi nacionalno-varnostnega sistema RS in znotraj Nata (Obrambna strategija 2012, 14).

Nevojaški del obrambnega sistema, ki obsega naloge dosedanjega sistema civilne obrambe, bo sistemsko in vsebinsko preoblikovan v del sodobnega kriznega upravljanja na obrambnem področju. Pozornost bodo posvetili tudi nadgradnji infrastrukture, opreme in naprav za tehnično varovanje vojaških objektov, nadgradnji telekomunikacijskega in optičnega omrežja ter posodobitvi infrastrukture tega omrežja (Obrambna strategija 2012, 15–17).

4.3.3 Zakonodaja na področju informacijske varnosti v RS

Za razvoj varnosti informacijske infrastrukture in z njo povezane informacijske varnosti se pojavi problem, saj v Sloveniji ne obstaja noben zakon o informacijski varnosti, ki bi povezoval krovni dokument ReSNV v točkah o ogrožanju informacijske varnosti z dokumenti kot so Zakon o tajnih podatkih, Uredba o varovanju tajnih podatkov, Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih. SI–CERT ima na svojih spletnih straneh opisano, kateri zakoni se dotikajo informacijske varnosti navkljub pomanjkanju omenjenega zakona o informacijski varnosti. Zapisano imajo, da vidike omrežne in informacijske varnosti obravnavajo različni zakoni. Kazenski zakonik recimo opredeljuje kazniva dejanja (kot je recimo vdor v informacijski sistem), Zakon o elektronskih

komunikacijah definira dolžnosti operaterjev varnosti obramvnavanih komunikacij in tudi nadzor nad delom operaterjev, medtem ko Zakon o elektronskem poslovanju na trgu širše opredeljuje delovanje vseh ponudnikov storitev. Zakon o elektronskem poslovanju in elektronskem podpisu opredeljuje, kdaj so elektronsko podpisani dokumenti enakovredni ročno podpisanim pogodbam in vloge overiteljev (SI–CERT 2012). Pomembnejše točke teh zakonodajnih dokumentov bi lahko združili v zakon o informacijski varnosti, ki je v RS nujno potreben predvsem zaradi naraščanja uporabe informacijske tehnologije, naše vedno večje odvisnosti od nje, večanja števila varnostnih incidentov ter informatizacije poslovanja tako javne uprave kot gospodarskih družb in ostalih organizacij.

Zakon o tajnih podatkih v 5. členu določa za tajne tiste podatke, ki se nanašajo (med drugim tudi) na sisteme, naprave, projekte in načrte, pomembne za javno varnost, obrambo, zunanje zadeve ter obveščevalno in varnostno dejavnost državnih organov Republike Slovenije (ZTP – UPB2 2001, 5. člen). Vsi ostali podatki so po opredelitvah Zakona o tajnih podatkih lahko javni.

Podatki, ki se nanašajo na obrambne načrte in načrte zaščite v organizacijah posebnega pomena za obrambo države, so označeni vsaj s stopnjo tajnosti interno. S tem je preprečen vpogled v načrtovanje zaščite nepooblaščenim osebam. Tovrstno postopanje se nanaša tudi na občutljive in ključne sisteme IKI. Nanje se v delu nanaša tudi 38. člen zakona, v katerem je določena zahteva po varovanju komunikacij, po katerih se prenašajo tajni podatki. Naslednji, 39., člen sledi zahtevam iz prejšnjega in organom prepoveduje prenašanje tajnih podatkov po nezaščitenih komunikacijskih sredstvih (ZTP–UPB2 2001, 38. – 39. člen). Če povzamemo, iz zakona je razvidno, da sisteme IKI, ki skrbijo za varno hranjenje, prenašanje in prikazovanje tajnih podatkov v organizacijah posebnega pomena za obrambo države, lahko štejemo med vitalnejše infrastrukturne dele organizacije, ki jih je potrebno normativno-tehnično in fizično ustrezno zaščititi in varovati.

Na tem mestu je potrebno omeniti, da morajo organi javne uprave[20] slediti IVPJU, ki ima namen zaščititi informacijsko premoženje, ki ga upravlja. Je dokument, ki ga morajo upoštevati vodstvo, zaposleni, osebe pogodbenih izvajalcev in vsi, ki imajo dostop do tega premoženja. Z njim so postavljena osnovna varnostna izhodišča za zaščito informacijskih sredstev pred nevarnostmi, bodisi notranjimi ali zunanjimi, namernimi ali naključnimi. Izvajanje te politike je pomembno za zagotavljanje informacijske varnosti (povzeto po Priporočila informacijske varnostne politike javne uprave 2010, 1. – 2. člen). Velja

[20] To ne zadeva organizacij posebnega pomena za obrambo države, avtorja pa dajeva v razmislek, ali bi bilo smotrno vključiti in od njih zahtevati sledenje tem priporočilom.

pomemben poudarek, da se ta priporočila nanašajo zgolj na organe javne uprave, potrebno bi bilo razmisliti če in kako razširiti priporočila na organizacije posebnega pomena za obrambo države, ki si z organi javne uprave izmenjavajo občutljive podatke in informacije, ki niso javni.

Javni podatki so vsi drugi podatki, katere lahko vsak posameznik pridobi iz različnih virov. Organizacije posebnega pomena za obrambo države operirajo z vsemi vrstami podatkov, zavedati pa se moramo, da so lahko tudi javno dostopni podatki tudi tarča potencialnih napadalcev (npr. teroristov) in lahko preko njih pridobijo potrebne informacije. Kot primer navedimo spletno stran Luke Koper d.d., kjer lahko obiskovalec pridobi podatke o viziji, poslanstvu in kapacitetah koprskega pristanišča. To ima za vizijo postati osrednje pristanišče srednje in vzhodne Evrope. Ta informacija je poslovno ambiciozna, vendar je lahko varnostno sporna, saj je s tem pristanišče regionalno pomembna infrastruktura, katere motenje bi imelo ne samo lokalne (državne), pač pa regionalne posledice in bi zajelo skoraj tretjino celine.

Z namenom varovanja tajnih podatkov v IK sistemih je bila leta 2007 sprejeta Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, katere namen je, da zagotovi standardizacijo varovanja in zaščite tajnih podatkov v omenjenih sistemih. Obravnavani dokument[21] predstavlja trenutno najpomembnejši in najkonkretnejši normativni akt s področja načrtovanja zaščite v IKI. IK sistemi morajo pred začetkom delovanja pridobiti varnostno dovoljenje, katerega izda predstojnik organa ali organizacije ter o tem obvesti Urad Vlade Republike Slovenije za varovanje tajnih podatkov. Pred izdajo varnostnega dovoljenja mora predstojnik organizacije za tajne podatke stopnje tajnosti zaupno ali višje od Urada Vlade Republike Slovenije za varovanje tajnih podatkov pridobiti mnenje o varnostni ustreznosti sistema (povzeto po Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih 2007, 3. – 4. člen). Mnenje sicer ni obvezujoče in je svetovalne narave. Da zagotovimo pozitivno mnenje prej omenjenega Urada, moramo zagotoviti ključne sestavine sistema, ki so strežniki, usmerjevalniki in delilniki prometa, oprema za upravljanje in nadzor, aktivna oprema za prenos podatkov v nešifrirani obliki, oprema za šifrirno zaščito podatkov, varnostne pregrade, oprema za odkrivanje in zaščito pred vdori, oprema za izdelavo varnostnih kopij. IK sistemi morajo biti v prostorih, kjer je onemogočeno neželeno elektromagnetno sevanje, ki se nekontrolirano razširja in omogoča odtekanje predvsem tajnih podatkov. Za vzpostavitev čim višje stopnje zaščite IK sistemov in prostorov za obravnavo

[21] Poleg Priporočil informacijske varnostne politike javne uprave, ki pa zadeva samo organe javne uprave.

tajnih podatkov, je v uredbi zapisano razlikovanje med varnostnimi okolji, katere delimo na (Uredba o varovanju tajnih podatkov v informacijsko komunikacijskih sistemih 2007, 3. – 4. člen):

– širše varnostno okolje sistema (ŠVO) – je celotna okolica objekta, v katerem je nameščen sistem;

– ožje varnostno okolje sistema (OVO) – je objekt, v katerem je nameščen sistem;

– elektronsko varnostno okolje sistema (EVO) – je programska in strojna oprema sistema.

V postopku načrtovanja zaščite oz. pri izdaji varnostnega dovoljenja za delovanje sistema mora upravljavec pripraviti načrt varovanja sistema, oceno varnostnih tveganj in varnostna navodila za delo v sistemu tudi za primer nepredvidenih dogodkov. Omenjeni dokumenti se pregledujejo najmanj enkrat letno. IK sistemi lahko delujejo na tri varnostne načine[22]: neselektivno, selektivno in dvojno selektivno.

Vsaka organizacija določi osebo, odgovorno za izvajanje uredbe, upravljanje in nadzor nad ukrepi in postopki varovanja tajnih podatkov v sistemu (vodja informacijske varnosti) in ji podeli ustrezna pisna pooblastila. Za dislocirane enote organizacij se imenuje lokalnega vodjo informacijske varnosti. V kolikor pride do t. i. kritičnega informacijskega dogodka[23] je vodja informacijske varnosti oziroma predstojnik organa ali organizacije dolžan pisno obvestiti Urad Vlade Republike Slovenije za varovanje tajnih podatkov o kritičnem informacijskem dogodku ter o ukrepih, sprejetih za preprečitev posledic dogodka (Uredba o varovanju tajnih podatkov v informacijsko komunikacijskih sistemih 2007, 9. – 10. člen).

Sistem mora biti sposoben identifikacije in overovitve dostopa, za kar je odgovoren upravljavec sistema, načine pa določi komisija, ki je sestavljena iz predstavnikov Ministrstva za javno upravo, Ministrstva za notranje zadeve, Ministrstva za obrambo, Ministrstva za zunanje zadeve, Slovenske obveščevalno varnostne agencije in Urada Vlade Republike Slovenije za varovanje tajnih podatkov. Omenjena komisija je odgovorna za pripravljanje tehničnih in normativnih rešitev za varovanje tajnih podatkov v komunikacijskih in informacijskih sistemih (Uredba o varovanju tajnih podatkov v informacijsko komunikacijskih sistemih 2007, 15. člen).

[22] Več o tem v Uredbi o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih (Ur. l. št. 48/2007). Posplošeno gre za nadzor in način selekcioniranja dostopa do IK sistemov.

[23] Kritični informacijski varnostni dogodek je vsak dogodek, ki ima ali bi lahko imel za posledico nerazpoložljivost sistema ali njegovih ključnih sestavin, razkritje varovanih podatkov ali izgubo oziroma nezaželeno spremembo podatkov, uničenje ali izgubo opreme in sredstev (glej Uredba o varovanju tajnih podatkov v informacijsko komunikacijskih sistemih 2007, 3. člen).

Za selekcijo dostopa uporabnikov do tajnih podatkov mora biti vzpostavljena in vzdrževana varnostna shema[24]. Upravljavec je odgovoren za določitev načina nadzora in spremljanja pristopa v sistem in dostopa do tajnih podatkov.

Za prenašanje tajnih podatkov po IK sistemih zunaj varnostnih območij veljajo posebna pravila. Tajne podatke se po IK sistemih zunaj varnostnih območij prenaša le in izključno v šifrirani obliki[25]. Do izjem lahko pride v izrednih okoliščinah kot so (Uredba o varovanju tajnih podatkov v informacijsko komunikacijskih sistemih 2007, 14. člen):

– preteče ali dejanske krize, spopad ali vojne razmere ali
– kadar je hitrost dostave bistvenega pomena in pri tem niso na voljo sredstva in metode za šifrirno zaščito ter se ocenjuje, da je možnost zlorabe poslanih tajnih podatkov zelo majhna.

Takrat se lahko tajni podatki stopnje tajnosti interno, zaupno in tajno izjemoma prenašajo v nešifrirani obliki, kar mora dovoliti predstojnik organa oz. od njega pooblaščena oseba. Z uporabo pomnilnih medijev se tajni podatki zunaj varnostnih oz. upravnih območij prenašajo v šifrirani oz. nešifrirani obliki, zavarovani pa morajo biti v skladu z Uredbo o varovanju tajnih podatkov (v komunikacijsko informacijskih sistemih).

Ker v resničnem svetu zaradi različnih vzrokov in razlog prihaja do povezovanja sistemov, je njihovo povezovanje dovoljeno le po nadzorovanih in varovanih vstopno-izstopnih točkah skozi katere potem potekajo vsi servisi in storitve. Iluzorno je pričakovati, da organizacije posebnega pomena za obrambo države ne bi bile medsebojno povezane, saj gre v večini primerov za gospodarske družbe in zavode v službi ljudstva. S spletom je dovoljeno povezati sisteme, v katerih se obravnavajo tajni podatki do stopnje tajnosti največ interno. Te sisteme je potrebno zaščititi in zavarovati v skladu z varnostnimi zahtevami komisije.

Vse sestavine sistemov, kjer se obravnavajo tajni podatki stopnje tajnosti najmanj zaupno, morajo biti zaščiteni proti neželenemu elektromagnetnemu sevanju. To zaščito zagotavljajo upravljavci sistemov obravnave tajnih podatkov. Meritve proti neželenemu elektromagnetnemu sevanju opravljajo MORS, Policija, SOVA in drugi, s strani komisije pooblaščeni organi. Kakšne varnostne zahteve in standarde zaščite proti neželenemu elektromagnetnemu sevanju morajo sistemi dosegati določi komisija.

Uredba o obveznem organiziranju varovanja (UR. l. RS, št. 80/12 z dne 17. 10. 2012) opredeljuje, da morajo organizacije, ki jih s sklepom določi Vlada RS, organizirati službo

[24] Seznam uporabnikov sistema, iz katerega so za vsakega uporabnika sistema razvidni njegovi identifikacijski podatki in njegove pravice dostopa do posameznih tajnih podatkov (glej Uredba o varovanju tajnih podatkov v informacijsko komunikacijskih sistemih 2007, 12. člen).
[25] Šifrirne oblike oz. rešitve morajo biti potrjene s strani komisije.

varovanja na način kot ga določa Zakon o zasebnem varovanju in omenjena uredba. Vlada RS s sklepom določi organizacijo, ki mora varovanje organizirati. Evidenco organizacij z organiziranim varovanjem vodi Ministrstvo za notranje zadeve RS. Uredba v 3. odstavku 5. člena tudi določa, da mora zavezanec (beri organizacija, ki organizira varovanje) zagotoviti varovanje tudi ob naravnih in drugih nesrečah, v krizi, izrednem in vojnem stanju. Zavezanec sam poda predlog, katere elemente organizacije bi bilo potrebno varovati in kakšen način varovanja predlaga. Ta predlog vključuje tudi IKI. V 6. členu je tudi določeno, da mora zavezanec zagotoviti ustrezne prostore, opremo in materialno-tehnična sredstva, potrebna za organiziranje obveznega varovanja, razen če se z imetnikom licence pogodbeno ne dogovorita drugače. Natančneje Uredba o obveznem organiziranju varovanja določa način in obseg varovanja, vsebino programa varovanja, načrt varovanja, ocene stopnje tveganja in varnostne ukrepe na varovanem območju za subjekte navedene v Zakonu o zasebnem varovanju (69. člen) med katere spadajo subjekti (Zakon o zasebnem varovanju 2011, 69. člen)[26]:

- uporabljajo ali hranijo radioaktivne snovi, jedrska goriva, odpadke in druge ljudem in okolju nevarne snovi in naprave;
- upravljajo zmogljivosti, sisteme ali njihove dele, ki so bistveni za vzdrževanje ključnih družbenih funkcij, zdravja, varnosti, zaščite, gospodarske in družbene blaginje ljudi ter katerih okvara ali uničenje bi imela resne posledice na nacionalno varnost Republike Slovenije zaradi nezmožnosti vzdrževanja teh funkcij (promet, energija, telekomunikacije);
- hranijo arhivsko gradivo in predmete, ki predstavljajo kulturno dediščino;
- upravljajo javna letališča ali morska pristanišča za mednarodni javni promet ali izvajajo prevoze v mednarodnem letalskem in morskem prometu ali
- je iz posebnih varnostnih razlogov nujno potrebno.

Pri pregledovanju različnih virov sva naletela na zelo dober in podroben opis standarda ISO 27001 (v nadaljevanju standard), ki je temelj pri načrtovanju zaščite IK sistemov na mednarodni ravni. Povzemava ga s strani PerKlik.

Družbe na podlagi zahtev, ki so opredeljene v standardu ocenijo tveganje na različnih področjih informacijske varnosti (standard zajema 11 področij) in poskrbijo za sprejetje ustreznih varnostnih mehanizmov (povzeto po Perklik 2014).

Prvo področje, ki ga navaja standard je sprejetje splošnega akta o varnostni politiki, ki je krovni dokument za načrtovanje, vzpostavitev in vzdrževanje politike varovanja informacij v družbi. Akt opredeljuje cilje, področja uporabe in način organiziranja sistema za varovanje

[26] Uredba o obveznem organiziranju varovanja. Ur. l. RS št. 80/2012.

informacij. Pri tem je pomembno, da vodstvo ozavešča in izobražuje svoje delavce, namenja zadostna sredstva, redno spremlja veljavne predpise ter standarde in ustrezno prilagaja interne akte na področju varovanja informacij (prav tam).

Drugo področje bolj podrobno namenja pozornost organizaciji informacijske varnosti. Zaveza vodstva so na tem področju jasna navodila, konkretno opredeljene naloge, razpoložljivost sredstev, redni varnostni pregledi in sledenje sprejeti politiki. Vsak zaposleni mora skrbeti za varovanje informacij. Potrebna je tudi priprava ocene tveganja s predvidenimi ukrepi, s katerimi se poskuša ugotovljena tveganja zmanjšati na sprejemljivo raven (prav tam).

Tretje področje se bolj natančno ukvarja z upravljanjem sredstev. Potrebno je popisati vse informacijske vire družbe, določiti skrbnike virov ter poskrbeti za ustrezno klasifikacijo posameznih virov. Tako zaposleni kot zunanji izvajalci morajo skleniti dogovore o varovanju informacij (prav tam).

Četrto področje se nanaša na varnost človeških virov. Družba mora poskrbeti za zmanjšanje človeških napak, kraj, prevar, odtekanja informacij. Kadrovske službe morajo pred zaposlitvijo delavce preveriti. Ko se delavce zaposli jih je potrebno ustrezno usposabljati in zagotavljati redno obnavljanje pridobljenega znanja. Določiti je treba tudi pravice delavcev glede varovanja informacij v primeru premestitev oziroma prenehanja delovnega razmerja.

Peto področje se nanaša na ustrezno zunanje in notranje fizično varovanje. Družba mora omejiti dostop do prostorov, v katerih so nameščene ključne sestavine informacijsko komunikacijskega sistema družbe, zagotoviti varstvo pred požarom, strelo, vodo, skrb za uničenje odpadnega papirja in drugih nosilcev podatkov z občutljivo vsebino (prav tam).

Šesto področje pozornost namenja komunikacijskemu in informacijskemu upravljanju. Z namenom zmanjšanja možnosti nepooblaščenega spreminjanja in zlorabe informacij ali storitev, mora družba poskrbeti za ločevanje izvajanj nalog na ključnih gradnikih informacijskega sistema (razdelitev skrbništva na več skrbnikov).pomembno je tudi, kako se postopa pri upravljanju sprememb. Slednje morajo biti namreč odobrene s strani pooblaščenih oseb, vpisane v dnevnik o spremembah (prav tam).

Sedmo področje namenja pozornost kontroli dostopa. Definirati je potrebno različne skupine ljudi, z različnimi vrstami dostopnih pravic. Uvesti je treba politiko skrbnega ravnanja z gesli in politiko čiste mize, ki predpostavlja varno hrambo nosilcev informacij in skrb, da se nosilci ne puščajo na odprtih pisarniških površinah ali drugih mestih, kjer bi dostop do njih lahko imele nepooblaščene osebe (prav tam).

Osmo področje govori o pridobitvi informacijskega sistema, razvoju in vzdrževanju. Potrebno je zagotoviti ustrezne kontrole, ki zagotavljajo sledljivost razvoja in upravljanja sprememb informacijskih rešitev. Poskrbeti je potrebno tudi za kriptiran prenos občutljivih podatkov (prav tam).

Deveto področje se ukvarja z obvladovanjem incidentov. Vodstvo mora biti seznanjeno z vsemi varnostnimi vprašanji in dogodki. Najlažje se to izvede z izdelavo varnostnih poročil.

Predzadnje področje se nanaša na upravljanje neprekinjenega poslovanja, katerega cilj je zmanjšati tveganost poslovanja družbe v primeru izrednega dogodka večje razsežnosti ter poskrbeti za potrebe nadaljevanja poslovnih procesov bodisi v omejenem bodisi v polnem obsegu. Z načrtom neprekinjenega poslovanja morajo biti seznanjeni vsi zaposleni, morebitni zunanji izvajalci in najpomembnejši dobavitelji družbe (prav tam).

Zadnje področje se nanaša na normativno skladnost informacijske varnostne politike tako s slovensko ustavo kot tudi s sprejetimi zakonskimi in podzakonskimi akti, z ratificiranimi mednarodnimi pogodbami ter s primarno in sekundarno zakonodajo EU (prav tam).

4.3.4 Strategija kibernetske varnosti RS 2014

V letu 2014 je bil v javno razpravo poslan osnutek Strategije kibernetske varnosti. Generalni direktor direktorata za informacijsko družbo na ministrstvu za izobraževanje, znanost in šport Marjan Turk je kot ključne cilje Strategije navedel zagotavljanje varnosti državljanov, razvoj gospodarstva in družbe ter zanesljivo delovanje kritične infrastrukture. Vodja centa SI–CERT Gorazd Božič je poudaril tudi nujnost ustanovitve nacionalnega laboratorija za preiskovanje škodljive kode. Božič je navedel več primerov kibernetskih groženj, od škodljivih programskih kod, ki ciljajo na končne uporabnike spletnih storitev ali podjetja, do ranljivosti v internetni infrastrukturi. Na posvetu so pojasnili tudi, da so glavni cilj kibernetskih kriminalcev podatki, ki imajo tržno vrednost, saj napadalcem prinašajo finančno korist (MojMikro 2014).

Strategija med drugim jasneje opredeljuje kibernetsko varnost kot » //… zbirko orodij, politik, varnostnih konceptov, varnostnih zaščitnih ukrepov, smernic, pristopov za obvladovanje tveganja, dejavnosti, usposabljanj, najboljših praks ter zagotavljanja tehnologij, ki se lahko uporabljajo za zaščito kibernetskega okolja, organizacije in uporabniških sredstev. Organizacija in uporabniška sredstva obsegajo povezane računalniške naprave, osebje, infrastrukturo, aplikacije, storitve, telekomunikacijske sisteme in skupek poslanih in/ali shranjenih podatkov v kibernetskem okolju. Kibernetska varnost si prizadeva zagotoviti doseganje in vzdrževanje varnostnih lastnosti organizacije in uporabniških sredstev ter ju ščiti

pred varnostnimi tveganji v kibernetskem okolju. Splošni varnostni cilji zajemajo zagotavljanje razpoložljivosti, celovitosti in zaupnosti.« (Strategija kibernetske varnosti 2014). V strategiji je tudi začrtana smer razvoja načrtovanja sistema varnosti in zaščite informacijsko-komunikacijskih sistemov, od katerih so nekateri neločljivi del kritične informacijsko komunikacijske infrastrukture.

Kot je navedeno v dokumentu je vizija strategije vzpostavitev celovitega sistema zagotavljanja kibernetske varnosti, ki kot pomemben integralni dejavnik nacionalne varnosti zagotavlja odprt, varen in varovan kibernetski prostor ter s tem podporo ključnim funkcijam države, osnovo za konkurenčno gospodarstvo ter blaginjo posameznikov in celotne družbe. Slovenija mora vzpostaviti učinkovit in polno delujoč sistem za zagotavljanje kibernetske varnosti, ki bo tako preprečeval kot tudi odpravljal posledice varnostnih incidentov. Za dosego tega cilja Strategija in RS zasledujeta naslednje cilje, načela in principe: varnost državljanov, razvoj in gospodarstvo, zanesljivo delovanje kritične infrastrukture, zatiranje kibernetskega kriminala, obrambna sposobnost države, krepitev nacionalne kibernetske varnosti skozi mednarodno sodelovanje, vzpostavitev nacionalnega organa za kibernetsko varnost. Pri zasledovanju teh ciljev in načel bo RS to poskušala doseči s preprečevanjem, odzivanjem in ozaveščanjem, kar je jasno zapisano v osnutku Strategije. (Strategija kibernetske varnosti 2014).

5 OBRAMBNO NAČRTOVANJE

5.1 Načrtovanje zaščite v okviru obrambnega sistema

Sistem nacionalne varnosti je hierarhično najvišji sistemsko urejen ustroj, ki s svojim delovanje zagotavlja nacionalno varnost RS. Sestavljajo ga trije podsistemi: obrambni sistem, sistem notranje varnosti, sistem varstva pred naravnimi in drugimi nesrečami. Ravno obrambni sistem je najpomembnejši raziskovani subjekt, znotraj katerega poteka večini družbe neznani proces obrambnega načrtovanja oz. obrambnega planiranja. Za potrebe nadaljnjega raziskovanja je potrebno najprej razrešiti manjšo terminološko nejasnost ključnega strokovnega pojma – obrambno načrtovanje vs. obrambno planiranje, ki nas pripelje do termina načrtovanje zaščite.

Jernej Ržen je v magistrski nalogi iz leta 2013 z naslovom Vpliv vključenosti Republike Slovenije v sistem obrambnega planiranja Nata na razvoj zmogljivosti njenega obrambnega sistema lepo opredelil razlikovanje med omenjenima terminoma, zatorej avtorja te magistrske naloge nadaljujeva delo in v naslednjih odstavkih povzemava njegove ugotovitve.

Ugotovila sva, da se v povezavi z obrambnim načrtovanjem poleg termina »načrtovanje« predvsem v upravnem delu MO uporablja tudi termin »planiranje« (dolgoročno planiranje, srednjeročno planiranje, poslovno planiranje, planski cikel itd.). V strokovni literaturi, ki je nastajala izven MO, pa je moč zaslediti predvsem termin »obrambno načrtovanje« (Ržen 2013, 23).

Obrambno načrtovanje je miselno-predlagalni proces v obrambnem sektorju in je eden temeljnih elementov organiziranega obrambnega sistema. Naloga obrambnega načrtovanja je preprosto, da z razpoložljivimi viri dosežemo postavljene cilje. Obrambno načrtovanje lahko označimo tudi kot celoten proces od določitve nacionalnih interesov, varnostnega tveganja države in virov ogrožanja države do nalog obrambnega sistema, določitve potrebnih virov za njihovo doseganje in uresničitve postavljenih ciljev. Proces obrambnega načrtovanja je torej zelo kompleksen in zahteven in poteka na različnih ravneh in področjih ter v časovnih intervalih (Koštrun 2007, 16–17).

Ržen (2013, 25) trdi, da je načrtovanje proces določanja ciljev, iskanje različnih poti za uresničevanje teh ciljev, ocenjevanje ter posledično izbira primernih ciljev, ki se jih oblikuje v načrte, politike, programe in poslovne plane. Pri načrtovanju torej ni pomemben samo cilj ampak tudi sredstva, ki nam bodo pomagala uresničiti ta cilj. Načrtovanje je torej proces, ki nam pomaga pri uspešnem delovanju določenega (poslovnega) sistema, s pomočjo

zastavljenih aktivnosti, sredstev, metod, želenih rezultatov ter s pomočjo predhodnega določanja kriterijev za ocenjevanje rezultatov.

Obrambno načrtovanje v RS je v pristojnosti MORS in je usmerjeno v integracijo nacionalnega obrambnega načrtovanja s sistemom obrambnega načrtovanja v Natu in EU. Ureja ga Pravilnik o planiranju v MO. Obrambno načrtovanje temelji na ciklični izdelavi razvojnih planskih dokumentov, ki pokrivajo dolgoročno, srednjeročno in kratkoročno plansko obdobje. Sistem obrambnega planiranja je namenjen opredeljevanju dolgoročnih strateških ciljev MORS, njihovemu ovrednotenju z vidika obrambnih virov in prioritet v srednjeročnih programih, ter njihovemu izvrševanju preko dvoletnih poslovnih planov in finančnih načrtov (SOPR 2007–2012 2006, 37).

V Strateškem pregledu obrambe (2004 v Koštrun 2007, 17) je zapisano, da "//...obrambno načrtovanje predstavlja pomembno orodje države za oblikovanje potrebnih zmogljivosti obrambnega sistema oziroma obrambnih sil in za razvoj nacionalne obrambne infrastrukture. Obrambno načrtovanje je sestavni del procesa načrtovanja, s pomočjo katerega lahko vlada izvaja nadzor in koordinira načrtovanje, vzdrževanje in racionalno porabo obrambnih virov za razvoj nacionalnega obrambnega sistema."

"Proces obrambnega načrtovanja se prične z oblikovanjem ciljev varnosti na nacionalni ravni. Nacionalni cilji varnosti predstavljajo tudi usmeritve za oblikovanje takšnega obrambnega sistema, ki bo omogočil oblikovanje in vzpostavitev takšnih obrambnih sil, ki bodo sposobne dosegati zastavljene cilje. Proces mora imeti več povratnih oziroma kontrolnih poti" (Strateški pregled obrambe 2004 v Koštrun 2007, 17).

Sam proces obrambnega načrtovanja poteka v treh časovnih fazah. Kratkoročni načrt oz. kratkoročna faza zajema načrtovanje za obdobje enega ali dveh let. Vsebuje izdelavo načrtov za realizacijo izvedbenih nalog kakor tudi načrte za zagotovitev virov (materialnih, finančnih, kadrovskih) za realizacijo le-teh. Srednjeročna faza zajema načrtovanje za obdobje do šest let. Običajno srednjeročno obrambno načrtovanje obsega izdelavo načrtov za doseganje določenih zmogljivosti ter izdelavo načrtov za zagotovitev virov za doseganje teh zmogljivosti. Dolgoročna faza pa zajema proces proučevanja možnega delovanja v operativnem okolju v bodočnosti. Obsega načrtovanje za obdobje desetih do tridesetih let (Koštrun 2004, 18).

V kolikor pa orišemo širše zgodovinsko in vsebinsko ozadje izpostavljene dileme ugotovimo, da so na MO pred letom 2003 termin »defence planning« prevajali kot »obrambno načrtovanje«, vendar je zaradi določenih posebnosti obrambnega sistema RS kmalu prišlo do zmede oz. mešanja pojmov. Eden izmed elementov v okviru obrambnega

sistema RS je (bila) namreč tudi civilna obramba[27], znotraj katere je bilo že pred nastankom samostojne države RS uveljavljeno obrambno načrtovanje, ki ga z vsebinskega vidika ne moremo primerjati z dolgoročnim, srednjeročnim in kratkoročnim načrtovanjem vojaških in nevojaških zmogljivosti obrambnega sistema[28] (Ržen 2013, 24).

Z namenom boljše preglednosti med omenjenima področjema načrtovanja je bila tako v prvem letu polnopravnega članstva v NATU sprejeta odločitev, da se bo v povezavi z obrambnim načrtovanjem v Natu ter dolgoročnim, srednjeročnim in kratkoročnim načrtovanjem vojaških in nevojaških zmogljivosti obrambnega sistema na nacionalni ravni uporabljal termin »planiranje«. Pri tem je potrebno opozoriti, da je tudi v prihodnje smiselno vztrajati pri »obrambnem planiranju«, ker se je ta termin že uveljavil tako v strateških usmerjevalnih dokumentih kot tudi v notranjih normativno-pravnih aktih (Ržen 2013, 24).

Razlikujemo dve osnovni obliki obrambnega planiranja, predikativno in reaktivno. Pri predikativnem planiranju se skuša vnaprej predvideti grožnje in se nanje sistematično pripraviti s pravočasno določitvijo ustreznih obrambnih virov, kar storijo pristojni državni organi skupaj z vojaškimi oblastmi. Pri reaktivnem planiranju država in oborožene sile vzdržujejo status quo, dokler država ni neposredno ogrožena ali vključena v krizo večjih razsežnosti. Slednje se dogaja iz različnih razlogov, bodisi zaradi podcenjevanja nevarnosti za nastanek kriznih razmer, zaradi podcenjevanja možnih nasprotnikov, bodisi zaradi napačne presoje razmer (Žabkar v Ržen 2013, 27).

Obrambno planiranje preoblikuje obrambno politiko v obrambni koncept ter obseg in strukturo obrambnih sil. Predstavlja tudi pomembno orodje države za oblikovanje potrebnih zmogljivosti obrambnega sistema ter za razvoj nacionalne obrambne infrastrukture. S

[27] »Civilna obramba je namenjena delovanju v izrednem in vojnem stanju ter ob krizah in združuje ukrepe ter dejavnosti državnih organov, organov lokalne samouprave, gospodarskih družb, zavodov in drugih organizacij ter državljanov, s pomočjo katerih se z nevojaškimi sredstvi in načini podpira ter dopolnjuje vojaška obramba države in se zagotavljajo delovanje oblasti v vojni, preskrba, zaščita in preživetje prebivalstva« (Frankovič in Najzer 2004 v Ržen 2013, 23).

[28] Za razliko od dolgoročnih, srednjeročnih in kratkoročnih obrambnih planov, ki določajo in usmerjajo razvoj vojaških in nevojaških zmogljivosti obrambnega sistema, obrambni načrt obsega organizacijske, kadrovske, materialne in druge rešitve, s katerimi se zagotavlja postopen, organiziran ter usklajen prehod na delovanje v izrednem in vojnem stanju, načrtuje opravljanje določenih nalog oziroma proizvodnje in storitev med mobilizacijo in v vojnem stanju ter določa organizacijo in način dela, tako da se zagotovi neprekinjeno opravljanje dejavnosti organa oziroma organizacije. Obrambni načrti vsebujejo tudi rešitve za krizna obdobja (Frankovič in Najzer 2004 v Ržen 2013, 24).

pomočjo obrambnega planiranja lahko vlada izvaja nadzor in koordinira načrtovanje, vzdrževanje in racionalno porabo obrambnih virov, ki so potrebni za razvoj nacionalnega obrambnega sistema. Gre za multidisciplinaren, večplasten in dolgotrajen planski proces v katerem sodeluje veliko število akterjev (Strateški pogled obrambe 2004, 19).

Načrtovanje obrambe je ena od najbolj kompleksnih funkcij vlade, saj mora upoštevati in oceniti mednarodno varnostno okolje, prepoznati grožnje in priložnosti ter upoštevati razvoj tehnologije in zmogljivosti, ki so na razpolago. V razmislek je potrebno zajeti tudi zgodovinsko in kulturno ozadje države (Shekhawat 2006, 689).

Planerji in strategi morajo pri planiranju predvideti morebitne spremembe znotraj države, spremembe v mednarodnem okolju ter tehnološke spremembe in to za precej dolgo obdobje (do 30 let), pri čemer ne morejo biti prepričani, v katero smer se bodo razvijali dejavniki, ki vplivajo na planiranje. Slednje nakazuje na to, da je učinkovito obrambno planiranje odvisno od kakovosti predvidevanja. Obrambno planiranje je po koncu hladne vojne postalo še bolj kompleksno kot v preteklosti, saj so se začele pojavljati nove grožnje varnosti kjer so nosilci tudi nedržavni subjekti (Žabkar v Ržen 2013, 29–31).

Načrtovanje obrambe mora potekati v okviru nacionalnih ciljev, ki so zastavljeni za obdobje več desetletij, čeprav niso javno izraženi . Realistično načrtovanje obrambe zahteva temeljito in podrobno analizo in evalvacijo varnostnega okolja, zaznave groženj, tehnološke ocene itd. in bi se moralo odražati v enotnem obrambnem načrtu. Tak načrt bi moral biti povezan z nacionalnimi zmogljivostmi v javnem sektorju in vključevati izkoriščanje virov kot so cestni promet, civilno letalstvo ter tehnično delovno silo in biti že vnaprej določen (Shekhawat 2006, 692–693).

Mišmaš (2014, 17–24) navaja 6 faz obrambnega planiranja. Kot prvo fazo navaja oblikovanje strateških dokumentov in sicer po potrebi, kadar prihaja do večjih sprememb varnostnega okolja ali spremenjenih prioritet razvoja obrambnega sistema. Na nacionalni ravni so to naslednji dokumenti: ReSNV, Strateški pregled obrambe in Obrambna strategija. Na nadnacionalni ravni so dokumenti naslednji: Strateški koncept Nata, Celostne politične usmeritve Nata, Ministrske usmeritve Nata, Evropska varnostna strategija.

Druga faza predvideva ocenjevanje varnostnega okolja. Zaradi tendence stalnega spreminjanja varnostnega okolja mora biti stalno tudi napovedovanje potencialnih groženj varnosti, tveganj in priložnosti za državo. Ocenjevanje varnostnega okolja mora zajemati mednarodno politično okolje, vojaško okolje, tehnološki razvoj, gospodarske razmere, družbeno in naravno okolje. Ocena se navezuje tudi na oceno varnostnega okolja mednarodnih organizacij, kot sta NATO in EU (Mišmaš 2014, 19).

Tretja faza je faza dolgoročnega planiranja za obdobje 12 ali več let. Ključni dokument na tem področju je Dolgoročni obrambni plan (ReSDPRO), ki je splošen usmerjevalni dokument, ki se pripravlja oz. dopolnjuje vsaka 4 leta, sprejema ga Državni zbor RS. Obstoječi ReSDPRO (2000, 2001, 2004) so dokaj podrobni in so imeli vlogo obrambnih programov, ko ti še niso obstajali (Mišmaš 2014, 20).

Četrta faza je faza srednjeročnega planiranja oz. programiranje. Ključni dokument na tem področju je Srednjeročni obrambni program (SOPR), ki je najpomembnejši planski dokument, saj povezuje dolgoročne plane s kratkoročnimi (proračun), razporeja obrambne kadrovske, finančne in tehnološke vire ter določa prioritete razvoja obrambnega sistema. Dokument predstavlja vez med nacionalnim in NATO/EU planiranjem. Izdeluje se vsake 2 leti, sprejema ga Vlada RS (Mišmaš 2014, 21–22).

Peta faza zajema kratkoročno planiranje (poslovno planiranje), ki vključuje dokument, ki se imenuje Poslovni plan in razdeljuje srednjeročne cilje v kratkoročnem obdobju. Izdeluje se vsako leto, za obdobje 2 let in je sestavljen iz plana vodenja in letnega programa dela, kjer gre za kratkoročne cilje iz načrta virov (finančni načrt, načrt delovnih mest, načrt nabav in gradenj, načrt razvojnih programov, itd.) ter iz načrta implementacije ciljev sil NATA. (Mišmaš 2014, 23).

Zadnja šesta faza vključuje vrednotenje in poročanje in omogoča spremljanje izvajanja sprejetih planov razvoja obrambnega sistema. V tej fazi se oblikujejo različna poročila (Mišmaš 2014, 24).

Kot že omenjeno ima na obrambno planiranje vpliv tudi hiter razvoj različnih tehnologij, predvsem informacijsko-komunikacijskih. Slednje je na področje obrambnega planiranja vneslo nove metode, kot sta simuliranje in modeliranje, ki omogočajo testiranje učinkovitosti različnih elementov v izbranih scenarijih, kar odločevalcem pomaga pridobiti podlago za primerne odločitve (Niemeyer v Ržen 2013, 32).

Na področju načrtovanja obrambe se vedno pojavlja tudi vprašanje glede transparentnosti na eni strani in zaupnosti obrambnih načrtov na drugi strani. Vsekakor je zaupnost pri obrambnih naročilih pomembna predvsem zaradi varnosti, pogajanj glede cene in konkurenčnosti med prodajalci. Zagotovo pa mora obstajati notranja transparentnost v procesih naročanja, pri formulaciji predlogov, obdelavi le teh, pri priporočilih na različnih ravneh ter pri finančnih in političnih odločitvah (Shekhawat 2006, 702).

Učinkovito obrambno planiranje omogoča uspešno transformacijo obrambnega sistema zaradi zagotavljanja povezljivosti med strateškimi (političnimi) dokumenti in usmeritvami ter planskimi (operativnimi/izvršilnimi) dokumenti, zaradi zagotavljanja učinkovite in racionalne

rabe (omejenih) obrambnih virov (kadrovskih, finančnih, tehnoloških), zaradi zagotavljanja povezljivosti z obrambnim planiranjem mednarodnih organizacij ter zaradi zagotavljanja transparentnosti (nacionalnih) planov razvoja obrambnega sistema (Mišmaš 2014, 26).

5.2 Obrambno planiranje in načrtovanje zaščite

V prejšnjem poglavju sva avtorja natančno razložila uporabo termina obrambno planiranje, ki ga nikakor ne smemo zamenjevati s terminom obrambno načrtovanje, znotraj katerega se je razvil koncept civilne obrambe že pred vstopom RS v zvezo NATO. Frankovič in Najzer (2004 v Ržen 2013, 23) trdita, da je //…civilna obramba namenjena delovanju v izrednem in vojnem stanju ter ob krizah in združuje ukrepe ter dejavnosti državnih organov, organov lokalne samouprave, gospodarskih družb, zavodov in drugih organizacij ter državljanov, s pomočjo katerih se z nevojaškimi sredstvi in načini podpira ter dopolnjuje vojaška obramba države in se zagotavljajo delovanje oblasti v vojni, preskrba, zaščita in preživetje prebivalstva."

V kolikor podrobno premislimo lahko obrambno načrtovanje tesno povežemo z opredeljevanjem nacionalnovarnostnih ciljev (in interesov), ki se odražajo tudi v ščitenju, zaščiti in (za)varovanju omenjenih organizacij posebnega pomena za obrambno države. Temu primerno lahko sklepamo, da obrambno načrtovanje obsega tudi načrtovanje zaščite organizacij, njihove infrastrukture in osebja, s tem pa dejavnosti, ki je tako posebnega pomena za obrambo države. Vse to se odrazi bodisi v obrambnih načrtih bodisi v internih načrtih zaščite v posamezni organizaciji. Kljub vsemu je termin obramba primeren bolj za opisovanje tradicionalne grožnje kot je vojna, ki preti družbi in njenemu blagostanju na nacionalni ravni ali širše ter preti z uničenjem. Termin zaščita pa je vezan na ožje področje načrtovanja predvsem posameznih sistemov na interni ravni in pred manj ogrožujočimi grožnjami oz. pred naravnimi in drugimi nesrečami.

5.3 Obrambni načrti

Obrambni načrti so temeljni akti, ki izhajajo iz koncepta civilne obrambe ter določajo konkretne usmeritve načrtovanja obrambe in zaščite RS s strani vladnih idr. služb ter organizacij posebnega pomena za obrambo države. V RS sta pomembnejša dva dokumenta s tega področja in sicer Uredba o obrambnih načrtih in Uredba o določitvi obrambnih potreb. Dokumenta obsegata tudi načrtovanje obrambe in zaščite IKI v organizacijah posebnega pomena za obrambo države.

Izdelavo obrambnih načrtov ureja Uredba o obrambnih načrtih (Ur. l .RS št. 11/2004) v kateri so določeni nosilci, postopek in podlage za izdelavo, vsebina obrambnih načrtov in naloge upraviteljev obrambnih načrtov. V vsaki organizaciji posebnega pomena za obrambo države je določen vsaj en upravitelj obrambnih načrtov.

1. odstavek 2. člena te uredbe določa, da je obrambni načrt celota organizacijskih, kadrovskih, materialnih in drugih rešitev, s katerimi se zagotavlja postopen, organiziran in usklajen prehod na delovanje v izrednem in vojnem stanju, načrtuje opravljanje določenih nalog oziroma proizvodnje in storitev v času izvajanja mobilizacije in v vojnem stanju ter določa organizacijo in način dela, tako da se zagotovi nepretrgano opravljanje dejavnosti organa oziroma organizacije. Obrambni načrti morajo biti izdelani tako, da omogočajo uporabo načrtovanih rešitev tudi ob krizah (Uredba o obrambnih načrtih 2004, 2. člen). Oba avtorja naloge v tem členu razumeva tudi zagotavljanje zaščite lastne IKI organizacij posebnega pomena za obrambo države, ki je tako vitalna/ključna za opravljanje njihovih dejavnosti.

V 3. členu te uredbe (1. odstavek) je določeno, da obrambne načrte izdelujejo Vlada Republike Slovenije, ministrstva, Banka Slovenije, gospodarske družbe, zavodi in druge organizacije, katerih dejavnost je po odločitvi vlade posebnega pomena za obrambo, Generalni sekretariat Vlade Republike Slovenije, Urad Vlade Republike Slovenije za informiranje, Slovenska obveščevalno varnostna agencija, Služba Vlade Republike Slovenije za zakonodajo in Center Vlade Republike Slovenije za informatiko, upravne enote, občine in pokrajine ter gospodarske družbe, zavodi in druge organizacije, s katerimi je sklenjena pogodba za opravljanje proizvodnje in storitev v vojnem stanju (Uredba o obrambnih načrtih 2004, 3. člen). Zanimivost, ki se pojavi v dokumentu je, da je Banka Slovenije določena kot organizacija, ki mora izdelovati obrambne načrte, ni je pa zaslediti na seznamu organizacij, katerih dejavnost je posebnega pomena za obrambo države.

1. odstavek 7. člena uredbe določa, da se v obrambnih načrtih gospodarskih družb, zavodov in drugih organizacij, katerih dejavnost je po odločitvi vlade posebnega pomena za obrambo, načrtuje (Uredba o obrambnih načrtih 2004, 7. člen):

- priprave za izvajanje določenih ukrepov za pripravljenost:
- mobilizacija:
- opravljanje dejavnosti iz njihove pristojnosti.

V 29. členu te uredbe je določeno, da so za določitev surovin, proizvodov in storitev, ki jih je potrebno zagotavljati v vojnem, izrednem in kriznem stanju; in za načrtovanje opravljanja dejavnosti oz. načrtovanje potrebnih organizacijskih, materialno tehničnih in drugih rešitev za

opravljanje proizvodnje in storitev, odgovorne organizacije posebnega pomena za obrambo države in tudi pristojna[29] ministrstva.

Vlada RS (na predlog ministrstev) je pristojna za določanje gospodarskih in drugih objektov ter naprav, za katere se načrtuje začasna onesposobitev v vojni (38. člen; Ur. l .RS št. 11/2004). Ti objekti in naprave lahko obsegajo tudi IKI v organizacijah posebnega pomena za obrambo države.

5.4 Načrtovanje zaščite

Načrtovanje zaščite se v različnih organizacijah izvaja različno in tudi ne obstaja enotna opredelitev, kaj naj bi načrtovanje zaščite pomenilo in obsegalo. Pri načrtovanju zaščite gre za miselni proces in aktivno sprejemanje ukrepov, ki povišujejo stopnjo zaščite sistemov in se izvaja na nižji ravni od obrambnega načrtovanja. Pri načrtovanju zaščite prav tako ne gre zgolj za vojaški oz. obrambni vidik, pač pa lahko zajema tudi različne krizne situacije od naravnih nesreč, kemičnih, radioloških, bioloških, jedrskih nesreč do terorističnih napadov. Vse našteto se vse bolj odraža tudi pri obrambnem načrtovanju, predvsem zaradi spreminjanja tradicionalnih nalog vojaških organizacij, ki niso več zgolj bojne. V našem primeru bomo govorili o načrtovanju zaščite, zajeli bomo tako vojaške kot nevojaške vire ogrožanja in preučili načrtovanje zaščite na obeh stopnjah ter jo aplicirali na obravnavana podjetja in organizacije.

Zakon o obrambi v poglavju o obrambnih ukrepih v podpoglavju o obrambnih potrebah v 28. členu govori o prostorskih aktih in infrastrukturnih objektih. Državni, občinski ali skupni prostorski akti morajo biti medsebojno usklajeni, v njih pa se mora upoštevati obrambne potrebe. Te se mora upoštevati pri projektiranju in gradnji železniških prog in objektov na njih, državnih cest in objektov na njih, mednarodnih letališč ter telekomunikacijskih in energetskih povezav. Naju zanimajo predvsem slednje, saj predstavljajo osrednjo temo naloge.

Člen 29 je že bil omenjen in je pomemben, zaradi področij gospodarske dejavnosti, ki jih v zvezi z obrambnimi ukrepi omenja. V nalogi preučujeva omenjene dejavnosti, znotraj teh pa naju zanima IKI. Za boljšo predstavo naredimo matrični prikaz povezanosti Sklepa z ZObr, ki se sicer ne nanaša neposredno na sektorje KI, ampak je najboljši približek oblikovanja sektorjev v letu 1994.

[29] Ministrstva, pristojna za gospodarstvo, okolje, prostor in energijo, promet, kmetijstvo, gozdarstvo in prehrano zunanje zadeve, gospodarstvo, energijo, informacijsko družbo ter zdravje, po potrebi pa tudi druga ministrstva.

Tabela 5.1: Povezanost Sklepa (1996) in ZObr (1994)

Organizacije posebnega pomena za obrambo države	Energetsko pomemben objekt (p.o.)	Telekomunikacijsko p. o.	Proizvodno p.o.	Transportno p.o.	Drugi p.o.
Aerodrom Ljubljana d.d.				X	
Eles - Elektro Slovenija d.o.o.	X				
Univerzitetni klinični center Ljubljana					X
Luka Koper d.d.				X	
Petrol d.d.	X		X		
Pošta Slovenije d.o.o.					X
Radiotelevizija Slovenija		X			
Slovenske železnice d.o.o.				X	
Telekom Slovenije d.d.		X			
Zavod RS za blagovne rezerve	X		X		X
Zavod RS za transfuzijsko medicino					X

V tabeli je 9 organizacij, katerim sva lahko nedvoumno določila področje pomembne dejavnosti in objektov, katere imajo v lasti. Med temi je 1 energetsko pomembna organizacija (Eles d.o.o.), 2 sta telekomunikacijsko pomembni organizaciji (RTV in Telekom Slovenije d.d.), nobena ni samo proizvodno pomembna organizacija, 3 so transportno pomembne organizacije (Aerodrom Ljubljana d.d., Luka Koper d.d., Slovenske železnice d.o.o.) in 3 organizacije so drugače pomembne (UKC Ljubljana, Pošta Slovenije d.o.o., Zavod RS za transfuzijsko medicino). 2 organizaciji izstopata, saj sta pomembni na več področjih in jih ne moremo uvrstiti samo pod eno samo. To sta Petrol d.d. in Zavod RS za blagovne rezerve.

Zakon o varstvu pred naravnimi in drugimi nesrečami posebej ne opredeljuje obrambnega načrtovanja, pač pa govori o izdelavah načrtov (npr. evakuacije) in izdelavah ocen ogroženosti, ki je lahko del obrambnega načrtovanja. Gospodarske družbe, zavodi in druge organizacije posebnega pomena za obrambo države so se dolžne ravnati po usmeritvah omenjenega zakona. Zakon predvideva sprejetje nacionalnega programa varstva pred naravnimi in drugimi nesrečami. To se je odrazilo v sprejetju Resolucije o nacionalnem

programu varstva pred naravnimi in drugimi nesrečami leta 2009. Slednja se v 4. točki Razvoj opazovalnih, informacijskih, komunikacijskih, logističnih in drugih sistemov za potrebe zaščite, reševanja in posredno nanaša tudi na organizacije posebnega pomena za obrambo države, predvsem pri vključevanju v sistem spremljanja, obveščanja in alarmiranja pred omenjenimi nesrečami. Kot večji deli IKI za potrebe zaščite in reševanja se omenjajo GIS UJME, TETRA in ZARE.

Zakon o varstvu pred naravnimi in drugimi nesrečami dopolnjuje uredba o vsebini in izdelavi načrtov zaščite in reševanja, kjer je v 6. členu zapisano, da morajo načrte zaščite in reševanja izdelati organizacije, ki (Uredba o vsebini in izdelavi načrtov zaščite in reševanja 2012, 6. člen):

– v delovnem procesu uporabljajo, proizvajajo, prevažajo ali skladiščijo nevarne snovi, nafto in njene derivate ter energetske pline ali opravljajo dejavnost oziroma upravljajo sredstva za delo, ki pomenijo nevarnost za nastanek nesreče; za nesreče, ki jih lahko povzročijo s svojo dejavnostjo,

– upravljajo velike infrastrukturne in druge sisteme; za nesreče, ki jih lahko povzročijo zaradi motenj v delovanju ali zaradi opustitve dejavnosti.

V dodatku te uredbe so podana merila za določitev organizacij. V dodatku veljajo merila za (Uredba o vsebini in izdelavi načrtov zaščite in reševanja 2012, Dodatek):[30]:

- Organizacije, ki v delovnem procesu uporabljajo, proizvajajo, skladiščijo nevarne (tudi jedrske) snovi;
- Organizacije, ki izvajajo energetsko dejavnost in imajo najmanj 3000 odjemnih mest;
- Organizacije, ki upravljajo sistem za oskrbo s pitno vodo z najmanj 3000 odjemnimi mesti;
- Organizacije, ki upravljajo sredstva za delo, ki pomenijo nevarnost za nastanek nesreče, kadar gre za nasipe in druge objekte za zadrževanje ali zbiranje vode, če količina zadržane ali skladiščene vode presega 5 milijonov m^3;
- Organizacije, ki opravljajo ali upravljajo površinske (kopenske ali morske) prevoze, pri katerih je zmogljivost posameznega prevoznega sredstva večja od 100 potnikov; pristanišča z več kot 10 privezi za ladje; mednarodna letališča;
- Organizacije s področja ravnanja z nevarnimi odpadki;
- Organizacije, ki v gospodarske namene izkoriščajo mineralne surovine v rudarskih objektih pod zemljo;

[30] Naveden je le del meril, pomemben za dotično nalogo. Več si preberite v Uredbi o vsebini in izdelavi načrtov zaščite in reševanja U.l. RS 3/2002.

- Organizacije, ki upravljajo cevovode za pretok nafte, naftnih derivatov, zemeljskega plina s premerom 300 mm in več;
- Organizacije, za katere je bila izvedena presoja vplivov na okolje, če iz poročila o vplivih na okolje za to presojo izhaja, da poseg pomeni posebno tveganje in nevarnost z nastanek ekoloških in drugih nesreč.

Nosilec načrtovanja (v tem primeru organizacija) je dolžan določiti skrbnika načrta. Načrt zaščite in reševanja obsega načrt in dodatke ter priloge k načrtu. Natančneje to pomeni da se z načrtom opredelijo (Uredba o vsebini in izdelavi načrtov zaščite in reševanja 2012, 8. člen):
– nesreča, za katero je izdelan načrt,
– obseg načrtovanja,
– koncept zaščite, reševanja in pomoči ob nesreči, za katero je izdelan načrt,
– potrebne sile in sredstva ter razpoložljivi viri,
– organizacija in izvedba opazovanja, obveščanja in alarmiranja,
– aktiviranje sil in sredstev,
– upravljanje in vodenje,
– ukrepi in naloge zaščite, reševanja in pomoči,
– osebna in vzajemna zaščita,
– razlaga pojmov in okrajšav.
Dodatki in priloge k načrtu so:
– načrti dejavnosti izvajalcev načrta zaščite in reševanja,
– zbirke podatkov, potrebnih za izvajanje načrta,
– program usposabljanja, urjenja in vaj,
– navodilo za vzdrževanje in razdelitev načrta zaščite in reševanja.

Načrt zaščite in reševanja ob vojaškem napadu na državo vsebuje poleg vsebin iz drugega in prejšnjega odstavka, tudi dokumente za izvajanje ukrepov za pripravljenost, če je tako določeno s predpisi o obrambnem načrtovanju. Iz te uredbe je torej vidna razlika med obrambnim načrtovanjem in načrtovanjem zaščite. Obrambno načrtovanje se še vedno izvaja na višjem nivoju, kljub temu se večinoma nanaša na vojaške grožnje varnosti, med katere včasih lahko štejemo tudi teroristične grožnje. Posebnost terorističnih groženj je predvsem v odzivanju državnih obrambno-varnostnih organov nanje. Potrebno je natančno določiti kdo je pristojen za odzivanje nanje. Določanje organov za odzivanje na različne tipe groženj je temeljna naloga načrtovanja zaščite.

6 ŠTUDIJA PRIMERA – NAČRTOVANJE ZAŠČITE IKI V IZBRANIH ORGANIZACIJAH

Poglavje pred vami je umeščeno v sklop empiričnega dela naloge, kjer sva avtorja sodelovala pri izvajanju anketiranja odgovornih oseb za načrtovanje zaščite v organizacijah posebnega pomena za obrambo države. Poleg tega je poglavje skupek dela obeh avtorjev, kjer sva odgovore analizirala ter skupaj tolmačila ugotovitve.

To poglavje obravnava tematiko navedeno v naslovu magistrskega dela, kjer gre predvsem za ugotavljanje pripravljenosti sistemske ravni na zagotavljanje zaščite informacijsko-komunikacijske infrastrukture v omenjenih organizacijah. Za načrtovanje zaščite v omenjenih organizacijah je nedvomno pomembno poznavanje vseh področij preučevanja v povezavi s kritično infrastrukturo. Pomembno je tudi poznavanje IKT sektorja, ki je le eden izmed sektorjev, čeprav ga lahko včasih opredelimo kot prvega med enakimi, saj je večkrat ključen za delovanje kateregakoli sektorja.

Ob začetku raziskave v letu 2012 je bilo v RS opredeljenih 11 podjetij posebnega pomena za obrambo države. Skozi čas in raziskave je bilo ugotovljeno, da je v letu 2014 prišlo na področju organizacij, katerih dejavnost je posebnega pomena za obrambo države, do premika pri sistemskih odločevalcih, ki so se zavedli pomena prenove spiska teh organizacij, ki nespremenjene vztrajajo na njem že slabih dvajset let. V tem času je prišlo do rasti pomena nekaterih organizacij in upadanja drugih, zato je bil seznam potreben prenove. Seznam je v letu 2014 doživel osvežitev, kar je tudi ena od ugotovitev raziskave.

V najini študiji primera se posvečava preučevanju načrtovanja zaščite informacijsko-komunikacijske infrastrukture v organizacijah posebnega pomena za obrambo države v luči naraščajočega pomena koncepta kritične infrastrukture, o kateri se zavedanje krepi tudi v RS.

V sledečem poglavju si bralci lahko preberejo, kako so te organizacije pripravljene na nove vidike varnostnih ogrožanj IKI, kako jo dojemajo ter kakšno videnje in predloge imajo glede sistemskega načrtovanja zaščite IKI v njihovih organizacijah. Metoda za preučevanje je prirejena zaradi slabšega odziva na sodelovanje pri organizacijah. Ta manjko sva raziskovalca nadomestila s poglobljeno analizo področja preučevanja pred in pri pripravi vprašalnikov, saj je bilo pričakovati neodzivnost nekaterih subjektov in težji dostop do anketirancev za izvedbo poglobljenega strukturiranega intervjuja. Slednje lahko podkrepiva z dejstvom, da nama je v pripravi na pisanje magistrske naloge uspelo vzpostaviti osebni stik samo z odgovornimi za

varnost v Petrol d.d. in v Luki Koper d.d. Na najino prošnjo izpolnjevanja ankete pa so se odzvali v Eles d.d., UKCLj, Telekom Slovenije d.d. ter MORS in MNZ.

S prvim anketnim vprašalnikom sva ciljala na vse organizacije v Sklepu in na MORS, MNZ RS, SV, Policija, SOVA, OVS, Sintal. Odgovore sva dobila samo od petih subjektov navedenih zgoraj.

Število prispelih odgovorov tudi podpira najino odločitev, da za izvedbo ankete izbereva oblikovanje ankete po vzoru strukturiranega intervjuja in pošiljanje po e-pošti ter je ne oblikujeva na portalu npr. 1-ka, zaradi majhnega vzorca in specifičnih vprašanj, iz katerih težje izluščimo odvisne in neodvisne spremenljivke za analizo. Ta je narejena na podlagi predhodnega raziskovanja področja načrtovanja zaščite IKI v omenjenih organizacijah v RS.

6.1 Oblikovanje seznama podjetij, zavodov in drugih organizacij, katerih dejavnost je posebnega pomena za obrambo države

Gospodarske družbe, zavodi in organizacije, katerih dejavnost je posebnega pomena za obrambo države, so določene na podlagi več različnih kriterijev. Po točno kakšnih kriterijih so bile dodane na seznam leta 1996, nama med vsemi opravljenimi razgovori ni uspelo ugotoviti. Gospod Roland Žel[31] je med razgovorom poudaril le, da je bil glavni kriterij določanja organizacij ključnost dejavnosti za zagotavljanje obrambne sposobnosti države, ki jo zagotavljajo omenjene organizacije. Prepričana sva, da bi bilo potrebno ugotoviti na podlagi katerih kriterijev so bile te organizacije določene. Kljub temu, da niso znani kriteriji, po katerih so bile omenjene organizacije dodane v omenjeni Sklep, je jasno, da jih lahko obravnavamo skozi teorijo oz. opredelitve o kritični infrastrukturi. Vse organizacije oz. njihova infrastruktura in dejavnost namreč izpolnjujejo vse opisne kriterije ključnosti, ki so v opredelitvi določeni kot pogoj kritične infrastrukture.

Kriteriji za določanje kritičnosti infrastruktur so različni, vsem pa je skupna ključnost, vitalnost in kritičnost delovanja v časih kriz oziroma vojn. Poleg teh treh dejavnikov omenimo še medsebojno povezanost in (so)odvisnost delovanja infrastruktur. Problem se pojavlja, ko govorimo o kritičnosti (ključnosti, vitalnosti) predvsem zaradi subjektivnosti procesa določanja nečesa kot ključnega/kritičnega. Zato lahko v toku razvoja znanosti pričakujemo tako spremembe opredelitev kritične infrastrukture kot tudi dodajanje, izvzemanje, spreminjanje kriterijev za določanje kritičnosti. Avtorji zaključnega poročila Definicija in zaščita kritične infrastrukture Republike Slovenije (2008, 10) poudarjajo, da so

[31] V času razgovora decembra 2011 je sogovornik opravljal funkcijo direktorja Direktorata za obrambne zadeve na MORS.

za določanje kritičnosti nujni pogoji kot npr. nujnost za delovanje sodobnih družb, ranljivost, kritičnost storitev (dejavnosti) za nacionalno varnost, motenje ima resne posledice za javnost, nujnost elementov za družbene zmogljivosti. Direktiva Sveta (ES) o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite kot pogoje kritičnosti določa: vzdrževanje ključnih družbenih funkcij, zdravja, varnosti, zaščite, gospodarske in družbene blaginje ljudi, katerih okvara ali uničenje bi imelo v državi članici resne posledice zaradi nezmožnosti vzdrževanja teh funkcij (Direktiva Sveta (ES) št. 114/2008, 2. člen).

Omenjeni kriteriji so dobri opisni kriteriji, ki na splošno opredelijo pomen določanja kritične infrastrukture, vendar je problem v tem, da so preveč posredni in točno ne določajo oprijemljivih kriterijev, preko katerih bi bila vidna odvisnost družbe, države, gospodarstva idr. Za določitev kriterijev bi bilo potrebno oblikovati npr. matrike z določenimi kriteriji odvisnosti in s (številsko) opredeljeno stopnjo odvisnosti teh kriterijev. To je predvsem zahtevna naloga, katera se je v času pisanja magistrske naloge na MORS bližala koncu[32], čeprav mogoče ne na način predstavljen zgoraj.

Opozarjava, da to ni edini način obravnave, na kar sva bila opozorjena tudi s strani MORS, saj organizacij posebnega pomena za obrambo in njihove infrastrukture ne moremo vedno obravnavati kot kritične (Čarni 2014).

Zavedati se je potrebno, da so bile organizacije uvrščene v Sklep, zaradi obrambnih potreb po zagotavljanju opravljanja njihove primarne dejavnosti, kar samo potrjuje zgoraj napisano. Torej so v ospredju prevladovali vojaški viri ogrožanja, medtem, ko se nevojaškim Vlada RS ni toliko posvečala. Sklepamo lahko, da se je izhajalo iz potreb zagotavljanja delovanja vojaških organizacij in osnovnih funkcij delovanja države. Usmeritev za določitev organizacij v Sklepu podaja že Zakon o obrambi (ZObr–UPB1) iz leta 1994, kjer je v 4. odstavku 29. člena določeno, da »…se v načrtih uporabe vojske lahko določijo pomembni energetski, transportni, proizvodni, telekomunikacijski in drugi podobni objekti ter sedeži organov oblasti na ravni države, kot objekti, pomembni za obrambo države.« (ZObr–UPB1). Iz tega sledi, da je lahko bilo tudi na podlagi zakona v letu 1996 določenih 11 organizacij posebnega pomena za obrambo države, saj zadostijo prav vsem pogojem iz omenjenega člena. Po drugi strani so iz Sklepa razvidni naslednji kriteriji: dejavnost, vojaški pomen[33], lastništvo (večinsko državno), gospodarski pomen, družbeni pomen in zemljepisna umestitev.

[32] Julija 2014 (natančneje 11. 7. 2014) je MORS sprejelo dokument Veljavni kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji (MORS 2014b).
[33] Tako za potrebe obrambe kot tudi potencialno vreden cilj nasprotnika.

V času pisanja magistrske naloge v aprilu 2014 je prišlo do revizije Sklepa VRS o določitvi gospodarskih družb, zavodov in drugih organizacij, katerih dejavnost je posebnega pomena za obrambo v RS, št. 80101-1/2014/5, z dne 17. 4. 2014. VRS je na novo določila status posebnega pomena za obrambo v RS trem subjektom, enemu subjektu pa je dosedanji status posebnega pomena odvzela.

Predvsem je pomembno to, da je bilo oblikovanje seznama teh organizacij v pristojnosti ministrstev in sicer na podlagi naslednjih izhodišč. Izhodišče za pripravo seznama teh pomembnih organizacij je Uredba o obrambnem načrtovanju (Ur. L. RS, št. 51/13), kjer so omenjene gospodarske družbe, zavodi in druge organizacije, katerih dejavnost je posebnega pomena za obrambo države. Ta določa, da je potrebno predvideti naloge in aktivnosti, ki so potrebne za zagotovitev povečanih obrambnih zmogljivost, ki jih bodo morale izvesti gospodarske družbe, zavodi in druge organizacije iz pristojnosti posameznih ministrstev. O potrebi po povečanih obrambnih aktivnostih govorimo tudi kadar je potrebno uveljavljati ukrepe kriznega odzivanja za zagotovitev delovanja obrambnega sistema RS v kriznih razmerah, ki pa so raznolike. Vodilo za določanje organizacije posebnega pomena za obrambo države je bilo, da ministrstva izhajajo iz vidika izvajanja nalog na področju obrambnega načrtovanja, priprav za izvajanje ukrepov za pripravljenost, priprav za zagotovitev obrambnih zmogljivosti ter zagotavljanje pogojev za delovanje celotnega obrambnega sistema (Čarni 2014).

Poseben status nekaterih podjetij, zavodov in drugih organizacij je še zapuščina sistema splošne ljudske obrambe in družbene samozaščite, ki je bil pomemben predvsem v prejšnjem družbenopolitičnem sistemu. Takrat so organizacijam naložili več (družbene) odgovornosti pri načrtovanju in pripravi načrtov za potrebe obrambe.

Oblikovanje seznama organizacij, katerih dejavnost je posebnega pomena za obrambo države, je torej plod pobude predvsem odločevalcev v obrambnem sistemu, natančneje dandanes MORS, ki določi izhodišča in poda usmeritve, na podlagi katerih naj za obrambno načrtovanje pristojna ministrstva preučijo primernost organizacij za uvrstitev na seznam.

Posledica tega je, da je Sklep VRS, ki določa te organizacije t. i. živa stvar in jo je potrebno osveževati, zaradi nenehno spreminjajočega se varnostnega okolja ter napredka tudi informacijskih tehnologij, ki vedno bolj prodirajo v družbo. Tako je npr. Pošta Slovenije izpadla iz prvotno preučevanega seznama, ker je bilo ocenjeno, da so naloge, ki so ji bile naložene doslej, glede na določila Uredbe o obrambnem načrtovanju in spremenjeno obrambno načrtovanje take narave, da zanje ni potrebe izdelovati obrambnega načrta v miru. Njena dejavnost se bo z vidika izvajanja nalog na področju obrambnega načrtovanja ter

zagotavljanja pogojev za delovanje celotnega obrambnega sistema ponovno proučila ob izrazitem poslabšanju varnostnih razmer (Čarni 2014).

Na seznamu so ostala vse energetsko in IK pomembne organizacije, ne le to, prišlo je do razširitve seznama, vse v luči spremembe varnostnega okolja in prilagoditve le temu. Na spremenjeno varnostno okolje in pomen IKI se pripravljajo tudi v organizacijah posebnega pomena za obrambo države, a te oz. anketiranci večinoma[34] ne pojmujejo IKT (sektorja)[35] kot najbolj ključnega, pač pa je to energetika. Izjemno zanimivo je, da je pomen energetike v zadnjih letih močno v porastu, celo bolj kot pomen razvoja IKT. Res pa je, da je delovanje IKI tudi odvisno od delovanja in zagotavljanja konstantne energije. To preprosto pomeni, da morajo organizacije primarno poskrbeti za oskrbo z energijo, kar bo zagotavljalo delovanje IKI oz. IKT. Zdrava kmečka pamet in zavedanje o dogodkih okoli nas nam pove, da je potreba po energiji v sodobni družbi izjemna, in šele ko zagotovimo varnost oz. zaščito preskrbe z energijo se lahko posvetimo načrtovanju zaščite same IKI, ki zagotavlja nemoteno opravljanje dejavnosti v organizacijah.

Problem pa se obrne v obliki spirale nazaj od IKI do energetike, saj dandanes večinoma sistemi IKI skrbijo za nemoteno oskrbo z energijo preko različnih računalniških sistemov in je zato načrtovanje zaščite IKI izjemno pomembno. Slednja trditev je lastna trditev in prepričanje avtorjev, s čimer se ne strinjajo v Eles-u, kjer trdijo, da delovanje njihove organizacije ni odvisno od IKT v tolikšni meri, da bi bilo delo oz. opravljanje dejavnosti zelo oteženo, v primeru njenega ogrožanja. Z različnim pojmovanjem pomena energetike in IKT tako prihajamo do diskurza o pomembnosti preskrbe z energijo oz. zagotavljanje delovanja IKI.

6.2 Viri ogrožanja IKI v organizacijah, katerih dejavnost je posebnega pomena za obrambo države

Spekter možnih virov ogrožanja IKI je izjemno širok in odvisen od dojemanja organizacij, katerih dejavnost je posebnega pomena za obrambo države. V raziskavi je bilo identificiranih več virov ogrožanja. Tako so grožnje IKI lahko vdor v IT sisteme in terorizem, organiziran kriminal in kibernetske grožnje, požari, naravne nesreče, izredne razmere, vojne, ki sicer posredno prizadanejo tudi IK sisteme (Cestnik 2013; Preradović 2013; Sektor za načrtovanje

[34] S trditvijo se ne strinjajo na MNZ, kjer trdijo, da lahko nedelovanje enega (katerega koli – op. a.) izmed navedenih sektorjev v dani situaciji močno ogrozi nacionalno varnost RS, zato je način prioritetnega sklepanja ogroženosti v tem kontekstu neumesten.

[35] Glede na pred kratkim sprejeto delitev sektorjev KI v RS je pravilno poimenovanje tega sektorja sektor kritične infrastrukture, ki zagotavlja informacijsko in komunikacijsko podporo.

MORS 2013; Služba za varnostno načrtovanje 2013). Ugotovljeno je bilo, da je dojemanje groženj v organizacijah posebnega pomena za obrambo države seveda različno in je predvsem odvisno od dejavnosti, s katero se te organizacije posebnega pomena za obrambo države ukvarjajo. Zanimivo pa je, da anketiranci v organizacijah, katerih dejavnost je tako posebnega pomena za obrambo države ne prepoznajo notranjih groženj v obliki izdajalcev notranjih informacij oz. "insiderjev", ki so lahko v določenih primerih veliko varnostno tveganje.

Z identifikacijo groženj tem organizacijam je načrtovanje zaščite IKI torej v različnih organizacijah usmerjeno v različne vire ogrožanja IKI. Razlogi ogrožanja IKI v organizacijah, katerih dejavnost je posebnega pomena za obrambo države, so (ponovno) povsem odvisni od dejavnosti, s katero se ukvarja organizacija. Spričo tega lahko kot možne razloge ogrožanja IKI v org. naštejemo globalizacijo in z njo povezana geopolitiko ter škoda v RS, ki bi nastala kot posledica uničenja telekomunikacijske infrastrukture; vdore v osebne podatke posameznikov, strank in zaposlenih, prekinitev delovanja informacijskega sistema; neposredno ogrožanje posamičnih sistemov, večje izpade energetskega sistema zaradi različnih dejavnikov (Cestnik 2014; Preradović 2013; Čarni in Palčič 2014).

Organizacije največ pozornosti posvečajo grožnjam varnosti IK sistemov na svojem področju delovanja oz. dejavnosti. Kot grožnje in varnostna vprašanja, katerim se organizacije najbolj posvečajo se izpostavljajo varnost IKT in telekomunikacijskega omrežja; varnost oz. nepooblaščen dostop do informacijskega sistema, ki ga uporabljajo v organizaciji za redno delo; vdori v informacijske sisteme preko spleta, nenamerne zlorabe, varovanje pred kibernetskimi vdori, varovanje pred zlonamerno programsko opremo. Kot pomembne grožnje IKI omenimo tudi organiziran kriminal in IK vohunjenje ter terorizem (Cestnik 2013; Cestnik 2014; Preradović 2013; Loborec 2013; Sektor za načrtovanje MORS 2013; Služba za varnostno načrtovanje 2013; Čarni in Palčič 2014).

Ob tem je potrebno omeniti, da Resolucija o strategiji nacionalne varnosti RS omenja nadnacionalne grožnje na področju proučevanja, ob tem so na MORS potrdili, da se na nivoju NATA zaznava tudi te omenjene grožnje, v RS pa so grožnje IKI omejene predvsem na krajo individualne lastnine in poslovnih podatkov (Sektor za načrtovanje MORS 2013; Čarni in Palčič 2014). S posvečanjem pozornosti preventivnemu delovanju in načrtovanju zaščite IKI lahko organizacije zagotovijo nemoteno delovanje IKI.

Prej obravnavane motnje težje uvrščamo v tradicionalne grožnje, kot je npr. vojna, in se zdijo omenjenim organizacijam pomembne, lahko jih uvrstimo med sodobnejše (kibernetske) grožnje, ki niso nič manj pomembne. Kot najverjetnejše in najpomembnejše lahko omenimo vseprisotne naravne in druge nesreče. Ker dandanes naravne in druge nesreče ter kibernetske

grožnje predstavljajo največjo nevarnost organizacijam posebnega pomena za obrambo države (njihovi IKI), bi jih pri načrtovanju zaščite IKI morali obravnavati prednostno. Poleg tega nikakor ne smemo zanemariti, da je vojna še vedno relativno izjemno pomembna grožnja organizacijam in njihovi IKI, predvsem zaradi nestabilnega varnostnega okolja[36] (Cestnik 2014; Čarni in Palčič 2014).

Predvsem zaradi nepredvidljivosti varnostnega okolja in skritih interesov ter z namenom zagotavljanja varnosti zaupnih podatkov v IK sistemih, se je potrebno povprašati tudi o njihovi robustnosti (sposobnosti preživetja) in zanesljivosti[37]. Splošno prepričanje državnih akterjev je tako, da je IKI v primerih različnih kriz ali huje vojn dovolj robustna in zanesljiva, da brez težav preživi vse najpogostejše krize in tudi vojno in da pri tem ni moteno zagotavljanje dejavnosti omenjene organizacije (Cestnik 2014; Čarni in Palčič 2014).

Medtem ko imajo sistemski odločevalci visoko mnenje o robustnosti/zanesljivosti IKI v organizacijah posebnega pomena za obrambo države, pa so po drugi strani v organizacijah, katerih dejavnost je posebnega pomena za obrambo države, mnenja, da je IKI sicer dovolj robustna (ocena 4), a je manj zanesljiva (ocena 2) v primerih kriz oz. vojn. Slednje dojemanje oz. dvomi v zanesljivost sistema zaščite IKI v organizacijah posebnega pomena za obrambo države je povsem razumljivo predvsem iz stališča nepredvidljivosti, izjemno hitrega poteka in totalnosti sodobnih kriz ali vojn, ki ne prizanašajo praktično nikomur (Cestnik 2014; Čarni in Palčič 2014).

Ostaja dejstvo, ki je bilo ugotovljeno skozi raziskavo, da se največ pozornosti pri načrtovanju zaščite posveča kibernetskim grožnjam IKI, kot najverjetnejše pa se pojavljajo tradicionalne grožnje v obliki naravnih nesreč (tudi zaradi pogostosti naravnih nesreč v zadnjih letih). Naravne nesreče predstavljajo do sedaj resnejše grožnje tudi zaradi obsega škode, ki finančno izjemno obremeni družbo in razne proračune, zato je pomembno, da so sistemi IKI zanesljivi in robustni.

Z ogrožanjem izvajanja dejavnosti organizacij posebnega pomena za obrambo države je neposredno povezana tudi povzročena škoda v organizaciji sami, gospodarstvu RS in slovenski družbi, ki je na splošno ocenjena srednja do visoka. MORS kot sistemski odločevalec gleda na problematiko seveda celovito, z upoštevanjem vpliva nedelovanja IKI vseh organizacij posebnega pomena za obrambo države. Zato tudi ocenjuje škodo kot visoko,

[36] Čeprav ne nujno v RS ali njeni bližnji okolici.
[37] Pri povpraševanju o robustnosti in zanesljivosti IKI je bilo ponujenih 5 stopenj na lestvici, pri čemer 1 pomeni najmanj robustno/zanesljivo IKI, 5 pa najbolj robustno/zanesljivo IKI.

saj so nekatere organizacije posebnega pomena za obrambo države tudi paradni konji slovenskega gospodarstva (Čarni in Palčič 2014).

Po drugi strani je UKCLj kot največja zdravstvena ustanova nedvomno pomemben člen zagotavljanja javnega zdravja prebivalcev, ki tvorijo delovno silo v državi. V kolikor zaradi zdravstvenih razlogov in nezagotavljanja zdravstvenih storitev izpade velik del izobražene delovne sile iz procesa dela, se to nedvomno pozna tudi na gospodarstvu in gospodarski učinkovitosti RS. Dojemanje pomena delovanja IKI v organizacijah posebnega pomena za obrambo države pa je pomembno predvsem za družbo kot celoto, saj le vzdržne in zanesljive storitve teh organizacij prinašajo učinkovito, delovno in zadovoljno družbo. Zato je vpliv ogroženosti IKI v organizacijah posebnega pomena za obrambo države na neposredno škodo v družbi srednje do visoke stopnje. V kolikor gledamo organizacije posebnega pomena za obrambo države kot celoto, bi bil vpliv nedelovanja njihove IKI in s tem vpliv na zagotavljanje dejavnosti in neposredna škoda v družbi srednja (Cestnik 2014).

6.3 Sistemske rešitve načrtovanja zaščite IKI v omenjenih organizacijah

Na ravni sistemske ureditve zaščite IKI v organizacijah, katerih dejavnost je posebnega pomena za obrambo države, je še dosti manevrskega prostora, saj zaščita IKI v omenjenih organizacijah oz. nasploh sistemsko še sploh ni ali pa je pomanjkljivo urejena. Največkrat je v omenjenih organizacijah opaziti, da so se slednje lotile oblikovanja lastnih načinov zaščite svoje IKI, kot je npr. potreba po omejitvi dostopa do osebnih podatkov (Cestnik 2013; Cestnik 2014; Preradović 2013; Loborec 2013).

V luči preventive in kurative vzrokov in posledic groženj varnosti IKI v organizacijah posebnega pomena za obrambo države je potrebno vključevanje raznih nacionalno-varnostnih idr. (npr. zaščita in reševanje) akterjev v različnih stopnjah ogroženosti (nizka, srednja, visoka). Za pojave (večino) nizke stopnje ogroženosti je odgovorno MNZ in organ v sestavi – Policija in to predvsem na področju organiziranega kriminala in terorizma. Potrebno je opozoriti tudi na dejstvo, da se navedeni akterji ne omejujejo na zaščito IKI zgolj organizacij posebnega pomena za obrambo države (Služba za varnostno načrtovanje 2013).

Za primerjavo dojemanja odgovornosti različnih akterjev zagotavljanja zaščite in varnosti IKI ob različnih vrstah ogrožanja v nadaljevanju podajava primerjalni tabeli. Pri njuni obravnavi ugotovimo popolnoma različno dojemanje nalog in odgovornosti na eni strani organizacij posebnega pomena za obrambo države in MORS na drugi strani. To kaže predvsem na nejasnosti zakonodajne ureditve, ki premalo natančno določi odgovornost in pristojnosti v primeru različnih stopenj ogrožanja IKI.

Tabela 6.1:Vključevanje akterjev za zaščito IKI - odgovor MORS

	STOPNJA OGROŽENOSTI IKI ORG. POSEBNEGA POMENA ZA OBRAMBO DRŽAVE		
GROŽNJE IKI	NIZKA	SREDNJA	VISOKA[38]
Zlonamerna koda	Policija, SI-CERT		
Teroristični idr. napad-fizični	Policija		
Organiziran kriminal	Policija		
Ribarjenje-phishing	Policija, SI-CERT		
Virusi	Policija, SI-CERT		
Kraja identitete	Policija		
Naravne idr. nesreče	URSZR, Civilna zaščita		
Gospodarsko idr. vohunjenje	Policija		
Notranji izdajalci informacij	Policija, OVS[39]		
Kibernetski napad na IKI	Policija, SI-CERT		
Nenamerne človeške napake	?		

Vir: Čarni in Palčič (2014)

[38] Pojasnitev nevključevanja MORS v primeru visoke stopnje ogroženosti na strani 97.
[39] Pojasnitev vključevanja OVS na strani 97–98.

Tabela 6.2: Vključevanje akterjev za zaščito IKI - odgovor UKCLj

	STOPNJA OGROŽENOSTI IKI ORG. POSEBNEGA POMENA ZA OBRAMBO DRŽAVE		
GROŽNJE IKI	NIZKA	SREDNJA	VISOKA
Zlonamerna koda	interno	interno	policija
Teroristični idr. napad-fizični	policija	policija	policija
Organiziran kriminal	policija	policija	policija
Ribarjenje-phishing	interno	interno	interno
Virusi	interno	interno	SI-CERT
Kraja identitete	interno	interno	SI-CERT[40]
Naravne idr. nesreče	interno	gasilci	URSZR, Civilna zaščita
Gospodarsko idr. vohunjenje	interno	policija	SOVA
Notranji izdajalci informacij	interno	policija	policija
Kibernetski napad na IKI	interno	policija	SI-CERT
Nenamerne človeške napake	interno	interno	interno

Vir: Cestnik (2013)

Najprej v oči pade vključevanje akterjev za zaščito IKI v organizacijah posebnega pomena za obrambo države kot ga vidijo na MORS. Akterji se v zaščito IKI vključujejo zgolj v nizki stopnji ogroženosti. Zanimivo je, da v primerih srednje ali visoke ogroženosti na nacionalni ravni ne bi imeli določenih akterjev za zaščito IKI. Sklepava lahko, da so na MORS napak tolmačili vprašanje in se večinoma osredotočili na obrambni sistem in ne toliko na organizacije, katerih dejavnost je posebnega pomena za obrambo države. Po podrobni preučitvi nama je ga. Alenka Čarni (2014) odgovorila, da je v tebeli izpolnjena rubrika pod nizko stopnjo ogroženosti, ker je kot taka zaznana iz strani MORS. Trdi tudi, da potencialnih napadov v tem obdobju ni bilo zaznanih. V zvezi s tem je še potrdila, da "...gospodarske družbe, zavodi in druge org., katerih dejavnost je posebnega pomena za obrambo so nosilci obrambnega načrtovanja, imajo dokumente s tajni podatki s področja obrambe, imajo aplikacijo ISPO kot del informacijsko komunikacijskega sistema NCKU, … V postopku pridobitve dovoljenja za dostop do tajnih podatkov odgovorne osebe za obrambo načrtovanje preverja OVS, ki se tudi odziva v primerih notranjih izdajalcev – išče vzroke za njihova dejanja. " (Čarni 2014). S tem tudi razrešimo vključevanje obveščevalno-varnostne službe MORS v zaščito IKI. Namreč, vključevanje obveščevalno varnostne službe (OVS) MORS v

[40] Pojasnitev vključevanja SI–CERT na strani 98.

zaščito organizacij, katerih dejavnost je posebnega pomena za obrambo države je lahko varnostno sporno, saj naj bi omenjena OVS delovala zgolj znotraj obrambnega sistema, kamor pa v mirnodobnem času nikakor ne sodijo organizacije, katerih dejavnost je posebnega pomena za obrambo države. Vsak sum organiziranega kriminala, terorističnih dejanj ali kibernetskega napada idr. bi OVS moral predati pristojnim ustanovam. S tem tudi razrešimo dilemo vključevanja akterjev v zaščito ob srednji ali visoki stopnji ogroženosti IKI, ko gre za obravnavo varnostnih incidentov ob katerih so ogroženi tudi tajni podatki višjih stopenj tajnosti in jih razrešujejo službe obrambnega sistema. Slednja problematika se bo brž kot ne razrešila z vzpostavitvijo MORS.Cert-a, ki bo deloval v okviru obrambnega sistema, za preostali del nacionalno-varnostnega sistema in javne uprave pa bosta zadolžena Gov.Cert in SI–CERT . Vsi trije bodo delovali pod okriljem Nacionalnega organa za kibernetsko varnost (Strategija kibernetske varnosti 2014).

V primerih odgovornosti varovanja oz. zaščite, ki jo izvajajo zasebne varnostne službe v organizacijah posebnega pomena za obrambo države, so omenjene varnostne službe odgovorne zgolj za fizično in tehnično varovanje prostorov, kjer se IKI nahaja. Zaščita računalniških oz. digitalnih omrežij ni v domeni varnostnih služb in jo izvajajo notranje strokovne službe organizacij posebnega pomena za obrambo države ali drugi pogodbeni partnerji (Cestnik 2014).

V tabeli opazimo veliko vlogo SI–CERT, predvsem v visoki stopnji ogroženosti. Na tem področju je RS naredila določen korak naprej z objavo Zakona o elektronskih komunikacijah, kjer je pomembno sedmo poglavje, ki se nanaša na varnost omrežij in storitev ter delovanje v izjemnih stanjih. V tem poglavju (79. do 87. člen) so najpodrobneje opisani tehnični in organizacijski ukrepi zaščite IKI, načrtovanje zaščite IK sistemov in infrastrukture ter izdelava varnostnega načrta IKI z odgovornimi osebami (ZEKom–1). Ta zakon trenutno predstavlja enega najnaprednejših zakonov, ki upošteva naraščajoč pomen IKT ter vključuje, opredeljuje in opisuje postopke, tehnične in organizacijske rešitve načrtovanja zaščite IKI. S tega vidika je izjemno pomemben normativni akt, ki ga zaradi narave dela in razširjenosti IKT v zagotavljanje dejavnosti, morajo slediti organizacije, katerih dejavnost je posebnega pomena za obrambo države.

In glede na to, da na področju zaščite IKI obstaja javno-zasebno partnerstvo samo do določene mere, lahko sklepamo o velikem pomenu IKI za delovanje organizacij, katerih dejavnost je posebnega pomena za obrambo države. Slednje imajo občutek, da obstaja srednja

do velika odvisnost[41] njihove organizacije od delovanja IKI. Po drugi strani pri sistemskih odločevalcih ostaja prepričanje, da ne obstaja nikakršna odvisnost delovanja IKI od nemotenega delovanja organizacij posebnega pomena za obrambo države. Nasprotnega mnenja so v organizacijah posebnega pomena za obrambo države, kjer trdijo, da v tem primeru prav tako obstaja velika odvisnost. Sklepamo lahko, da v primeru vdora v njihove sisteme lahko pride do uhajanja osebnih podatkov, ki imajo lahko neposreden vpliv na varnost uporabnikov IKT (Cestnik 2014; Čarni in Palčič 2014).

Za zagotavljanje inf. storitev, infrastrukture in/ali omrežja se v gospodarskih družbah, zavodih in drugih organizacijah posebnega pomena za obrambo države organizirajo različne službe in sektorji: Sektor za storitve, Sektor za dostopovna omrežja, Sektor za konvergentno jedrno omrežje, Sektor za informatiko, Informacijski center idr. Na tej stopnji raziskave je ugotovljeno, da te službe, čeprav v različnih organizacijah, predstavljajo podoben organ za zagotavljanje varnosti in zaščite inf. storitev, infrastrukture in/ali omrežja oz. jih lahko imenujemo kot odgovorne za načrtovanje zaščite IKI v svojih organizacijah (Cestnik 2013; Cestnik 2014; Preradović 2013; Loborec 2013; Sektor za načrtovanje MORS 2013; Služba za varnostno načrtovanje 2013: Čarni in Palčič 2014).

Ti subjekti sledijo dvema dokumentoma in sicer Uredbi o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih in Sklepu o določitvi pogojev za varnostno tehnično opremo, ki se sem vgrajevati v varnostna območja, ki sta najnatančnejša dokumenta v opredelitvi potrebnih zaščitnih ukrepov pri načrtovanju zaščite v IK sistemih, vsaj kar se tiče ravnanja s tajnimi podatki. V omenjenima, Uredbi in Sklepu, so torej našteti sistemi in oprema, ki jih je potrebno uporabiti pri načrtovanju in zagotavljanju zaščite IKI, organizacije posebnega pomena za obrambo države so obvezane slediti tem dokumentom in jih implementirati, kar pa so povečini že storile (Cestnik 2013; Preradović 2013; Loborec 2013; Sektor za načrtovanje MORS 2013; Služba za varnostno načrtovanje 2013).

Organizacije posebnega pomena za obrambo države morajo (poleg drugih nacionalnovarnostnih idr. subjektov, ki ravnajo s tajnimi podatki) imeti vzpostavljena varnostna območja za ravnanje s tajnimi podatki, tako fizičnimi kot tudi v digitalni obliki. Zaključimo lahko, da je IKI v preučevanih organizacijah zaščitena in varovana v skladu s predpisi. Kaj to pomeni si lahko natančneje preberemo v omenjenih dokumentih.

Kot raziskovalca naju je do te točke raziskave najbolj zanimalo, kdo je v organizacijah s Sklepa zadolžen za varnost (fizično, omrežno/spletno, drugo) IK infrastrukture oz. sistemov.

[41] Odgovori so vzeti iz anketnega vprašalnika, kjer je bila oblikovana 5 stopenjska lestvica odvisnosti: 0-neobstoječa, 1-majhna, 2-srednja, 3-velika, 4-popolna.

Omenili smo že, da v preučevanih organizacijah obstajajo interne službe, ki se ukvarjajo z varnostjo in zaščito IKI v teh organizacijah. Omenjeni so tudi zasebniki, ki se ukvarjajo z dejavnostjo varovanja. Ali na tem področju lahko govorimo o neke vrste javno-zasebnem partnerstvu, seveda, kakšne vrste pa je predmet debate. Neizpodbitno je, da so organizacije zaščito, varovanje IKI in tudi načrtovanje zaščite le-te odstopile zasebnikom, a to le do mere, ki je v skladu z Zakonom o zasebnem varovanju (69. člen) in s pogodbo med naročnikom in izvajalcem varovanja. Obstaja torej neke vrste javno-zasebni odnos[42] na podlagi pogodbe o izvajanju varnostnih storitev. Varovanje izvajajo licencirane zasebne varnostne službe pri teh organizacijah v vseh varnostnih razmerah (naravne in druge nesreče, kriza, izredno stanje in vojna), nadzor nad izvajanjem nalog zasebnega varovanja izvaja Inšpektorat RS, pristojen za notranje zadeve in policija v okviru svojih pristojnosti (Cestnik 2014; Čarni in Palčič 2014).

Ostali nacionalno varnostni elementi (subjekti) se vključijo v zaščito IKI teh organizacij v primeru njenega resnejšega ogrožanja. Omenimo lahko organizacije kot so SOVA, MNZ (Policija), MORS, MIZŠ, SI–CERT, in pogojno SV. Sklepamo lahko, da se uporaba SV pri ogrožanju IKI teh organizacij ne izvaja oz. se SV uporabi v skladu z ZObr in podrejenimi akti, kar pomeni izključno v vojni ali pri grožnji z njo. MORS ima predvsem preventivno vlogo, saj je zadolžen za urejanje področja na sistemski ravni, s čimer poskuša zagotoviti čim učinkovitejši sistem, da grožnje ne bi povzročile škode.

Kot primer navedimo 29. člen ZObr, kjer so navedeni sektorji: telekomunikacije, energetika, transport, proizvodnja, drugo. Določbe tega člena se nanašajo izključno na posamične objekte, katerih varovanje lahko zaradi njihove funkcije izvaja tudi vojska. Določbe tega odstavka niso mišljene kot opredelitev sektorjev kritične infrastrukture[43], ampak kot opisni kriterij, katere objekte lahko vojska v svojih načrtih določi kot objekte, pomembne za obrambo države. Ti objekti so lahko tudi objekti organizacij, katerih dejavnost je posebnega pomena za obrambo države. Na to razlikovanje sva bila raziskovalca posebej opozorjena s strani MORS. Ne moremo pa mimo dejstva, da je organizacijam, posebnega pomena za obrambo države že s strani države oz. Vlade RS dodeljen poseben status v primeru vojne oz. kriz, prav tako pa njihovi IKI. Vse to je posledica sistema civilne obrambe (Čarni 2014; Čarni in Palčič 2014).

Tako z vidika obrambe države kot pri načrtovanju zaščite IKI bi bilo smiselno usmeriti se v načrtovanje sektorizacije organizacij s Sklepa, saj s tem dosežemo transparentnost in

[42] Temu težko rečemo partnerstvo, ker gre povsem za poslovno delovanje in razmerje naročnik – izvajalec.
[43] Ti so posebej opredeljeni s Sklepom VRS št. 80200-1/2012/5, z dne 17. 10. 2012 z naslovom Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji.

postavimo temelje načrtovanju zaščite IKI skozi prizmo koncepta zaščite in varovanja kritične infrastrukture. Navedene določbe trenutno nimajo neposredne povezave s področjem zaščite KI, res pa je, da je njihova infrastruktura (tudi IKI) lahko opredeljena kot vitalna/ključna/kritična in s tem umeščena med kritično infrastrukturo.

Ugotovljeno je bilo, da organizacije s Sklepa[44] pokrivajo le del načrtovanih sektorjev, za učinkovito obrambo države in zaščito KI pa je potrebna celovitost. V prejšnji poglavjih sva raziskovalca že opozorila, da je za opredelitev organizacije kot posebnega pomena za obrambo države odvisna dejavnost, ki jo ta organizacija opravlja. Na podlagi tega so na MORS odgovorili, da je bil v času najinega preučevanja nabor organizacij posebnega pomena za obrambo države v ponovni preučitvi po resorjih, s čimer so želeli zagotoviti celovitost dejavnosti in storitev (Sektor za načrtovanje MORS 2013). Posledica tega je bilo sprejetje prenovljenega seznama gospodarskih družb, zavodov in ostalih organizacij, katerih dejavnost je posebnega pomena za obrambo države.[45]

Pri tem je pomembno tudi, katera ministrstva so sodelovala pri oblikovanju in sprejemanju prenovljenega seznama teh organizacij oz. so bila s Sklepom VRS vsaj seznanjena. Sodelovala so: Ministrstvo za obrambo, Ministrstvo za infrastrukturo in prostor, Ministrstvo za gospodarski razvoj in tehnologijo, Ministrstvo za izobraževanje, znanost in šport, Ministrstvo za zdravje, Ministrstvo za notranje zadeve, Ministrstvo za kulturo.

Pri tem je MNZ nosilec podsistema notranje varnosti in zato ».. prepoznan kot eden od nosilcev sistema nacionalne varnosti, zato je vloga MNZ v sistemu zagotavljanja nacionalne varnosti velika. MNZ tako zagotavlja varnost državnega omrežja in lastnih IKS, sicer pa MNZ in policija delujeta skladno z zakonskimi predpisi. Pri pojavu kaznivih dejanj pa Policija sodeluje z državnim tožilstvom in preiskovalnim sodnikom.« (Služba za varnostno načrtovanje 2013).

Zaščita IKI v organizacijah posebnega pomena za obrambo države ni samostojno opredeljena v nobenem normativno-pravnem aktu, tovrstni posebni akti niti ne obstajajo s področja zaščite kritične infrastrukture (prav tako ne na državni ravni). Trenutno je tovrstna zakonodaja v intenzivni fazi oblikovanja, kar se je potrdilo tudi z opravljenim delom v zadnjih dveh do treh letih. Od začetka raziskovanja področja zaščite IKI v organizacijah posebnega

[44] Sklep o določitvi gospodarskih družb, zavodov in drugih organizacij, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji (Sklep št. 311-21/95-3/3-8) z dne 16. maja 1996 in Sklep o določitvi gospodarskih družb, zavodov in drugih organizacij, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji, z dne 17. april 2014.

[45] Sklep o določitvi gospodarskih družb, zavodov in drugih organizacij, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji, Sklep VRS št. 80101-1/2014/5, z dne 17. 4. 2014.

pomena za obrambo države v letu 2012 do danes, je bil glavni premik narejen v smeri zaščite kritične infrastrukture, oblikovanja kriterijev za določanje le te in določanja kritične infrastrukture. To lahko potrdimo z navedenimi dokumenti v prejšnjih odstavkih, ki jih je Vlada RS sprejela v letih med 2012 in 2014. V teh dokumentih je načelno zajeta tudi zaščita IKI, ki je opredeljena kot kritična infrastruktura, ni pa nujno, da je med to tudi IKI organizacij, katerih dejavnost je posebnega pomena za obrambo v RS.

Vlada RS je v preteklem obdobju imenovala nosilce ZKI in jim naložila opredelitev ukrepov le te. Področje ZKI bo urejal normativno-pravni akt, ki ga morajo imenovani nosilci pripraviti do konca leta 2015, urejal pa bo tudi razmerja med državnimi organi in lestvico ter opredelitev stopenj ogrožanja (Čarni 2014). Določanje kriterijev ogroženosti IKI spada v pristojnost MNZ in MIZŠ, kriteriji pa so tajni podatek in niso javno dostopni. Za področje ogroženosti IKI bi se pri načrtovanju zaščite le te morali upoštevati tudi kriteriji kot so gospodarska škoda (npr. izpad BDP ali sami prihodki podjetij) ter vrste in frekvenca napadov (omrežnih, kibernetičnih, fizičnih) na IKI v organizacijah posebnega pomena za obrambo države in tudi širše.

Potrebno se je zavedati, da organizacije s Sklepa upravljajo z infrastrukturo, ki je ključna za opravljanje njihove dejavnosti in bi predvidoma lahko tvorila tudi jedro kritične infrastrukture v RS[46]. Zato je pomembno, da se v RS zgodi premik pri zavedanju o pomenu načrtovanja zaščite in varnosti na tem področju in da je potrebno oblikovati določene kriterije, merila za vključevanje različnih nacionalnovarnostnih subjektov v zaščito in varovanje te infrastrukture ob različnih situacijah.

Prvi korak k temu bi bilo oblikovanje enotnega modela zaznavanja oz. ocenjevanja ogroženosti infrastrukture organizacij posebnega pomena v RS, kateri po odgovorih anketirancev sodeč, trenutno ne obstaja. Izpostavili so, da na skupnih koordinacijah in sestankih mnogokrat ugotovijo, da si odgovorni različno razlagajo stopnje ogroženosti, kriterije za delovanje različnih služb in organizacij ter merila ogroženosti (Cestnik 2013; Cestnik 2014; Preradović 2013; Loborec 2013). S poenotenjem omenjenega bi na celotnem območju RS dosegli poenoteno razumevanje (ocen) ogroženosti IKI in druge infrastrukture. Merila, stopnje in kazalci bi bili vsem enako razumljivi.

Logična posledica oblikovanja modela je izdelava načrta varovanja, ki vsebuje tudi lestvice stopenj ogrožanja, ki pa je v RS oblikovana na podlagi Uredbe o obveznem organiziranju

[46] Katera infrastruktura v RS je opredeljena kot kritična je opredeljeno v predpisih, ki pa so širši javnosti nedostopni in tako zaradi varnostne narave in kritičnosti označeni s stopnjo tajnosti.

varovanja, ki opredeljuje tako lestvico oz. natančneje oceno stopnje ogrožanja[47], kot tudi nalaga naloge ministrstvom o oblikovanju seznama subjektov, ki si morajo varovanje organizirati[48]. Ugotovljeno je bilo, da morajo dotično uredbo spoštovati (vsaj nekateri)[49] subjekti s Sklepa. Ta Uredba ureja obvezno organiziranje varovanja vseh elementov in področij v organizaciji in zajema tudi organizacijo varovanja za IKI v sklopu varnostnega področja. Na področju varovanja in načrtovanja zaščite IKI obstaja tudi Zakon o elektronskih komunikacijah (ZEKom – 1), ki tudi opredeljuje izdelavo varnostnih načrtov za elektronske komunikacije. Trditve potrjujejo tudi odgovori organizacij posebnega pomena za obrambo države (Cestnik 2013; Cestnik 2014; Preradović 2013; Loborec 2013).[50] Pri raziskovanju nama je bilo ponujenih več različnih lestvic, kar kaže na to, da le-te niso poenotene, niso nam pa znani niti kazalci oz. kriteriji, ki opredeljujejo, kdaj nek dogodek uvrstiti v nizko, srednjo oz. katero koli drugo stopnjo ogrožanja.

Načrt varovanja (kot ga določa Uredba o obveznem organiziranju varovanja) bi moral vsebovati tudi načrt varovanja IKI – predvsem fizično in tehnično varovanje. Trenutno je to področje delno urejeno v ZEKom. Da bi imele organizacije posebnega pomena za obrambo države sprejete ločene načrte varovanja IKI še ni za pričakovati, predvsem glede še nedorečenih sistemskih rešitev. Trenutno je bil dosežen korak naprej s tem, da so se organizacije posebnega pomena za obrambo države začele zavedati pomena IK varnosti in v varnostne načrte vključile tudi načrte zaščite oz. varovanja svoje IKI. Natančnejše sistemske rešitve v obliki normativno-pravnih aktov se bodo iskale po sprejetju nacionalne strategije kibernetske varnosti v bližnji prihodnosti. Na področju sistemske zaščite IKI pa, kot je že bilo omenjeno, trenutno obstajajo politike in navodila, ki določajo smernice načrtovanja zaščite IKI. Načrti varovanja IKI so torej izzivi za prihodnost, ko bodo skoraj nedvomno potrebni, če gledamo tempo razvoja in naraščanja pomena IKT.

Izvajanje same Uredbe o obveznem organiziranju varovanja in nadzor nad njim je v pristojnosti MNZ, zatorej bi bilo tudi izdelovanje načrtov varovanja oz. zaščite IKI potrebno uskladiti s pristojnim ministrstvom. Pomembna pri načrtovanju zaščite je določitev kriterijev, na podlagi katerih lahko določimo stopnjo ogroženosti (nizka, srednja, visoka) subjektov varovanja in zaščite. Omenjeni kriteriji so nejasni, zato je organizacijam posebnega pomena

[47] Ocena stopnje tveganja vključuje tudi oceno stanja varovanja podatkov in drugih ranljivosti, če je to potrebno zaradi drugih predpisov ali zaradi narave poslovanja zavezanca (povzeto po Uredba o obveznem organiziranju varovanja).
[48] Tudi na podlagi Zakona o zasebnem varovanju (ZZasV-NPB3).
[49] Izjemno težko je z gotovostjo trditi za koga vse velja Uredba in tudi Zakon o zasebnem varovanju, saj si lahko pravni strokovnjaki različno razlagajo obveze iz določenih aktov, kar se je pokazalo tudi v pravni praksi v RS v zadnjem času.
[50] Odgovori UKCLj na 2. Vprašalnik.

za obrambo države prepuščena določena mera samostojnosti pri razvoju lastnih sistemov ocenjevanja tveganj in na podlagi lastnih kriterijev. Kot primer lahko navedemo lestvico, ki so jo razvili v eni od organizacij posebnega pomena za obrambo države. V tej so uporabili številčni sistem ter tveganje ocenili z lestvico od 1 do 5. To lestvico so uredili v razrede: 1 – 2 nizka stopnja tveganja, 3 – 4 srednja stopnja tveganja in 5 visoka stopnja tveganja. Poleg te uporabljajo tudi odstotkovno metodo, pri kateri so stopnje tveganja razdeljene po odstotkih (Cestnik 2013; Cestnik 2014).

Tveganja se normalno poskušajo zmanjšati tudi s prenosom nalog varovanja na zasebne varnostne družbe, ki pa v večini primerov opravljajo samo t. i. zunanja varovanja, kar pomeni, da ne opravljajo varovanj vitalnih sistemov v organizaciji, ki jo varujejo (Cestnik 2013; Cestnik 2014).

V organizacijah posebnega pomena za obrambo države organizacija sama zagotavlja varovanje IKI v primerih naravnih nesreč, izrednega ali vojnega stanja oz. ostalih vrst kriz. Na primeru UKCLj lahko potrdimo, da varovanje zagotavlja varnostna služba UKCLj. Organizacije posebnega pomena za obrambo države so se v večini primerov opredelile, da naravne nesreče, izredna oz. vojna stanja ter krize predstavljajo glavne primere tveganj njihovi IKI. V primerih izrednega oz. vojnega stanja in kriz, ki niso naravne nesreče, pri zaščiti IKI pomaga Policija. Kot primer lahko navedimo npr. fizični napad na infrastrukturo ali pa vdor v informacijski sistem. To sta samo dva od kriterijev, ki bi jih lahko navedli kot resnejše ogrožanje IKI organizacij posebnega pomena za obrambo države (Cestnik 2013; Cestnik 2014).

Načrt varovanja je primarno potreben za zagotovitev modela varovanja območja in tudi po možnosti sistema IKI. Po Uredbi o obveznem organiziranju varovanja mora zavezanec[51] imeti izdelan načrt varovanja (fizično in tehnično varovanje vsaj prostorov organizacije), ki vsebuje: oceno stopnje tveganja, program varovanja, načrt fizičnega varovanja. Izdela ga licencirani varnostni menedžer (Uredba o obveznem organiziranju varovanja 2012, 7. – 10. člen):

Ocena stopnje tveganja vsebuje obvezne elemente:

1. podatki o zavezancu;
2. opis varovanega območja;
3. analiza ranljivosti;
4. analiza ogroženosti;

[51] Vsak, ki je dolžan upoštevati omenjeno uredbo-glej Uredba o obveznem organiziranju varovanja oz. 69. člen Zakona o zasebnem varovanju, Ur. L RS 9/06 z dne 27. 1. 2006.

5. analiza tveganj;
6. splošna ocena o stopnji tveganja z oceno verjetnosti nastanka posledic.

Ko določimo obvezne elemente, je ocena stopnje tveganja pripravljena v treh prej omenjenih stopnjah: nizki, srednji, visoki. V tem delu imajo vlogo tudi pristojne državne službe, ki spremljajo ogroženost organizacij. Policija, Slovenska obveščevalno-varnostna agencija in obveščevalno varnostna služba MORS, v okviru svojih pristojnosti spremljajo varnostno tveganje in grožnje in če pri tem pridobijo podatke, ki bi lahko vplivali na oceno stopnje tveganja posameznega zavezanca, jih takoj odstopijo MNZ (povzeto po Uredba o obveznem organiziranju varovanja 2012, 7. – 10. člen).

Obvezni elementi programa varovanja so:

1. opredelitev namena varovanja;
2. pregled pravnih podlag;
3. zahteve, kriteriji, merila, pristojnosti in dolžnosti službe varovanja;
4. izhodišča in drugi ukrepi za izvedbo učinkovitega varovanja.

Obvezni elementi načrta fizičnega varovanja so:

1. opis varovanega območja;
2. načrt ali skica varovanega območja;
3. skice fizičnega varovanja z varnostnim osebjem in/ali sistemi tehničnega varovanja;
4. organizacija in obseg varovanja:

a) način izvedbe (opis varnostnih ukrepov in postopkov varnostnega osebja),
b) opis sistema tehničnega varovanja,
c) načrt za uporabo zvez,
d) varnostni ukrepi in postopki varovanja ob naravnih in drugih nesrečah, v krizi, izrednem stanju in vojni;

5. načrtovani ukrepi za preverjanje postopkov in varnostnih ukrepov;
6. požarni načrt;
7. opredelitev sodelovanja s pristojnimi službami (policijo, regijskim centrom za obveščanje, gasilci, reševalno službo in drugimi pristojnimi službami).

Z lestvico ogroženosti in načrtom varovanja so neposredno povezani tudi kriteriji ogroženosti IKI oz. kriteriji operativnosti organizacije oz. njenih IK sistemov. Na tem mestu sva želela ugotoviti kakšno škodo IK sistemov prenese določena organizacija posebnega pomena za obrambo države, da je še zmožna zagotavljati dejavnost, storitve oz. proizvode. Organizacije posebnega pomena za obrambo države so zmožne prenesti določeno stopnjo škode npr. majhno, srednjo, visoko, da je organizacija še zmožna zagotavljati storitve kot to

pričakuje družba oz. uporabniki. Operativnost teh organizacij bi morala biti opredeljena na podlagi kriterijev operativnosti, ki bi določali prej omenjeno lestvico škode. Zato predlagava uvedbo enotne lestvice, po kateri bi škodo ocenili na npr. majhno, srednjo, veliko (podobno kot je oblikovana v Uredbi o obveznem organiziranju varovanja) oz., da je v obstoječi lestvici jasno opredeljeno, kaj so kriteriji za uvrščanje v določeno stopnjo na lestvici.

Leta 2010 ministrstvo odgovorno za javno upravo v RS izdalo Priporočila informacijske varnostne politike javne uprave, ki postavljajo osnovna varnostna izhodišča za zaščito informacijskih sredstev pred nevarnostmi, bodisi notranjimi ali zunanjimi, namernimi ali naključnimi. Organizacije posebnega pomena za obrambo države še vedno delajo na implementaciji teh priporočil (Cestnik 2013; Preradović 2013; Loborec 2013). Omenjena priporočila predvsem izhajajo iz dejstev, da je razvoj informacijske tehnologije izjemno hiter in mu je težko slediti. Za zaščito IKI in podatkov znotraj IK sistemov v RS sledimo tudi že omenjenim Zakonu o elektronskih komunikacijah, Uredbi o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih in Sklepu o določitvi pogojev za varnostno tehnično opremo, ki se sme vgrajevati v varnostna območja. Organizacije posebnega pomena za obrambo države so mnenja, da je nedvomno potrebno slediti razvoju IKT in skladno s tem posodabljati tudi krovne dokumente, ki se dotikajo zaščite IKI. Za tovrstne naloge je v RS zadolžena Komisija za informacijsko varnost, v kateri sodeluje tudi predstavnik MORS. Pomembne dokumente s področja zaščite IKI bi bilo potrebno revidirati vsaj na dve leti (Cestnik 2014). Na tem mestu je potrebno poudariti, da moramo razločevati med strateškimi in operativnimi dokumenti. Prvi so dolgoročnejši, drugi bi se lahko revidirajo tudi na mesečni ravni.

Organizacije s Sklepa so primarno dolžne skrbeti za lastno varnost in zaščito IKI, kar lahko dosežejo tudi z oblikovanjem lastnih modelov in izvajanjem simulacij, s čimer dosežejo večjo pripravljenost in poskušajo predvideti vzroke, reakcije, potek in posledice dogodkov. S poglobljenim načrtovanjem zaščite tudi s pomočjo modelov in simulacij lahko organizacije posebnega pomena za obrambo države minimalizirajo vpliv kritičnih dogodkov na delovanje organizacije. Predvsem gospodarske družbe lahko preprečijo tudi večje denarne šoke, ki so lahko reparacije po krizi ali izpad dohodka. Večinoma so organizacije s Sklepa še v fazi razvoja ali uveljavljanja modelov v prakso, nekateri pa že imajo utečeno prakso izvajanja simulacij in modeliranja dogodkov. Pri teh je potrebno upoštevati tudi vlogo notranjih ali zunanjih zasebnih varnostnih služb, saj so organizacije obvezane zagotavljati varovanje tudi ob naravnih in drugih nesrečah, v krizi, izrednem in vojnem stanju (povzeto po 5. členu Uredbe o obveznem organiziranju varovanja). Zagotavljanje varovanja poleg ocene stopnje

ogrožanja zahteva tudi izdelavo drugega dokumenta – načrta varovanja, to je program varovanja in tudi načrt fizičnega varovanja. Slednje je podrobneje opisano v Uredbi o obveznem organiziranju varovanja.

Naslednji pomemben mednarodni akt je Direktiva o določanju EKI iz leta 2008, ki nalaga tudi izdelavo t. i. varnostnega načrta upravljavca, čeprav za objekte kritične infrastrukture. Kljub vsemu je pomembno, da ta dokument omenimo, saj se razvija v smeri zaščite objektov in infrastrukture, tudi IKI. Ta načrt ali enakovredni ukrepi, ki vključujejo opredelitev pomembnih infrastrukturnih zmogljivosti, oceno tveganja ter ugotavljanje, izbiro in prednostno razvrstitev protiukrepov in postopkov, bi morali biti pripravljeni za vso določeno EKI (11. člen Direktive Sveta (ES) 114/2008).

V tem členu je določeno, da ob opredelitvi EKI v določeni članici EU morajo te, določene, organizacije izdelati varnostni načrt upravljavca (VNU). V RS EKI še nimamo določene, je pa VNU dober primer, kaj bi lahko organizacije s Sklepa izdelale za potrebe področja IKI in načrtovanja zaščite le-te. Ugotovljeno je bilo, da nobena od treh anketiranih organizacij nima izdelanega VNU, so si pa odgovorni v organizacijah enotni, da bi morala, po njihovem mnenju, biti infrastruktura njihove organizacije določena kot kritična vsaj na nacionalnem nivoju (Cestnik 2013; Preradović 2013; Loborec 2013).

Z razvojem in poglabljanjem raziskave sva se raziskovalca osredotočila predvsem na notranje sistemsko zaščito IKI na ravni organizacij posebnega pomena za obrambo države. Pri tem naju je zanimala vzdržnost sistema IKI in njena zaščita. S tem namenom sva se raziskovalca dotaknila načrta o neprekinjenem poslovanju, ki po pričevanjih anketirancev nikakor ne cilja samo na ekonomsko vzdržnost organizacije v času kriz, pač pa mora (oziroma bi moral) vsebovati tudi varnostno komponento. Slednja komponenta se nanaša predvsem na vključevanje varnostnih akterjev v primerih groženj, katerih obvladovanje presega zmožnost delovanja organizacij (tudi organizacij posebnega pomena za obrambo države). V najinem primeru to pomeni, da ima npr. UKCLj oblikovan načrt o neprekinjenem poslovanju, ta pa se nanaša na zagotavljanje zdravstvene oskrbe v času kriz na bolj ogroženi sekundarni in terciarni ravni (Cestnik 2014). Ti ravni sta predvsem bolj dovzetni za posledice groženj, saj kot bolj specialno usmerjeni ravni potrebujeta za delovanje stabilno varnostno okolje, ki pa ga nepredvidljivost in nekonstantnost kriz ruši. Ravno zato je predvsem potrebno natančno in resno načrtovati zaščito (in varovanje) IKI, tudi s pomočjo oblikovanja sistemskih idr. dokumentov, kot je načrt o neprekinjenem poslovanju, ki še dodatno zaščitijo občutljivo in tudi ključno IKI.

Načrt o neprekinjenem poslovanju je temelj delovanja organizacije v krizi oz. vojni. Neprekinjeno poslovanje pomeni zagotovitev neprekinjenega delovanja in razpoložljivosti informacijskih sistemov, omogoča hitro vzpostavitev poslovanja po katastrofalnih dogodkih in posledično pomaga graditi zaupanje v poslovanje organizacije (S&T.si 2014). Ta lahko pripravi zanesljiv in učinkovit načrt neprekinjenega poslovanja samo z predhodno analizo tveganja, s katero določijo najbolj bistvene procese za nemoteno delovanje v primeru grožnje. Osnova delovanja organizacije v krizi oz. vojni je tudi obvezno zagotavljanje varovanja ob naravnih in drugih nesrečah, v krizi, izrednem in vojnem stanju. Ta načrt se nedvomno dotika tudi delovanja IKI, ki je temelj za delovanje družbe/organizacije, saj se te dandanes vedno bolj naslanjajo na IKT. Ugotovljeno je bilo, da omenjeni načrti v organizacijah posebnega pomena za obrambo države obstajajo (Cestnik 2013; Preradović 2013; Loborec 2013). Kaj vsebujejo je predmet vsake organizacije posebej, morajo pa vsebovati tudi postopke ob kriznih razmerah oz. v primerih, ko v ospredje stopi krizno upravljanje.

Načrt o neprekinjenem poslovanju se velikokrat naslanja na primere najpogostejših varnostnih tveganj (IKI), na podlagi katerih se ga lahko tudi izdeluje. Organizacije posebnega pomena za obrambo države imajo večinoma razvite načrte o neprekinjenem poslovanju, ki pa se nanašajo na najpogostejša varnostna tveganja. Velikokrat so ti načrti lahko tudi narave poslovne skrivnosti (Loborec 2013), a v nadaljevanju navajava najpogostejša varnostna tveganja za katere se oblikujejo načrti o neprekinjenem poslovanju, kot so jih navedle organizacije, katerih dejavnost je posebnega pomena za obrambo države (Cestnik 2013; Preradović 2013; Loborec 2013):

- Okvara strojne opreme
- Zlonamerna koda
- Kršenje pooblastil in sabotaža

Slednja trditev posredno že potrjuje eno izmed hipotez in kaže na izjemno pomembnost sodobnejših informacijsko-komunikacijskih varnostnih tveganj IKI v njihovi organizacij.

Pri načrtovanju zaščite IKI obstaja več standardov, ki opredeljujejo smernice, pravila, postopke in tehnologijo, ki zagotavljajo kar najvišjo stopnjo zaščite IKI. Eden takih je standard 27001. Ko govorimo o standardu 27001, govorimo o aktu, ki vzpostavlja sistem upravljanja na področju informacijske varnosti na mednarodni ravni (ang. *Information Security Management System-ISMS*). Nekatere organizacije s Sklepa so standard že implementirale, v večih pa je standard še v fazi implementacije(Cestnik 2013; Preradović 2013; Loborec 2013; Sektor za načrtovanje MORS 2013). Predvsem slednji odgovor lahko kaže na to, da se organizacije očitno ne čutijo ogrožene iz mednarodnega okolja.

Nacionalni nosilec področja kibernetske varnosti v RS je Ministrstvo za izobraževanje, znanost in šport, natančneje Direktorat za informacijsko družbo. Slednji pripravlja nacionalno strategijo kibernetske varnosti, pri njenem oblikovanju pa sodeluje tudi MORS. Ta je koncept kibernetske obrambe v obrambnem resorju v okviru delovne skupine izdelal 24. 7. 2013. To predvsem pomeni, da je na področju zaščite IKI v organizacijah posebnega pomena za obrambo države aktivnih več državnih akterjev, ki oblikujejo sistemske rešitve zaščite IKI v teh organizacijah. Poudarjava, da brez sprejete nacionalne strategije delne rešitve zaščite IKI organizacij posebnega pomena za obrambo države niso trajne. Trenutno se organizacije same spopadajo z načrtovanjem zaščite lastne IKI in so tudi same odgovorne za to in za nemoteno delovanje le te. Organizacije posebnega pomena za obrambo države izražajo tudi potrebo po rednih srečanjih odgovornih akterjev za zaščiti IKI v organizacijah posebnega pomena za obrambo države. Organizacije same bi jih predlagale vsaj 1 – 2 krat letno, kar bi predvsem okrepilo sodelovanje med akterji obrambnega načrtovanja (Cestnik 2014).

Tovrstni sestanki sicer že potekajo v okviru delovanja Medresorske koordinacijske skupine za usklajevanje priprav za zaščito kritične infrastrukture[52] (Čarni 2014). Organizacije posebnega pomena za obrambo države na teh sestankih sodelujejo po potrebi oz. preko pristojnih ministrstev, ki jih zastopajo. Sestanki potekajo na približno dva meseca, s predhodno določenimi konkretnimi nalogami in cilji: določanje kriterijev kritičnosti, določanje kritične infrastrukture[53]; pa so potekali tudi na tedenski ravni. Na teh sestankih tudi lahko uskladijo potrebe po načrtovanju zaščite IKI v organizacijah posebnega pomena za obrambo države.

Organizacije posebnega pomena za obrambo države same menijo, da je trenutna zakonodaja dovolj natančna v smislu opredelitve tehnične zaščite in pogojev, da pa bi na področju zaščite IKI v njihovih organizacijah bil dovolj en predpis, ki bi generalno urejal to področje(Cestnik 2013; Cestnik 2014; Preradović 2013; Loborec 2013; Sektor za načrtovanje MORS 2013; Služba za varnostno načrtovanje 2013; Čarni in Palčič 2014).

Sodobni viri ogrožanja, grožnje IKT in zavedanje je v letu 2014 privedlo do premika pri oblikovanju in sprejemanju rešitev na najvišjih ravneh tudi v RS. V času pisanja magistrske naloge je bil v javno razpravo dan osnutek Strategije kibernetske varnosti z naslovom Digitalna Slovenija 2020, kjer predvidevajo ustanovitev Nacionalnega organa za kibernetsko varnost, kateri bi ime eno izmed nalog koordinacija zmogljivosti za zagotavljanje kibernetske varnosti na nacionalnem in tudi na mednarodnem nivoju. Poleg tega bi koordiniral aktivnosti

[52] Omenjena skupina je bila ustanovljena s Skelpom Vlade RS št. 01203-17/2012/3, z dne 27.9.2012.
[53] V času pisanja magistrskega dela so ti cilji bili doseženi.

samostojnih odzivnih centrov za sisteme v javni upravi (SIGOV-CERT) ter za področje obrambe države (MORS-CERT) (Strategija za kibernetsko varnost 2014).

Omenjeni organ bi preko omenjenih (podrejenih) institucij nadzoroval tudi zanesljivost zagotavljanja IKI dejavnosti organizacij posebnega pomena za obrambo države in preprečeval motnje. Teh se v organizacijah posebnega pomena ne spomnijo, MORS navaja naravno nesrečo iz leta 2014 žled, ko je v ledeni oklep oklenilo večino Slovenije in je bila resno motena oskrba z električno energijo. Takrat so se v odpravljanje posledic vključili gasilci, Civilna zaščita, Slovenska vojska in tudi elektrogospodarstva doma in v tujini (predvsem Nemčija, Avstrija, Slovaška, Hrvaška, Romunija idr.).

Eden od mehanizmov načrtovanja zaščite IKI v organizacijah posebnega pomena za obrambo države so tudi t.i. kriteriji operativnosti organizacije oz. njenih IK sistemov, ki so popolnoma v domeni vseh organizacij posebnega pomena za obrambo države in ne sistemskih odločevalcev kot npr. MORS. Omenjene organizacije z raziskovalcema niso želele deliti teh kriterijev zaradi njim lastnih razlogov, ki jih kot raziskovalca zaradi kočljivosti informacij varnostne narave spoštujeva (Cestnik 2014; Čarni in Palčič 2014).

6.4 Vrste IK povezav in njihova zaščita

Med organizacijami posebnega pomena za obrambo države obstajajo močne poslovne vezi, ki jih povezujejo tudi obstoječa IK omrežja. Pri tem je pomembno ugotoviti kakšna je njihova medsebojna odvisnost od delovanja IK sistemov. To problematiko lahko obravnavamo z dveh zornih kotov. Prvič lahko opazujemo eno organizacijo in ocenjujemo v kolikšni meri je delovanje IKI v organizacijah s Sklepa odvisno od zagotavljanja dejavnosti določene (ene) organizacije. To je pomembna tematika z vidika medsebojne odvisnosti in s tem povezanega delovanja IKI organizacij s Sklepa. Nekatere organizacije so praktično nepogrešljivi členi zagotavljanja delovanja IKI in zagotavljanja dejavnosti drugih organizacij in so zato milo rečeno ostale organizacije v največji meri odvisne od delovanja ene same.

Drugič lahko vidik ugotavljanja odvisnosti obrnemo in pogledamo z drugačne perspektive, kjer nas lahko zanima, v kolikšni meri je delovanje IKI dotične (ene) organizacije odvisno delovanja ostalih organizacij s Sklepa. Pri tem lahko prepoznamo srednjo do visoko odvisnost organizacij s Sklep predvsem v povezavi z energetiko in prenosom informacij, kar zopet nakazuje na pomembnost zagotavljanja informacijske in tudi energetske varnosti ter načrtovanja zaščite le-te (Cestnik 2013; Cestnik 2014; Preradović 2013; Loborec 2013; Sektor za načrtovanje MORS 2013; Služba za varnostno načrtovanje 2013; Čarni in Palčič 2014).

V primerih kriznih dogodkov in pojava groženj v ospredje stopi koncept kriznega upravljanja, s katerim subjekti izvajajo kurativne dejavnosti za odpravljanje krize. Na nacionalni ravni je za to zadolžen NCKU, pri katerem je predvsem pomembno na kakšen način so organizacije posebnega pomena za obrambo države z njim povezane. Dejstvo je že, da so in tudi, da v primerih kriz omenjene organizacije opravljajo vsaka svojo vlogo. V medkriznih oz. vsakdanji, normalnih obdobjih imajo organizacije posebnega pomena za obrambo države z NCKU vzpostavljeno IK povezavo, za katero so v teh organizacijah odgovorne (notranje) službe za varnost (Cestnik 2013; Preradović 2013; Loborec 2013; Sektor za načrtovanje MORS 2013).

Zakonsko določeno je kakšne povezave se uporabljajo in do katere stopnje zaščite mora biti dograjena IK povezava. NCKU je z organizacijami posebnega pomena za obrambo države povezan preko več povezav med katerimi lahko omenimo varno elektronsko pošto (VEP) in medresorni komunikacijski sistem med izrednim dogodkom (MKSID). Obe povezavi sta namenjeni za komuniciranje v izrednih razmerah, preverjanje povezave se izvaja najmanj tedensko. Povezava je nameščena v varnostnem območju II. stopnje, z njo lahko v organizacijah, katerih dejavnost je posebnega pomena za obrambo države, rokujeta po večini 2 uslužbenca, ki imata dostop do tajnih podatkov stopnje tajnosti najmanj zaupno (Cestnik 2013; Cestnik 2014; Preradović 2013; Loborec 2013; Sektor za načrtovanje MORS 2013; Služba za varnostno načrtovanje 2013; Čarni in Palčič 2014).

Povezava z NCKU se vzpostavlja po potrebi in ob izrednih dogodkih. Zakonsko je določeno, da se tedensko preverja IK povezava z NCKU preko VEP. Organizacije, katerih dejavnost je posebnega pomena za obrambo države, imajo vzpostavljeno nadzorovano IK povezavo med sabo in z vsemi ministrstvi v RS. Z analizo pridemo do zaključkov, da obstaja ločen IK sistem, ki je neodvisen od svetovnega spleta. Za zaščito tega sistema je primarno odgovoren NCKU, vzdržuje ga SIK (sektor za informatiko in komunikacije) MORS, anketirane organizacije pa zanikajo, da bi že kadarkoli prišlo do poskusa vdora v sistem oz. povezavo.

IK sistemi in varnost le-teh v organizacijah je predvsem naloga samih organizacij. V načrtovanje in organiziranje varovanja in zaščite IKI državne ustanove ne posegajo, v primeru njihovega ogrožanja pa se vključijo predvsem SOVA, MO, MNZ, MIZŠ in SI–CERT (Cestnik 2014; Čarni in Palčič 2014).

Državne ustanove in organizacije posebnega pomena za obrambo države so medsebojno povezane preko IK povezave kot je že omenjena varna VEP, sistem ISPO (deluje na omrežju NCKU) ali MKSID (Cestnik 2013; Cestnik 2014; Preradović 2013; Sektor za načrtovanje

MORS 2013, Čarni in Palčič 2014). ISPO (Informacijski sistem za podporo pri odločanju v kriznem upravljanju v RS) uporabljajo tudi organizacije posebnega pomena za obrambo države. Sam NCKU ima določeno stalno ekipo, ki na nacionalnem oz. makro nivoju podpira izvajanje in načrtovanje zaščite IKI v organizacijah posebnega pomena za obrambo države. NCKU povezuje različne resorje in ima v svoji sestavi operativno, odločevalsko in analitično skupino, po drugi strani v delovnem telesu, ki deluje v NCKU, ni predstavnikov gospodarskih družb, so pa vzpostavljene stalne prej omenjene IK povezave z njimi. Poudariva lahko, da so povezave med NCKU in organizacijami vzpostavljene, niso pa vzpostavljene povezave med organizacijami in npr. Policijo oz. MNZ, katerih predstavnik je ob kriznih dogodkih tudi član delovnega telesa v NCKU. Skrbnik teh povezav je NCKU, upravitelj pa skrbnik v organizaciji posebnega pomena za obrambo države. NCKU v skladu uredbo[54] zagotavlja informacijsko in komunikacijsko povezavo za izmenjavo informacij in podatkov med najpomembnejšimi državnimi organi RS in tudi organizacijami posebnega pomena za obrambo države. Povezave, programi in oprema se skladno z razvojem tehnologij tudi nadgrajujejo in posodabljajo. S tem se zagotavlja brezhibnost sistema oz. infrastrukture, ki, kot trdijo na MNZ, do zdaj še ni utrpel poskusa vdora (Služba za varnostno načrtovanje 2013).

Da bi preprečili ogrožanje IKI v organizacijah posebnega pomena za obrambo države je potrebno oblikovati varnostne načrte. Eden teh je t. i. varnostni načrt upravljavca po Direktivi o določanju EKI iz leta 2008, a ta ne opredeljuje nacionalnega nivoja. Lahko pa je dober pripomoček in vodilo. MNZ organom, organizacijam in drugim, ki organizirajo obvezno službo varovanja skladno z Zakonom o zasebnem varovanju posreduje oceno ogroženosti, ki je podlaga za izdelavo načrta varovanja, iz katerega pa izhaja, kaj je namen varovanja in kaj se varuje v taki organizaciji. Ocena ogroženosti je lahko samo pripomoček pri oblikovanju načrta varovanja (Služba za varnostno načrtovanje 2013). Ta načrt (upravljavca) določa le evropsko KI, nacionalna je še v oblikovanju. V tej direktivi so lepo opisani koraki za določanje EKI, s čimer je povezano tudi določanje nacionalne KI. Za oblikovanje KI se uporabijo (med)sektorska merila ter nacionalne metode in kriteriji za določanje KI. Postopki določanja EKI v RS so v teku, pogoj za določitev EKI pa je primarno določena nacionalna KI. Logično sledi, da moramo v RS imeti določeno najprej nacionalno KI in potem razmišljati ali sploh imamo infrastrukturo oz. organizacije primerne za označitev kot EKI.

Pogoj uspešnega načrtovanja zaščite na sistemski ravni je enotnost modelov. Najprej se dotaknimo modelov za klasificiranje stopnje ogroženosti organizacij posebnega pomena za

[54] Uredba o organizaciji in delovanju Nacionalnega centra za krizno upravljanje.

obrambo države. V RS, po ugotovitvah sodeč, ne obstaja enoten model in ne lestvica za označevanje stopnje ogroženosti teh organizacij. Na MORS ocenjujejo, da ogroženost ni razdelana v obliki enotnega modela. Res pa je, da oceno ogroženosti v organizacijah imajo, če ne drugače jim jo posreduje MNZ skladno z Zakonom o zasebnem varovanju (Cestnik 2013; Preradović 2013; Loborec 2013; Sektor za načrtovanje MORS 2013).

Modeli in izvajanje simulacij dogodkov, ki pomenijo grožnjo varnosti IK sistemom organizacij posebnega pomena za obrambo države, se izvajajo zaenkrat le na mednarodni ravni z vključenostjo državnih struktur (ministrstev), ne pa tudi na nivoju samih organizacij. V prihodnosti lahko pričakujemo tovrstne simulacije oz. vaje tudi na ravni elementov kritične infrastrukture in organizacij, katerih dejavnost je posebnega pomena za obrambo države (Sektor za načrtovanje MORS 2013; Čarni in Palčič 2014).

Na tovrstnih simulacijah oz. vajah se preverja tudi vzdržnost organizacij, kar preprosto pomeni ugotavljanje koliko škode lahko organizacije prenesejo, da so še zmožne zagotavljati storitve oz. proizvode. Odgovornost za zagotavljanje 'storitev oz. proizvodov' nosijo organizacije same (mikro nivo). Državne ustanove so aktivne na makro nivoju, kar pomeni ustvarjanje okolja in sistema na nacionalnem nivoju, ki bo vzdržen v primeru kriz oz. vojne. Kot primer tovrstnih vaj lahko izpostavimo vajo kriznega upravljanja CMX 2009 in CMX 2011.

6.5 Načrtovanje zaščite IKI organizacij posebnega pomena za obrambo države v luči naraščajočega pomena koncepta kritične infrastrukture

V času pisanja naloge je v RS prišlo do premika na področju načrtovanja nacionalne kritične infrastrukture. Vlada RS je v letu 2014 določila opredelitev kritične (in ne ključne) infrastrukture in zato uporabljamo besedno zvezo »kritična infrastruktura«, česar se bova držala tudi raziskovalca, pa naj se s terminom strinjava ali ne. Tako je delno razrešena dilema poimenovanja tovrstnega koncepta.

Na podlagi definicije in osnovnih ter sektorskih kriterijev za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji so ministrstva in Banka Slovenije ob usklajevanju v Medresorski koordinacijski skupini za usklajevanje priprav za zaščito kritične infrastrukture v Republiki Sloveniji predlagali in utemeljili konkretno kritično infrastrukturo Republike Slovenije po sektorjih kritične infrastrukture, ki je bila predložena Vladi Republike Slovenije v obravnavo in potrditev. Vlada je s sklepom naložila nosilcem kritične infrastrukture državnega pomena oblikovanje ukrepov za njeno zaščito, Medresorski koordinacijski skupini za usklajevanje priprav za zaščito kritične infrastrukture v Republiki

Sloveniji pa pripravo predloga normativno-pravnega akta, ki bo urejal kritično infrastrukturo Republike Slovenije (povzeto po Zaščita kritične infrastrukture).

Vlada RS je opredelila kriterije kritičnosti s sklepom št. 80200-1/2012/5, z dne 17. 10. 2012 ter jih dopolnila in spremenila s sklepom št. 80200-2/2013/3, z dne 9. 1. 2014. Prav tako je kasneje Vlada RS določila kritično infrastrukturo državnega pomena v RS s sklepom št. 80200-2/2014/8, z dne 10. 4. 2014. Javna objava tega sklepa ni možna zaradi stopnje tajnosti INTERNO in zato tudi ni obravnavan v tem, javnem, raziskovalnem delu. Temu sledi, da ne moreva dokončno potrditi ali je IKI organizacij posebnega pomena za obrambo države opredeljena tudi kot kritična infrastruktura državnega pomena v RS. Vsi zaključki na to temo bi bili v tem primeru zgolj domneve, kar pa na tej stopnji raziskave nikakor ni sprejemljivo. Zato se raziskovalca osredotočava izključno na kriterije kritičnosti in na podlagi tega ocenjujeva pomembnost IKI organizacij posebnega pomena za obrambo države ter potrebo po njeni zaščiti.

Vlada RS je v preteklih mesecih določila tudi sektorje kritične infrastrukture v RS (Sklep VRS, št. 80200-2/2014/8, z dne 10. aprila 2014), in sicer osem (8) sektorjev, med katerimi je tudi sektor informacijsko komunikacijske podpore[55]. Poudariti velja, da je Vlada RS določila tudi t. i. sektorske kriterije kritičnosti za določanje kritične infrastrukture državnega pomena v RS in da je bila v aprilu 2014 določena tudi kritična infrastruktura državnega pomena v RS, a je Sklep Vlade označen s stopnjo tajnosti INTERNO. S slednjim je Vlada RS določila tudi nosilce kritične infrastrukture v RS, kar so predvsem pristojna ministrstva. Tem je Vlada RS naložila oblikovanje ukrepov zaščite kritične infrastrukture do januarja 2015. V tem mesecu (januarju 2015) je potrebno pripraviti tudi normativno-pravni akt, ki bo urejal zaščito kritične infrastrukture državnega pomena, s čimer bo najverjetneje sistemsko urejena tudi ZKI.

Raziskovalca sva se v najinem delu osredotočila samo na zaščito (K)IKI. Glede na napisano lahko potrdiva, da je Vlada kot enega izmed izjemno ključnih sektorjev prepoznala tudi sektor t. i. informacijsko komunikacijske podpore, še vedno pa ne moreva z gotovostjo potrditi ali je kot kritična infrastruktura v RS prepoznana tudi infrastruktura organizacij posebnega pomena za obrambo države. Pomembno je, da ne gre enačiti kritične infrastrukture z organizacijami posebnega pomena za obrambo države. Ta dva koncepta sta različna in imata vsak svoj namen (Čarni 2014). Kritična infrastruktura v RS je natančneje določena v Sklepu o

[55] Vlada Republike Slovenije je s sklepom, št. 80200-2/2014/8, z dne 10. aprila 2014, določila kritično infrastrukturo državnega pomena v Republiki Sloveniji.

določitvi kritične infrastrukture državnega pomena v RS iz aprila 2014[56], ki je označen s stopnjo tajnosti interno in torej ni javno dostopen. Slednje je povsem razumljivo, saj gre za infrastrukturo tako vitalnega pomena za RS, da bi njeno ogrožanje lahko resno ogrozilo normalno delovanje družbe.

V naslednjem odstavku obelodanimo razmejitev in ločevanje gospodarskih družb, zavodov in drugih organizacij, katerih dejavnost je posebnega pomena za obrambo države, od kritične infrastrukture v RS. Organizacije posebnega pomena za obrambo države nikakor niso isto kot kritična infrastruktura in jih zato ne moremo enačiti[57]. Kritična infrastruktura v RS je določena na podlagi kriterijev določenih v dokumentu *Veljavni kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena* (MORS 2014b) in se nanašajo zgolj na infrastrukturne objekte ter na neprekinjeno zagotavljanje dejavnosti kritične infrastrukture. Pri organizacijah posebnega pomena za obrambo države gre za kompleksnejše izvajanje nalog na področju obrambnega načrtovanja, ko organizacije v času kriz prevzamejo del družbene (narodne) odgovornosti in udejanjijo v naprej pripravljene obrambne načrte ter zagotovijo nemoteno opravljanje dejavnosti in storitev za državljane RS (Čarni 2014). Slednje organizacije v primerih kriz in vojn sistematično sprožijo postopke civilne idr. obrambe, ki so jih načrtovali kot sistemsko rešitev v primerih potrebe po zaščiti in obrambi RS.

V najboljšem primeru lahko poiščemo povezave med kritično infrastrukturo v RS in organizacijami posebnega pomena za obrambo države v zagotavljanju dejavnosti infrastrukture obeh konceptov. Tako je lahko infrastruktura organizacij posebnega pomena za obrambo države vključena v sezname objektov kritične infrastrukture in obratno. Skupna pa jima je potreba po načrtovanju zaščite dejavnosti in infrastrukture, tudi IKI.

Glede na predstavljeno je očitno, da sektor informacijsko komunikacijske podpore in sama IKT pridobiva na pomenu, če že ni med vsemi najpomembnejša. Glede na to je pomembno tudi, da organizacije posebnega pomena za obrambo države vse dojemajo IKI, tehnologijo in storitve kot enoten sektor, nekateri[58] ga zaradi njegovega pomena v sodobni družbi dojemajo tudi kot nadsektor (Cestnik 2013; Loborec 2013; Preradović 2013). Seveda, ga lahko razumemo v obeh pomenih, v opredelitvi kritične infrastrukture RS pa je pomembno, da je natančno opredeljen, da ne bi prihajalo do mešanja pomenov in zmot pri razlagi.

Pomembno dejstvo je, da se sektor in IKI dotika vseh raziskovanih organizacij, zato je nedvomno ključen oz. kritičen, kot je kritična, po njihovem lastnem mnenju, tudi njihova

[56] Sklep o določitvi kritične infrastrukture državnega pomena v RS, VRS, št. 80200-2/2014/8, z dne 10. 4. 2014 (stopnja tajnosti Interno).
[57] Tako je 09. decembra 2014 trdila ga. Alenka Čarni z ministrstva za obrambo.
[58] V tem primeru Telekom Slovenije d.d.

infrastruktura. Slednje potrjuje tudi MNZ, ki trdi, da je : »del infrastrukture MNZ in Policije že tudi zakonsko opredeljen kot infrastruktura ključnega pomena, ne sicer s tako terminologijo, vendar pa so zakonske zahteve opredeljene tako v Zakonu o obrambi, policijski zakonodaji in zakonodaji na področju elektronskih komunikacij.« (Služba za varnostno načrtovanje 2013).

Z analizo je bilo ugotovljeno, da je IKI izjemno pomembna za delovanje sodobnih organizacij in da se sodobna družba vedno bolj zanaša na delovanje le-te. To pa tudi pomeni, da od nje postaja vedno bolj odvisna, kar jo naredi za družbo ključno. Krize se torej lahko začenjajo tudi zaradi napak ali napadov na IKI. Ravno zato je pomembno, da je bil na sistemski oz. nacionalni ravni narejen prvi korak k oblikovanju nacionalne kritične infrastrukture, saj zato obstaja znanje, mnenja, dokazi in obstajajo resursi. Pomen načrtovanja zaščite te infrastrukture, predvsem pa IKI, je iz dneva v dan večji.

V prejšnjih odstavkih je bilo omenjeno, da je Vlada RS sprejela kriterije za določanje kritične infrastrukture v RS, sektorje kritične infrastrukture ter sektorske kriterije določanja kritične infrastrukture v RS[59] (dokumenti so javno dostopni na spletni strani MORS[60]). Znotraj teh kriterijev so tudi določeni kriteriji za sektor informacijsko-komunikacijske podpore. Slednje še ne pomeni, da je IKI organizacij posebnega pomena za obrambo države tudi opredeljena kot kritična infrastruktura sektorja IKP na nacionalni ravni. Tukaj prihaja do razhajanj vidikov umestitve IKI organizacij posebnega pomena za obrambo države na seznam kritične infrastrukture znotraj sektorja IKP. Nekatere organizacije trdijo da bi morala biti njihova IKI avtomatsko opredeljena kot kritična, ker *»...predstavlja IKI ključni del za delovanje ustanove.«* omenjene organizacije pa da imajo že tako ali tako na nacionalni ravni opredeljen poseben status v primerih obrambe RS (Cestnik 2013; Cestnik 2014). Tu prihaja do razhajanj s pogledi sistemskih odločevalcev (beri MORS), ki trdijo, da bo IKI organizacij posebnega pomena za obrambo države uvrščena oz. sprejeta kot del sektorja IKP le, če izpolnjuje kriterije kritičnosti določene v prej omenjenih sklepih Vlade RS (Čarni 2014). V teh odgovorih se predvsem ugotavlja ozko gledanje organizacij posebnega pomena za obrambo države na načrtovanje zaščite lastne IKI, ki zagovarjajo interese svoje organizacije v želji po čim večji stopnji zaščite svoje IKI. Kot primer navedimo UKCLj ki ocenjuje, da so računalniški center in celotno omrežje (infrastruktura) ključni za opravljanje njihove dejavnosti- predvsem tudi vsi inštituti in klinike na lokaciji Zaloška cesta 2 in 7 v Ljubljani. Vsi ti objekti so kot najpomembnejši ocenjeni z lastnimi kriteriji in s strani upravljavca, torej

[59] Sklep VRS št. 80200-1/2012/5, z dne 17. 10. 2012 ter Sklep VRS št. 80200-2/2013/3, z dne 09. 01. 2014.
[60] http://www.mo.gov.si/si/delovna_podrocja/zascita_kriticne_infrastrukture/ (21. 09. 2014).

same organizacije posebnega pomena za obrambo države – UKCLj (Cestnik 2014). Pri določanju državne kritične infrastrukture pa je potrebno slediti formalno določenim kriterijem sprejetih v sklepih Vlade RS in pristojnih ministrstev.

Ukrepi zaščite KIKI so v času pisanja magistrske naloge[61] v fazi priprave na ministrstvih, pri področnih nosilcih zaščite kritične infrastrukture ter se usklajujejo na medresorski ravni. Organizacije posebnega pomena za obrambo države se zavzemajo za sprejetje tako fizične, tehnične kot tudi kibernetične dimenzije zaščite oz. varovanja KIKI. V RS obstaja več akterjev, ki skrbijo za področje informacijske varnosti (MORS, MNZ, MIZŠ, SI–CERT,…) in delujejo na področjih svojih pristojnosti, čeprav so v organizacijah posebnega pomena za obrambo države prepričani, da jih je verjetno preveč in njihove posamezne pristojnosti niso jasne.

[61] Na dan 21. 09. 2014.

7 SKLEP

V preteklosti je imelo varnostno okolje predvsem vojaško-politične razsežnosti, danes vključuje tudi druge socialne in kulturno-civilizacijske dimenzije. Družbeno in naravno okolje je postalo spremenljivo, nepredvidljivo in bolj kompleksno. Grožnje varnosti so večdimenzionalne, saj se sodobne države soočajo s hkratnim obstojem groženj iz različnih dimenzij. Med indikatorji posameznih dimenzij varnosti obstaja cela vrsta povezav. Grožnje so tudi transnacionalne, ker se širijo ne glede na umetno vzpostavljene meje držav. Spremenili so se tudi referenčni objekti varnosti. Namesto države, so v ospredju družba, posamezniki, okolje in vse bolj tudi informacijska omrežja in kritična infrastruktura.

V zadnjem obdobju se soočamo z krizami, ki jih povzročajo teroristični napadi, naravne nesreče, vojne ipd.. Napadi v New Yorku, Madridu in Londonu so v celotnem spektru ogrožanja varnosti prispevali k prioritiziranju terorizma kot ključne grožnje. Slednje ima vpliv na oblikovanje zaščite kritične infrastrukture. Vendar se je treba zavedati, da obstajajo tudi številne druge krize, ki s svojim nastankom in obsegom, ki presega nacionalne meje opozarjajo, da terorizem nikakor ni nujno glavna grožnja varnosti ter da je potrebno pri izgradnji nacionalnega sistema kriznega upravljanja upoštevati vse vidike ogrožanja.

Omembe vredna je tudi odvisnost infrastrukturnih podsistemov, kot so promet, energetika, bančništvo, zdravstvo, javna uprava ter sistem zaščite in reševanja. Neučinkovita preskrba s hrano, vodo in temeljnimi energenti (nafta, plin, elektrika) ter nedelovanje finančnih sistemov plačevanja ter sistemov zdravstvene oskrbe bi prinesli specifično družbeno krizo. V kolikor se te krize ne bi uspešno obvladovale, bi prišlo do varnostnih situacij, v katerih bi bil ogrožen fizični obstoj posameznikov. Republika Slovenija je v letu 2014 oblikovala sektorje kritične infrastrukture, eden izmed njih je tudi sektor informacijsko komunikacijske podpore (IKP). Sektor IKP bi bilo potrebno preučevati znotraj- in tudi medsektorsko in ne samostojno, ravno zaradi možnosti prelitja posledic ogrožanja med različnimi sektorji. Slednje je relevantno, ker ima lahko informacijska dimenzija zaradi svoje razširjenosti v sodobnem svetu vpliv na različne druge dimenzije. Družbe so namreč tehnološko napredne in zato odvisne od IK sistemov, ki so temeljni del delovanja institucij, industrije in gospodarstva. To lahko potrdimo s povsem vsakdanjim primerom uporabe računalniške tehnologije za komunikacijo in upravljanje različnih sistemov, tako doma kot v gospodarstvu kamor spadajo tudi gospodarske družbe, zavodi in druge organizacije posebnega pomena za obrambo države v RS. Predvsem navedimo sisteme za upravljanje z bolnišničnimi bazami podatkov ali centralami v sklopu

UKCLj ali pa sisteme za nadzor železniškega prometa v Slovenskih železnicah. V obeh primerih gre za internet reči, ki torej nezavedno pridobiva na veljavi tudi v preučevanih organizacijah in ima lahko neposredne varnostne poseldice za posameznika ali družbo.

Grožnje varnosti informacijsko-komunikacijski infrastrukturi od vseh pristojnih akterjev zahtevajo nenehno pozornost pri načrtovanju zaščite te vedno vitalnejše infrastrukture. Sklep o določitvi gospodarskih družb, zavodov in drugih organizacij, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji združuje nekatere najpomembnejše organizacije, ki slovenski družbi zagotavljajo dejavnosti, storitve in proizvode ter s tem nemoteno delovanje družbe, gospodarstva in javnega življenja v Republiki Sloveniji. V raziskavi je bilo ugotovljeno, da je v letu 2014 prišlo do posodobitve seznama organizacij, kjer so Pošti slovenije odvzeli status posebnega pomena za obrambo države, Kontroli zračnega prometa Slovenije, UKCMb in Nacionalnemu inštitutu za javno zdravje pa ta status dodelili. Primerno je, da se je seznam organizacij po določenem času osvežil, pomembno pa je omeniti, da se ta skupek organizacij s časom in z razvojem IKT vedno bolj naslanja na njeno uporabo, saj je le ta primerna za hiter in učinkovit nadzor nad sistemi, ki uravnavajo delovanje procesov, tehnologije in infrastrukture za zagotavljanje dejavnosti, storitev in proizvodov teh organizacij. To trditev potrjujejo tudi organizacije posebnega pomena za obrambo države.

Zelo pomembno je zaznavanje virov ogrožanja pri gospodarskih družbah, zavodih in drugih organizacijah posebnega pomena za obrambo države, saj se lahko zgodi, da organizacije določenih groženj ne zaznavajo ali pa jih celo podcenjujejo, kar lahko pripelje do težav na izvedbeni ravni takrat, ko bi se bilo potrebno z grožnjo soočiti. Preučevane organizacije trenutno kot grožnje IKI zaznavajo vdore v IT sisteme in terorizem, organiziran kriminal in kibernetske grožnje, požare, naravne nesreče, izredne razmere, vojne. Kot vidimo gre tukaj za skupek tradicionalnih in sodobnejših groženj, vse pa so enako pomembne, čeprav so npr. naravne nesreče v očeh organizacij verjetnejše od vseh drugih.

Ko govorimo o akterjih in sami omrežni varnosti je potrebno opozoriti, da se je zaradi uporabe vedno bolj prefinjene (sofisticirane) IKT opreme, samostojno ali kot sestavni del večjega sistema, spremenilo tudi oblikovanje politik v mednarodni skupnosti, ki se predvsem trudi držati tempo z razvojem tehnologije. Poleg omenjenih akterjev ogrožanja omrežne varnosti lahko omenimo še (tradicionalne) akterje ogrožanja IKT, ki lahko ogrozijo IKI na tradicionalen, konvencionalen način ali s fizičnim uničenjem IKI, kar ima za posledico nedelovanje celotnega sektorja IKT. EU na prvo mesto postavlja teroriste oz. teroristične grožnje IK varnosti, ki so lahko tradicionalno konvencionalne ali kibernetske. Temeljne pravice, demokracijo in pravno državo je potrebno varovati tudi v kibernetskem prostoru. Da

bi slednji lahko ostal odprt in svoboden, bi morali na spletu veljati isti predpisi, načela in vrednote, ki jih EU promovira v ne-spletnem okolju. Kot vidimo se percepcija virov ogrožanja v EU in v organizacijah, katerih dejavnost je posebnega pomena za obrambo države, ne razlikuje preveč. Terorizem in teroristične grožnje IK varnosti oboji pojmujejo kot pomembne.

Pri zaznavanju virov ogrožanja je najprej potreben konsenz o oblikovanju kriterijev ogroženosti pri čemer morajo sodelovati vsi akterji tako organizacije posebnega pomena za obrambo države kot sistemski odločevalci, ki morajo upoštevati in oceniti mednarodno varnostno okolje, prepoznati grožnje in priložnosti ter upoštevati razvoj tehnologije in zmogljivosti. Na podlagi tega morajo doseči dogovor o oblikovanju kriterijev za ocenjevanje ogroženosti IKI na nacionalnem nivoju, s čimer bi zagotovili poenoteno dojemanje groženj in odzivanje nanje. Trenutno pri zaščiti IKI v organizacijah, katerih dejavnost je posebnega pomena za obrambo države, še nismo dosegli te želene ravni. Kibernetski napadi pa postajajo vse pogostejši, uspešnejši, bolj predrzni, tehnično dovršeni in uničujoči, čeprav jih v Republiki Sloveniji uradno še nismo zaznali. Kljub naštetemu si nekateri še vedno zatiskajo oči pred omenjenimi napadi iz kibernetskega prostora.

Kibernetska kriminaliteta se na splošno nanaša na vrsto različnih kriminalnih dejavnosti, pri katerih so računalniki in informacijski sistemi osnovno orodje ali glavna tarča.

Tudi NATO se ves čas prilagaja novi vrsti varnostnih izzivov. Za razliko od EU se ukvarja z ogrožanjem omrežne varnosti predvsem na vojaško-politični ravni. Nov strateški koncept Nata opozarja, da so kibernetski napadi vse pogostejši, bolj organizirani in dražji, kar se tiče odpravljanja njihovih posledic. Predvsem se kibernetske grožnje nanašajo na ogrožanje varnosti in vpliv na vladne ustanove, gospodarstvo, posledično pa lahko prizadenejo tudi transportne in oskrbovalne mreže ter tudi kritično infrastrukturo. Tovrstni napadi ogrožajo evro-atlantsko blaginjo, rast, varnost in stabilnost. V konceptu je tudi opredeljeno, da lahko napadi izvirajo tudi od tujih vojaških, obveščevalnih struktur, organiziranega kriminala, terorističnih in ekstremističnih skupin (*Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization 2010*).

Gospodarske družbe, zavodi in druge organizacije, katerih dejavnost je posebnega pomena za obrambo v Republiki Slovenij se mnogokrat zgledujejo po nadnacionalnih konceptih in usmeritvah, katere potem upoštevajo v svojih dokumentih načrtovanja zaščite lastne pomembne infrastrukture. Glede na to, da se premiki pri načrtovanju zaščite dogajajo v logičnem sosledju sprejemanja odločitev na nadnacionalni ravni, kateri sledi prenos na nacionalno raven in nato v praktično implementacijo v omenjenih organizacijah, lahko

sklepamo, da motivi za načrtovanje zaščite IKI ne prihajajo od znotraj, pač pa od zunaj. Upamo lahko, da bodo v bodoče motivi prihajali od organizacij, saj jim mora biti v interesu ščititi lastno infrastrukturo. Trenutno se organizacije, katerih dejavnost je posebnega pomena za obrambo države ne čutijo toliko ogrožene, da bi bile nenehno motivirane iskati sistemske rešitve.

Zakonodaja je v Republiki Sloveniji do določene stopnje primerno razvita, čeprav izkazuje posamezne pomanjkljivosti. Na področju obrambnega planiranja in načrtovanja zaščite IKI je v RS sprejetih več aktov, ki sistemsko urejajo zaščito interaktivnega prostora: Resolucija o strategiji nacionalne varnosti iz leta 2010, Zakon o obrambi, Zakon o tajnih podatkih, Zakon o elektronskih komunikacijah, Uredba o obrambnem planiranju, Uredba o varovanju tajnih podatkov, Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, Uredba o obveznem organiziranju varovanja, Sklep o določitvi pogojev za varnostno-tehnično opremo, ki se sme vgrajevati v varnostna območja. Kot vidimo obstaja množica dokumentov med katerimi je kopica splošnih in univerzalnih, malo pa se jih specifično nanaša na informacijsko-komunikacijsko oz. kibernetsko varnost. Kot najbolj specifične normativne akte in sistemske rešitve lahko navedemo Zakon o elektronskih komunikacijah, Uredbo o obrambnem planiranju, Uredbo o varovanju tajnih podatkov, Uredbo o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih, Uredbo o obveznem organiziranju varovanja, Sklep o določitvi pogojev za varnostno-tehnično opremo, ki se sme vgrajevati v varnostna območja ter nastajajočo Strategijo o kibernetski varnosti.

S tem je tudi RS začela postavljati v ospredje kibernetske grožnje varnosti. Kot je navedeno v dokumentu je vizija strategije vzpostavitev celovitega sistema zagotavljanja kibernetske varnosti, ki kot pomemben integralni dejavnik nacionalne varnosti zagotavlja odprt, varen in varovan kibernetski prostor ter s tem podporo ključnim funkcijam države, osnovo za konkurenčno gospodarstvo ter blaginjo posameznikov in celotne družbe. V strategiji je tudi začrtana smer razvoja načrtovanja sistema varnosti in zaščite informacijsko-komunikacijskih sistemov, od katerih so nekateri neločljivi del kritične informacijsko komunikacijske infrastrukture.

Koncept obrambnega planiranja je zapuščina sistema civilne obrambe, ki se je uspešno prilagodil novodobnim izzivom in na podlagi katerega RS trenutno razvija obrambne sposobnosti organizacij, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji. Nauk tega je, da se pozitivnih zgodb iz preteklosti ni potrebno otepati, pač pa jih je potrebno prilagoditi sodobnemu času in jih primerno koncipirati za delovanje danes in tudi jutri.

Rado se zgodi, da so preučevane organizacije prepuščene lastni kreativi pri načrtovanju zaščite IKI, kot se je to zgodilo v primeru UKCLj pri omejitvi dostopa do osebnih podatkov bolnikov.

Dojemanje groženj v organizacijah posebnega pomena za obrambo države je različno in predvsem odvisno od dejavnosti, s katero se te organizacije ukvarjajo. Skozi raziskavo je bilo ugotovljeno, da organizacije posebnega pomena za obrambo države največjo pozornost posvečajo kibernetskim grožnjam, kljub temu, da so najverjetnejše grožnje v obliki naravnih nesreč.

Kot lahko vidimo, nadnacionalne organizacije, kot sta EU in NATO vse bolj v ospredje postavljajo kibernetske grožnje varnosti, zato v ospredje te grožnje postavlja tudi RS. Posledično kibernetskim grožnjam varnosti veliko pozornost namenjajo tudi gospodarske družbe, zavodi in druge organizacije, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji, saj to od njih zahtevajo odločevalski akterji (MORS), pri oblikovanju načrtovanja zaščite oz. bolj konkretno pri samih načrtih zaščite. Ker so načrti strateškega pomena za te organizacije, dostop do jih seveda ni možen. Iz odgovorov anketirancev pa lahko sklepamo o zgoraj napisanem. Torej s tem lahko potrdiva najino prvo hipotezo.

Ogroženost IKI v organizacijah posebnega pomena za obrambo države je posledica več dejavnikov, pri tem je najpomembneje zaznati in identificirati grožnje, da lahko pripravimo sistemske in tehnične rešitve.

Ključna grožnja je pomanjkanje usposobljenih kadrov, ki razumejo in vzdržujejo IKT. Drugače so grožnje bolj fizične, obstajajo pa tudi nenamerne grožnje, kot rezultat proizvodov. Pri IKT je problem testiranja in vse krajših razvojnih ciklov novih tehnologij. Ciklusi razvoja se zelo krajšajo. Testna faza se krči, celo preskakuje, kriteriji se nižajo zaradi pritiska trgov, uporabniki so se sprijaznili z razmeroma veliko nezanesljivostjo informacijskih in komunikacijskih sistemov. Tudi simulacije v laboratorijih ne odražajo vedno realnega časa. Grožnje pa so seveda tudi namerne. Vsak, ki je priključen na omrežje, je že s tem ogrožen, saj je nevede uporabnik konepta interneta reči. Rešitev je samo v popolnoma ločenem omrežju oziroma celo v analognih oblikah podatkov, kajti po nekaterih informacijah naj bi bilo mogoče prestreči vse elektronske oziroma električne signale, pa naj so povezani v omrežja ali pa ne.

Ko govorimo o popolnoma ločenih omrežji so izsledki raziskave pokazali, da obstajajo popolnoma ločena komunikacijsko-informacijska omrežja med organizacijami posebnega pomena za obrambo države in sistemskimi odločevalci (MORS oz. NCKU). Tako govorimo o več tovrstnih sistemih kot so VEP (Varna elektronska pošta), MKSID (Medresorni

komunikacijski sistem ob izrednih dogodkih). Obe povezavi sta namenjeni komuniciranju v izrednih razmerah, preverjanje povezave je najmanj tedensko. Povezava je nameščena v varnostnem območju II. stopnje, z njo pa lahko v organizaciji, katere dejavnost je posebnega pomena za obrambo države, rokujeta po večini 2 uslužbenca, ki imata dostop do tajnih podatkov stopnje tajnosti najmanj zaupno. Obstaja tudi sistem ISPO (Informacijski sistem za podporo pri odločanju v kriznem upravljanju v RS), uporabljajo ga tudi organizacije posebnega pomena za obrambo države. Sam NCKU ima določeno stalno ekipo, ki na nacionalnem oz. makro nivoju podpira izvajanje in načrtovanje zaščite IKI v organizacijah posebnega pomena za obrambo države.

Ko je govora o odzivanju na grožnje trenutno v RS poznamo tri stopnje ogroženosti IKI: nizko, srednjo, visoko. V primerih nizkega ogrožanja IKI se težave večinoma rešujejo interno, šele v srednji in visoki stopnji ogroženosti se ob različnih grožnjah vključijo različni varnostni akterji: gasilci, Policija, SI–CERT, Civilna zaščita. Izjema so le teroristični napadi in organiziran kriminal, kjer se že ob nizki stopnji ogroženosti vključi v reševanje Policija. V našem primeru bi večjo vlogo moral imeti nacionalni organ za odkrivanje in reševanje kibernetskih in omrežnih groženj SI–CERT, ki bi v sodelovanju s Policijo tovrstne grožnje moral preprečevati. Stanje na področju zaščite IKI se bo predvidoma izboljšalo z uveljavitvijo Strategije kibernetske varnosti (trenutno v oblikovanju in sprejemanju) in z oblikovanjem Nacionalnega organa za kibernetsko varnost, ki bo pod seboj združeval tudi Gov.Cert (javna uprava, SI–CERT in Mors.Cert (obrambni sistem).

Trenutno najbolj ogroženi sistemi IKI v organizacijah, katerih dejavnost je posebnega pomena za obrambo države, so njihovi telekomunikacijski objekti in omrežja. Predvsem so občutljivi na fizične oblike ogrožanja, kot so terorizem, sabotaže ali naravne nesreče. Seveda so popolnoma odvisni tudi od električnega omrežja, kajti ob njegovem izpadu je onemogočeno tudi delovanje telekomunikacijske infrastrukture. Občutljivi so na vdore, tako fizične kot programske oziroma virtualne. Sicer Telekom v primeru naravnih nesreč že lahko zagotovi obhodne poti oziroma nadomestne povezave. Veliko težavo bi pomenili simultani teroristični napadi na več točkah hkrati. Če bi prišlo do napada tako direktnih kot obhodnih poti, ni nobenega operaterja, ki bi to lahko zaščitil. Velika grožnja je seveda tudi uničenje komunikacijskega centra oziroma obeh glavnih central Telekoma Slovenije in inštituti ter klinike UKCLj na Zaloški cesti 2 in 7.

Zaščita IKI se začne na sistemski ravni najvišjih državnih odločevalcev, ki s svojim znanjem, proaktivnostjo in zanosom ter delom oblikujejo sistemske rešitve, ki vplivajo na načrtovanje zaščite celotnega sistema IKI v organizacijah posebnega pomena za obrambo

države. Načrtovanje se začne na najnižji, mikro ravni – pri posamezniku, ki s pomočjo navodil, usmeritev, zakonodaje in znanja oblikuje predloge za oblikovanje sistemskih rešitev načrtovanja zaščite IKI. Posamezniki se združujejo v delovne skupine, odgovorne za določena področja, delovne skupine so lahko organizirane v oddelke in naprej v sektorje, ki podajajo predloge rešitev načrtovanja zaščite določenih sistemov in infrastrukture v obravnavo in sprejem najvišjim državnim odločevalcem.

Če se osredotočimo na organizacije, katerih dejavnost je posebnega pomena za obrambo države lahko zatrdimo, da se organizacije same dosti angažirajo pri načrtovanju zaščite lastnih sistemov IKI, so pa omejeni z zakonodajo, ki jo oblikujejo na različnih ravneh državni odločevalci – ministrstva.

Strategija kibernetske varnosti je v omenjenih organizacijah postala ključna za zagotavljanje dejavnosti, storitev in proizvodov, kot jih pričakuje družba in država v primerih ogrožanja njihove lastne IKI. Ugotovljeno je bilo, da je večina preučevanih subjektov v veliki meri odvisna od delovanja IKI, pa najsi gre za infrastrukturo, ki upravlja z dobavo energentov, z naročanjem bolnikov na preiskave, samosklicem zdravnikov, zagotavljanjem spleta in storitev, krmilnimi sistemi železnic in pristanišč idr. IKI je postala za te organizacije ključna tudi za pridobivanje poslov ali opravljanje osnovnega poslanstva služenja družbi in jo zato vsaj znotraj skupine organizacij, katerih dejavnost je posebnega pomena za obrambo v RS, opredelimo kot KIKI, če ne že na ravni celotne države.

S tem lahko potrdiva najino drugo hipotezo, ki pravi, da je primarna dejavnost gospodarskih družb, zavodov in drugih organizacij posebnega pomena za obrambo RS v veliki meri odvisna od IKI, zato lahko slednjo opredelimo kot ključno/kritično IKI (KIKI). V tem primer ne gre za opredeljevanje izključno objektov kot kritičnih pač pa gre tukaj za opredeljevanje dejavnosti, storitev in proizvodov kot kritičnih. Za podkrepitev trditve navedimo posledice Žleda 2014, ko so bile za več dni motene IK storitve in oskrba z energijo na večini zahodne polovice države, posledice pa je najbolj občutilo (in jih čuti še danes) podjetje Slovenske železnice d.o.o.

Debata ali lahko IKI opredelimo kot KIKI na nacionalnem nivoju je namenjena diskurzu ob upoštevanju na novo sprejetih sektorjev kritične infrastrukture v RS in sektorskih kriterijev kritičnosti v RS, kar je lahko predmet popolnoma nove, interne in neodvisne raziskave, s katero bi dobili vpogled v to, ali je (IK) infrastruktura gospodarskih družb, zavodov in drugih organizacij, katerih dejavnost je posebnega pomena za obrambo države, dejansko opredeljena kot kritična infrastruktura v Republiki Sloveniji. Za to je v RS primeren čas, saj se ravno zdaj EU in NATO.

Z Direktivo o določitvi EKI iz leta 2008 je EU Sloveniji naložila opredelitev kritične infrastrukture v RS. Čeprav se je RS že dalj časa zavedala naraščajoče pomena koncepta kritične infrastrukture v Evropi, je bilo potrebno dalj časa in mednarodne, zunanje usmeritve, da smo bili zmožni oblikovati kriterije za določanje kritičnosti infrastrukture in opredeliti kritično infrastrukturo v RS, kar se je zgodilo v letu 2014.

Impulzi, ki so pospešili razvoj oblikovanja sistemskih (proti)ukrepov za ogrožanje IKI je bilo samospoznanje, da je tovrstna infrastruktura ključna za normalno delovanje države, družbe in organizacij, katerih dejavnost je posebnega pomena za obrambo države. Te organizacije in njihova večja vloga pri obrambnem planiranju, oblikovanju obrambnih načrtov in načrtov zaščite izhaja še iz koncepta civilne obrambe in še prej splošne ljudske obrambe in družbene samozaščite, ko je bila nekaterim podjetjem, zavodom in drugim organizacijam naložena večja družbena odgovornost ob pojavu različnih groženj. Koncept civilne obrambe in z njim obstoja nekaterih organizacij s privilegiranim statusom v smislu večje družbene odgovornosti je namenjen državljanom in njihovem blagostanju v času kriz in ni zato nič slabega. Potrebno je le slediti duhu časa in ga prilagajati vedno spreminjajoči se družbeni pogodbi in grožnjam, ki mutirajo, se spreminjajo in rojevajo v novih oblikah.

Današnje grožnje so različne, sodobne in tradicionalne, so manj ali bolj intenzivne in zato od gospodarskih družb, zavodov in drugih organizacij, katerih dejavnost je posebnega pomena za obrambo v RS, zahtevajo, da v zaščito in njeno načrtovanje vključujejo različne varnostne akterje, javne in zasebne. Kljub vsemu so najverjetnejše grožnje IKI dandanes v RS naravne idr. nesreče, pomen tradicionalne grožnje kot je vojna tudi ni zmanjšan, največ pa se organizacije posebnega pomena za obrambo države posvečajo kibernetskim grožnjam varnosti, ki imajo lahko večplastne vplive, denarne tokove, javno zdravje, logistiko, preskrbo, komunikacije, splet ipd. Javni varnostni akterji v RS zato pokrivajo širok spekter odkrivanja, preprečevanja in odzivanja na grožnje ter imajo družbeno odgovornost do tovrstnega delovanja, saj so porabniki državnega proračuna in iz njega plačani za opravljanje tovrstnih nalog. Zasebni varnostni akterji pa so visoko specializirani subjekti, katerih vodilo je dobiček. V RS je pri načrtovanju zaščite preučevanih organizacij splošna praksa, da zasebniki opravljajo fizično in tehnično zaščito ter varovanje predvsem prostorov in osebja, za te naloge izdelujejo tudi varnostne načrte, katere lahko izdela licencirani varnostni menedžer. Zaščita in varovanje IKI in kibernetskega prostora pa je, zaradi verjetnega rokovanja s tajnimi podatki, večinoma v domeni notranjih varnostnih služb in pristojnih odgovornih posameznikov ter državnih organov (Policija, varnostne službe, SI–CERT, pogojno NCKU in SV). Odzivanje na naravne in druge nesreče je nedvomno še vedno domena državnih organov zaščite in

reševanja kot so Civilna zaščita, gasilci, vojska idr. Vse pristojnosti in naloge so urejene z normativnimi akti, kateri točno opredeljujejo pristojnosti in naloge različnih varnostnih akterjev, ob različnih vrstah ogrožanj.

In glede na to, da na področju zaščite IKI obstaja javno-zasebno partnerstvo samo do določene mere, lahko sklepamo o velikem pomenu IKI za delovanje organizacij, katerih dejavnost je posebnega pomena za obrambo države. V tem primeru nedvomno obstaja srednja do visoka odvisnost organizacije od delovanja IKI. Po drugi strani pa pri sistemskih odločevalcih ostaja prepričanje, da ne obstaja nikakršna odvisnost delovanja IKI od nemotenega delovanja organizacij posebnega pomena za obrambo države. Nasprotnega mnenja so v organizacijah posebnega pomena za obrambo države, kjer trdijo, da v tem primeru prav tako obstaja velika odvisnost.

Z navedenim sva dokazala, da različne vrste groženj in njihova intenziteta od gospodarskih družb, zavodov in drugih organizacij, katerih dejavnost je posebnega pomena za obrambo v RS nedvomno zahtevajo, da pri načrtovanju zaščite (tudi IKI) vključujejo različne varnostne akterje, javne in zasebne, v okviru pristojnosti, znanja in sposobnosti ter zakonodaje. Na tej točki lahko govorimo o zametkih javno-zasebnega partnerstva, težava je le o kakšni vrsti in do katere stopnje. Primernejše poimenovanje tega bi bil javno-zasebni odnos v primeru načrtovanja zaščite IKI organizacij posebnega pomena za obrambo države.

Namen najine naloge je bil tudi podati predloge za bodoče urejanje področja načrtovanja zaščite IKI v RS. Najpomembnejše je stalno ocenjevanje ogrožanja varnosti in sledenje trendom ogrožanja varnosti. Predvsem pa je pomembno, da se uvede skupen pristop do omenjenega področja načrtovanja in se vse zakonodajne dokumente iz področja informacijske varnosti združi v en krovni dokument, ki bo v pomoč tako odločevalcem kot organizacijam, katerih dejavnost je ključnega pomena za obrambo države. Korak naprej bi bilo že poenotenje kriterijev ogroženosti IK in druge infrastrukture omenjenih organizacij na ravni države. Čeprav se akterji trudijo držati korak z razvojem ukrepov zaščite IKT, prihaja do zaostankov pri načrtovanju zaščite. Pomanjkljiva (včasih pa preobsežna in nerazumljiva) dokumentacija, nedorečenost postopkov, dolžnosti ter omrežnih politik, povzroča dodatne ranljivosti v sistemih kritične infrastrukture. Z vključevanjem standarda ISO 27001 v načrtovanje zaščite se zmanjšujejo vplivi ranljivosti na preučevano infrastrukturo. Večjo pozornost bi morali nameniti tudi mikro ravni analize vzrokov kriz; človeškim napakam, saj je najbolj kritičen člen v verigi zagotavljanja učinkovite informacijske varnosti je še vedno človek, bodisi s svojo namerno ali nenamerno dejavnostjo.

8 LITERATURA

Amies, Nick. 2010. NATO includes threat of cyber atteck in new strategic concept document. *Deutsche Welle*, 14. oktober. Dostopno prek: http://www.dw-world.de/dw/article/0,,6072197,00.html (25. september 2011).

Aradau, Claudia. 2010. Security that Matters: Critical infrastructure and Objects of Protection. *Security Dialogue* 41: 491.

Aron, R. 1954. *The Century of Total War*. Garden City: Doubleday.

Auerswald, Philip, Lewis Branscomb, Tod La Porte in Erwann Michel-Kerjan. 2005. The Challenge of Protecting Critical Infrastructure. *Issues in Science and Technology*, Fall.

Biščak, Bogdan. 2011. Intervju z Maržun in Karničar. Ljubljana, 6. december.

Boin Arjen, Mark Rhinard in Magnus Ekengren. 2007. *Institutionalizing Homeland Security Cooperation in Europe: Counter-terrorism and Critical Infrastructure Protection Compared.* Panel 19-14: European Responses to "New" Security Threats: The Role of the European Union.

Bukinac, Zorica. 1996. *Metoda simulacijskih iger v obrambni politiki: Oblike in rabe simulacijskih iger za podporo odločanju, izobraževanju in usposabljanju*. Ljubljana: MORS.

Buzan Barry, Ole Wæver in Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. London: Lynne Rienner Publishers, Inc.

Carr, Jeffrey, 2009. *Inside Cyber Warfare*. Sebastopol: O'Reilly Media Inc.

CCDCOE. 2014. *Locked Shields*. Dostopno prek: https://ccdcoe.org/locked-shields-2014.html (14. december 2014).

Cestnik, Alojz. 2013. *1. vprašalnik – Organizacije posebnega pomena za obrambo države.* Ljubljana, 16. september 2013.

--- 2014. *2. vprašalnik – Organizacije posebnega pomena za obrambo države.* Ljubljana, 28. julij 2014.

Coward, Martin. 2009. Network-Centric Violence, Critical Infrastructure and the Urbanization of Security. *Security Dialogue* 40: 399.

Čaleta, Denis in Gorazd Rolih. 2011. Kibernetska varnost v družbi in delovanje kritične infrastrukture – Analiza stanja na obrambnem področju v Republiki Sloveniji. *Sodobni vojaški izzivi* 13 (3): 3–20.

Čarni, Alenka in Romeo Palčič. 2014. *2. vprašalnik – Organizacije posebnega pomena za obrambo države – Ministrstva*. Ljubljana, 22. avgust 2014.

Čarni, Alenka. 2014. *E-poštno dopisovanje o organizacijah, katerih dejavnost je posebnega pomena za obrambo države*. Ljubljana, 28. julij 2014.

Definicija kritične infrastrukture, sklep Vlade RS št. 80000-2/2010/3, z dne 19. 4. 2010. Dostopno prek: http://www.mo.gov.si/si/delovna_podrocja/zascita_kriticne_infrastrukture/ (10. november 2014).

Deibert, Ronald in Rafal Rohozinski. 2008. Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet. V *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge: MIT Press.

Detektivska agencija Satja 2014, *Informacijska varnost*. Dostopno prek: http://www.detektivska-agencija-satja.com/index.html (14. december 2014).

Direktiva Sveta (ES) o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite. Št. 114/2008, z dne 8. decembra 2008. Dostopno prek http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/zki/DirektivaEU_114_ULEU2312 2008_slo.PDF (1. januar 2015).

Dokl, Jure. 2012. *Kibernetska varnost omrežij*. Magistrsko delo. Ljubljana: FDV.

Dunn, Myriam. 2005. The Socio-political Dimension of Critical Information Infrastructure Protection. *International Journal of Critical Infrastructures* 1 (2/3).

Egan, Mark. 2005. *Varnost informacij: grožnje, izzivi in rešitve: vodnik za podjetja*. Ljubljana: Pasadena.

Eles. Predstavitev družbe. Dostopno prek: http://www.eles.si/predstavitev-druzbe.aspx (3. januar 2014).

eMarketer. 2014. *Internet to Hit 3 Billin Users in 2015*. Dostopno prek: http://www.emarketer.com/Article/Internet-Hit-3-Billion-Users-2015/1011602 (14. december 2014).

Evropska komisija. 2004. *Zelena knjiga o javno zasebnih partnerstvih in o zakonodaji Skupnosti o javnih naročilih in koncesijah*. 30. 04. 2004–COM (2004) 327 final.

---. 2005. *Zelena knjiga o evropskem programu za varovanje ključne infrastrukture.* COM (2005) 576. Dostopno prek: http://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:52005DC0576&from=EN (14. december 2014).

Feiler, Lucas. 2011. Outages of Critical Information Infrastructure under EU and US LAw--transparency versus Secrecy. *Journal of Internet Law* 15 (3).

Flere, Sergej. 2000. *Sociološka metodologija: temelji družboslovnega raziskovanja*. Maribor: Pedagoška fakulteta.

Furlan, Branimir. 2006. *Vojaška doktrina*. Ljubljana: MORS, PDRIU.

Grošelj, Klemen. 2007. *Slovenija v svetu mirovnih operacij*. Ljubljana: FDV.

Harvey, Andrew in Conor Mullan. 2003. *Best Practices In the Development of Simulation Scenarios For Validation Activities in Fast and Real-Time Simulation*. EUROCONTROL Reserch Centre. Dostopno prek: http://www.tc.faa.gov/acb300/ ap5_workshops/documents/AP5_report_v05_Final_112003.pdf (15. november 2011).

Hellstrom, Tomas. 2006. Critical Infrastructure and Systemic Vulnerability. Towards a Planning Framework. *Safety Science*.

Hyeung-Sik J. Min, Walter Beyeler, Theresa Brown, Young Jun Son in Albert T Jones. 2005. Toward modeling and simulation of critical national infrastructure interdependencies. *IIE Transactions* 39: 57–71.

Weber, Rolf .2010. Internet of things – New security and privacy challenges. *Science Direct* 26 (1): 23–30. Dostopno prek: http://www.sciencedirect.com/science/article/pii/S0267364909001939 (1. februar 2014).

Techopedia. 2014. *Internet of Things (IoT)*. Dostopno prek: http://www.techopedia.com/definition/28247/internet-of-things-iot (01. februar 2014).

DeLoach, Don. 2014. *Internet of things Part 3: Critical Security Issues for the Internet of Things*. 2014. Dostopno prek: https://www.infobright.com/index.php/ceo-blog-critical-security-issues-for-the-internet-of-things/#.VM5jSSzfQgs (01. februar 2014).

Koštrun, Matjaž. 2007. *Načrtovanje vojaških zmogljivosti Republike Slovenije za krizno odzivanje.* Diplomsko delo. Ljubljana: FDV.

Le Grand, Gwendal, Franck Springinsfeld in Michel Riguidel. 2003. Slika: Hierarhija infrastruktur v povezavi z analitičnimi metodami in perspektivami. V *Definicija in zaščita kritične infrastrukture Republike Slovenije: raziskovalni projekt: končno raziskovalno poročilo*, 21. Ljubljana: FDV, Obramboslovni raziskovalni center.

Lewis, Ted G. 2006. *Critical Infrastructure Protection in Homeland Security (Defending a Networked Nation).* New Jersey: John Wiley&Sons, Inc.

Loborec, Igor. 2013. Ljubljana. *1. vprašalnik – Organizacije posebnega pomena za obrambo države.* Ljubljana, 16. oktober 2013.

Longstaff, T., A., Chittister, C., Pethia, R., Haimes, Y. Y. 2000. Are we forgetting the risk

Lukman, Miloš in Igor Bernik. 2009. *Ogrožanja kritične infrastrukture iz kibernetskega prostora. Zbornik*. Dnevi varstvoslovja 2009. Dostopno prek: http://www.fvv.uni-mb.si/dv2009/Zbornik/clanki/lukman.pdf (5. april 2012).

Malešič, Marjan, ur. 2004. *Krizno upravljanje in vodenje v Sloveniji: izzivi in priložnosti.* Ljubljana: FDV.

Maria, Anu. 1997. *Introduction to modeling and simulation*. State University of New York at Binghamton: Binghamton.

Marinčič, Dušan. 2005. *Simulacija in analiza mirovne operacije*. Doktorska disertacija. Ljubljana: FDV.

--- 2008. Operacije kriznega odzivanja: Računalniška simulacija. *Revija Obramba* 40 (2).

Markulec, M. 2008. SCADA Systems: Unknown Connections Could Spell Trouble. *Power*

Mesec, Blaž. 2011. *Študija Primera*. *Kvalitativna metodologija, akcijsko in evalvacijsko raziskovanje - arhiv dr. Blaža Meseca*. Dostopno prek: https://sites.google.com/site/kvalitativnametodologija/kvalitativna-metodologija/studija-primera (14. december. 2014).

Michel-Kerjan, Erwan. 2003. New Challenges in Critical Infrastructures: A US Perspective. *Journal of Contingencies and Crisis Management* 11 (3).

Ministrstvo za infrastrukturo, Informacijski portal energetika. 2014. Dostopno prek: http://www.energetika-portal.si/novica/arhiv/2012/10/n/vlada-potrdila-kriterije-za-dolocitev-kriticne-infrastrukture-drzavnega-pomena-v-republiki-sloven/ (3. januar 2015).

Mišmaš, Aleš. 2014. *Obrambno planiranje v Ministrstvu za obrambo RS*. Dostopno prek: http://studentski.net/gradivo/ulj_fdv_po1_obm_sno_obrambno_planiranje_01?r=1 (12. december 2014).

MORS. 1996. *Sklep o določitvi gospodarskih družb, zavodov in drugih organizacij, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji* (Sklep št. 311-21/95-3/3-8) z dne 16. maja 1996.

--- 2014a. *Sklep o določitvi gospodarskih družb, zavodov in drugih organizacij, katerih dejavnost je posebnega pomena za obrambo v Republiki Sloveniji* (Sklep št. 80101-1/2014/5) z dne 17. april 2014.

--- 2014b. *Veljavni kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena.* Dostopno prek: http://www.mo.gov.si/si/delovna_podrocja/zascita_kriticne_infrastrukture/ (10. november 2014).

---, Medresorska koordinacijska skupina za usklajevanje priprav za zaščito kritične infrastrukture. 2015. Dostopno prek:

http://www.mo.gov.si/si/delovna_podrocja/zascita_kriticne_infrastrukture/medresorska_koordinacijska_skupina_za_usklajevanje_priprav_za_zascito_kriticne_infrastrukture/ (3. januar 2015).

---, Omrežje za opozarjanje o ogroženosti kritične infrastrukture. 2015. Dostopno prek: http://www.mo.gov.si/si/delovna_podrocja/zascita_kriticne_infrastrukture/omrezje_za_opozarjanje_o_ogrozenosti_kriticne_infrastrukture/ (3. januar 2015).

Moj Mikro. 2014. *Strategija kibernetske varnosti*. Dostopno prek: http://www.mojmikro.si/news/strategija_kibernetske_varnosti (13. oktober 2014).

Načrt kibernetske varnosti EU za zaščito odprtega interneta ter svobode in priložnosti na spletu. Dostopno prek: http://europa.eu/rapid/press-release_IP-13-94_sl.htm (20. avgust 2014).

NATO Requests Cyber Security Cooperation From India. Dostopno prek: http://ictps.blogspot.com/2011/09/nato-requests-cyber-security.html (19. april 2012).

Navodila za operativno načrtovanje (GOP) Rev 1. Koordinirani osnutek 2004.

Navodilo za štabno delo. Osnutek. 2007.

Obrambna strategija 2012. Vlada RS, št. 80000-1/4 z dne 7.12.2012. Dostopno prek: http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/javne_objave/2012/obr_strategija.pdf (14. december 2014).

Osnovni in sektorski kriteriji kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji, sklep Vlade RS št. 80200-1/2012/5, z dne 17. 10. 2012. Dostopno prek: http://www.mo.gov.si/si/delovna_podrocja/zascita_kriticne_infrastrukture/ (10. november 2014).

Pederson P., D. Dudenhoeffer, S. Hartley in M. Permann. 2006. *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. Idaho Falls: Idaho National Laboratory.

Peerenboom, J. 2001. *Infrastructure Interdependencies. Overwievs of Concepts and Terminology*. Infrastructure Assurance Center, Argonne.

Pelaj, Avdulla in Teodora Ivanuša. 2011. Načrtovanje obrambe pred orožjem za množično uničevanje v Sloveniji. *Sodobni vojaški izziv* 13 (1).

PerKlik. 2014. *Kako se spoprijeti z ISO 27001?* Dostopno prek: http://www.perklik.si/?q=node/37 (3. januar 2014).

Pišlar, Marko. 2014. Kibernetska varnost – Globalni izziv prihodnosti. *Slovenska vojska,* 10. Dostopno prek: http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/revija_sv/2014/sv_10_14.pdf (14. december 2014).

Poročilo o omrežni varnosti za leto 2011. Dostopno prek: http://www.varninainternetu.si/content/uploads/2012/03/Letno_porocilo_Arnes_WEB1.pdf (2. april 2012).

Predpisi o obrambi in zaščiti. Ur. l. .RS 1992. Ljubljana: Tiskarna Tone Tomšič.

Preradović, Željko. 2013. *1. vprašalnik – Organizacije posebnega pomena za obrambo države.* Ljubljana, 16. september 2013.

Prezelj, Iztok. 2002. Kompleksno ogrožanje varnosti in nastajanje kompleksnih kriz. V *Nacionalna in mednarodna varnost*, ur. Marjan Malešič, 59–77. Ljubljana: Fakulteta za družbene vede.

Prezelj, Iztok. 2005. *Nacionalni sistemi kriznega menedžmenta*. Ljubljana: FDV.

--- 2007. Uvod v ocenjevanje ogrožanja nacionalne varnosti. V *Model celovitega ocenjevanja ogrožanja nacionalne varnosti Republike Slovenije*, ur. Iztok Prezelj, 7–27. Ljubljana: Ministrstvo za obrambo, Direktorat za obrambne zadeve, Sektor za civilno obrambo.

--- 2008. *Definicija in zaščita kritične infrastrukture Republike Slovenije: raziskovalni projekt: končno raziskovalno poročilo*. Ljubljana: Fakulteta za družbene vede, Obramboslovni raziskovalni center.

--- 2009. Nacionalna kritična infrastruktura v Republiki Sloveniji. *Teorija in praksa.* 46 (4).

--- 2010. *Kritična infrastruktura v Sloveniji*. Ljubljana: Fakulteta za družbene vede.

--- 2010a. O pomenu kritične infrastrukture. V *Kritična infrastruktura v Sloveniji*, ur. Iztok Prezelj, 5–9. Ljubljana: FDV.

--- 2010b. Koncept kritične infrastrukture. V *Kritična infrastruktura v Sloveniji*, ur. Iztok Prezelj, 9–29. Ljubljana: FDV.

Prezelj, Iztok in Simona Kustec Lipicer. 2010c. *Public and Policy Management of Critical Infrastructure: Lessons from Integra National Cross-sectoral Scanning in Slovenia.* IRSPM Conference Berne, Panel: Risk and Crisis Management in the Public Sector.

Priporočila informacijske varnostne politike javne uprave. Dostopno prek: http://www.mnz.gov.si/fileadmin/mnz.gov.si/pageuploads/JAVNA_UPRAVA/DIES/IVPJU_01.pdf (28. maj 2014).

Proposal on European Strategy for Internet Security. Dostopno prek: http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf (16. april 2012).

Radvanovsky, Robert. 2006. *Critical Infrastructure (Homeland Security and Emergency Preparedness)*. New York: Taylor&Francis Group.

Reference. Dostopno prek: http://www.actual.si/?main=2&sub=3 (6. junij 2012).

Resolucija o splošnem dolgoročnem programu opremljanja slovenske vojske do leta 2025 (ReDPRSV25). Ur. l. RS 99/2010. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=201099&stevilka=5106 (25. september 2011).

Resolucija o strategiji nacionalne varnosti Republike Slovenije (ReSNV-1). Ur. l. RS 27/2010. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=201027&stevilka=1189 (25. september 2011).

Rolih, Gorazd. 2011. *Kibernetske grožnje in nacionalna varnost v Republiki Sloveniji*. Zaključna naloga. Maribor: Poveljniško štabna šola.

Rosenthal, Uriel, Arjen R. Boin, in Louise K. Comfort, 2001. *Managing crises: Threats, Dilemmas, Opportunities*. Springfield, Illinois: Charles C. Thomas: Publisher, LTD.

Same, Jasna. 1987. *Obrambno-zaščitna funkcija prostorskega načrtovanja*. Diplomsko delo. Ljubljana: FSPN.

Savšek, Tomaž. 2000. *Sodobni vojaški simulacijski sistemi: operacijske raziskave, vojne igre in vojne simulacije.* Ljubljana: MORS.

Schneier, Bruce. 2000. *Secrets and Lies: Security in a networked World.* New York: John Wiley.

Sektor za načrtovanje MORS. 2013. *1. vprašalnik – Nacionalnovarnostni subjekti o organizacijah posebnega pomena za obrambo države*. Ljubljana, 7. oktober 2013.

SI-CERT. 2012. Dostopno prek: http://www.cert.si/zakonodaja.html (20. junij 2012).

Simčič, Simon. 2007. *Ogrožanje kritične informacijske infrastrukture v Republiki Sloveniji*. Diplomsko delo. Ljubljana: Fakulteta za družbene vede.

Sklep o določitvi pogojev za varnostnotehnično opremo, ki se sme vgrajevati v varnostna območja (Ur. l. RS št. 94/2006) z dne 8. septembra 2006.

Slovar slovenskega knjižnega jezika. Dostopno prek: http://bos.zrc-sazu.si/sskj.html (24. april 2012).

Služba za varnostno načrtovanje MNZ. 2013. *1. vprašalnik – Nacionalnovarnostni subjekti o organizacijah posebnega pomena za obrambo države.* Ljubljana, 16. oktober 2013.

Sotlar, Andrej in Bernarda Tominc. 2014. Zaznava deklarativnih virov ogrožanja nacionalne varnosti v slovenski družbi. *Varstvoslovje* (3): 231–258.

Souček Morača, Hana. Zagotavljanje varnosti, pomoč Nata in ozaveščanje posameznikov. *Slovenska vojska*, 9, september 2014.

Spremembe in dopolnitve osnovnih in sektorskih kriterijev kritičnosti za določanje kritične infrastrukture državnega pomena v Republiki Sloveniji, sklep Vlade RS št. 80200-2/2013/3, z dne 9. 1. 2014. Dostopno prek: http://www.mo.gov.si/si/delovna_podrocja/

zascita_kriticne_infrastrukture/ (11. november 2014).

Srednjeročni obrambni program 2007 – 2012. Dostopno prek: http://www.mo.gov.si/fileadmin/mo.gov.si/pageuploads/pdf/ministrstvo/SOPR_2007-2012_cistopis.pdf (25. maj 2012).

Standard ISO/IEC 27001 - Information technology - Security techniques - Information security management systems – Requirements. 2005. Dostopno prek: http://www.iso27001security.com/html/27001.html (1. oktober 2011).

Statistični urad Republike Slovenije. Uporaba interneta v gospodinjstvih in pri posameznikih, Slovenija, 2014 – končni podatki. Dostopno prek: http://www.stat.si/StatWeb/glavnanavigacija/podatki/prikazistaronovico?IdNovice=6560 (14. december 2014).

Statistični urad Republike Slovenije. Postne storitve in elektronske komunikacijske storitve, Slovenija, 1. četrtletje 2011. Dostopno prek: http://www.stat.si/novica_prikazi.aspx?id=3998 (17. avgust 2011).

Statistični urad Republike Slovenije. Svetovni dan telekomunikacij in informacijske družbe 2011. Dostopno prek: http://www.stat.si/novica_prikazi.aspx?id=3908 (22. avgust 2011).

Strategic Concept for the Defence and Security of the Members of The North Atlantic Treaty Organization. 2010. Dostopno prek: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf (19. april 2012).

Strategija kibernetske varnosti: Vzpostavitev sistema zagotavljanja visokega nivoja kibernetske varnosti. Osnutek, v2.3. avgust 2014. Dostopno prek: http://www.mizs.gov.si/fileadmin/mizs.gov.si/pageuploads/Informacijska_druzba/pdf/Digitalna_Slovenija_2020_29_8_14_Strategija_kib_varnost1.pdf (14. december 2014).

Strategija za kibernetsko varnost Evropske unije „Odprt, varen in zavarovan kibernetski prostor“. 2013. Dostopno prek: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security (20. avgust 2014).

Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana: FDV.

--- 2006. Informacijsko-komunikacijska tehnologija in sodobne varnostne teorije. V Varnost v postmoderni družbi, ur. Marjan Malešič, 47–71. Ljubljana: FDV.

--- 2007a. Informacijsko ogrožanje nacionalne varnosti. V *Model celovitega ocenjevanja ogrožanja nacionalne varnosti Republike Slovenije*, ur. Iztok Prezelj, 27–51. Ljubljana: Ministrstvo za obrambo, Direktorat za obrambne zadeve, Sektor za civilno obrambo.

--- 2007b. Zaščita informacijske infrastrukture v precepu državne varnostne politike. V Pinterič, U., Svete, U. (ur.). *Elektronsko upravljanje in poslovanje v službi uporabnika.* Ljubljana: FDV, 159–176.

--- 2010. Informacijska in komunikacijska kritična infrastruktura. V *Kritična infrastruktura v Sloveniji*, ur. Iztok Prezelj, 43–65. Ljubljana: FDV.

Svete, Uroš, Damijan Guštin in Damir Črnčec. 2011. *Asimetrija in nacionalna varnost: od zgodovinskih izkušenj do sodobnih izzivov*. Ljubljana: Defensor, d.o.o.

Šuligij, Rok. 2011. *Varnostni izzivi in totalna obramba*. Ljubljana. Fakulteta za družbene vede.

Telekom Slovenije. Letno poročilo 2010. Dostopno prek: http://www.telekom.si/_files/866/Letno_porocilo_2010.pdf (19. avgust 2011).

Theiler, Olaf. 2011. Nove grožnje: Kibernetska razsežnost. *Revija Nato*. Dostopno prek: http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/SL/index.htm (14. december 2014).

Udovyk, Oleg. 2007. Risk governance and crisis management in the field of critical infrastructure protection. V *Oblikovanje politik, sistemov in mehanizmov kriznega upravljanja v sodobnih državah*, ur. Iztok Prezelj, 140–55. Ljubljana. Ministrstvo za obrambo, Direktorat za obrambne zadeve, Sektor za civilno obrambo.

Urbanc, Mimi, Drago Perko in Franci Petek. 2008. Prihodnost alp in delfi metoda. *Geografski vestnik* 80 (2): 143–153. Dostopno prek: http://zgs.zrc-sazu.si/Portals/8/Geografski_vestnik/gv80-2-urbancperkopetek.pdf (14. december 2014).

Urad Vlade RS za varovanje tajnih podatkov 2014. *Varnost KIS*. Dostopno prek: http://www.uvtp.gov.si/si/delovna_podrocja/varnost_kis/ (14. december 2014).

Uredba o evropski kritični infrastrukturi. Ur. l RS št. 35/2011(13. maj 2011). Dostopno prek: http://www.uradni-list.si/1/content?id=103668 (14. december 2014).

Uredba o obrambnih načrtih. Ur. l RS št. 11/2004 (6. februar 2004).

Uredba o obveznem organiziranju varovanja. Ur. l. RS št. 80/2012 (3. januar 2014).

Uredba o organizaciji in delovanju Nacionalnega centra za krizno upravljanje. Ur. l. RS št. 9/2006 (26. januar 2006).

Uredba o varovanju tajnih podatkov v komunikacijsko informacijskih sistemih. Ur. l. RS, št. 48/2007 (1. junij 2007).

Uredba o varovanju tajnih podatkov. Ur. l. RS št. 74/2005 (5. avgust 2005).

Uredba o vsebini in izdelavi načrtov zaščite in reševanja. Ur. l. RS, št. 24/2012 (15. junij 2012).

Wikipedia. 2014. *Informacijska varnost*. Dostopno prek: http://sl.wikipedia.org/wiki/Informacijska_varnost (14. december 2014).

Zakon o elektronskih komunikacijah (ZEKom-1). Ur.l. RS št. 109/2012 (31. december 2012).

Zakon o graditvi objektov (ZGO-1). Ur.l. RS št. 110/2002 (18. december 2002).

Zakon o obrambi (ZObr-UPB1). Ur. l. RS, št. 103/2004 (23. september 2004).

Zakon o tajnih podatkih (ZTP-UPB2). Ur. l. RS št. 87/2001. (8. november 2001).

Zakon o varstvu pred naravnimi in drugimi nesrečami. Ur. l. RS, št. 51/2006 (18. maj 2006).

Zaščita kritične infrastrukture. Dostopno prek http://www.mo.gov.si/si/delovna_podrocja/zascita_kriticne_infrastrukture/ (18. december 2014).

Zavezniška združena doktrina za operativno načrtovanje AJP-5. STANAG XXXX. Ratificirani osnutek. 2006.

Žel, Roland. 2011. Intervju z Maržun in Karničar. Ljubljana, 7. december.

PRILOGA

Priloga: Objekti z določenimi obrambnimi potrebami

Objekti, pri katerih je treba pri projektiranju in graditvi upoštevati prilagoditve potrebam obrambe, so:

1. prometni objekti in naprave:

– glavne železniške proge I. in II. reda in regionalne železniške proge,

– državne ceste in spremljajoči objekti na njih, kot so predori, viadukti, mostovi, podvozi, nadvozi, podhodi in drugi podobni objekti, daljši kot 20 m,

– letališča in vzletišča s pripadajočimi objekti,

– pristanišča z globino vode več kot 2 m,

– javno telekomunikacijsko omrežje,

– objekti in stacionarne naprave javnega radiodifuznega in televizijskega sistema,

– navigacijski sistemi in objekti, namenjeni za navigacijo v pomorskem in zračnem prometu;

2. energetski objekti in naprave:

– daljnovodi za napetost 110 kV in več ter razdelilne in transformatorske postaje na teh daljnovodih,

– cevovodi in pripadajoče naprave za transport nafte, naftnih derivatov, plina in kemikalij s premerom 300 mm in več,

– skladišča nafte in naftnih derivatov zmogljivosti več kot 1000 m3;

3. vodnogospodarski objekti, naprave in posegi:

– vodni zbiralniki nad 100.000 m3 vsebine,

– nasipi ali utrditve morske obale v dolžini 200 m ali več,

– regulacije večjih vodotokov celinskih voda 1. reda;

4. drugi objekti, kot so:

– objekti in naprave za proizvodnjo in skladiščenje eksplozivnih sredstev, razen pirotehničnih izdelkov,

– skladišča vnetljivih tekočin s kapaciteto 250 m3 in več,

– rezervoarji z napravami za polnjenje in praznjenje gorljivih, strupenih in zdravju škodljivih plinov, s prostornino posameznega rezervoarja nad 100 m3,

– objekti in naprave za pridobivanje, predelavo in skladiščenje radioaktivnih snovi in z izvori ionizirajočega sevanja,

– objekti in naprave za ravnanje z odpadki, ki vsebujejo nevarne snovi, s kapaciteto 1000 t letno ali več,
– objekti, katerih višina nad terenom presega 42 m ter objekti izven območja naselja, katerih višina nad terenom presega 18 m;
5. skladišča, silosi in hladilnice za živila ter skladišča za državne blagovne rezerve z zmogljivostjo več kot 600 m3.