UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Janja Štucin

Uporaba informacijsko - komunikacijske tehnologije v okviru kriznega komuniciranja ob naravnih in drugih nesrečah

Diplomsko delo

Ljubljana, 2010

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Janja Štucin
Mentor: doc. dr. Uroš Svete

Uporaba informacijsko - komunikacijske tehnologije v okviru kriznega komuniciranja ob naravnih in drugih nesrečah

Diplomsko delo

Ljubljana, 2010

ZAHVALA

Zahvaljujem se staršem in mentorju
za potrpežljivost in pomoč pri nastajanju diplomskega dela!

Uporaba informacijsko-komunikacijske tehnologije v okviru kriznega komuniciranja ob naravnih in drugih nesrečah

Živimo v času hitrega tehnološkega napredka, prav tako pa je to tudi čas vse pogostejših in večjih naravnih ter drugih nesreč. Da bi se čim bolj pripravili na nesreče in potem tudi čim hitreje odpravili ali vsaj zmanjšali posledice nesreč, je pomembno krizno komuniciranje, kot eden izmed glavnih elementov kriznega upravljanja, kajti sistem varstva pred naravnimi in drugimi nesrečami predstavlja enega od treh stebrov nacionalne varnosti Republike Slovenije. Znotraj kriznega komuniciranja pa je pomembna uporaba informacijsko-komunikacijske tehnologije, ki je postala temelj preventivnega, kakor tudi kurativnega delovanja v primeru naravnih in drugih nesreč. Informacijsko-komunikacijska tehnologija med drugim omogoča, da so podatki in pozneje informacije pravočasno na pravem mestu, saj le-to omogoča hitro in učinkovito ukrepanje v kriznih razmerah. Vsak sistem pa poskušajo usklajeno posodabljati in razvijati v skladu z izkušnjami in znanjem, saj se lahko zgodi, da sistem v normalnih razmerah deluje nemoteno, ko pa nastopi kriza, pa marsikaj ne deluje in tako sistem pokaže svoje pomanjkljivosti, ki jih je potrebno v najkrajšem možnem času popraviti.

Ključne besede: nesreča, kriza, komuniciranje, informacijsko-komunikacijska tehnologija.

Information-communication technology use within crisis communication in case of natural and other disasters

We live in an era of rapid technological progress, and it is also a time of more frequent and larger natural and other disasters. To be well prepared for disasters and then also quickly eliminate or at least reduce the impact of disasters, it is important crisis communications, as one of the key elements of crisis management, because the system of protection against natural and other disasters is one of the three pillars of the national security of the Republic of Slovenia . In side of crisis communication is an important use of information and communication technology, which has become the foundation of preventive and curative action in the case of natural and other disasters. Information and communication technology also enables that the data and later time information are in the right place, because they allow rapid and effective emergency response. Each system must be updated and developed in line with the experience and knowledge, because it can happen that the system every day runs smoothly, but in crisis time, many thing do not operate such as should be and shows its weaknesses, which should be corrected as soon as possible.

Key words: disaster, crisis, communication, information and communications technology.

KAZALO

SEZNAM SLIK

1 UVOD

Krize so postale neizogibno dejstvo v sodobnem svetu. Zdi se, da jih je vsak dan več in da smo kot družba vedno bolj ranljivi. To je še zlasti pomembno, če se krize nanašajo na ogrožanje življenj, materialnih dobrin in velikih tehničnih sistemov. Tako smo se v globalnem merilu soočali s krizami, ki so jih povzročali teroristični napadi, naravne nesreče, vojne, epidemije nalezljivih bolezni in podobno. Še posebej je naše obdobje zaznamovano z 11. septembrom 2001 in nato s številnimi terorističnimi napadi v Evropi, ter je tako prispevalo k prioritiziranju terorizma kot ključne grožnje nacionalni in mednarodni varnosti. Vendar pa so se po drugi strani pojavile številne druge krize, ki s svojim nastankom in obsegom opozarjajo, da terorizem nikakor ni nujno glavna grožnja varnosti. Na to so opozorile številne naravne nesreče, kot sta na primer cunami v Aziji in orkan Katrina v Ameriki, kakor tudi številne nesreče v Sloveniji. Vse to pa pripelje do spoznanja, da je potrebna pripravljenost na vse možne vrste kriz.

Število naravnih in drugih nesreč vsako leto narašča, tako da nesreče, bodisi naravne ali tehnološke, in različne oblike nasilja vsak dan znova in znova prizadenejo vse večje število ljudi po svetu, in sicer tako materialno, fizično, psihično in socialno. Tako se tudi v Sloveniji vse pogosteje srečujemo z raznimi nesrečami, v zadnjih letih so najpogostejši požari v naravi, suša, potresi, zemeljski plazovi, močni vetrovi in neurja, še vedno pa najbolj prevladujejo poplave.

Naravne in druge nesreče so predmet raziskovanja kriznega upravljanja in vodenja vsake države, kot najobčutljivejša točka slednjega pa se pojavlja krizno komuniciranje, ki se odraža tudi v (ne)uspehu nekaterih drugih prvin tega procesa, kot so preventiva in priprave na krizo, vodenje, odločanje ter politično-organizacijsko sodelovanje in konflikt. Ob vsem tem pa je pomemben odnos med razpoložljivimi informacijami, njihovim ustreznim in pravočasnim razširjanjem in zaznavanjem krize in ukrepi, ki so bili sprejeti, da bi krizo presegli. Prav tako je izjemno pomemben pretok informacij v krizi, ki jih je treba ustrezno izbrati in obdelati ter nato posredovati naprej. Pri tem pa je potrebno poiskati primerno razmerje med ključnimi informacijami in njihovo prenasičenostjo, ki lahko naredi še večjo krizo.

Zavedati pa se je potrebno tudi dejstva, da poleg vseh nesreč živimo tudi v svetu, kjer se hitro razvija tehnologija in s tem tudi telekomunikacijski informacijski sistem, ki je lahko v veliko pomoč sistemu varstva pred naravnimi in drugimi nesrečami. Tako je ena od najpomembnejših sprememb sodobnih družb povezana z uporabo informacijsko-komunikacijske tehnologije (IKT), ki je predvsem zaradi zmožnosti obdelave podatkov in njihovega prenosa (komunikacijska raven) povzročila spremembe v delovanju gospodarstva, državnih organov in institucij, pa tudi posameznika. Zato govorimo o vstopu v informacijsko družbo. Razvoj oboroženih sil je zelo povezan s tehnološkimi in družbenimi spremembami, zato je potrebno upoštevati omenjene spremembe ter se jim prilagoditi, kar zahteva preoblikovanje skoraj vsakega sistema, tako tudi komuniciranja ob naravnih in drugih nesrečah.

Informacijska družba, v kateri živim, izredno ceni količino informacij, s katero razpolagata posameznik in organizacija. Seveda vse informacije, s katerimi se vsak dan srečujemo, niso verodostojne ali točne. Nekatere so celo namenoma zavajajoče. Prav gotovo pa si vseh tudi ne moremo zapomniti. Človeški možgani so narejeni tako, da morajo nekatere informacije potisniti v podzavest ali celo pozabiti, da si lahko zapomnimo nove. Zato so ljudje začeli informacije zapisovati na papirnate in pozneje na ostale analogne medije. Vendar pa je njihova zanesljivost omejena. Papir se lahko založi, uniči ali kako drugače izgubi. Z izumom računalnika pa smo pridobili okolje, ki omogoča shranjevanje velike količine podatkov, s katerimi razvijemo več informacij in jih shranimo na enem mestu. Tu so se namreč razvile podatkovne baze, kjer je večje količine podatkov mogoče ne le shraniti, temveč jih s pomočjo določenih orodij tudi interpretirati, analizirati. Ti tako imenovani informacijski sistemi olajšajo delo na vseh področjih, kjer se dela s podatki.

Človek je bitje, ki svojo okolico zaznava omejeno. Osredotoči se na določeno dogajanje in nezavedno zanemari vse ostalo. Če je to dogajanje vrh vsega še nevsakdanje in stresno, kot je nesreča, je to zaznavanje še bolj okrnjeno ter prežeto s subjektivnim doživljanjem. Odločanje v takšnem primeru je znatno oteženo, če ne celo onemogočeno. Ljudje se vedno bolj zavedamo svojih omejitev in se zaradi tega vse bolj opiramo na znanost in njene tehnološke pridobitve. Tako se v primeru nesreče odzovejo za to usposobljeni strokovnjaki, ki se danes opirajo na sodobno tehnologijo. Prav s pomočjo

tehnologije, kot prvo, ti strokovnjaki pridobijo informacije o nesreči, kot drugo pa je tehnologija tudi orodje za samo pomoč na kraju nesreče.

Področje varnosti pred naravnimi in drugimi nesrečami predstavlja skupek ljudi, nalog in tehnologije, ki nam omogočajo razmeroma nemoteno življenje. Nepredvidljive naravne sile nas silijo, da neprestano iščemo nove načine, da bi jih preprečili, se jim izognili ali pa jih vsaj omilili. Razvoj tehnologije nam na tej poti pomaga, vendar nam hkrati prinaša nove nevarnosti, ki smo jih opredelili kot druge nesreče.

Poleg tehnologije pa je kompleksen pojav tudi zagotavljanje nacionalne varnosti, ki zahteva večdisciplinarno in meddisciplinarno odzivanje. Na ravni države se to izraža v večresorskih in medresorskih pristopih, zato mora vsaka država oblikovati primerno strukturo za horizontalno delovanje vseh relevantnih resorjev, organov, uprav, agencij, sektorjev in drugih organizacij.

2 METODOLOŠKO-HIPOTETIČNI OKVIR

2.1 Predmet preučevanja

Vsak dan se soočamo z vse večjimi in vse pogostejšimi nesrečami, zato me v tej diplomski nalogi zanimajo predvsem nesreče in krizno komuniciranje, ki predstavlja pomemben del reševanja nesreč. Sprva bom proučila krizo in krizno komuniciranje, v okviru kriznega komuniciranja me pa še zlasti zanima vloga informacijsko-komunikacijske tehnologije, za katero je znano, da se hitro razvija in širi, zato tudi pri kriznem komuniciranju ne moremo brez nje.

2.2 Opredelitev ciljev preučevanja

Cilj preučevanja v diplomski nalogi je predvsem predstaviti pomen informacijsko-komunikacijske tehnologije v okviru kriznega komuniciranja in katere vrste IKT se uporabljajo. Predstaviti želim, da lahko učinkovita informacijsko-komunikacijska tehnologija in zraven ljudje, ki jo znajo uporabljati, v veliki meri pospeši samo reševanje krize, v nekaterih primerih pa lahko krizo celo prepreči.

2.3 Hipoteze

Pri preučevanju problematike sem si zastavila dve hipotezi:

H1: Uporaba informacijsko-komunikacijske tehnologije omogoča hitrejše zbiranje in obdelavo informacij, ki morajo biti za učinkovito krizno komuniciranje dobro organizirane in pravočasno razširjenje.

H2: Gleda na to, da je informacijsko-komunikacijska tehnologija pomemben element kriznega komuniciranja, se mora ta tehnologija v skladu z razvojem posodabljati in v sodelovanje vključiti čim več akterjev.

2.4 Metode dela

Pri izdelavi diplomske naloge sem uporabila več različnih raziskovalnih metod, in sicer:

1. Metodo zbiranja primarnih in sekundarnih virov, kar je predpogoj za uporabo vseh nadaljnjih metod;
2. Deskriptivno metodo, s katero sem opisala predvsem temeljne pojme;
3. Metodo analize in interpretacije primarnih virov, s katero sem raziskala zakonodajo, pravne akte in uradne dokumente s področja kriznega upravljanja in vodenja;
4. Metodo analize in interpretacije sekundarnih virov, na podlagi katere sem raziskala in analizirala strokovne publikacije, kot so zborniki, knjige, članki ter druga strokovna dela, tako v tiskani kot tudi elektronski obliki;
5. Primerjalno-pravno metodo, s pomočjo katere sem naredila primerjalno analizo zakonov in drugih pravnih aktov.

3 OSNOVNI POJMI

Za lažje razumevanje tega diplomskega dela bi najprej predstavila osnovne pojme, ki so temelj nadaljnjega dela. Ti pojmi so: nesreča, kriza, krizno komuniciranje in informacijsko-komunikacijska tehnologija.

3.1 Nesreča

V strokovni literaturi s področja naravnih in drugih nesreč ne najdemo enotne opredelitve temeljnih pojmov, kot so nesreče, naravne in druge nesreče, zato bom navedla nekaj različnih opredelitev teh pojmov. In sicer Zakon o varstvu pred naravnimi in drugimi nesrečami (2006) pravi, da je nesreča dogodek ali vrsta dogodkov, povzročenih po nenadzorovanih naravnih in drugih silah, ki prizadenejo oziroma ogrozijo življenje ali zdravje ljudi, živali ter premoženje, povzročijo škodo na kulturni dediščini in okolju v takšnem obsegu, da je za njihov nadzor in obvladovanje potrebno uporabiti posebne ukrepe, sile in sredstva, ker ukrepi rednih dejavnosti, sile in sredstva ne zadostujejo.

Podobno opredeljuje nesrečo tudi Polič v svoji raziskavi, ki pravi, da je nesreča relativno hiter in v prostoru skoncentriran dogodek, ki vpliva na prepoznaven družbeni podsistem (na primer skupnost, sosesko) zaradi nastanka velike nevarnosti in/ali uničenja, prekinja sposobnost sistema, da preskrbi za svoje člane pričakovane življenjske razmere in se pojavlja v kontekstu, v katerem obstaja soglasje o pomenu situacije, o ustreznih normah in vrednotah ter prednostih, ki jih je treba upoštevati (Polič 1994, 19).

Prav tako predpostavlja, da nesrečo povzročijo krize oziroma jih celo enači s krizami, čeprav poudarja, da vsaka kriza še ni nesreča. S psihološkega vidika je kriza in s tem nesreča določena čustveno napeta situacija. V takšni situaciji pa so naše sposobnosti mišljenja omejene, pri nekaterih celo za določen čas onemogočene, odzivni čas pa je zelo majhen, saj dogodki potekajo zelo hitro in jim je zelo težko slediti. V takšni situaciji je izredno težko pripraviti načrt delovanja, zato se le-ta v okviru sil za zaščito in reševanje okvirno pripravi že prej (Polič 1994, 350).

Marshall (v Polič 1994, 126) pravi, da se nesreče pojavljajo v značilnem zaporedju, tako navaja naslednje značilne faze kriz:

- opozorilo,
- grožnja,
- prizadetje,
- pregled prizadetosti,
- reševanje,
- odpravljanj posledic,
- povrnitev v prvotno stanje.

Nato in OZN pa opredeljujeta nesrečo kot dogodek ali vrsto dogodkov, povzročenih po nenadzorovanih naravnih in drugih silah, ki prizadene oziroma ogrozi življenje ali zdravje ljudi, živali ter premoženje, povzroči škodo na kulturni dediščini in okolju ter kot resno prekinitev delovanja družbe in povzroči veliko človeških žrtev, materialno in okolijsko škodo (Slovar ZiR).

Nesreča je torej dogodek, ko so ogrožene temeljne človekove vrednote in ki zahteva določeno ukrepanje in delovanje, za katerega so odgovorne sile za zaščito, reševanje in pomoč.

3.1.1 Naravne in tehnološke nesreče

Lerbinger (1997, 23) glede na izvor okolja loči tehnološke nesreče in velike naravne nesreče ter jih skupno poimenuje krize fizičnega okolja. Naravne nesreče so pravzaprav še vedno velikokrat sinonim za 'veliko krizo'. Takšne velike krize' so poplave, potresi in druge naravne nesreče, ki ogrožajo človeška življenja in premoženje. Mednje sodijo tudi žgoči okoljevarstveni problemi, kot sta na primer učinek tople grede ali tanjšanje ozonske plasti.
Vse več pa je tudi kriz, ki jih povzroča tehnologija. Sodobni svet je namreč vse bolj odvisen od tehnologije. Če pa ta tehnologija odpove, nastanejo tehnološke nesreče, katerih posledice so v večini primerov katastrofalne (White in Mazur 1995, 204).

Naravna nesreča je dogodek, osredotočen na čas in prostor, v katerem družba ali njena relativno samostojna podskupina doživi resno škodo. Ob tem so izgube njenih članov in fizičnih dobrin takšne, da porušijo socialno strukturo in onemogočijo zadovoljivo delovanje vseh ali nekaterih bistvenih družbenih funkcij (Kline in drugi 1998, 175).

Naravne nesreče so pojav, s katerim se človeštvo spoprijema že tisočletja in njihova glavna značilnost je še vedno, da za seboj pustijo razdejanje. Marshall (v Polič 1994) pravi, da naravne nesreče, kot so vulkani, potresi, plimski valovi, prekinejo delovanje celotne družbe ali pa le delovanje dela družbe, izzovejo begunce, propad proizvodnje in distribucijskih sistemov ter še okrepijo boj za surovinami.
Polič pravi, da so naravne nesreče razmeroma znani pojavi, ki zajemajo močne in nenadne klimatske meteorološke (tornado, orkan), geofizikalne (potres), pa tudi biološke (epidemije) spremembe. Vse vrste nesreč pa se ne pojavljajo povsod, temveč je vsaka značilna za določeno območje (Polič 1994, 22).

Zakon o varstvu pred naravnimi in drugimi nesrečami (2006) uvršča med naravne nesreče potres, poplave, zemeljske in snežne plazove, visok sneg, močan veter, točo, žled, pozebo, sušo, požar v naravnem okolju, množični pojav nalezljive človeške, živalske ali rastlinske bolezni in druge nesreče, ki jih povzročijo naravne sile. Za naravno nesrečo se štejejo tudi neugodne vremenske razmere po predpisih o kmetijstvu in odpravi posledic naravnih nesreč, ki jih povzročijo žled, pozeba, suša, neurje, toča ali živalske in rastlinske bolezni ter rastlinski škodljivci.

Ta isti zakon pa za druge nesreče opredeljuje nesreče v cestnem, železniškem in zračnem prometu, požar, rudniška nesreča, porušitev jezu, nesreče, ki jih povzročijo aktivnosti na morju, jedrske nesreče in druge ekološke ter industrijske nesreče, ki jih povzroči človek s svojo dejavnostjo in ravnanjem, pa tudi vojna, izredno stanje, uporaba orožij ali sredstev za množično uničenje ter teroristični napadi s klasičnimi sredstvi in druge oblike množičnega nasilja.

Nekatere nesreče so posledica uporabe sodobnih tehnologij, kot je avto, v primeru nesreče v prometu, ali umetno zgrajenih objektov, kot je jez, če obravnavamo njegovo nenadno porušitev. Te nesreče so neizpodbitno posledice človeškega ravnanja, določene oblike rabe teh objektov ali njihove zlorabe, in so zato antropogenega nastanka. Prav

tako pa lahko človek zaradi svoje malomarnosti ali neprevidnosti sproži nesrečo, ki jo sicer navadno uvrščamo med naravne nesreče. Erozija tal, poplave, snežni plazovi in epidemije sicer povzročajo naravni dejavniki, ki pa so spodbujeni s človekovo nepravilno uporabo oziroma zlorabo. Tudi požar je lahko popolnoma naravni pojav, vendar pa se uvršča med druge nesreče, saj je zanj največkrat kriv človek.

Veliko novejši pojav, kot so naravne nesreče, so vsekakor tehnološke nesreče. Še pred nekaj časa so bile razmeroma malo znane, sedaj pa se z njimi srečujemo skoraj vsak dan. Pripetijo se lahko povsod, kjer obstaja tehnologija, saj tam obstaja hkrati tudi možnost, da izgubimo nadzor nad njo. To so na kratko »nesreče, ki jih povzroči človek« (Marshall v Polič 1998, 162).

Tehnološke nesreče so prav tako razmeroma nenadne in močne ter niso napovedljive. Če lahko rečemo, da so naravne nesreče vsaj v majhni meri lahko napovedljive, pa se zdi, da za tehnološke še ta nizek odstotek napovedljivosti ne drži. Različnost, pogostost in območje izbruha pri tehnoloških nesrečah niso tako znani kot pri naravnih. Resda so tudi naravne nesreče razmeroma nenadne, močne ter nenapovedljive, vendar lahko pogostost in območje izbruha tudi v nekaterih primerih s predhodnim preučevanjem statistike napovemo. Tako vemo, da so nekatere naravne nesreče omejene na določen čas v letu in določena območja.

Sodobne tehnološke nesreče pa namreč niso omejene niti časovno niti prostorsko. Uničujejo okolje in čeprav ga lahko zapustijo na videz neokrnjenega, se šele čez čas pojavijo posledice, kot so na primer radioaktivnost, dekontaminacija, poznejši pojav bolezni …

Uničevalni učinek naravnih in drugih nesreč je nesporen. Razlika je le v tem, da z nesrečami, ki jih povzroči človek sam, uničuje samega sebe. Večina teh nesreč ni izzvanih namerno, tiste, ki pa so, pa imajo lahko tudi najširše posledice. Sem sodijo vojna, genocid, skupinski samomor in teroristična dejanja, s katerimi človek dejansko, namerno in usmerjeno uničuje svojo lastno vrsto. Iz tega zornega kota lahko razumemo tudi uvrstitev teh nesreč med samouničevalne nesreče.

Ne glede na njihovo različno naravo se je treba pri vseh vrstah nesreč enako odzivati. Pri vseh vrstah nesreč je strategija ukrepanja pravzaprav enaka, razlike pa so v taktiki, konkretnih posamičnih ukrepih (Kline in drugi 1998, 212).

Podobno meni tudi Tierneyjeva, ki pravi, da posebni načrti ukrepov za različne vrste nesreč niso smiselni, saj povzročajo zmedo, neusklajenost, podvajanje služb za ukrepanje, dodatne stroške … (Tierney v Kline in drugi 1998, 212).

3.2 Kriza

Preden opredelimo krizno komuniciranje, je potrebno opredeliti sam pojem kriza* in njene značilnosti, pri čemer pa je zelo težko podati neko univerzalno definicijo krize, saj so oblike kriz in obseg njihovih posledic zelo raznolike, toda kljub temu lahko za vsako krizo trdimo, da ima neke specifične lastnosti in posebnosti, ki jo zaznamujejo in ločujejo od podobnih dogodkov, ostajajo pa krizam določene značilnosti še vedno skupne.

Zaradi slednjega so se oblikovale različne definicije, ki poudarjajo določene lastnosti, vse pa poskušajo najti skupno nit med dogodki, kjer so po besedah Malešiča ogrožene temeljne vrednote in norme subjekta, na katerega se kriza nanaša. Prav tako so za krizo značilni tudi časovni pritisk pri sprejemanju odločitev, negotovost razmer in stres. Kriza je dogodek, ki ni vedno jasno umeščen v prostor in čas, kar še dodatno poveča učinek nenadnosti in nenapovedanosti (Malešič 2004, 402).

Pojem krize bi lahko na manj abstraktni in bolj operacionalizirani ravni zajel naravne in druge nesreče, različne (vojaške) konflikte in prevrate, (oborožene) vstaje in revolucije, politične nemire in teroristične dejavnosti, ne smemo pa zanemariti tudi drugih kriz, ki so lahko posledica spleta neugodnih okoliščin in odnosov v našem fizičnem in socialnem okolju (lakote, epidemije …) (Malešič 2004, 402).

V londonski šoli za odnose z javnostmi opredeljujejo krizo kot resen incident, ki vpliva na človekovo varnost, na okolje in izdelke ali ugled organizacije. Za takšen incident pa je značilno, da ga mediji obravnavajo sovražno (Novak 2000, 34).

Podobno tej opredelitvi je pojmovanje krize kot okoliščine, v kateri so ogroženi življenje, varnost ali celo obstoj posameznika ali organizacije. Za krizo je značilen časovni pritisk, kar pomeni, da morajo upravljavci hitro sprejemati odločitve in obvladati stres vseh udeležencev v krizi (Novak 2000, 35).

Vzroki za krize, kakor tudi oblike in posledice kriz so različne, kljub temu pa so, po mnenju Boina in Lagadeca (v Malešič in drugi 2006, 12), ključne značilnosti sodobnih kriz naslednje:

- imajo velik vpliv na velik delež prebivalstva določene države,
- prinašajo visoke ekonomske stroške, ki presegajo običajne zavarovalniške zmogljivosti,
- povzročijo učinek 'snežne kepe' (snow-ball effect),
- sistemi kriznega upravljanja in vodenja sprejemajo napačne in nepotrebne ukrepe,
- povzročajo izjemno visoko stopnjo negotovosti,
- trajajo daljše obdobje, pri čemer se viri ogrožanja spreminjajo,
- povzročijo pojav velikega števila akterjev na kraju dogodka krize,
- prinašajo raznovrstna tveganja,
- razkrijejo probleme komuniciranja, in sicer med odgovornimi akterji, z množičnimi mediji, z javnostmi, z žrtvami in celo z javnostmi, ki so časovno in prostorsko precej oddaljene od kraja dogajanja.

Prav tako tudi Wiener in Kahn (v Malešič 2004) identificirata 12 skupnih elementov, značilnih za vsako krizo, in sicer pravita, da je kriza:

- pogosto preobrat dogodkov in aktivnosti,
- situacija, ki zahteva akcijo s strani udeležencev,
- ogroža cilje vpletenih,
- sledijo pomembne posledice, ki vplivajo na prihodnost udeležencev,
- konvergenca dogodkov, ki vzpostavijo nove okoliščine,
- poraja negotovosti pri ocenjevanju situacije in formuliranju alternativ za njeno reševanje,
- zmanjša nadzor nad dogodki in njihovimi posledicami,
- poveča nujnost, kar se odraža v povečanem stresu in bojazni (strahu),

- okoliščina, v kateri je na voljo neobičajno malo informacij,
- povečuje časovne pritiske za vpletene,
- povzroči spremembe odnosov med vpletenimi in povzroči napetost med njimi.

3.3 Komuniciranje

Komuniciranje[1] v najširšem pomenu je kakršno koli verbalno ali neverbalno vedenje ene osebe, ki ga zazna druga oseba, s katero prva oseba komunicira. Tudi podjetja in organizacije komunicirajo, in sicer z javnostmi v svojem notranjem in zunanjem okolju. Upravljanje komuniciranja organizacije z njenimi javnostmi pa je bistvena naloga stroke odnosov z javnostmi (Novak 2000, 252).

Schramm, Wright, Lipovec in Možina pa se strinjajo, da je komuniciranje proces sporazumevanja, katerega bistvo je, da morajo biti osebe, ki med seboj komunicirajo, med seboj uglašene, da bi dosegle namen in cilj komuniciranja (Možina 1998, 23).

Pri komuniciranju o naravnih in drugih nesrečah pa se srečujemo tudi z besedno zvezo komuniciranje o nevarnosti (angl. risk communication), ki je nekoliko širši pojem od kriznega komuniciranja.

Covell in njegovi sodelavci (v Malešič in drugi 2006, 13–14) so tako komuniciranje o nevarnosti opredelili kot katero koli namerno izmenjavo znanstvene informacije o zdravju ali okolijskih nevarnostih med zainteresiranimi strankami oziroma kot pošiljanje ali prenašanje informacij o ravni zdravstvenih ali okolijskih nevarnosti ali odločitev, akcij ali politik, usmerjenih v obvladovanje ali nadzor takšnih nevarnosti, med zainteresiranimi strankami.
Glede na to opredelitev razlikujemo štiri področja uporabe komuniciranja o nevarnosti:

1. Obveščanje in izobraževanje, kjer gre za neusmerjeno, a namerno dejavnost, preko katere laična javnost prejme uporabno in pojasnjevalno informacijo;
2. Spodbujanje vedenjskih sprememb in sprejemanje zaščitnih ukrepov uporabljamo:

[1] Latinsko communicare pomeni napraviti skupno, deliti s kom.

a. Kadar raziskave kažejo, da so določena vedenja, dejavnosti ali razmere nevarne za ljudi, pa hočejo oblasti svetovati javnosti, naj blaži nevarnost,
b. Kadar javnost podcenjuje nevarnost;

3. Objavljanje opozoril o nevarnostih in nujnih informacij je usmerjeno k oskrbi javnosti z obvestili o nevarnosti. Razlikujemo komuniciranje pred krizo, ki naj bi obveščalo o njej, preden se pripeti, ter komuniciranje med njo, ko je ta neizbežna, se dogaja ali pa se je pravkar zgodila;
4. Izmenjava informacij in skupni pristop k nevarnosti je namenjen izmenjavi obvestil in skupnemu pristopu državljanov, vlade drugih k nevarnosti.

3.4 Informacijsko-komunikacijska tehnologija

Za razumevanje informacijsko-komunikacijske tehnologije in njenega razmerja do družbe in posameznika je potrebno definirati nekatere najosnovnejše pojme, kot so informacija, komunikacija in tehnologija. Čeprav si načeloma lahko predstavljamo vsebino posameznih pojmov, pogosto preziramo nekatere njihove elemente, aplikacije in pomene.

Informacija tako ni zgolj vsebina sporočila, ki ima navadno za posameznika določen pomen in lahko tako ali drugače vpliva na njegovo ravnanje, ampak je tudi zasebno ali javno dobro, življenjsko pomemben resurs, sprožilni element določenega ravnanja. Informacija, je, ne glede na primitivnost živega organizma, pomembna za minimalen obstoj družbe in njeno preživetje. Na družbeni ravni informacijo predstavlja vsebina sporočila, ki je namenjena širšemu krogu posameznikov in katera je potrebna za nemoteno življenje in razumsko delovanje posameznikov (Pinterič in Grivec 2007, 15).

Komunikacija je proces sporočanja informacij ter se lahko deli glede na kanal sporočanja ter glede na razmerje med oddajnikom in prejemnikom informacij. Glede na razmerje med oddajnikom ter prejemnikom sporočila lahko ločimo v osnovi enosmerno ali dvosmerno komunikacijo, pri čemer je mogoče ločiti tudi glede na število prejemnikov sporočila, kjer gre lahko za medosebno ali pa množično komunikacijo. Pri medosebni komunikaciji je navadno en oddajnik sporočila ter en prejemnik sporočila, pri čemer se vloga prejemnika in oddajnika v primeru dvosmerne komunikacije izmenjuje; enako velja tudi v primeru, ko je prejemnikov več in v naslednjem koraku

nekdo izmed prejemnikov prevzame vlogo oddajnika sporočila. Pri enosmerni komunikaciji je vloga oddajnika in prejemnika sporočila navadno vnaprej določena, pri čemer povratna informacija s strani prejemnikov sporočila ni relevantna (ukaz, sporočilo za javnost …).

Glede na komunikacijski kanal v osnovi ločimo pisne in ustne komunikacijske kanale. Pisne komunikacijske kanale predstavljajo vse oblike pisnega izražanja, od množičnih medijev z izjemo radia, internetnih strani, elektronske pošte (dvosmerna komunikacija) in ne nazadnje tudi knjig in drugih neperiodičnih besedil. Med ustne komunikacijske oblike pa sodijo medosebni razgovori, telefonski razgovori, radijski prenosi in drugi zvočni zapisi (Pinterič in Grivec 2007, 15–16).

Komunikacijski kanal je torej pot, po kateri potuje sporočilo od pošiljatelja k prejemniku. Lahko so to neposredni stiki med pošiljateljem in prejemnikom, pisma ali razni tehnični posredniki, zlasti telekomunikacijske zveze. Komunikacijski kanal tehnično sicer lahko obstaja, vendar zaživi v organizacijskem smislu šele tedaj, ko ga uporabimo za komuniciranje.

Zmogljivosti (kapaciteta) vsakega komunikacijskega kanala je omejena, čeprav se nam pogosto dozdeva, da ni tako. Omejuje jo največja količina informacij, ki jo je še mogoče prenesti po komunikacijskem kanalu. Učinkovitost komuniciranja terja, naj komunikacijski kanal v časovni enoti čim bolj natančno prenese čim večjo količino informacij ob gospodarni uporabi sredstev.

Pomembna je varnost prenosa. V komunikacijskih kanalih nastajajo motnje, ki zmanjšujejo učinkovitost prenosa, ovirajo natančen in hiter prenos sporočila, skratka – povzročajo entropijo (neurejenost) prenosnega sistema. Entropija lahko pomeni, da sporočilo v celoti ali deloma ne prispe do prejemnika ali pa ga doseže vsebinsko popačeno (Možina 1998, 44).

Tehnologija je v okviru prenosa informacij vsakršno tehnično sredstvo, ki pripomore k prenosu sporočila z informacijo v okviru komunikacijskega procesa. V preteklosti so temeljne komunikacijske tehnologije predstavljali predvsem aparati in stroji, ki so omogočali razmnoževanje pisnih informacij (tiskarski in pisalni stroj) in ustnih

informacij (telefon, radio). V tem okviru ima televizija dvojno vlogo, saj predstavlja v osnovi prenos zvočnih informacij z dodatnim vizualnim učinkom. Danes pa se v svetu pojavlja nova oblika komuniciranja, ki nadgrajuje in presega pretekle komunikacijske tehnologije na podlagi konvergence tehnologij ter z razvijanjem novih potencialov. V tem okviru se je razvil pojem sodobne »Informacijsko-komunikacijske tehnologije – IKT«.

V literaturi pa najdemo različne definicije pojma informacijsko-komunikacijske tehnologije (IKT). V širšem pomenu IKT predstavlja sredstva, orodja, sisteme in tehnike oziroma je definiran kot vse elektronske aparature, na primer računalnik, internet, DVD-zapisovalnik, kalkulator, televizija, interaktivni kabelski sistem, sateliti, teletekst, multimedijski komunikacijski sistemi itd. (Hawkridge 1985, 9).

V novejših teorijah pa IKT predstavlja tehnologijo v bolj družbenem smislu, saj zajema različne načine elektronskega komuniciranja med ljudmi, ne glede na uporabo v osebne, korporativne ali servisne namene (Jussawalla v Pinterič in drugi 2007, 30).

Sodobne IKT predstavljajo predvsem tiste tehnologije, ki temeljijo na združevanju predhodnih tehnologij za prenos informacij ter omogočanje komunikacijskih procesov. V tem okviru je najpogosteje obravnavana internetna tehnologija, ki poleg osnovne internetne aplikacije omogoča še vrsto dodatkov, kot so elektronska pošta, interaktivne klepetalnice, spletni forumi, hkrati pa v zadnjem obdobju omogoča preprosto konvergenco radia in televizije. Druga pomembna IKT pa je prenosni telefon, ki omogoča boljšo dosegljivost posameznikov v okviru učinkovitejšega posredovanja informacij. V zadnjem obdobju pa z vgrajevanjem avdio-video snemalnih naprav omogoča konvergenco tehnologij za tvorbo informacij (kamere, mikrofoni) ter konvergenco tehnologij za posredovanje in sprejemanje informacij. Tako prenosni telefoni predstavljajo danes integrirano tehnologijo, ki omogoča izvedbo vseh treh faz komunikacijskega procesa, to je generiranje sporočila z informacijo, njegovo posredovanje in sprejemanje.

Podobno pa Information Technology Association of America (ITAA 2005) definira informacijsko tehnologijo, saj pravi, glede na to, da je informacija znanje o določenem dogodku ali situaciji, ki je bilo zbrano ali pridobljeno preko komunikacij, da je

informacijska tehnologija proučevanje, oblikovanje, razvoj, implementacija, podpora ali upravljanje z računalniškimi informacijskimi sistemi za upravljanje. To velja predvsem za programsko in strojno opremo, s katero je možno elektronsko vnesti, procesirati, shraniti, izvleči, prenesti in sprejeti podatke in informacije, vključno z besedilom, slikami, zvokom, videom, kot tudi zmožnost elektronsko nadzorovati stroje.

Informacijsko-komunikacijska tehnologija torej obsega računalnike, računalniške mreže, komunikacijske satelite, robotiko, videobesedila, kabelsko televizijo, elektronsko pošto, videoigrice in avtomatizirano pisarniško opremo (Answer.com – ICT).

Informacijsko-komunikacijska tehnologija omogoča uporabnikom hitri dostop do spoznanj in izkušenj od velikega obsega ljudi, skupnosti in kultur, in prav to, hitri dostop, je izrednega pomena v vseh kriznih razmerah.

Znanstveniki vedno znova in znova dokazujejo, da živa bitja kot posamezniki v izoliranem okolju odmrejo ter da je za sobivanje nujno potrebna komunikacija, ki jo razumejo istorodna živa bitja ter katero v določenih segmentih razumejo tudi drugorodna živa bitja.

Razvoj informacijsko-komunikacijske tehnologije (IKT) in njena uporaba v sodobnih družbah sta doživela razmah revolucionarnih razsežnosti. Uporaba IKT-a namreč že dolgo ni več omejena zgolj na raziskovalne akademske ter obrambno-vojaške okvire, temveč je postala temelj delovanja vseh pomembnejših družbenih podsistemov (upravno-političnega, znanstveno-raziskovalnega, gospodarskega, medijskega in telekomunikacijskega in navsezadnje nacionalnovarnostnega), hkrati pa korenito spremenila delovanje posameznika, družbenih skupin in institucij. Kot takšna je postala cilj in sredstvo za doseganje njihovih interesov tudi na področju varnosti (Rattray 2001).

Uporaba IKT-a je torej postala vir sprememb družbenega okolja, varnostnih akterjev, pa tudi njihovih virov ogrožanja. Značilnosti, kot so:

- Nizki vstopni stroški (v primerjavi z izdelavo visokotehnoloških oborožitvenih sistemov so vstopni stroški pri IKT-u bistveno nižji, kar omogoča disperzijo med družbene skupine ali države z manjšo finančno zmogljivostjo);

- Nejasnost tradicionalnih razmejitev (IKT – internet – je zameglila oziroma presegla geografske, birokratske in jurisdikcijske meje, pa tudi razsežnosti obravnavanja varnosti v tradicionalnem državocentričnem (realističnem) smislu);
- Povečana možnost vplivanja na zaznavo stvarnosti (nove informacijske tehnike bistveno povečujejo število in moč manipulativnih aktivnosti);
- Možnost uporabe v oboroženih silah na strateški kot tudi taktični in operativni ravni ter nacinalnovarnostnih sistemih v celoti;
- Geografsko-prostorska neomejenost ne povzroča samo sprememb tradicionalnih varnostnih akterjev in njihovega delovanja, temveč omogoča tudi pojav novih (Svete v Malešič 2006b, 47–48).

4 KRIZNO KOMUNICIRANJE

Ko nastopi kriza, si vsi prizadeti in odgovorni s tega področja prizadevajo, da se kriza čim prej konča in se vzpostavi pred krizno stanje, kolikor je to sploh mogoče. Da bi to dosegli, pa je pomemben element prav komuniciranje med akterji, torej krizno komuniciranje, saj so pravočasne in verodostojne informacije ključnega pomena. Tako Novak (2000, 253) pravi, da je krizno komuniciranje posebno področje odnosov z javnostmi, ki zajema predvidevanje potencialnih kriznih dogodkov, pripravo nanje, reševanje kriz in komuniciranje s prizadetimi in drugimi ključnimi javnostmi organizacije ter pokrizno ocenjevanje ukrepov.

Pomemben element pri vseh fazah razvoja krize je komuniciranje, in sicer z javnostjo in drugimi udeleženci krize. Pri tej komunikaciji gre za obveščanje o prihajajoči nevarnosti, za prepričevanje ljudi za sprejem zaščitnih ukrepov, za vzpostavljanje pripravljenosti na možno grožnjo ali pa za ukrepanje ob nesreči ali pa po njej. Malešič s sodelavci (2006, 13) tako navaja, da je pogosto prav ustrezno komuniciranje ključni začetni dejavnik ustreznega ukrepanja.

Kot sem že omenila, ko nastopi kriza, je vpletenih veliko ljudi in skupin (gasilci, zdravstveno osebje, novinarji, policija, organi zaščite in reševanja …), da pa bi bila njihova pomoč zares učinkovita, pa je potrebno med njimi vzpostaviti komuniciranje.
Tako Malešič, Hrvatin in Polič (2006, 53−55) opozarjajo, da mora biti pretok informacij zagotovljen v petih smereh, in sicer:

1. Znotrajorganizacijski pretok informacij. Že v normalnih razmerah poteka v organizaciji komuniciranje med njenimi deli in člani. Komunikacijski sistem predeluje in izmenjuje vnaprej določene vrste in količine informacij. Med krizo se število notranjih uporabnikov komunikacijskega sistema bistveno poveča zaradi sprememb, ki jih od organizacije zahtevajo razmere (na primer več izmen, daljši delovni čas, prostovoljci). Trenutni informacijski sistem morda tega ne zmore, saj zahteve presežejo njegove zmogljivosti in postane preobremenjen. Zaradi preobremenjenosti lahko sistem razpade, informacije se izgubijo ali pa so prepozno prejete. Prav tako postane med krizo pretok informacij po organizaciji bolj zapleten in manj jasno določen, kot v normalnih razmerah (na primer več

ljudi zaseda isti položaj, pojavijo se nevsakdanje naloge, ljudje so premeščeni na začasne položaje ipd.). Normalni komunikacijski kanali torej ne zadostujejo več. Načrtovanje lahko opozori na te probleme, še vedno pa obstaja velika vloga ustvarjalnosti v njihovem reševanju, zato meni Malešič s sodelavci, da so koristnejše vaje v ustvarjalnosti v kriznih razmerah, kot pa pretirano podrobni načrti komuniciranja.

2. Medorganizacijski pretok informacij. Med krizo je treba pogosto med različnimi organizacijami vzpostaviti formalne stike s prej neznanimi ljudmi, včasih celo s skupinami, za katerih obstoj sploh nismo vedeli. Takšen informacijski tok je zato težko vzpostaviti in ohraniti. Z načrtovanjem je treba predvideti najverjetnejše ključne organizacije, ki bodo vključene v odzivanje na nesrečo. Usposabljanje in vaje morajo zato poudariti in predvideti pomen dela z neznanimi uradniki in skupinami ter načini njihovega identificiranja.
3. Informacijski pretok od organizacij k javnosti. V normalnih razmerah mora le malo organizacij (razen sredstev množičnega obveščanja) komunicirati s celotno populacijo. Med krizo pa morajo organizacije posredovati ljudem različne informacije. Žal pogosto ne upoštevajo, kaj je za prebivalce pomembno, ter posredujejo informacije, ki se zdijo pomembne le osebju organizacije. Pogosto spuščajo za prebivalce pomembne podrobnosti in jih puščajo v negotovosti. Zavedati se je treba, da obvestila, ki se zdijo jasna pošiljateljem, niso nujno razumljiva prejemnikom, se pravi ogroženim prebivalcem. Načrtovanje lahko predvidi določene splošne vsebine, ki jih organizacija hoče sporočiti, podrobnosti pa ostajajo zadeve taktičnega premisleka.
4. Informacijski pretok od javnosti k različnim organizacijam. Prebivalci pogosto iščejo pomoč in napotke pri različnih organizacijah. Najvidnejše organizacije pogosto ne zmorejo učinkovito predelati velike količine informacij in vprašanj (na primer preobremenjenost policije, civilne zaščite ali centra za obveščanje s telefonskimi klici ob krizi). Ta preobremenitev lahko zmoti še druge informacijske tokove. Ob normalnih zahtevah po informacijah se organizacija v kriznih razmerah sooči še z dodatnimi, ki niso del običajnega informacijskega toka. Le redke organizacije lahko učinkovito odgovorijo na nevsakdanja vprašanja, večina pa zadeve več ne obvlada. V načrtu pa lahko organizacije predvidijo najverjetnejše potrebe po informacijah za nesreče nasploh in določene

posebne krize. Obvladovanje problema pa je bolj zadeva upravljanja, zato se mora organizacija na takšne razmere predčasno pripraviti.

5. Informacijski pretok med različnimi sistemi organizacij. Pogosto se pojavijo informacijski problemi zaradi mobilizacije različnih sistemov organizacij. Pozablja se namreč, da organizacije ne delujejo neodvisno druga od druge, ampak kot sistem medsebojno povezanih specializiranih subjektov, ki opravljajo določene naloge. Tako na primer zdravstveni sistem omogoča zdravstvene, policijski varnostne, sistem varstva pred nesrečami pa zaščitno-reševalne storitve. Izpolnjevanje teh in drugih s krizo povezanih nalog zahteva več kot zgolj enosmeren informacijski tok med udeleženimi organizacijami. Obstaja več dvosmernih in verižnih komunikacij med različnimi skupinami akterjev kriznega upravljanja. Čeprav lahko marsikaj predvidimo, še veliko zadev ostaja stvar taktike. Tako Malešič s sodelavci domneva, da bo lažje obvladljiv informacijski tok v navpično povezanih sistemih, kot pa če so organizacijske enote povezane vodoravno (Malešič in drugi 2006, 53–55).

Ko je zagotovljen ta pretok informacij, pa so, po mnenju Bacot, Mccabe in Fitzgeralda (v Malešič in drugi 2006), za učinkovito komuniciranje potrebne še štiri prvine, ki skupaj sestavljajo strategijo kriznega komuniciranja, in sicer:

- razširjanje informacij – pomembne informacije morajo biti dobro organizirane, pripravljene za uporabo in pravočasno razširjene,
- identificiranje zainteresiranih strank v zvezi z določenim potencialnim dogodkom in navezava neposredne komunikacije z njimi,
- vzpostavljanje stika s skupnostjo,
- vzpostavljanje odnosov z množičnimi mediji.

Ker pa je kriza zelo stresen dogodek, pa Arpan in Pompper (v Malešič 2004) opozarjata, da moramo biti pri kriznem komuniciranju pozorni predvsem na tri omejitve, in sicer:

1. Tveganje, ki ga lahko odkrito govorjenje o krizi, njenih vzrokih in posledicah prinese v pravnem smislu. Na eni strani sta torej interes in potreba različnih javnosti po informacijah, na drugi strani pa interes subjekta, na katerega se kriza nanaša (razpetost med verodostojnostjo subjekta in njegovo potencialno pravno odgovornostjo za krizne razmere).

2. Koordiniranje informacijskega toka, posredno pa zadeva tudi strategijo sodelovanja organizacije z množičnimi mediji in javnostjo. V primerih, ko množični mediji sami odkrivajo krizo in njene posamične razsežnosti, subjekt izgubi možnost usmerjanja informacijskega toka, saj ga mediji prehitevajo in odpirajo vprašanja, na katera ni pripravljen in nanje nima odgovora.
3. Nadzor nad oblikovanjem informacij. Heath (v Malešič in drugi 2006, 34) meni, da je sposobnost nadzora oblikovanja informacij v krizi lahko velika prednost, saj subjekt ne more neposredno vplivati na odziv množičnih medijev in javnosti, lahko pa ponuja informacije in vrednostne sodbe, s čimer pokaže sposobnost nadziranja krize. S proaktivnostjo komuniciranja pa ne smemo pretiravati, saj nas lahko to pripelje do pretiranega medijskega pokrivanja krize in umetnega povečanja le-te, kar pa prinaša nove težave in nepredvidljivosti (Malešč in drugi 2006, 21–22).

Ko je enkrat zagotovljeno komuniciranje med prej naštetimi akterji, pa je pomembno, kako poteka komuniciranja. Tako Lerbinger (1997, 39–49) navaja nekaj navodil, kako naj bi komuniciranje potekalo, in sicer:

- krizo je treba priznati in se z njo soočiti,
- določiti je treba krizni komunikacijski center,
- opreti se je treba na dejstva in izbrati čim več natančnih informacij, ki jih preko množičnih občil posredujemo javnosti,
- subjekt, ki ga prizadene kriza, naj ´govori z enim glasom´, ki naj preprosto posreduje najbolj sveže informacije,
- uporabljati je treba različne oblike komuniciranja in posredovati vse informacije, brez prikrivanja,
- treba je sodelovati z lokalnimi skupnostmi in drugimi akterji kriznega upravljanja in vodenja.

Na uspešnost komuniciranja pa vpliva tudi kakovost informacij, ki lahko zadevajo vsebino, varnost prenosa in pravočasnost sporočila.

Vsebina informacij je seveda odvisna predvsem od pošiljatelja in okoliščin, v katerih nastaja sporočilo. Tehnologija komuniciranja je lahko v prid – saj podpira pridobivanje informacij za sporočilo tako po obsegu kot tudi po širini in pravočasnosti.

Seveda pa slaba pripravljena informacija ostane slaba tudi ob najpopolnejši tehnologiji komuniciranja.

Varnost prenosa se v povprečju izboljšuje z izpopolnjevanjem tehnologije komuniciranja, ki odpravlja ali omejuje motnje na prenosnih poteh – telekomunikacijske povezave so vse boljše, zapisi informacij na raznih medijih pa obilnejši in zato varnejši pred nesporazumi, ki jih prinaša pretirana jedrnatost. Tehnologija komuniciranja pa mora le malo vplivati na proces kodiranja in dekodiranja sporočil, saj je oboje odvisno od ljudi – pošiljateljev in prejemnikov sporočil.

Zanesljivost prenosa je pomembnejša, kot se zdi na prvi pogled. Velikokrat se lahko zgodi, da so nečitljivi telefaksi, zasedene telefonske linije in še kaj.

Zaupnost prenosa je pri komuniciranju zelo pomembna – zato je potrebno uporabljati tehnologije, ki zagotavljajo primerno varnost ob zmernih stroških in primerni učinkovitosti.

Pravočasnost sporočila je relativna in je v povprečju popolnejša tehnologija komuniciranja ne izboljšuje, čeprav pa je za uspešno delovanje v kriznih razmerah izredno pomembno, da sporočilo prispe pravi čas, ko še ni storjena prevelika škoda (Možina 1998, 104).

4.1 Štiristopenjska metoda analize krize

Poleg prej omenjenih navodil za potek komuniciranja, pa je na koncu pomembna tudi analiza krize, ki nam omogoča, da vidimo naše napake, kakor tudi pozitivna ukrepanja ob nesrečah.

Tako Stern in sodelavci (v Možina 2001) opozarjajo, da je ključna metoda pri analizi krize štiristopenjska metoda, tako imenovana metoda kognitivno-institucionalnega pristopa, ki naj bi bila, na podlagi njihovih izkušenj in spoznanj, sestavljena iz naslednjih raziskovalnih korakov:

1. Umestitev krize v kontekst zahteva umestitev vsake proučevane krize v njen zgodovinski, institucionalni in politični kontekst. Ta korak je zaradi občutljivosti

in nujnosti kontekstualne interpretacije kriznega vedenja nujen, kajti vsaka kriza je vpeta v svoj kontekst, ki vpliva na kognitivni okvir, organizacijski repertoar in politično občutljivost akterjev kriznega upravljanja in vodenja.

2. Opredelitev časovnega okvira oziroma oblikovanje sintetičnega opisa krize. Časovni okvir običajno temelji na kronološki razmejitvi, ki je za večino kriz relativno preprosta. Vendar pa se prepogosto srečujemo s primeri, kjer preprosta kronološka razmejitev ne zadostuje oziroma ne omogoča oblikovanja časovnega okvira krize. Gre predvsem za krize, pri katerih eskalacija oziroma deeskalacija nista jasno razvidni in ki lahko preidejo v dolgotrajno kronično politično travmo.
3. Analiza akutne krize oziroma identifikacija odločitvenih priložnosti razcepi akutni del krize na zaznane odločitvene priložnosti oziroma dileme, ki dejansko tvorijo krizo. Da bi se izognili pretirani subjektivnosti, se lahko opremo na naslednje kriterije izbire odločitvenih priložnosti:
    a. Pomembnost in zahtevnost sprejete odločitve v kontekstu celotnega procesa kriznega upravljanja in vodenja.
    b. *Post hoc* pomembnost odločitve, pri kateri je temelj analize njen retrospektivni vpliv na potek kriznega upravljanja in vodenja ter na razvoj krize.
    c. Pedagoška vrednost odločitve z vidika najboljšega oziroma najslabšega primera odločanja.
    d. Dileme, ki so jih odločevalci zaznali, vendar so bile razrešene kot rutinske in so med krizo povzročile nepredvidene zaplete.

Z razrezom krize na najmanjše odločevalske priložnosti se raziskovalec, kljub določeni ravni subjektivnosti, približa kompleksnosti odločevalskega procesa oziroma realnosti, v kateri so delovali akterji kriznega upravljanja in vodenja.

4. Vnovično sestavljanje krize in njena usmeritev v širši družbeni kontekst. Subjektivni presoji posameznega raziskovalca je sicer prepuščeno, katere analize bi izvedel, čeprav je analitično najoptimalnejša primerjava lastnih ugotovitev v okviru izbranih analitičnih tem z že izvedenimi analizami v kompatibilnem analitičnem pristopu, kar omogoča oblikovanje novih generaliziranih spoznanj o fenomenu kriznega upravljanja in vodenja.

Holističnemu delu analize sledi poglobljena parcialna analiza v obliki analitičnih tem. V primeru analize kriznega upravljanja in vodenja so ključne analitične teme naslednje: preventiva in priprave na krizo, organi kriznega odločanja, vodenje in vodeni, zaznavanje in oblikovanje krize, vrednostni konflikt, politično organizacijski konflikt in sodelovanje, krizno komuniciranje in kredibilnost, internacionalizacija, časovni učinki in pridobljene izkušnje in znanja (Grošelj v Malešič 2006b, 73–74).

Med zgoraj naštetimi analitičnimi temami se bom osredotočila predvsem na krizno komuniciranje in kredibilnost, saj je ta tema ključna za razumevanje mojega diplomskega dela. Ta analitična tema analizira procese kriznega komuniciranja na naslednjih ravneh: na prenos informacij znotraj sistema kriznega upravljanja in vodenja, odnose med akterji kriznega upravljanja in vodenja ter mediji ter komuniciranje akterjev kriznega upravljanja in vodenja s prizadetim prebivalstvom.

Krizno komuniciranje je strateškega pomena za uspeh kriznega upravljanja in vodenja, saj, kot ugotavljajo Lindy, Stern in Svedin (v Malešič 2004, 469–170), da še tako učinkovito krizno upravljanje in vodenje lahko mediji prikažejo kot popoln neuspeh. Zato je zaradi vse pomembnejše vloge medijev v delovanju sodobnih družb uspešnost komuniciranja med sistemom kriznega upravljanja in vodenja ter mediji oziroma javnostmi strateški del priprav in delovanja kriznega upravljanja in vodenja.

Izredni dogodki, kot so katastrofe, krize, konflikti, zločini in korupcija, pritegnejo veliko medijsko pozornost, saj ustvarjajo zgodbo. Stern in Sundelius (v Novak 2000) tako opredeljujeta dve strategiji pristopa h kriznemu komuniciranju: obrambno ali zaprto in proaktivno ali odprto držo. Obrambna ali zaprta drža akterjev kriznega upravljanja in vodenja pogosto antagonizira medije in povzroči izgubo kredibilnosti, medtem ko z odprto, proaktivno držo vzdržujejo iniciativo pri zagotavljanju informacij in prijateljskega odnosa z mediji.

Uspešnost kriznega komuniciranja temelji na uspešnih pripravah. Grošelj (2006) povzema, da so kot osnovni pogoji za uspešno komuniciranje priprave na javno podajanje informacij in profesionalizacijo te funkcije ter sposobnost spremljanja medijskega poročanja, ki omogoča primerno razlago oziroma dojemanje povratnih informacij.

Novak (2000) pa pravi, da je ključnega pomena za uspeh kriznega komuniciranja priprava načrta kriznega komuniciranja, ki mora biti kratek, jedrnat in prožen, tako da bi zagotavljal uspešno delovanje v nepredvidljivih okoliščinah krize. Kljub pripravam in načrtom pa se mora vsak akter kriznega vodenja in upravljanja zavedati, da ima z mediji med krizo in po njej tako divergentne kakor tudi konvergentne interese, pri čemer je cilj vsakega akterja kriznega upravljanja in vodenja preprečitev pojava informacijske praznine oziroma najplodnejšega obdobja za pojav govoric ter popačen prikaz dogajanja, ki pogosto vodi v izgubo kredibilnosti.

Pomembni vidik kriznega komuniciranja so tudi prenos, obdelava in posredovanje informacij znotraj sistema kriznega upravljanja in vodenja. Grošelj ugotavlja, da vsaka kriza izpostavlja krizno upravljanje in vodenje velikim informacijskim zahtevam, zato postajajo vse pomembnejši vidiki kriznega komuniciranja znotraj sistema kriznega upravljanja in vodenja pridobivanje informacij in njihovi pretoki znotraj sistema. Uspešnost tega segmenta kriznega komuniciranja je odvisna od začetnega informacijskega toka, ki vsebuje informacije, ki odločujoče vplivajo na zaznavanje in okvirjanje krize, posledično pa tudi na potek kriznega upravljanja in vodenja. Poleg pridobivanja imata pomembni vlogi tudi učinkovita izraba in obdelava informacij, ki je pogosto pogojena predvsem z delitvijo dela med različnimi akterji in ravnjo centralizacije (Grošelj v Malešič 2006b, 81−82).

5 VARNOST IN UPORABA INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE

Hiter vsesplošen razvoj po 2. svetovni vojni je prinesel nove razsežnosti tudi tehničnemu in tehnološkemu razvoju, ki je vplival na razvoj in razmah informacijsko-komunikacijskih tehnologij.

Informacijsko-komunikacijska tehnologija (IKT), temelječa na mikroelektroniki, je pomemben rezultat znanstveno-tehnološkega napredka in eden glavnih elementov razvoja celotne družbe v drugi polovici 20. stoletja. Danes lahko rečemo, da je informacijsko-komunikacijska tehnologija zaradi ekonomskih oziroma gospodarskih, sociooloških in kulturnih implikacij postala pomemben del obče razvojne strategije informacijsko razvitih držav. Zaradi svojih značilnosti je izpostavila pomen informacijske moči, temelječe na podatkih, informacijah, znanju in razumevanju, kot elementih kognitivnega procesa, zato nekateri avtorji govorijo tudi o revoluciji v informacijskih oziroma strateških zadevah (Wik – revolution in information affairs, Freedman – revolution in strategic affairs) (Pinterič in Svete 2007, 158).

5.1 Družbene implikacije uporabe informacijsko-komunikacijske tehnologije

Za pomen mojega diplomskega dela pa ne morem mimo družbene implikacije uporabe informacijsko-komunikacijske tehnologije, kajti družba, v kateri živimo, je tako imenovana informacijska družba, katere najpomembnejša osnova je digitalizacija.

Medtem ko so se včasih za shranjevanje in prenos informacij uporabljali materialni nosilci in analogne tehnike prenosa, pa je danes večina področij informacij digitalnih. Digitalizacija pomeni razčlenitev informacij v najpreprostejše elementarne dele (bite), pri čemer ni pomembno, ali gre za govor, pisavo, tonske zapise, slike grafike ali video. Popolna objektivizacija informacij, ki jo omogoča digitalna tehnika, je tako temelj poenotenega shranjevanja vseh vrst informacij, stroškovno ugodnega in praktično poljubnega razmnoževanja oziroma širjenja, zamenjave do sedaj različnih načinov prenosa informacij z enotnim medijem njihovega prenosa in obdelave – računalniškimi mrežami, ter integracije različnih vrst informacij na eni platformi (multimedija). Na

digitalni tehniki temelječa računalniška omrežja predstavljajo tako »super« medij, ki je sposoben združiti vse dosedanje informacijske in komunikacijske medije ter jih hkrati dopolniti s funkcionalnimi zmogljivostmi, ki še niso bile na razpolago (Svete 2005b, 25–28).
Mikroelektronika je osrednjega pomena za razvoj novih informacijskih tehnologij. Šele njen razvoj je namreč omogočil elektronsko obdelavo velikih količin podatkov. Lahko rečemo, da so tehnične izboljšave in znižanje stroškov na tem področju v zadnjih treh desetletjih v zgodovini tehnike enkraten primer. Hkrati pa lahko pričakujemo nadaljnji razvoj tako zmožnosti obdelave logičnih procesov kot tudi shranjevanja podatkov.

Drugi, osrednji element informacijske revolucije pa je povezan z razvojem tehnologij za prenos podatkov, ki imajo dejansko revolucionarni vpliv na komuniciranje v sodobnih družbah. Eno samo optično vlakno, ki ima manjši premer kot človeški las, je tako sposobno prenosa več deset tisoč telefonskih pogovorov ali več deset televizijskih programov praktično brez izgube podatkov. Tako kot na področju živčnega prenosa podatkov, je bil velik razvoj dosežen tudi na področju brezžičnega prenosa tako s satelitskimi tehnologijami kot tudi mobilnimi zemeljskimi povezavami (danes smo že vstopili v tretjo generacijo mobilne telefonije UMTS). Izredno hiter razvoj, razširjenost in konkurenca so glavni vzroki za izreden padec cen IKT (Svete 2005b, 30–31).

Informacijska revolucija ima torej izjemne učinke na gospodarstvo, družbo in politiko. Velik nivo učinkov se nanaša na zaznavo prostora, časa in informacij. Informacije in komunikacije sta osrednja dejavnika za delovanje na delitvi dela temelječih družb. Na eni strani igrajo informacije pomembno vlogo v storitvenem sektorju pri upravljanju in reguliranju avtomatiziranih procesov, na drugi strani pa zahteva delitev dela in specializacija organizacijske stroške, ki terjajo informacijsko podporo in intenzivno komuniciranje med udeleženci. Informacije in komunikacije so določene s prostorom in časom. Premagovanje prostorskih razdalj je bilo s tradicionalnimi analognimi tehnologijami zelo drago, prav tako pa je bilo, z izjemo telefona in telefaksa, tudi zelo počasno. Z digitalno tehnologijo in povezovanjem računalnikov v mreže shranjevanje in posredovanje informacij ni več povezano zgolj z enim materialnim podatkovnim nosilcem, zato lahko prejemnik informacije brez časovne izgube posreduje naprej. Tako se je izjemno večala zmogljivost prostorsko neodvisnih družbenih interakcij, prav tako

pa je možna sinhronizacija poteka dela pri istočasnem zmanjševanju komunikacijskega šuma oziroma izgube informacij.

Svete pravi, da ugotovitve na področju družboslovne informatike namreč kažejo, da posamezne lokalne oblasti celo znotraj iste države selektivno sprejemajo ter različno razvijajo posamezne vrste informacijskih sistemov, na kar vpliva zlasti oblika njihove notranje organizacije ter odnos do pomena tehnologije same. To kombinacijo opreme, ljudi, vladnih struktur ter informacijsko-komunikacijskih politik Svete, po Klingu, imenuje lokalni računalniški paket (Svete 2005b, 32–35).

Ena izmed najpomembnejših idej družboslovne informatike v odnosu do predmeta preučevanja je nedvomno povezana z družbenim kontekstom razvoja ter uporabe informacijske tehnologije, ki ključno vpliva na način, kako ljudje uporabljajo tehnologijo pri delu, v organizacijah in drugih družbenih odnosih (Svete 2005b, 36).

6 UREDITEV SISTEMA VARSTVA PRED NARAVNIMI IN DRUGIMI NESREČAMI TER INFORMACIJSKO-KOMUNIKACIJSKE TEHNOLOGIJE

Slovenska zakonodaja določa, kateri so poglavitni preventivni ukrepi ob naravnih nesrečah. Kljub temu se nanje le odzivamo, za preventivo pa ni zagotovljenih dovolj sredstev. Najpomembnejši akti, ki opredeljujejo razmerje slovenske družbe do naravnih nesreč, so (Komac in Zorn 2008, 53–59):

- Nacionalni program varstva pred naravnimi in drugimi nesrečami (poglavitni akt, na katerem temelji varstvo pred naravnimi nesrečami in določa preventivne ukrepe po vrstah nesreč),
- Resolucija o nacionalnem programu varstva okolja (strateški dokument, katerega cilj je izboljšanje okolja in kakovosti življenja),
- Zakon o varstvu pred naravnimi in drugimi nesrečami (temelji na prejšnjih dveh in govori o zaščiti in reševanju ob konkretnih nesrečah, ter zahteva določene preventivne ukrepe),
- Strategija prostorskega razvoja Slovenije (novosti sta zahtevi po obveznem upoštevanju naravnih procesov in preventivnem načrtovanju),
- Zakon o prostorskem načrtovanju (ključni cilji so: omogočati skladen prostorski razvoj z obravnavo in usklajevanjem različnih potreb in interesov razvoja z javnimi koristmi na področjih varstva okolja, ohranjanja narave in kulturne dediščine, varstva naravnih virov, obrambe in varstva pred naravnimi in drugimi nesrečami),
- Zakon o vodah (opredeljuje ogrožena območja in določa možne posege glede na stopnjo ogroženosti),
- Zakon o graditvi objektov,
- državni razvojni program,
- regionalni razvojni programi.

Čeprav slovenska zakonodaja ob naravnih nesrečah določa poglavitne preventivne ukrepe, so dokumenti praviloma namenjeni upravljanju z naravnimi nesrečami in sanaciji. Premalo pozornosti pa posvečamo preventivi; zanjo ni zagotovljenih dovolj sredstev.

V Sloveniji so se po letu 1991 na področju varstva pred nesrečami zgodile pomembne spremembe. Sprejeta je bila nova zakonodaja, ki je varstvo pred nesrečami povezala v organizacijsko in funkcionalno celoto, v podsistem nacionalne varnosti Republike Slovenije. Nova zakonodaja je zahtevala spremembe na področju opazovanja, obveščanja in javnega alarmiranja, operativnih govornih in podatkovnih zvez, organiziranja sil za zaščito, reševanje in pomoč, izobraževanja in usposabljanja za varstvo pred nesrečami ter drugih področjih. Z novo zakonodajo so bile jasneje razmejene pristojnosti med državo in občinami. Občine so po sedanji ureditvi primarno odgovorne za varstvo pred nesrečami na svojem območju (Ušeničnik 2002, 462).

Slovenija je bila v tem času zelo dejavna tudi na področju mednarodnih odnosov. Takoj po osamosvojitvi se je odprla v svet in stopila na pot enakopravnega sodelovanja z drugimi članicami mednarodne skupnosti in z mednarodnimi organizacijami. S sosednjimi in drugimi državami v regiji je pogodbeno uredila medsebojno pomoč in sodelovanje na področju varstva pred nesrečami ter ustvarila najnujnejše kadrovske in materialne možnosti za sodelovanje v mednarodnih humanitarnih akcijah (Ušeničnik 2002, 462).

Varstvo pred naravnimi in drugimi nesrečami, kakršnega poznamo danes, oziroma h kakršnemu težimo, obsega vse preventivne, zaščitne in reševalne, sanacijske in druge dejavnosti, ki prispevajo k večji varnosti ljudi, premoženja, kulturne dediščine in okolja pred nevarnostmi naravnih in drugih nesreč. Zavedati pa se je potrebno, da se težišča teh dejavnosti spreminjajo, ker se spreminjajo tudi nevarnosti in ogroženost. Danes nas na primer jedrske nesreče, nesreče s strupenimi kemikalijami, nakopičeno jedrsko orožje in naraščajoči terorizem skrbijo prav tako, če ne celo bolj, kot potresi, poplave, suša in druge naravne nesreče. Seveda se zavedamo, da popolne zaščite pred nevarnostmi ni mogoče zagotoviti, toda žrtve in škodo, ki jo povzročajo nesreče, je mogoče zmanjšati, še zlasti s preventivnimi ukrepi in vsestransko pripravljenostjo za ukrepanje.

Naravne in druge nesreče ogrožajo fizično, socialno in ekonomsko varnost prebivalcev ter splošno varnost in blaginjo v državi. Zato je varstvo pred nesrečami eden od strateških nacionalnih interesov Republike Slovenije. Slovenska država se je na te nevarnosti odzvala z organiziranjem sistema varstva pred nesrečami (Ušeničnik 2002, 462).

Z novo zakonodajo, ki je bila sprejeta po letu 1992, je bilo varstvo pred naravnimi in drugimi nesrečami v Sloveniji izločeno iz obrambnega sistema z namenom, da se organizira kot celovita interdisciplinarna dejavnost, ter da se vse reševalne službe in druge namensko organizirane sile za zaščito, reševanje in pomoč povežejo v organizacijsko in funkcionalno enoten sistem. Tako so se na tem področju odprle možnosti najširšega sodelovanja nevladnih organizacij ter možnosti postavitve in uporabe skupne telekomunikacijske, informacijske, izobraževalne in druge infrastrukture. Preventiva je formalnopravno postala temeljna usmeritev in naloga tega sistema, težišče njegovega delovanja pa je v lokalnih skupnostih.

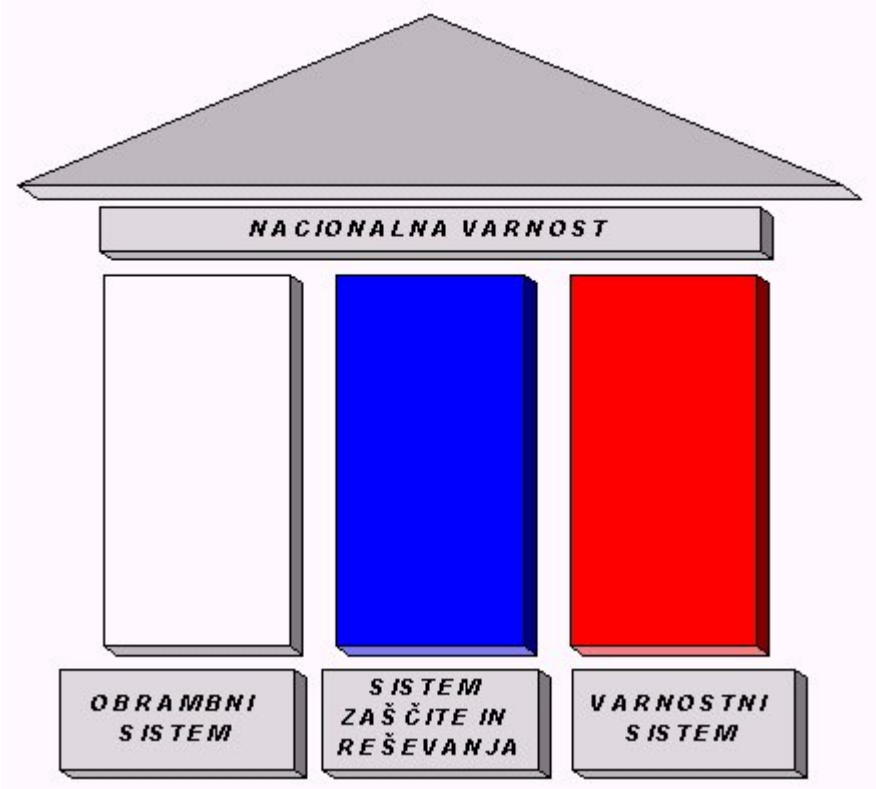
Nova zakonodaja zagotavlja, da se vse oblike zaščite, reševanja in pomoči izvajajo v skladu z načeli mednarodnega humanitarnega prava in mednarodnega prava o varstvu ljudi, živali, kulturne dediščine in okolja pred škodljivimi vplivi naravnih in civilizacijskih nesreč ter v skladu s sprejetimi mednarodnimi obveznostmi, da so vse te dejavnosti humanitarne in nevojaške narave ter da se zmogljivosti za zaščito, reševanje in pomoč, ki so na voljo, lahko uporabijo tudi v mednarodnih humanitarnih akcijah in pri uresničevanju drugih oblik humanitarnega poslanstva (Zakonodaja s področja zaščite, reševanja in pomoči 1992).

Sistem varstva pred naravnimi in drugimi nesrečami obsega celoto ukrepov, dejavnosti in postopkov za varstvo pred nesrečami ter izvajalce, ki se s tem ukvarjajo. Pravni temelj SNVRS (Sistem nacionalne varnosti Republike Slovenije) predstavljajo Ustava, zakoni in drugi predpisi, sklenjene mednarodne pogodbe ter splošno veljavna načela mednarodnega prava (Ušeničnik 2002, 466).

Nacionalni varnostni ustroj Republike Slovenije temelji na treh stebrih (glej Slika 6.1), in sicer stebru:

- obrambnega sistema,
- zaščite in reševanja (kamor sodi tudi zaščita pred nesrečami),
- varnostnega sistema.

Slika 6.1: Sistem nacionalne varnosti Republike Slovenije (SNVRS)



Vir: Zakonodaja s področja zaščite, reševanja in pomoči (1992).

Glavni cilj varstva pred nesrečami je zmanjšanje števila nesreč ter preprečitev oziroma zmanjšanje števila žrtev in drugih posledic (Ušeničnik 2002, 482).

Temeljne naloge sistema varstva pred nesrečami so:

- proučevanje nevarnosti in nesreč,
- izvajanje preventivnih ukrepov,
- zagotavljanje pripravljenosti za ukrepanje,
- zaščita, reševanje in pomoč,
- odpravljanje posledic in obnova (Ušeničnik 2002, 482).

Upravne in strokovne naloge v sistemu varstva pred naravnimi in drugimi nesrečami, v skladu z Zakonom o varstvu pred naravnimi in drugimi nesrečami, opravlja Uprava Republike Slovenije za zaščito in reševanje, ki je organizacijski organ v sestavi Ministrstva za obrambo. Pomembno vlogo v sistemu varstva pred naravnimi in drugimi nesrečami predstavlja sistem opazovanja, obveščanja in alarmiranja. Ta pa temelji na telekomunikacijsko-informacijskih sistemih, ki jih v grobem lahko razdelimo na:

- komunikacijski sistem:
  - sistem radijskih zvez in osebnega klica,
  - sistem fiksnih zvez,
- sistem javnega alarmiranja,
- informacijski sistem za zaščito in reševanje.

Skupna značilnost vseh sistemov je zahtevana visoka stopnja zanesljivosti, razpoložljivosti in varnosti delovanja. Komunikacijski sistemi so grajeni kot namenski profesionalni sistemi, temelječi na zasebnih namenskih komunikacijskih infrastrukturah in povezavah, ki so zaradi hitrega razvoja komunikacijsko-informacijskih tehnologij praviloma že zastarele ali iztrošene. Sistemi med seboj niso povezani, razen nekaj izjem. Prav zaradi tega v zadnjih letih pospešeno uvajajo nove tehnologije, ki temeljijo na enotni komunikacijsko-informacijski podlagi (Tavčar 2006a).

6.1 Zakonodaja in IKT

Prvi strateško-doktrinarni dokument, ki izpostavlja pomen uporabe IKT kot novega ogrožanja, je Resolucija o Strategiji nacionalne varnosti Republike Slovenije. Ob upadanju pomena vojaških virov ogrožanja se namreč vedno jasneje kažejo nevojaški viri ogrožanja, tveganja in izzivi, ki pa lahko, prav tako kot vojna, močno ogrozijo sodobne države in družbe. Ti so pogosto medsebojno povezani in soodvisni in delujejo transnacionalno. Republika Slovenija, kot razvita informacijska družba, postaja tako ranljiva tudi na področju informacijske varnosti (Resolucija o strategiji nacionalne varnosti republike Slovenije 2010).

Obrambna strategija Republike Slovenije je naslednji dokument, ki zelo splošno opredeljuje odnos do IKT. Uporabo IKT sicer identificira kot možni vir ogrožanja varnosti, saj med drugimi nevojaškimi grožnjami varnosti izpostavlja tudi pomen motenja delovanja in vdorov v informacijske sisteme (Strategija nacionalne varnosti Republike Slovenije 2000).

Nič pa obrambna strategija ne govori o varnostnih mehanizmih, ki bi obravnavali IKT, če izvzamemo načrte, v skladu s katerimi se bo sistem civilne obrambe preoblikoval v

celovit sistem kriznega upravljanja, namenjenega tudi za obvladovanje kriz v regionalnem ali širšem strateškem okolju, ne glede na njihove vzroke (Obrambna strategija Republike Slovenije 2000).

Na tem mestu bi omenila še SPOR (Strateški pregled obrambnega resorja 2009), ki z letom 2009 prvič pregleduje tudi področje varstva pred naravnimi in drugimi nesrečami, kajti prej so se omejili samo na obrambni sistem. Ugotovili so, da se nekatere naloge obrambnega resorja podvajajo, nekatere nujne naloge pa se celo ne opravljajo, zato želijo v prihodnosti obsežnejše in zahtevnejše naloge učinkovito opraviti z manj viri in se usmeriti proti ključnim in dosegljivim ciljem, prilagoditi obseg in strukturo zmogljivosti obrambnega resorja in se znebiti nekaterih nepotrebnih in neperspektivnih zmogljivosti, preusmeriti neizkoriščene kadrovske in finančne vire na prednostna področja, razvijati ključne zmogljivosti po načelu selektivne specializacije ter izboljšati usposobljenost, pripravljenost in operativno povezljivost zmogljivosti resorja med seboj in z drugimi resorji. Sistem varstva pred naravnimi in drugimi nesrečami dela dobro, toda še vedno so mogoče izboljšave, kar je nujno zaradi še boljših storitev za vse državljane in ker se tudi ta resor srečuje z vse manjšo razpoložljivostjo predvsem finančnih virov. Prav tako tudi državljani pričakujejo bolj poenoteno kakovost delovanja sil za zaščito in reševanje, kajti tu se srečujejo poklicne in prostovoljne enote (Strateški pregled obrambnega resorja 2009)

Ključni doktrinarni dokument v Sloveniji, ki predvideva uporabo IKT zaznava kot grožnjo nacionalne varnosti ter izpostavlja potrebo po oblikovanju varnostnih mehanizmov, je nedvomno doktrina civilne obrambe, sprejeta 25. 4. 2002 v Vladi Republike Slovenije. Doktrina je namreč temelj za sprejemanje vseh nadaljnjih ukrepov na področju civilne obrambe. Za IKT se tako predvideva načrtovanje in sprejetje ukrepov za zagotovitev delovanja v izrednem in vojnem stanju ter ob motnjah tako v državi kot tudi mednarodno. Posebej bodo načrtovani tudi ukrepi za zagotovitev sodelovanja med državnimi organi in Slovensko vojsko (Doktrina civilne obrambe Republike Slovenije 2002, 43–45).

6.2 Organizacijska ureditev

Pri integralnem upravljanju sistema nacionalne varnosti Republike Slovenije imata pomembno vlogo Svet za nacionalno varnost (SNAV) in Nacionalni center za krizno upravljanje (NCKU).

Že v Resoluciji o izhodiščih zasnove nacionalne varnosti je bilo zapisano, da vlada kot nosilka izvršne veje oblasti skrbi za uresničevanje nacionalnovarnostne politike in sistema nacionalne varnosti na vseh področjih in ravneh. Vlada kot najvišji organ izvršilne veje oblasti in državne uprave lahko za izpolnjevanje svojih nalog ustanavlja delovna telesa, delovne skupine in svete vlade. Za odzivanje na grožnje nacionalni varnosti pa je še zlasti pomemben Svet za nacionalno varnost (Prezelj v Malešič 2006b, 104–105).

SNAV je na podlagi veljavnega odloka pristojen za usklajevanje nacionalnovarnostne politike ter usmerjanje in usklajevanje dejavnosti, ki se izvajajo za uresničevanje interesov in ciljev nacionalne varnosti. SNAV ima sekretariat, ki ga tudi imenuje vlada, njegova naloga pa je operativno usklajevanje aktivnosti za delovanje SNAV-a, skrb za usklajeno izvedbo njegovih stališč in še druge naloge (Prezelj v Malešič 2006b, 104–107).

Leta 1998 je začel MORS sodelovati v ameriški pobudi, v okviru katere naj bi bili v državah Srednje in Vzhodne Evrope z ameriško pomočjo na strateški ravni ustanovljeni centri za krizni menedžment (National Military Command Center), ki bi zagotovili enotno vodenje v kriznih razmerah na nacionalni ravni, regionalno povezovanje teh držav, izmenjavo informacij za ukrepanje v kriznih razmerah. NCKU je začel delovati 1. 1. 2004.

NCKU je organiziran pri Ministrstvu za obrambo, od koder zagotavlja prostorske, tehnične, informacijske in telekomunikacijske pogoje za delo Vlade Republike Slovenije v skladu z zakonom v izrednem in vojnem stanju ter ob pojavih in dogodkih oziroma krizah v državi oziroma v regionalnem ali strateškem okolju, ki lahko pomembno ogrozijo nacionalno varnost.

NCKU deluje 24 ur na dan in ima naslednje naloge:

1. zagotavljanje informacijske in komunikacijske povezave za izmenjavo podatkov in informacij z Uradom predsednika RS, Generalnim sekretariatom DZ RS in Vlade, Svetom za nacionalno varnost, ministrstvi, vladnimi službami, Operativno komunikacijskim centrom Generalne policijske uprave, Centrom za obveščanje RS, Poveljniškim centrom Slovenske vojske ter operativnimi centri in dežurnimi službami drugih državnih organov ter z gospodarskimi družbami, zavodi in drugimi organizacijami, ki so po sklepu vlade posebnega pomena za obrambo;
2. zagotavljanje informacijske in komunikacijske povezave za izmenjavo podatkov in informacij, skladno s sprejetimi mednarodnimi obveznostmi države;
3. zagotavljanje prenosa odločitev za izvajanje ukrepov za pripravljenost, povelja za izvajanje mobilizacije in drugih ukrepov, načrtovanih za odzivanje na krizne pojave in dogodke;
4. opravljanje nalog državnega centra upravnih zvez;
5. opravljanje drugih nalog v skladu z navodili ministrstva za obrambo, ki pa ne smejo omejevati izvajanja nalog iz prejšnjih alinej (Prezelj v Malešič 2006b, 111–112).

Z ustanovitvijo NCKU se je spremenila struktura sistema kriznega upravljanja v RS, kot je prikazano na spodnjih slikah. Pri tem pa je potrebno poudariti, da je NCKU le del celotnega sistema podpore enotnega vodenja nacionalno-varnostnega sistema oziroma nacionalne varnosti in obrambe strani Vlade RS in da naj bi deloval v povezavi in koordinaciji z mnogimi drugimi centri v okviru tega sistema. V bistvu je temeljna funkcija NCKU pomoč pri koordinaciji med podsistemi nacionalno-varnostnega sistema (Prezelj v Malešič 2006b, 113).

7 KOMUNIKACIJSKO-INFORMACIJSKI SISTEMI

Komunikacijsko-informacijsko podporo na področju varstva pred naravnimi in drugimi nesrečami zagotavlja Uprava Republike Slovenije za zaščito in reševanje v okviru področja opazovanja, obveščanja in alarmiranja. Za lažje razumevanje posameznih komunikacijsko-informacijskih sistemov pa bi najprej na kratko predstavila sam razvoj telekomunikacijskih sistemov ter omenila še, katere so bistvene lastnosti, ki jih naj bi ti sistemi vsebovali, za njihovo učinkovitost, nato pa bom nadaljevala s kratkim pregledom že prej omenjenih komunikacijsko-informacijskih sistemov.

Razvoj telekomunikacijsko-informacijskih sistemov na področju varstva pred naravnimi in drugimi nesrečami poteka hitro, tako da ga lahko razdelimo, po mnenju strokovnjaka na tem področju, Boštjana Tavčarja (2003), v različna časovna obdobja.

Za prvo obdobje pred letom 1994 je značilno, da razen razdrobljenega in medsebojno nepovezanega sistema javnega alarmiranja ni bilo vzpostavljenih drugih sistemov. Prav zaradi te razdrobljenosti in medsebojne nepovezanosti je bila težnja k večji povezljivosti teh sistemov, ki bi posledično vplivali na večjo učinkovitost.

Drugo obdobje, od leta 1994 do leta 2002, je bilo obdobje pospešenega prenavljanja in uvajanja telekomunikacijsko-informacijskih sistemov. V tem času je bil zgrajen sistem operativnih radijskih zvez in osebnega klica. Prenovili, poenotili in centralizirali so sistem javnega alarmiranja, vzpostavili interni sistem fiksnih zvez in globalno računalniško omrežje. Vsi sistemi so bili načrtovani kot neodvisne zaključene celote brez medsebojnih povezav.

V tretjem obdobju, ki še vedno poteka, sta zastavljena dva ključna cilja. Kot prvo, posodobiti sistem, predvsem z namenom zagotavljanja učinkovitejšega prenosa podatkov, še zlasti v mobilnih radijskih omrežjih, in kot drugo, vzpostaviti enotno telekomunikacijsko-informacijsko podlago vseh sistemov.

Enotna telekomunikacijsko-informacijska podlaga bo omogočila vzpostavitev posameznih sistemov na navideznih nivojih, ki so prilagodljivejši od ločenih fizičnih

omrežij posameznih sistemov, omogočajo pa tudi medsebojno izmenjavo podatkov med posameznimi sistemi in njihovo centralno upravljanje in nadzor (Tavčar 2002).

7.1 Zagotavljanje zanesljivosti, varnosti in razpoložljivosti

Tri bistvene lastnosti telekomunikacijsko-informacijskih sistemov na področju varstva pred naravnimi in drugimi nesrečami so: zanesljivost, varnost in razpoložljivost. Včasih je strategija zagotavljanja zanesljivosti, varnosti in razpoložljivosti temeljila predvsem na dveh predpostavkah:

- lastnem ali nadzorovanem najetem fizičnem omrežju,
- popolnem državnem nadzoru nad telekomunikacijskimi in državnim operaterjem.

Z graditvijo lastnih fizičnih omrežij in najemom fizičnih telekomunikacijskih povezav pri državnem operaterju telekomunikacij so lahko zagotavljali zanesljive, varne in razpoložljive poti. Z razvojem telekomunikacijske tehnologije so fizične povezave vse bolj izgubljale na pomenu oziroma so postajale del enotnega javnega telekomunikacijskega omrežja. Poleg tega pa so fizične povezave v primerjavi z drugimi možnostmi postajale vse dražje.

Z liberalizacijo trga telekomunikacij in privatizacijo nekdaj edinega državnega operaterja država izgublja nadzor nad telekomunikacijami. To je vodilo k spremembi strategije zagotavljanja zanesljivosti, varnosti in razpoložljivosti. Nova strategija temelji predvsem na dveh predpostavkah:

- najemu navideznih prenosnih poti v različnih relativno zanesljivih javnih omrežjih,
- zagotavljanju varnosti s kriptozaščito prenesenih podatkov (Tavčar 2002).

Tavčar (2009) pa je bil na svoji predstavitvi prepričan, da sta poleg teh treh lastnosti za zagotavljanje nemotenega delovanja informacijsko-komunikacijskih sistemov na področju varstva pred naravnimi in drugimi nesrečami potrebni še dve lastnosti, in sicer zmožnost in vzdržljivost.

Tako naj bi bila zmožnost sposobnost informacijsko-komunikacijskih sistemov, da s svojimi storitvami zadostijo vsem realnim potrebam uporabnikov, kar vključuje uporabljene tehnologije, orodja za izdelavo programske opreme in aplikacije.

Kot druga je zanesljivost, ki je sposobnost informacijsko-komunikacijskih sistemov in njegovih posameznih sklopov, da zagotavljajo zahtevane funkcije pod danimi pogoji in v zahtevanem časovnem intervalu.

Razpoložljivost je sposobnost informacijsko-komunikacijskih sistemov, da je na razpolago uporabnikom v vseh razmerah in v skladu s prednostmi posameznih uporabnikov.

Naslednja je vzdržljivost, ki je odpornost sistemov na preobremenitve, motnje, okvare ter druge predvidene in nepredvidene dogodke.

Kot zadnja lastnost, a prav tako zelo pomembna, je varnost, ki je sposobnost sistemov, da zagotavljajo varnost in po potrebi zaupnost podatkov (organizacija varovanja, tehnično varovanje, fizično varovanje) (Tavčar 2009).

7.2 Sistem radijskih zvez in osebnega klica

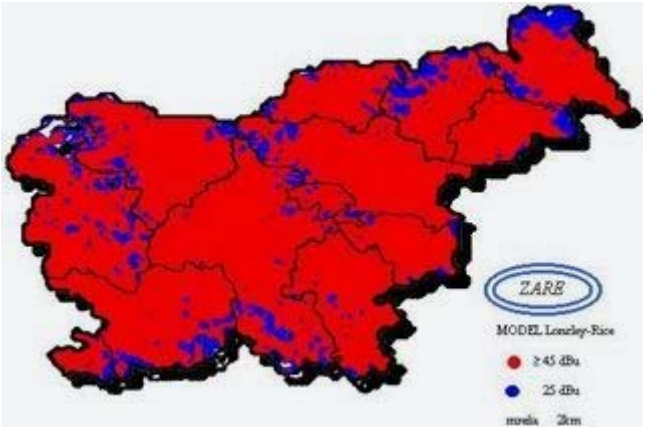
Sistem radijskih zvez in osebnega klica je največji profesionalni radijski sistem v državi, namenjen operativnim, govornim in podatkovnim komunikacijskim povezavam med pripadniki enot za zaščito, reševanje in pomoč. Razdeljen je v tri podsisteme:

- podsistem konvencionalnih radijskih zvez ZARE,
- podsistem snopovnih radijskih zvez ZARE PLUS,
- podsistem osebnega klica.

Podsistem konvencionalnih radijskih zvez ZARE omogoča zgolj govorne komunikacije in je namenjen množičnim radijskim povezavam med pripadniki posameznih enot za zaščito, reševanje in pomoč (Tavčar 2006b).

Sistem zvez ZARE zagotavlja 95-odstotno pokritost (glej Slika 7.1) terena z radijskim signalom stacionarne repetitorske mreže in popolno pokritost terena ob uporabi mobilnih repetitorskih postaj.

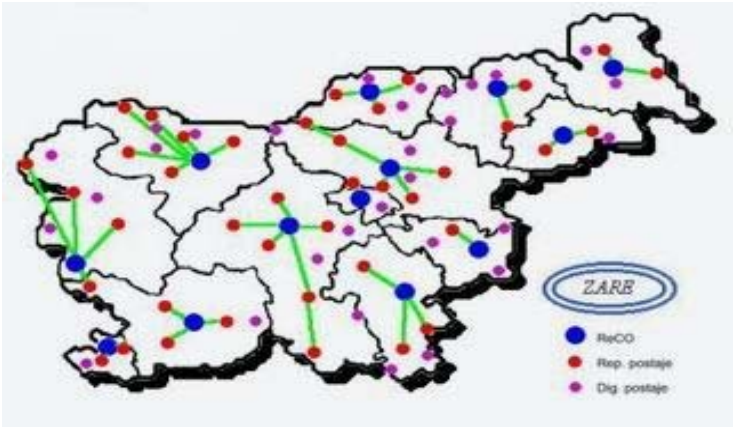
Slika 7.1: Pokritost sistema zvez ZARE



Vir: Telekomunikacijski sistem (1995).

Po obsegu je največji enotni profesionalni sistem radijskih zvez (PMR) v državi. Njegovo omrežje sestavlja 40 repetitorskih postaj zgornje in 56 digitalnih repetitorskih postaj spodnje oddajniške mreže (glej Slika 7.2). Spodnjo oddajniško mrežo sproti dograjujemo.

Slika 7.2: Repetitorske postaje oddajniških mrež



Vir: Telekomunikacijski sistem (1995).

Tehnologije na področju telekomunikacij so ene izmed najhitreje razvijajočih se tehnologij na svetu. To ima za posledico zelo hitro tehnološko staranje opreme.

Klasično analogno tehnologijo vse bolj izpodriva zmogljivejša in cenejša digitalna tehnologija. Na področju profesionalnih radijskih zvez po svetu trenutno prevladujejo še klasični analogni sistemi, ki jim je že oziroma jim bo v nekaj letih potekla življenjska doba. V naslednjih nekaj letih zato pričakujemo pospešeno graditev novih digitalnih sistemov profesionalnih radijskih zvez. Z namenom poenotenja standardov na področju digitalnih profesionalnih radijskih zvez je Evropski telekomunikacijski inštitut za standardizacijo (ETSI) predpisal enotne standarde novega digitalnega snopovnega sistema, poimenovanega TETRA (TErrestrial Trunked RAdio). Enotni standardi zagotavljajo medsebojno povezljivost radijskih sistemov in možnost uporabe radijskih postaj različnih proizvajalcev. V Evropi deluje že kar nekaj sistemov zvez TETRA (Telekomunikacijski sistem 1995).

Tudi v Republiki Sloveniji bi bilo potrebno medorganizacijsko krizno povezljivost na operativni ravni dopolniti z uvedbo enotnega nacionalnega sistema kriznega brezžičnega komuniciranja po standardu TETRA (TErrestrial Trunked RAdio). Gre za digitalno radijsko omrežje, ki bi slovenskim organom kriznega upravljanja omogočilo kompatibilnost radijskih postaj, kar v splošnem smislu še ne obstaja. Z možnostjo poljubnega oblikovanja navidezno samostojnih mrež bi bila zagotovljena maksimalna fleksibilnost kombiniranja komunikacijske povezljivosti na lokalni, regijski in nacionalni ravni. TETRA omogoča tudi prenašanje videoposnetkov s terena (letala, helikopterja ipd.) v digitalno računalniško mrežo in nasprotno, kar se pri sodobnem kriznem upravljanju zelo potrebuje. Strategija graditve enotnega digitalnega omrežja za potrebe državnih organov se ne izvaja s pričakovano dinamiko. Ciljno stanje v državi mora biti v tem, da imajo vsi državni organi (in tudi institucije, ki sodelujejo z državo) kompatibilne radijske postaje (Prezelj 2007, 192).

Podsistem snopovnih radijskih zvez ZARE PLUS omogoča avtomatske govorne in podatkovne komunikacije in je namenjen predvsem službam nujne medicinske pomoči, gasilskim enotam posebnega pomena in štabom civilne zaščite.

Radijske postaje snopovnega sistema radijskih zvez ZARE PLUS so preproste za uporabo. Vsaka radijska postaja ima svojo klicno številko, podobno kot prenosni telefoni. Uporabnik lahko kliče individualno, skupinsko, kliče v javno telefonsko omrežje in pošilja kratka pisna sporočila. Možen je prenos podatkov. Hitrost prenosa

podatkov je majhna, zato je mogoč le prenos omejene količine podatkov, na primer kratkih sporočil, lokacije kličočega in drugo.

Podsistem osebnega klica omogoča enosmerni prenos sporočil in je namenjen hitremu aktiviranju reševalnih enot. Deluje po sistemu POCSAG, ki je standard za digitalni prenos osebnih klicev. Sistem omogoča hitro in zanesljivo pošiljanje osebnih klicev. V sistem je vključenih več kot 15.000 sprejemnikov osebnega klica.

7.3 Sistem fiksnih zvez

Sistem fiksnih zvez vključuje povezave v javna telekomunikacijska omrežja za prenos klicev s številke 112, najete povezave za neposredne povezave z reševalnimi službami, povezave med telefonskimi centralami in alternativne povezave preko omrežja svetovnega spleta. Komunikacijska središča predstavljajo telefonske centrale ISDN v regijskih centrih za obveščanje.

7.4 Sistem javnega alarmiranja

Sistem javnega alarmiranja v Republiki Sloveniji je zasnovan kot enoten, hierarhično povezan sistem siren. Obsega tri ravni:

- državno,
- regijsko,
- lokalno.

Regijske alarmne centrale so na državno alarmno centralo priključene preko fiksnega omrežja Uprave Republike Slovenije za zaščito in reševanje. Sirene in lokalne alarmne centrale so na regijske centrale lahko priključene preko fiksnih najetih telekomunikacijskih povezav Telekoma Slovenije ali preko radijskih povezav. Fiksno povezavo vzpostavi Telekom Slovenije med sireno ali lokalno alarmno centralo in regijsko alarmno centralo. Radijsko povezavo vzpostavi izbrani ponudnik med sireno ali lokalno alarmno centralo in radijsko vstopno točko na regijskem centru za obveščanje. Povezava je lahko neposredna ali preko digitalnih repetitorjev (Tavčar 2006a).

7.5 Informacijski sistem za zaščito in reševanje

Informacijski sistem ZIR je samostojen in celovit informacijski sistem varstva pred naravnimi in drugimi nesrečami na podlagi globalnega računalniškega omrežja ZIR.

Sestavljajo ga lokalna računalniška omrežja Uprave Republike Slovenije za zaščito in reševanje, Izobraževalnega centra za zaščito in reševanje in trinajstih izpostav Uprave Republike Slovenije za zaščito in reševanje. Lokalna omrežja so medsebojno povezana preko IP VPN povezav, vzpostavljenih v omrežju svetovnega spleta, in rezervnih povezav preko omrežja ISDN Telekoma Slovenije. Omrežje je povezano s partnerskimi omrežji za varstvo pred naravnimi in drugimi nesrečami in omrežjem HCOM, preko njega pa z omrežjem Evropske unije.

Aplikacije in storitve omrežja ZIR se delijo na tiste, ki so namenjene podpori in delovanju centrov za obveščanje, še zlasti v povezavi s klici na telefonsko številko 112, in tiste, ki so namenjene silam za zaščito, reševanje in pomoč in drugim akterjem v sistemu varstva pred naravnimi in drugimi nesrečami (Tavčar 2006a).

7.6 Informacijski sistem

Informacijski sistem o naravnih in drugih nesrečah obsega zbiranje, obdelavo, shranjevanje, posredovanje in uporabo podatkov o:

- stanju meteoroloških, hidroloških, seizmoloških, radioloških, ekoloških, zdravstvenih in drugih razmer,
- izrednih stanjih in dogodkih v cestnem, železniškem, zračnem in pomorskem prometu,
- dogajanjih v zračnem prostoru,
- motnjah, omejitvah in pretrganju oskrbe s pitno vodo, energijo, javnih telekomunikacijskih in drugih sistemih,
- nevarnostih in nesrečah ter drugih dogodkih, pomembnih za varstvo pred nesrečami,
- škodi, ki jo povzročijo naravne in druge nesreče,
- reševalnih intervencijah,

– silah in sredstvih za zaščito, reševanje in pomoč.

Viri podatkov, obveznosti, povezane z njihovim sporočanjem ter uporabo, so določeni z zakonom in mednarodnimi sporazumi.

Podatke zbirajo, obdelujejo, posredujejo in uporabljajo centri za obveščanje. V Sloveniji deluje državni in 13 regijskih centrov za obveščanje (glej Slika 7.3) (Informacijski sistem 1995).

Slika 7.3: 13 regijskih centrov za obveščanje

Vir: Informacijski sistem (1995).

7.7 Krizni informacijsko-komunikacijski podporni mehanizmi

Vse države poskušajo razviti neko vrsto informacijskih in komunikacijskih mehanizmov za podporo kriznemu odločanju na najvišji državni ravni. Gre za oblikovanje in razvoj kriznih informacijskih in komunikacijskih podpornih mehanizmov, ki akterjem kriznega upravljanja omogočajo, da pridobijo čim natančnejšo informacijsko podobo vsega, kar je povezano z neželeno situacijo. Ti podporni mehanizmi temeljijo na najvišji informacijski in komunikacijski tehnologiji, kar jo države premorejo, in torej predstavljajo pomembno sredstvo kriznega komuniciranja brez fizične prisotnosti vseh ključnih akterjev v istem prostoru, kar je izjemnega pomena.

V Sloveniji so krizni komunikacijsko-informacijski podporni mehanizmi vezani na strukturo organov za krizno odločanje. Ministrstva imajo svoje komunikacijsko-informacijske podporne sisteme, ki omogočajo pretok informacij v nekriznih in kriznih razmerah. Na integralni vladni ravni deluje Nacionalni center za krizno upravljanje, ki zagotavlja prostorske, tehnične, informacijske in telekomunikacijske pogoje za delo Vlade Republike Slovenije 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. NCKU zagotavlja informacijske povezave z drugimi operativnimi centri v državi in integrira zbrane informacije v izčrpna poročila svojim uporabnikom (Prezelj 2007, 182-183).

Za sodobne krize je po eni strani značilna informacijska eksplozija (Rosenthal in drugi v Prezelj 2005), po drugi strani pa informacijski primanjkljaj. S stališča akterjev kriznega upravljanja je ključno, da pridobijo čim natančnejšo informacijsko podobo vsega, kar je povezano z neželenim dogodkom. V kompleksni krizi bodo informacije pritekale iz dokaj velikega števila virov, kar pomeni, da jih je treba na neki točki integrirati, saj bo le na ta način mogoče zmanjšati negotovost. Neizpodbitno je, da lahko na tej točki bistveno pripomore nova informacijska tehnologija, kot pomembno sredstvo informacijske integracije in medorganizacijskega sodelovanja ter povezovanja nasploh. Ta tehnologija omogoča tudi medorganizacijsko sodelovanje med akterji, ki ne delijo fizične bližine. Pri tem gre za oblikovanje kompatibilnih komunikacijskih kanalov, ki so vzporedni medčloveškim medorganizacijskim odnosom. Comfort, Sungu, Johnson in Dunn (v Prezelj 2007, 145) ter Comfort in Chang (v Prezelj 2007, 184) menijo, da je treba ustvariti krizne socio-tehnične sisteme, pri katerih tehnična kapaciteta za izmenjavo pravočasnih in točnih informacij med številnimi udeleženci povečuje organizacijsko kapaciteto reševanja deljenih problemov (shared problems), ki zahtevajo delovanje na lokalni, regijski, nacionalni in mednarodni ravni. Mreža računalnikov podpira mrežo organizacij oziroma komunikacijske mreže med računalniki na tehnični ravni podpirajo povezave med odločevalci na organizacijski ravni. S tem ustvarimo potencial za inovativne pristope, kolektivno učenje in samoorganiziranje. Hillyard (v Prezelj 2005) govori o integriranem informacijskem sistemu kriznega upravljanja (integrated crisis management information system), ki temelji na deljeni komunikacijski mreži, to pa omogoča medorganizacijsko izmenjavo kriznih informacij na operativni in strateški ravni.

7.8 Komunikacijsko-informacijska podpora v centrih za obveščanje

Na področju varstva pred naravnimi in drugimi nesrečami v Republiki Sloveniji deluje Center za obveščanje Republike Slovenije in trinajst regijskih centrov za obveščanje. Vsi delujejo neprekinjeno 24 ur dnevno, vse dni v letu.

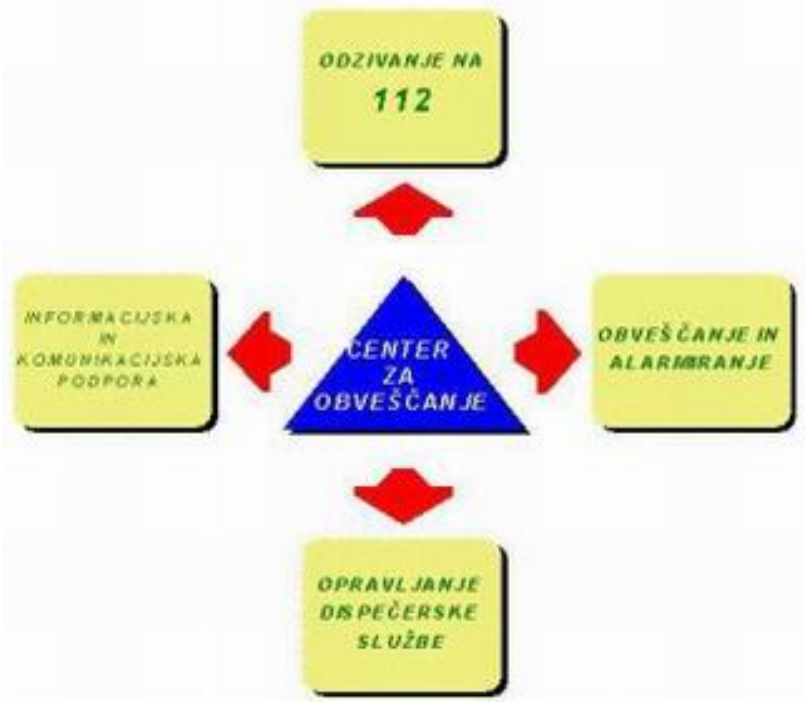
Slovenija je glede varstva pred naravnimi in drugimi nesrečami razdeljena na trinajst regij in v vsaki deluje po en regijski center za obveščanje, ki sprejema klice na enotno evropsko številko za klic v sili 112.

Naloge centrov za obveščanje so (glej Slika 7.4):

- zbiranje in obdelava podatkov,
- posredovanje podatkov reševalnim službam, državnim organom, županom idr.,
- razglašanje nevarnosti,
- javno alarmiranje,
- posredovanje napotkov prebivalcem za ravnanje ob nevarnostih oziroma nesrečah,
- opravljanje dispečerske službe za gasilstvo, nujno medicinsko pomoč, gorsko, jamarsko, podvodno in druge reševalne službe,
- posredovanje pri zagotavljanju logistične podpore reševalnim službam,
- mednarodna izmenjava podatkov.

Centri za obveščanje se lahko vključujejo v televizijske in radijske programe, objavljajo obvestila, napovedi in opozorila na teletekstu nacionalne televizije ter izdajajo dnevne, polletne in letne informativne biltene (Informacijski sistem 1995).

Slika 7.4: Center za obveščanje



Vir: Informacijski sistem (1995).

Kljub stalnemu razvoju bo v prihodnje treba precej pozornosti nameniti prenovi nekaterih komunikacijsko-informacijskih sistemov, predvsem pa z zadostnim številom zaposlenih zagotoviti stalno navzočnost vsaj dveh operativnih tehnikov na izmeno za sprejemanje klicev v sili na enotno evropsko številko 112 in za ukrepanje (Tavčar 2006a).

7.9 Obstoječi informacijski sistemi v posameznem regijskem centru za obveščanje (ReCo)

Širša javnost pozna delo ReCO predvsem po telefonski številki 112, ki jo kliče v primeru naravne ali druge nesreče oziroma drugega pojava, ki je lahko pomemben za življenje in varnost ljudi, živali ali premoženja, če je potrebna nujna medicinska pomoč, pomoč gasilcev, gorskih in jamarskih reševalcev oziroma drugih reševalnih služb. ReCO pristojnim organom in javnosti nudi informacije o stanju ter daje napotke za ravnanje, razglasi nevarnost ali pa na kraj izrednega dogodka napoti sile za zaščito, reševanje in pomoč (sile ZRP) in obvesti pristojne organe in službe. Še zlasti v primeru,

da je potrebna intervencija sil ZRP, je ključnega pomena hitro in pravilno ukrepanje, ki mora temeljiti na točnih informacijah. ReCO posreduje tudi pri zagotavljanju logistične podpore silam ZRP na terenu, ter spremlja in beleži potek intervencije.

Za opravljanje nalog, povezanih z ukrepanjem ob klicu na številko 112, ReCO uporabljajo informacijske in komunikacijske sisteme, ki zagotavljajo beleženje vseh vhodnih in izhodnih telefonskih klicev, orientacijo v prostoru, določanje lokacije dogodka in sil ZRP, ki delujejo na območju ter pregled podatkov o teh silah, aktiviranje pripadnikov sil ZRP s pošiljanjem kratkih besedilnih sporočil imetnikom sprejemnikov osebnega klica, izvajanje javnega alarmiranja in pregledovanje podatkov o nevarnih snoveh ter postopkov za ravnanje ob nesreči z nevarno snovjo.

Obstoječi informacijski sistemi, ki so namenjeni podpori delu operativcev, so se v delovanje ReCO uvajali postopoma, kar se odraža tudi v njihovi tehnologiji in načinu delovanja. Njihova osnovna značilnost je, da delujejo samostojno in lokalno, nekateri med njimi še niso vključeni v računalniško omrežje URSZR. Vsak od njih je skupaj s potrebnimi bazami podatkov nameščen na računalniku v posameznem ReCO, kar je po eni strani posledica zgodovine razvoja informacijske infrastrukture v ReCO in URSZR v celoti, po drugi strani pa posledica zahtev po avtonomnem delovanju posameznega centra in vsakega od njegovih sistemov, saj morebitni izpad povezav ali katerega od sistemov ne sme vplivati na delo v izrednih razmerah (Juroš 2004).

Informacijski sistemi v posameznem regijskem centru za obveščanje so:

- Geografski informacijski sistem GIS-UJMA – predstavlja prostorski del informacijskega sistema zaščite in reševanja;
- Sistem za proženje pozivov sprejemnikom osebnega klica (ZAPP) – aplikacija za pošiljanje kratkih besedilnih sporočil imetnikom sprejemnikov (»pager«);
- Sistem za računalniško obdelovanje klicev (ROK) – sprejemanje in beleženje vhodnih ter beleženje izhodnih telefonskih klicev preko ISDN telefonske centrale centrov za obveščanje;
- Daljinski nadzor javnega alarmiranja (DUNJA) – sistem za izvajanje sistema javnega alarmiranja;

- Baze nevarnih snovi – aplikacija NevSnov – namenjena iskanju preko 2.000 nevarnih snovi po petih različnih kriterijih: kemijskem imenu, sinonimu, UN-številu, nevarnosti in transportnem razredu;
- Aplikacija Evidenca nesreč in intervencij – namenjena elektronski izdelavi in zbiranju poročil o nesreči (Svete 2007).

Vsi ti opisani sistemi so razviti na podlagi izkušenj ReCO in podajajo pregledno sliko uporabniških zahtev, ki se kažejo pri opravljanju nalog s področja aktiviranja in obveščanja ob nesrečah in drugih izrednih dogodkih. Skozi pregled obstoječega stanja je bilo ugotovljeno, da je z integracijo vseh sistemov v učinkovito funkcionalno celoto mogoče optimizirati način ukrepanja.

Obstoječi sistemi bodo medsebojno povezani v enoten sistem, ki bo omogočal:

- upravljanje in uporabo vseh komponent sistema z enega mesta,
- čim hitrejši odziv na klic v sili,
- hitrejše in natančnejše določanje lokacije nesreče,
- hitrejše in učinkovitejše aktiviranje in obveščanje,
- dokumentiranje ukrepanja operativca ob nesreči in ga povezati s poročili o istem dogodku s terena.

Jedro sistema bo predstavljala aplikacija, ki bo nameščena na lokalnem računalniku v ReCO. Jedro sistema bo zagotavljalo naslednje funkcije:

- sprejemanje klicev preko telefonskih linij,
- določanje lokacije klicev in lokacije nesreč,
- podporo operativcu pri aktiviranju in obveščanju na osnovi načrtov ukrepanja,
- aktiviranje in obveščanje preko telefonskih linij,
- posamični in skupinski klici na sprejemnike osebnega klica preko sistema radijskih zvez ZARE,
- javno alarmiranje,
- hitro in učinkovito iskanje podatkov o nevarnih snoveh,
- sprotno beleženje aktivnosti operativca (sprejemanje klicev, aktiviranje, obveščanje),
- izdelava poročil ReCO o ukrepanju ob nesrečah.

Osnovni cilj razvoja SPU 112 je upravljanje vseh sistemov iz enega delovnega mesta na ReCO tako, da bo komunikacija med sistemi neopazna. Skoraj vse naštete funkcije se bodo dejansko izvajale v posameznih podsistemih. Jedro aplikacije bo zagotavljalo preprost dostop do teh funkcij. Vzpostavljena bo komunikacija med jedrom sistema in podsistemi. Posamezni podsistemi bodo zato ustrezno nadgrajeni tako, da bo omogočena njihova integracija z jedrom aplikacije. Kljub integraciji bo zagotovljena takšna operativnost posameznih podsistemov kot pred integracijo. Morebitna prekinitev delovanja jedra aplikacije ne bo vplivala na funkcionalnost posameznih podsistemov. Napaka v posameznem podsistemu ali prekinitev komunikacije med posameznim podsistemom in jedrom aplikacije ne bo povzročila motenj v ostalih podsistemih ali prekinitve delovanja jedra aplikacije (Juroš 2004).

8 UPORABA IKT OB NARAVNIH IN DRUGIH NESREČAH

8.1 IKT kot pomoč pri vodenju in upravljanju: primer potresa v Posočju leta 1998 in poplav 18. in 19. september 2010

Pri vsaki naravni ali drugi nesreči ima velik pomen usklajenost informacijskih virov in služb, na kar opozarja tudi Svete v svojem članku (2006, 221), saj opozarja na težave, ki jih informacijsko razvitim družbam povzročata zasičenost s podatki in razdrobljenost informacijskih virov, predvsem z vidika informacijsko-komunikacijskih rešitev, in predstavi nekatere konkretne primere uporabnosti informacijsko-komunikacijske tehnologije za preprečevanje oziroma napovedovanje naravnih in drugih nesreč, kakor tudi za zmanjševanje posledic oziroma njihovo čim hitrejše odpravljanje.

Medtem ko strokovna javnost razpravlja o družbeno-ekonomskih in geoznanstvenih vzrokih, ki naj bi povzročili nesreče, in hkrati išče ukrepe za preprečitev in blažitev le-teh, je prepoznavanje in analiziranje groženj mnogo lažje, če imamo na razpolago čim več natančnih podatkov z različnih področij, ki so povezana v informacije, na podlagi katerih se lahko odloča. To pa ne pomeni, da obilje podatkov istočasno zagotavlja točne napovedi nastanka in obsega nesreč, saj se številni dejavniki dopolnjujejo, prepletajo in tvorijo kompleksen sistem, ki ga tudi s poznavanjem velikega števila spremenljivk ne moremo do potankosti analizirati in še manj, podati točne in zagotove napovedi dogodka.

Krizno upravljanje in vodenje se v razvitem svetu ukvarja predvsem z vprašanjem, kako povezati informacijske sisteme velikega števila javnih institucij, ki se vsaka na svojem področju ukvarja z naravnimi in drugimi nesrečami. Nasičenost s podatki je tako postala pomembna motnja tudi v sistemu zaščite in reševanja pred nesrečami, ki otežuje delovanje vseh bolj kompleksnih sistemov. Tako je možnost deljenja vseh pomembnih informacij, še zlasti o čezmejnih nesrečah, zelo omejena. Še celo v tistih primerih, ko je izmenjava podatkov načelno možna, različni podatkovni zapisi in servisi ovirajo takšno izmenjavo, težavo pa predstavljajo tudi različni strokovni pogledi na problematiko nesreč. Zato je potrebnega veliko »ročnega« dela, da se iz različnih zbirk podatkov

pridobijo informacije, na podlagi katerih je mogoče učinkovito podpreti proces odločanja in to predvsem, ko pride do izraza časovni element krize (Svete 2006, 222).
Če se obrnemo na določen primer, in sicer na potres[2], ki je prizadel Posočje leta 1998, lahko nakažem, kakšen je dejanski vpliv informacijsko-komunikacijske tehnologije pri kriznem komuniciranju ob naravnih nesrečah.

Ta potres je značilen primer sodobne kompleksne krize, kar pomeni, da soočenje s to krizo zahteva sodelovanje različnih akterjev znotraj in tudi izven sistema kriznega upravljanja in vodenja.

Potres, ki je bil VIII. stopnje po evropski potresni lestvici, je prizadel Posočje na velikonočno nedeljo, 12. 4. 1998. Žarišče potresa pa je bilo v goratem območju Krnskega pogorja med Bovcem in Kobaridom. Tako je bilo najhujše prizadeto širše območje Bovca, Kobarida in Tolmina, kjer je nastala tudi največja materialna škoda.
Prav pri določanju epicentra potresa je že nastal problem. Čeprav so bile potresne terenske opazovalnice, so le-te bile zastarele in so dokaj normalno delovale v normalnih razmer, v teh razmerah, ki pa so bile daleč od normalnih, pa so se najbolj kritične potresne opazovalnice zaradi jakosti potresa in zastarela tehnologije zaustavile ali pa so bile zaradi izpada telefonskih zvez nedosegljive. Tako so se morali pri določanju epicentra in lokacije potresa opreti na mednarodno izmenjavo podatkov, na podatke iz še delujočih opazovalnic in celo na poročanje množičnih občil. Tako je tudi prva o potresu poročala italijanska državna televizija (Grošelj 2004).

Tako je bilo pomembno delo kriznega komuniciranja določanje lokacije potresa, predvsem v luči težav v prvih trenutkih krize, kjer prispele informacije dramatično vplivajo na razumevanje in zaznavanje problema ter na nadaljnji potek kriznega upravljanja in vodenja. Prenos informacij so leta 1998 zaznamovale prav počasnost prenosa podatkov in informacij med Upravo Republike Slovenije za geofiziko (URSG) in Centrom za obveščanje Republike Slovenije (CORS) ter kadrovske in postopkovne pomanjkljivosti v delovanju CORS. Ko je javnost bila obveščena o potresu, je to sprožilo plaz klicev prebivalstva in medijev na številko 112, tako na regionalni kot tudi

[2] Potres je naravna nesreča, ki jo za razliko od na primer poplav ne moremo predvideti in je ne moremo preprečiti z izvajanjem preventivnih ukrepov. Potresa ni mogoče napovedati, ni mogoče vnaprej oceniti njegovega obsega, moči in škode, ki jo povzroči, predvidimo lahko le območje, kjer se lahko pojavi (krizno upravljanje in vodenje v Sloveniji: izzivi in priložnosti, Ljubljana 2004: 166).

na nacionalni ravni, in tudi na Observatorij na Golovcu. Ker niti CORS niti ReCo Nova Gorica kadrovsko nista bila pripravljena na soočanje s takšno množico klicev, je prišlo do začasne blokade obeh centrov, kar je onemogočilo izmenjavo informacij. CORS se je, ker mu je URSG več kot uro in pol po prvem potresnem sunku ni podala podatkov o natančni lokaciji potresa, soočal še s problemom informacijskega vakuuma glede lokacije potresa. Množica telefonskih klicev v CORS in ReCo Nova Gorica je povzročila blokado obeh centrov in tudi njuno medsebojno izmenjavo podatkov ter predvsem v primeru ReCo onemogočila njegovo komunikacijo z lokalnimi akterji kriznega upravljanja in vodenja (Grošelj 2004).

Torej je eno največjih težav kriznega komuniciranja predstavljal sistem zvez. K temu pa moramo dodati še preobremenitev stacionarne telefonije in takrat še slabo pokritost območja s signalom mobilne telefonije. Težave so reševali na dva načina, in sicer so s postavitvijo mobilnega repetitorja povezali poverjenike in štabe CZ, prebivalce pa je obveščal VAL 202, ki je preko oddajnika Kanin oddajal lokalne novice. Poleg radia so prebivalce obveščali tudi s plakati in preko lokalne televizije v Bovcu.

Čeprav so se največji problemi v sistemu komunikacij odvijali na regijski in lokalni ravni, pa je glede na delitev pristojnosti v zvezi s sistemom varstva pred naravnimi in drugimi nesrečami med državo in lokalno skupnostjo, po katerem je država med drugim pristojna tudi za organiziranje sistema zvez, za težave z zvezami gotovo soodgovorna državna raven oziroma URSZR. Glede samega komunikacijskega sistema lahko rečemo, da je bila največja težava neavtonomnost komunikacijskega sistema na lokalni in regijski ravni, kjer so kot glavno sredstvo uporabljali mobilno telefonijo NMT, pa še to sprva preko zasebnih aparatov. Ta se je takoj po potresu sesul in do njegove vnovične vzpostavitve ter postavitve mobilnega repetitorja je bil sistem v resnih težavah. Zaščita in reševanje imata sicer svoj avtonomni sistem ZARE, ki pokriva 98 % ozemlja Republike Slovenije. Največji problem je bilo gotovo izredno veliko število uporabnikov, predvsem pa neizkušenost in slaba tehnična izurjenost uporabnikov na nižjih nivojih. Na področju izobraževanja in usposabljanja bi prav gotovo morali storiti več, saj so bili predvsem gasilci izurjeni za rabo starejšega komunikacijskega sistema, ki je deloval na spodnjem frekvenčnem spektru. Na področju izobraževanja in usposabljanja je bilo torej narejenega premalo, za to pa je pristojna tudi država. Glede

na dostopne podatke pa je bila tudi postavitev mobilnega repetitorja zagotovljena razmeroma pozno (Malešič 2004, 204–213).

Ko že govorim o samem primeru naravne nesreče, pa bi tu omenila še zadnje poplave, ki so nas doletele 18. in 19. septembra 2010, kajti pod vodo je bila skorajda vsa Slovenija in veliko vasi in celo mest je bilo praktično odrezanih od sveta. Tu pa je nastal velik problem, kajti na teh območij, poleg tega, da so imeli ljudje probleme s pitno vodo, so jim, zaradi preprečitve še večje katastrofe, odklopili električno energijo, tako da so ljudje ostali v izredno težkih razmerah. Ljudje so seveda iskali pomoč, tako da so klicali na številko 112, vendar je tu nastal problem, ki je podoben kot pri prej omenjenem potresu iz leta 1998, saj zveze nikakor ni bilo mogoče vzpostaviti vsem klicateljem, tako da je zopet prišlo do preobremenitve zvez in v dvanajstih letih še vedno ni rešen ta problem. Ker je bilo to iskanje pomoči neuspešno, so se nekateri ljudje le spomnili, da bi lahko poklicali urad župana, ki pa je med drugim tudi odgovoren za civilno zaščito na lokalni ravni in da so se potem tam organizirali skupaj Rdeči križ in civilna zaščita, ki so potem dejansko odšli na teren in pomagali ljudem ter jim delili nujne življenjske dobrine.

Veliko število ljudi je potrebovalo pomoč, ki se seveda najprej išče na lokalni ravni in če ta ni sposobna sama zagotoviti dovolj pomoči, se potem zaprosi za dodatno pomoč iz regije ali države. Prav to pa je bil tudi problem teh poplav, čeprav je bil velik del Slovenije pod vodo, voda le ni zajela vse države, tako da so na primer prostovoljni gasilci iz Haloz ves čas čakali, da jih kdo pokliče na pomoč, kajti bili so pripravljeni pomagati državljanom, kajti po medijih so slišali, da primanjkuje gasilcev na tistih najbolj prizadetih območjih, vendar jih ni nihče poklical, tako da so na koncu sami klicali in nudili pomoč. To pa nakazuje, da bi tudi organizacijsko še morala država, kakor tudi lokalna skupnost več narediti, ko gre za naravne nesreče (24ur 2010).

Pri tej nesreči pa lahko opazimo, da je veliko ljudi tudi snemalo to krizo, ki se je dogajala pred njihovimi očmi in te posnetke nato posredovalo, preko mobilnega interneta, različnim medijem. To bi pa lahko sistem za zaščito in reševanje tudi upošteval, kajti videoposnetki bi jim prav gotovo prikazali več podatkov o nesreči, kot pa jih dobijo preko telefonskih pogovorov in posledično bi lahko bilo tudi ukrepanje učinkovitejše. S tem bi pa dosegli tudi to, da ne bi le sistem za zaščito in reševanje

preko medijev poročal javnosti, ampak bi tudi sistem za zaščito in reševanje preko medijev dobil določene informacije.

Prognostične službe Agencije Republike Slovenije za okolje so sicer že predčasno opozarjale na bližajočo se povodenj, in sicer v petek, 17. in soboto, 18. septembra sta bili organizirani tiskovni konferenci, kjer so bili novinarji podrobno obveščeni o bližajoči se povodnji. Prav tako so vse dni do 22. septembra poročali o hidrološkem stanju po Sloveniji, na podlagi meritev pretokov na vodomernih postajah celotne Slovenije, ki sta jih izvajala Sektor za hidrometrijo in Oddelek za meritve površinskih voda (Agencija RS za okolje 2010).

Vendar sem pri teh napovedih zasledila, da so preveč napovedovali za zahodno Slovenijo in kar malo pozabili na večletni problem reke Savinje, kajti na to so začeli opozarjati šele takrat, ko je v bistvu Laško že plavalo v vodi.

Torej, za te poplave lahko rečemo, da so bile velika kriza, kajti poleg tega, da sta bila kar dva vrhunca poplav, torej 18., kakor tudi 19. septembra, se je zaradi teh poplav sprožilo ogromno število plazov, ki so prav tako ogrozili veliko število ljudi.

Tako bi se morali odgovorni v Republiki Sloveniji malce zamisliti in dejansko kaj storiti in ne le govoriti. Tudi okoljevarstvenik Anton Komat opozarja na dejstvo, da je Slovenija poplavno ogrožena in to si je treba priznati in več truda in denarja vložiti na to področje (TVSLO 2010).

Tako bi morala biti poplavna varnost prioriteta države kot del nacionalne varnosti in v ta namen je potrebno preventivno delovati, kajti tako bi lahko preprečili kakšno poplavo, pa še stroški preventivnega ukrepanja so precej nižji, kakor posledice poplav.

Da bi bile posledice poplav manjše, pa bi v določeni meji lahko prispeval vsak posameznik, ki živi na poplavnem območju, kajti zaradi napredka tehnologije so postale poplave dokaj napovedljive, tako da je že dan prej bil razglašen rdeči alarm poplavne ogroženosti, kar pomeni največjo stopnjo nevarnosti, tako da bi ljudje lahko vsaj nekaj stvari umaknili na varno, če že država tako počasi izvaja preventivne ukrepe.

8.2 Prevzem in prenova sistema javnega alarmiranja

Zgornji primer potresa nas opozarja na določene pomanjkljivosti sistema varstva pred naravnimi nesrečami, zato bo, poleg obnovitve in postavitve novih potresnih opazovalnic, za večjo učinkovitost informiranja in s tem samega varstva pred nesrečami Ministrstvo za obrambo, Uprava Republike Slovenije za zaščito in reševanje, na podlagi novele Zakona o varstvu pred naravnimi in drugimi nesrečami do leta 2011, postopoma prevzela sistem javnega alarmiranja na lokalni ravni. Izvzete bodo le alarmne naprave, za katere morajo skrbeti gospodarske družbe, zavodi in druge organizacije. Tako bo pod okrilje države prišlo upravljanje in vzdrževanje celotnega sistema javnega alarmiranja. Država je do sedaj skrbela za sistem javnega alarmiranja na državni in regijski ravni, medtem ko je bil sistem javnega alarmiranja na lokalni ravni v pristojnosti lokalnih skupnosti.

Zasnova sistema javnega alarmiranja v Republiki Sloveniji je hierarhična in obsega tri ravni:

- državno,
- regijsko,
- lokalno (LN).

Državna alarmna centrala se nahaja v Centru za obveščanje Republike Slovenije, regijske alarmne centrale pa v regijskih centrih za obveščanje. Te so na državno alarmno centralo povezane preko računalniškega omrežja WAN Uprave Republike Slovenije za zaščito in reševanje. Sirene in lokalne alarmne centrale so z regijskimi alarmnimi centralami povezane preko fiksnih najetih telekomunikacijskih povezav ali preko radijskih povezav.

8.2.1 Predviden potek prevzema in prenove sistema javnega alarmiranja

V Sloveniji je po podatkih iz zadnjega popisa 1.563 siren, od katerih jih večina še ni povezana v enotni sistem javnega alarmiranja. Večina siren je starih, motornih. Te bo treba zamenjati. Dinamika in vrstni red prevzema in menjave siren sta odvisna od razpoložljivih sredstev in potreb na terenu.

Prednost pri prevzemanju imajo sistemi na gosto naseljenih območjih in sistemi na območjih, ki jih še posebej ogrožajo naravne nesreče, kamor sodi tudi Posočje.

Pri prevzemu siren bo treba upoštevati njihovo amortiziranost in tehnološko iztrošenost. Motorne sirene so že amortizirane in tehnološko iztrošene, zato jih bo treba zamenjati. Pri elektronskih sirenah bo potrebno pregledati stanje vsakega posameznega sistema. Sistemi, ki še niso amortizirani in so že povezani v enotni državni sistem javnega alarmiranja, bodo samo prevzeti.

Sirene, ki še niso povezane v enotni državni sistem javnega alarmiranja, bodo v sistem povezane preko radijskih povezav. Njihova uporaba je praviloma cenejša od fiksnih najetih telekomunikacijskih povezav. Zato bo v sklopu prenove sistema javnega alarmiranja na lokalni ravni prenovljen tudi radijski del javnega alarmiranja (Podberšič 2007).

8.2.2 Prenova radijskega dela sistema javnega alarmiranja

Namen prenove radijskega dela sistema javnega alarmiranja je v čim večji meri poenotiti radijski način prenosa podatkov med alarmnimi centralami in sirenami, ki mora omogočati dvosmerno komunikacijo za daljinsko krmiljenje in nadzor s sodobno tehnologijo.

Prenova obstoječe infrastrukture radijskega dela sistema javnega alarmiranja je tudi sicer nujna, saj se je prometna aktivnost sistema radijskih zvez ZARE tako povečala, da postaja sistem javnega alarmiranja moten in nezanesljiv. Prihaja do elektromagnetnega motenja.

V prenovi sistema javnega alarmiranja bo sedanja uporaba simpleksnih frekvenc zamenjana z uporabo dvofrekvenčnega para. Na repetitorskih kotah bodo govorni repetitorji ZARE in repetitorji za javno alarmiranje zamenjani z DMR repetitorji. Ti imajo dva logična kanala; preko enega kanala bomo prenašali govorni promet DMR, preko drugega pa podatke sistema javnega alarmiranja. Preko repetitorja DMR je možen tudi klasični analogni promet, ki zasede oba kanala. Prednostna nastavitev prometa DMR pred analognim prometom je možna. V tej fazi prenove radijskega dela sistema

javnega alarmiranja ostanejo v uporabi vsi obstoječi protokoli za prenos podatkov preko radijskih zvez (Tavčar 2007a).

S prenovo bodo odpravljene vse pogostejše elektromagnetne motnje zaradi delovanja sistema radijskih zvez ZARE na skupnih repetitorskih kotah. V celoti bo prenovljen in posodobljen tudi govorni del sistema radijskih zvez ZARE.

8.2.3 Radijski sistemi DMR

Razvoj analogne tehnologije je končan. Radijski sistemi DMR predstavljajo naslednjo generacijo profesionalnih radijskih zvez. Temeljijo na uporabi tehnologije TDMA, kar jim omogoča dva logična kanala. Hkrati lahko prenašajo dva pogovora ali pogovor in podatke hkrati.

Nova digitalna platforma omogoča uporabnikom dodatne storitve in ugodnosti:

- Prenos digitalnega govora, podatkov in nadzora preko istega dela radio frekvenčnega spektra.
- Tehnologija DMR temelji na časovnem sodostopu (TDMA), kar ji omogoča dva logična kanala znotraj 12.5 kHz fizičnega kanala, kar pomeni podvojitev zmogljivosti sistema in znižanje stroškov.
- Posebna tehnologija odprave napak omogoča boljšo kakovost zvoka in boljšo pokritost terena z radijskim signalom.
- Nižja poraba električne energije kot posledica uporabljene tehnologije TDMA. Ta podatek je pomemben predvsem, kadar naprava dela na baterijsko napajanje.
- DMR radijski sistemi omogočajo, da se preko dveh logičnih kanalov prenašata dva pogovora hkrati ali da se preko enega kanala prenaša govor, preko drugega pa podatki (Podberščič 2007, 173-176).

8.2.4 Zgradba radijskega dela sistema javnega alarmiranja po prenovi

Radijski del sistema javnega alarmiranja po končani prenovi naj bi bil sestavljen iz naslednjih podsistemov in naprav:

- Alarmne centrale z ustrezno programsko opremo

Nameščene bodo v Centru za obveščanje Republike Slovenije, v vseh regijskih centrih za obveščanje in v Izobraževalnem centru za zaščito in reševanje na Igu. Povezane bodo v lokalno računalniško omrežje centra za obveščanje, v katerem se nahajajo, ter medsebojno povezane preko širokega računalniškega omrežja ZIR.

Programska oprema bo namenska in bo služila za daljinsko krmiljenje perifernih postaj ter za nadzor nad njimi. Zasnovana bo tako, da lahko vsak regijski center za obveščanje prevzame vlogo Centra za obveščanje Republike Slovenije in tako, da bo s to programsko opremo od koder koli možno prožiti in nadzirati vse sirene v Sloveniji. Pogoj je, da je računalnik ali alarmna centrala povezana v omrežje ZIR.

Spremljanje in krmiljenje sistema javnega alarmiranja bo potekalo preko dveh ekranov »na dotik« ali z miško. Dva ekrana bosta uporabljena zato, da med posameznimi funkcijami ne bo treba preklapljati slik, kar bo pospešilo upravljanje. Možno bo delati tudi z enim ekranom.

- Računalniško omrežje ZIR (omrežje LAN/WAN)

Računalniško omrežje LAN se nahaja znotraj enega centra za obveščanje. LAN/WAN je dejansko obstoječe omrežje ZIR, ki je v upravljanju in pod nadzorom Uprave RS za zaščito in reševanje. To računalniško omrežje se neprestano posodablja in nadgrajuje. V sistemu javnega alarmiranja služi kot infrastrukturna povezava med alarmnimi centralami z ustrezno programsko opremo, ki se nahajajo v Centru za obveščanje RS, vseh regijskih centrih in Izobraževalnem centru za zaščito in reševanje na Igu.

- Radijska vstopna točka

Radijska vstopna točka bo nameščena v vsakem regijskem centru za obveščanje. Radijska vstopna točka je radijska naprava VHF, ki bo povezana v računalniško omrežje ZIR. Služi kot strojni in programski vmesnik med alarmno centralo z ustrezno programsko opremo in perifernimi postajami, ki bodo povezane preko dvosmernih radijskih zvez VHF zasebnega radijskega omrežja. Potrebno število radijskih vstopnih točk je 32.

- Zasebni digitalni sistem radijskih zvez

Daljinsko krmiljenje in nadzor nad sistemom javnega alarmiranja bo delovalo preko zasebnega digitalnega sistema radijskih zvez (v nadaljnjem besedilu: sistem DMR). Kljub temu, da je v ta namen mogoče uporabiti različne prenosne poti, je ta utemeljitev utemeljena z naslednjimi argumenti:

- Izgradnja sistema DMR hkrati pomeni posodobitev govornih radijskih zvez ZARE in izgradnjo radijske infrastrukture za sistem javnega alarmiranja.
- Sistem DMR omogoča lastniku popolno samostojnost pri gradnji in vzdrževanju.
- Za potrebe sistema javnega alarmiranja bo zgrajen sistem DMR, ki bo temeljil na polduplexsnih radijskih zvezah. Analiza na podlagi praktičnih izkušenj kaže, da je to zelo robusten sistem, ki je ob ujmah najmanj ranljiv in ga je mogoče zelo hitro delno ali v celoti obnoviti.
- Sistem DMR omogoča veliko prožnost in prilagodljivost ob zaradi ujm spremenjenih potrebah ali možnostih.
- Terminali sistema DMR so cenovno ugodni.

V študiji prevzema sistema javnega alarmiranja na lokalni ravni so natančno prikazane prednosti in pomanjkljivosti uporabe radijskega sistema DMR, radijskega sistema TETRA, najetih žičnih povezav in omrežja internet. Ugotovljeno je, da je uporaba radijskega sistema DMR najboljša izbira, zato je bilo odločeno, da se za prenosne poti v sistemu javnega alarmiranja uporabi radijski sistem DMR. Osnovni napravi, ki bosta zagotavljali prenosne poti v sistemu javnega alarmiranja, sta: radijski repetitor VHF in po potrebi radijska povezava UHF (Tavčar 2007a).

Radijski repetitor VHF je dupleksni repetitor DMR, ki deluje v frekvenčnem območju VHF. Služi za pokrivanje ozemlja z radijskim signalom in je nameščen na višinski koti. Preko njega se vzpostavljajo radijske zveze med opremo, nameščeno v centrih za obveščanje, in elektronskimi sirenami. Takšen repetitor VHF imenujemo tudi »prvi repetitor v vrsti«.

Radijska povezava UHF je radijska naprava, ki povezuje repetitor VHF in opremo, nameščeno v centrih za obveščanje, kadar neposredna radijska zveza med njima ni mogoča. Repetitor in povezava sta povezana na način »hrbet v hrbet« in sta skupaj

nameščena na višinski koti. Povezava UHF deluje v polduplekSnem načinu. Repetitor VHF, ki je na opremo, nameščeno v centru za obveščanje, povezan preko povezave UHF, imenujemo »drugi repetitor v vrsti«.

- Periferna postaja

Periferna postaja je v sistemu javnega alarmiranja sestavljena iz:

- elektronske sirene,
- sistema osnovnega napajanja,
- radijske postaje VHF z radijskim modemom.

Elektronska sirena je naprava, ki preko ojačevalnikov NF in zvočnikov zbira zvočne alarme in govorna sporočila. Alarmne znake je mogoče aktivirati lokalno na napravi ali daljinsko iz centra za obveščanje. V sistemu javnega alarmiranja bodo uporabljene elektronske sirene različnih moči NF in z enakimi funkcijami. Vse sirene bodo elektronske (Podberščič 2007)

- Prenosni sistem javnega alarmiranja

Prenosni sistem javnega alarmiranja je sestavni del osnovnega sistema javnega alarmiranja, vendar z nekaterimi posebnostmi, zaradi česar ga je treba obravnavati ločeno. Namen prenosnega sistema javnega alarmiranja je interventna postavitev sistema javnega alarmiranja na področjih, na katerih je prebivalstvo zelo ogroženo zaradi ujm. Prenosni sistem javnega alarmiranja se imenuje zato, ker omogoča hitro začasno postavitev. Če potreba preide v trajno, ga je treba temu primerno preurediti v fiksni sistem javnega alarmiranja.

Sestavni deli prenosnega sistema so:

- avtomatska opazovalnica,
- prenosna elektronska sirena,
- semafor.

Vsi sestavni deli so v bistvu posebne periferne postaje, ki jih je moč daljinsko krmiliti in nadzorovati iz pripadajočega regijskega centra za obveščanje in Centra za obveščanja

RS. Vendar pa na lokalni ravni prenosni sistem javnega alarmiranja lahko deluje povsem samostojno in prav v tem je njegova največja posebnost.

Do leta 2011 naj bi upravljanje in vzdrževanje celotnega sistema javnega alarmiranja prešlo pod okrilje države. Prevzem poteka postopno, skladno s študijo prevzema sistema javnega alarmiranja na lokalni ravni. Hkrati s prevzemom javnega alarmiranja na lokalni ravni bo Uprava RS za zaščito in reševanje prenovila tudi radijski del sistema javnega alarmiranja. Prenova je nujna, saj bo večina siren, ki še niso povezane v enotni sistem javnega alarmiranja, vanj vključenih preko radijske komunikacije (Podberšič 2007, 173–179).

Prenova sistema bo prav gotovo pripomogla k izboljšanju komuniciranja ob naravnih in drugih nesrečah, vendar je potrebno, poleg prenove samega sistema, izvajati tudi izobraževanje in usposabljanje vseh akterjev, ki bodo v krznih razmerah uporabljali prenovljeno tehnologijo, kajti brez tega je lahko vsaka prenova zaman.

9 ZAKLJUČEK IN VERIFIKACIJA HIPOTEZ

Ko nastopi kriza in le-to poskušamo čim hitreje rešiti ali vsaj omiliti posledice, dobi ključno vlogo komuniciranje, ki je hkrati tudi eden izmed najbolj kritičnih dejavnikov, ki vplivajo na uspeh ukrepanja v krizi. Na učinkovitost kriznega komuniciranja pa v veliki meri vpliva informacijsko-komunikacijska tehnologija, ki lahko to komuniciranje olajša in pospeši, ob morebitnem nedelovanju te tehnologije pa lahko pride do še večje krize.

Tako bi se tu vrnila na mojo prvo hipotezo, ki pravi, da uporaba informacijsko-komunikacijske tehnologije omogoča hitrejše zbiranje in obdelovanje informacij, ki morajo biti za učinkovito krizno komuniciranje dobro organizirane in pravočasno razširjene.

V Sloveniji je še vedno kot ključna informacijsko-komunikacijska tehnologija na področju varstva pred naravnimi in drugimi nesrečami razširjeni sistem radijskih zvez in osebnega klica, ki je namenjen operativnim, govornim in podatkovnim komunikacijskim povezavam med pripadniki enot za zaščito, reševanje in pomoč in je razdeljen na tri podsisteme. In sicer prvi je podsistem konvencionalnih zvez ZARE, ki omogoča zgolj govorne komunikacije in je namenjen množičnim radijskim povezavam med pripadniki posameznih enot za zaščito, reševanje in pomoč. Drugi je podsistem snopovnih radijskih zvez ZARE PLUS, ki omogoča avtomatske govorne in podatkovne komunikacije in je preprost za uporabo, kajti vsaka radijska postaja ima svojo klicno številko. Kot tretji pa je podsistem osebnega klica, ki pa omogoča enosmerni prenos sporočil in je namenjen hitremu aktiviranju reševalnih enot.

Že na začetku pa sem omenila, da mora biti pretok informacij v krizi zagotovljen v različnih smereh in med različnimi akterji, kar omogoča predvsem, da so informacije pravočasno razširjene, in sicer znotrajorganizacijski pretok informacij, ki poteka že v normalnih razmerah med člani neke organizacije, naslednji je medorganizacijski pretok, potem je informacijski pretok od organizacij k javnosti in tudi nasprotno, in sicer informacijski pretok od javnosti k različnim organizacijam in ne nazadnje še informacijski pretok med različnimi sistemi organizacij.

Tako lahko svojo prvo hipotezo le deloma potrdim, kajti k večji učinkovitosti naj bi pripomogli še informacijski sistemi v regijskih centrih za obveščanje (ReCo), ki so javnosti najbolj znani po številki 112, ki jo kličejo v primeru nesreče. Ti informacijski sistemi pa so GIS-UJMA, ki predstavlja prostorski del informacijskega dela zaščite in reševanja, nato je sistem za proženje pozivov prejemnikom osebnega klica (ZAPP), ki je aplikacija za pošiljanje kratkih besedilnih sporočil imetnikom sprejemnikov (»pager«), naslednji pa so še Sistem za računalniško obdelovanje klicev (ROK), daljinski nadzor javnega alarmiranja (DUNJA), baze nevarnih snovi – aplikacija NevSnov ter aplikacija Evidenca nesreč in intervencij.

Vendar pa sem na podlagi potresa v Posočju leta 1998 in poplav septembra 2010 ugotovila, da ti sistemi vendarle ne delujejo povsem brezhibno, kajti regijski centri za obveščanje so v času krize preobremenjeni in ne morejo sprejeti vseh klicev, prav tako pa tudi komunikacija med lokalno skupnostjo in regijskim centrom ni bila dobro organizirana, kajti lokalna skupnost je tista, ki mora zaprositi za pomoč, če jo potrebuje, ne pa da drugi ponujajo pomoč, kot je to bilo v primeru PGD Haloze v primeru zadnjih poplav.

Kot drugo hipotezo pa sem predpostavila, da, glede na to, da je informacijsko-komunikacijska tehnologija pomemben element kriznega komuniciranja, se mora ta tehnologija v skladu z razvojem posodabljati in v sodelovanje vključiti čim več akterjev.

To hipotezo pa lahko v celoti potrdim, kajti posredno se navezuje tudi na ugotovitve v prvi hipotezi, kajti prej navedeni sistemi v ReCo so razviti na podlagi izkušenj, hkrati pa podajajo pregledno sliko uporabniških zahtev, tu pa je bilo ugotovljeno, da je z integracijo vseh sistemov v učinkovito funkcionalno celoto mogoče optimizirati način ukrepanja. Tako naj bi ti sistemi bili povezani v enotni sistem, ki bi omogočal upravljanje z enega mesta, hitrejši odziv na klic, hitrejše določanje lokacije nesreče, hitrejše aktiviranje in obveščanje, jedro sistema pa bo predstavljala aplikacija, ki bo nameščena na lokalnem računalniku v ReCo.

Prav tako pa sta predvidena prevzem in prenova sistema javnega alarmiranja, kajti večina siren je starih in še ni povezanih v enotni sistem javnega alarmiranja, ter prenova radijskega dela sistema javnega alarmiranja. Tako bodo govorni repetitorji ZARE in

repetitorji za javno alarmiranje zamenjani z DMR repetitorji, ki omogočajo dva logična kanala.

Sistemi se torej razvijajo, obnavljajo in posodabljajo, ampak kljub temu pravo delovanje pokažejo šele v primeru nesreč, ko pa na žalost še vedno ni tako učinkovito, kot bi si to želeli, ampak z optimizmom in voljo upam, da bodo kmalu tudi v kriznih razmerah delovali, tako kot je predvideno.

Veliko vlogo ima torej povezovanje posameznih sistemov in sodelovanje z različnimi organizacijami, toda pri vsem tem pa moramo velik pomen dati tudi izobraževanju in usposabljanju akterjev, kajti tudi še tako razvita tehnologija je lahko učinkovita le v primeru, da so ljudje usposobljeni za ravnanje z njo.

Na žalost je res, da nas krize vse pogosteje prizadenejo in tudi z vse večjo močjo, tako da je en človek nemočen, toda če se vzpostavi povezava več ljudi, večjih organizacij, večjih držav in sodobne tehnologije, lahko nekaj nesreč celo preprečimo, tiste, ki pa se zgodijo, pa s hitrim ukrepanjem zamejimo in kar se da hitro obvladamo.

10 LITERATURA

1. Agencija Republike Slovenije za okolje. 2010. *Hidrološko poročilo o povodnji v dneh od 17. do 21. septembra 2010*. Dostopno prek: http://www.arso.gov.si/vode/poro%C4%8Dila%20in%20publikacije/Poplave%2017.%20-%21.%20september%202010.pdf (3. oktober 2010).
2. Answers. 2002. *Natural disasters*. Dostopno prek: http://www.answers.com/topic/natural-disasters-1 (14. september 2009).
3. --- 2005. *Information and communication technology*. Dostopno prek: http://www.answers.com/topic/information-communication-technology (14. september 2009).
4. *Doktrina civilne obrambe Republike Slovenije.* 2002. Ljubljana: Ministrstvo za obrambo Republike Slovenije.
5. *Informacijski sistem.* 1995. Dostopno prek: http://www.sos112.si/slo/page.php?src=pr13.htm (8. oktober 2009).
6. ITAA. 2005. *Information Technology Association of America*. Dostopno prek: www.itaa.org (14. septebmer 2009).
7. Grošelj, Klemen. 2004. *Potres v Posočju leta 1998*. Dostopno prek: http://www.sos112.si/slo/tdocs/ujma/2004/posocje.pdf (10. september 2010).
8. Hawkridge, David. 1985. *New information technology in education*. Sydney, London: Croom Helm.
9. IGEA. 2007. *Portal GIS_UJME*. Dostopno prek: http://gis3.sos112.si/portal-gis_ujme/index.php?id=28 (8. april 2010).
10. Juroš, Katja. 2004. *Informacijski sistem za podporo ukrepanju ob klicu na 112*. Dostopno prek: http://www.sos112.si/slo/tdocs/ujma/2004/ukrepanje.pdf (15. oktober 2009).
11. Kline, Miro, Marko Polič in Vlasta Zabukovec, ur. 1998. *Javnost in nesreče: Obveščanje, opozarjanje, vplivanje*. Ljubljana: Znanstveni inštitut Filozofske fakultete.
12. Klotz, Robert, J. 2004. *The politics of Internet communication.* Dostopno prek: http://www.loc.gov/catdir/toc/ecip045/2003014126.html (8. oktober 2009).

13. Kotnik, Igor. 2008. *Oblikovanje sodobnega sistema kriznega upravljanja v Republiki Sloveniji s preoblikovanjem in nadgradnjo dosedanjih rešitev*. Dostopno prek: http://www.sos112.si/slo/tdocs/ujma/2008/209.pdf (14. april 2010).
14. --- 2009. *Strateški pregled obrambnega resorja*. Dostopno prek: http://www.mors.si/fileadmin/mors/pdf/sporocila/2009/STRATESKI_PREGLED_tiskovna.pdf (14. april 2010).
15. Krupenko, Grigorij in Karmen Jenko. 2005. *Informacijski sistem za poročanje o intervencijah in nesrečah*. Dostopno prek: http://www.sos112.si/slo/tdocs/ujma/2005/spin.pdf (2. oktober 2009).
16. Lerbinger, Otto. 1997. *The crisis manager: facing ris kand responsibility*. Mahwah: Lawrence Erlbaum Associates.
17. Malešič, Marjan. 2004. *Krizno upravljanje in vodenje v Sloveniji: Izzivi in priložnosti*. Ljubljana: Fakulteta za družbene vede.
18. --- 2006a. *Teorija kriznega komuniciranja*. Dostopno prek: http://www.sos112.si/slo/tdocs/ujma/2006/malesic_2.pdf (2. oktober 2009).
19. --- 2006b. *Varnost v postmoderni družbi*. Ljubljana: Fakulteta za družbene vede.
20. Malešič, Marjan, Sandra Bašič Hrvatin in Polič Marko. 2006. *Komuniciranje v krizi*. Ljubljana: Fakulteta za družbene vede.
21. Možina, Stane. 1998. *Poslovno komuniciranje*. Maribor: Obzorja.
22. *Nacionalni program varstva pred naravnimi in drugimi nesrečami*. 2002. Dostopno prek: http://www.uradni-list.si/1/content?id=36416 (10. december 2009).
23. Nohria, Nitin in Robert G. Eccles, ur. 1992. *Networks and organizations: structure, form and action*. Boston: Harvard Business School Press.
24. Novak, Božidar. 2000. *Krizno komuniciranje in upravljane nevarnosti*. Ljubljana: Gospodarski vestnik.
25. Ozimek, Igor. 2009. *Uporaba TETRA za daljinsko merjenje in krmiljenje pri varovanju pred naravnimi in drugimi nesrečami*. Dostopno prek: http://www.sos112.si/slo/tdocs/ujma/2009/160.pdf (8. april 2010).
26. Pinterič, Uroš in Malči Grivec. 2007. Informacijsko-*komunikacijske tehnologije v sodobni družbi: multidisciplinarni pogledi*. Nova Gorica: Fakulteta za uporabne družbene študije.

27. Pinterič, Uroš in Urša Šinkovec. 2008. *Informacijska družba*. Nova Gorica: Fakulteta za uporabne družbene študije.
28. Podberšič, Marko. 2007. *Prevzem in prenova sistema javnega alarmiranja na lokalni ravni*. Dostopno prek: http://www.sos112.si/slo/tdocs/ujma/2007/173.pdf (2. oktober 2009).
29. --- 2009. *Prevzem sistema javnega alarmiranja na lokalni ravni in prenova mobilnih siren*. Dostopno prek: http://www.sos112.si/slo/tdocs/ujma/2009/167.pdf (8. april 2010).
30. Polič, Marko, ur. 1994. *Psihološki vidik nesreč*. Ljubljana: Uprava Republike Slovenije za zaščito in reševanje pri Ministrstvu za obrambo.
31. Prezelj, Iztok. 2005. *Nacionalni sistem kriznega menedžmenta*. Ljubljana: Fakulteta za družbene vede.
32. --- 2007. *Oblikovanje politik, sistemov in mehanizmov kriznega upravljanja v sodobnih državah*. Ljubljana: Ministrstvo za obrambo Republike Slovenije, Direktorat za obrambne zadeve, Sektor za civilno obrambo.
33. --- 2010. *Kritična infrastruktura v Sloveniji*. Ljubljana: Fakulteta za družbene vede.
34. Rattray, Gregory J. 2001. *Strategic warfare in cyberspace*. London: MIT Press.
35. *Resolucija o strategiji nacionalne varnosti Republike Slovenije.* 2010. Dostopno prek: http://zakonodaja.gov.si/rpsi/r01/predpis_RESO61.html (15. maj 2010).
36. Sills, David. 1968. *International Encyclopedia of the Social Science*. New York: The Macmillan Company: The Free Press.
37. *Slovar izrazov, ki se nanašajo na varstvo pred naravnimi in drugimi nesrečami*. 2001. Dostopno prek: www.sos112.si/slo/tdocs/slovar_def.doc (8. oktober 2009).
38. Stare, Metka. 2005. *Učinki informacijsko-komunikacijskih tehnologij*. Ljubljana: Fakulteta za družbene vede.
39. *Strategija nacionalne varnosti Republike Slovenije*. 2000. Ljubljana: Ministrstvo za obrambo Republike Slovenije.
40. *Strateški pregled obrambnega resorja*. 2009. Dostopno prek: http://www.mors.si/fileadmin/mors/pdf/sporocila/2009/STRATESKI_PREGLED_tiskovna.pdf (15. junij 2010).

41. Svete, Uroš in Uroš Pinterič. 2008. *E-država: upravno-varnostni vidiki*. Nova Gorica: Fakulteta za uporabne družbene študije.
42. Svete, Uroš. 2005a. *Varnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.
43. --- 2005b. *Varnostne implikacije uporabe informacijsko komunikacijske tehnologije*. Ljubljana: Fakulteta za družbene vede.
44. --- 2006. *Uporaba informacijsko-komunikacijske tehnologije ob naravnih in drugih nesrečah: od napovedovanja in preprečevanja do obvladovanja posledic*. Dostopno prek: http://www.sos112.si/slo/tdocs/ujma/2006/svete.pdf (2. oktober 2009).
45. --- 2007. *Informacijske razsežnosti sodobnega terorizma – teoretična vprašanja in praktični vidiki.* Dostopno prek: http://www.sos112.si/slo/tdocs/ujma/2007/124.pdf (2. oktober 2009).
46. Tavčar, Boštjan. 2002. *Telekomunikacijsko-informacijski sistemi na področju varstva pred naravnimi in drugimi nesrečami*. Dostopno prek: http://www.sos112.si/slo/tdocs/tksistemi.pdf (2. oktober 2009).
47. --- 2003. *Varnost v zasebnih sistemih radijskih zvez*. Dostopno prek: http://www.sos112.si/slo/tdocs/vitel14bt.pdf (8. oktober 2009).
48. --- 2006a. *Komunikacijsko-informacijska podpora sistema varstva pred naravnimi in drugimi nesrečami*. Dostopno prek: http://www.sos112.si/slo/tdocs/ujma/2006/tavcar.pdf (2. oktober 2009).
49. --- 2006b. *Telekomunikacijski sistem ZARE*. Dostopno prek: http://www.sos112.si/slo/tdocs/telsis.pdf (10. oktober 2009).
50. --- 2007a. *Ali je nov standard Digitalnega mobilnega radia DMR konkurenca Prizemnega snopovnega radia TETRA*. Dostopno prek: www.sos112.si/slo/tdocs/vitel2007_clanek.pdf (2. oktober 2009).
51. --- 2007b. *Spletni in WAP portal varstva pred naravnimi in drugimi nesrečami*. Dostopno prek: http://www.sos112.si/slo/tdocs/dsi2007_clanek.pdf (8. oktober 2009).
52. --- 2009. *Zagotavljanje nemotenega delovanja informacijsko-komunikacijskih sistemov na področju varstva pred naravnimi in drugimi nesrečami*. Dostopno prek: http://www.sos112.si/slo/tdocs/itkt.pdf (12. marec 2010).

53. *Telekomunikacijski sistem.* 1995. Dostopno prek: http://www.sos112.si/slo/page.php?src=pr12.htm (8. oktober 2009).
54. TV SLO. 2010. *Pogledi Slovenije*. Dostopno prek: http://tvslo.si/predvajaj /pogledi-slovenije/ava2.82149738/#ava2.82807342 (29. september 2010).
55. Ušeničnik, Bojan. 1996. *Odpravljanje posledic naravnih in drugih nesreč*. Ljubljana: Ministrstvo za obrambo.
56. --- 1998. *Varstvo pred naravnimi in drugimi nesrečami v Republiki Sloveniji*. Ljubljana: Ministrstvo za obrambo.
57. --- 1999. *Protection against natural and other disasters in the Republic of Slovenia*. Ljubljana: Ministrstvo za obrambo.
58. --- 2002. *Nesreče in varstvo pred njimi*. *Uprava RS za zaščito in reševanje*. Ljubljana: Ministrstvo za obrambo.
59. *Uredba o organizaciji in delovanju sistema opazovanja, obveščanja in alarmiranja*. 2007. Dostopno prek: http://zakonodaja.gov.si/rpsi/r09/ predpis_URED589.html (3. oktober 2009).
60. Watts, Duncan. 1997. *Political communication today*. New York: Manchester University Press.
61. White, Jon in Laura Mazur. 1995. *Strategic Communications Management*. Wokingham: Addison-Wesley.
62. *Zakonodaja s področja zaščite, reševanja in pomoči*. 1992. Dostopno prek: http://www.sos112.si/slo/clanek.php?catid=5&id=104 (10. december 2009).
63. *Zakon o varstvu pred naravnimi in drugimi nesrečami*. 2006. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?urlid=200651&stevilka=2182 (10. december 2009).
64. ZARE. 1995. *Načrt radijskih zvez za primer večjih naravnih in drugih nesreč*. Dostopno prek: http://www.sos112.si/slo/tdocs/nacrtzvez.pdf (10. oktober 2009).
65. Zorn, Matija, Blaž Komac, Miha Pavšek in Polona Pagon. 2008. *Naravne nesreče v Sloveniji: 1. Trinealni znanstveni posvet*. Ljubljana: ZRC.
66. 24ur. 2010. *TV Klub.* Dostopno prek: http://24ur.com/bin/ video.php?media_id=60522947 (29. september 2010).