Metodološki okvir za določanje kritične infrastrukture

Gregor Garb, Andrej Osolnik

Povzetek:

Namen prispevka:
Predvsem z namenom preventivnega delovanja je v letu 2004/2005 na območju EU nastal predlog programa za zaščito kritične infrastrukture, ki temelji na pristopu upoštevanja vseh nevarnosti s prednostno nalogo preprečevanja groženj terorizma. Skladno s tem je potrebno upoštevati tudi ostale dejavnike ogrožanja kot so človeški, tehnološki, naravne nesreče, prioriteta pa mora biti na grožnji terorizma.
Glede na dejstvo, da objekti oziroma sektorji, ki so »bolj« pomembni za delovanje države že obstajajo, vendar so pogostokrat imenovani z različnimi pojmi, je namen mojega prispevka, na konceptualni ravni, definirati pojem kritične infrastrukture ter v sklopu le-tega poudariti tudi nujnost ustreznega varnostnega upravljanja kritične infrastrukture kot temelj njene zaščite. Iz namena izhaja tudi cilj prispevka, ki je opredeliti potrebo po skupnem metodološkem okvirju kateri predstavlja temeljno podlago za določanje in zaščito kritične infrastrukture.

Metodologija:
Uporabljeni so bili naslednji metodološki pristopi: metoda analize primarnih in sekundarnih virov, deskriptivna metoda ter študija primera. Skozi celotno besedilo prispevka pa sta nedvomno nepogrešljivi metoda dedukcije, predvsem v vsebinskem delu, in metoda indukcije, ki je uporabljena v zaključku prispevka.

Ugotovitve:
Iz predmeta in cilja prispevka je sledila tudi teza, ki se glasi:
Skupni metodološki okvir določa zahtevane podlage za usklajeno in enotno določanje ter zaščito kritične infrastrukture. Potrditev teze podajava z naslednjimi zaključnimi mislimi..
Številna evropska podjetja poslujejo prek državnih meja in zato zanje veljajo različne obveznosti. V interesu držav članic in EU je, da se vzpostavijo enotni standardi ter ukrepi za zaščito kritične infrastrukture in da vsaka država članica ustrezno zaščiti svojo nacionalno kritično infrastrukturo vendar znotraj skupnega okvira, predvsem z namenom poenotenja in preglednosti ter s tem odprave velikega števila različnih metodologij in dodatnih stroškov, ki izhajajo prav iz nepreglednosti in nestandardiziranih postopkov. Države članice so, na podlagi ustreznih kriterijev in metodologije, dolžne določiti nacionalno kritično infrastrukturo ter opredeliti katera zaradi svoje dejavnosti lahko sodi tudi v okvir evropske kritične infrastrukture. Poleg določitve kritične infrastrukture je dolžnost vsake države članice tudi razviti nacionalne programe za njeno zaščito. Za vsako raven ogroženosti namreč obstaja določena stopnja pripravljenosti, po kateri je mogoče na splošno sprožiti dodatne varnostne ukrepe oziroma po potrebi uveljaviti stopnjevane varnostne ukrepe. Posamezne članice, ki ne bi želele sprožiti določenega ukrepa, bi lahko na določeno grožnjo odreagirale z alternativnimi ukrepi. Ukrepi katere izvaja država članica pa so lahko tudi strožji od tistih, ki bodo standardizirani in predvideni z Direktivo.

Izvirnost/pomembnost prispevka:
Prispevek je namenjen predvsem strokovni javnosti, kot eden od pripomočkov, ki sodeluje oziroma bo sodelovala pri določanju zmogljvosti nacionalne kritične infrastrukture predvsem z namenom poenotenja omenjene zmogljivosti. To je pomembno predvsem zaradi dejstva, saj

kritična infrastruktura kot pojem oziroma njene zmogljivosti v R. Sloveniji na konceptualni ravni **še *nista*** *opredeljeni*.

Ključne besede: kritična infrastruktura

1 UVOD

S koncem obdobja hladne vojne in tradicionalne blokovske delitve sveta so dotedanje grožnje varnosti nadomestila nova varnostna tveganja in asimetrične varnostne grožnje, ki porajajo različne vidike občutljivosti in ranljivosti držav ter posledično zmanjšujejo njihovo varnost. Če je včasih vse temeljilo na vojaških virih ogrožanja, danes vse bolj vidno vlogo dobivajo nevojaški viri ogrožanja, ki pa lahko prav tako kot vojna močno ogrozijo države in družbe. Nevojaški viri ogrožanja so danes medsebojno mednarodno povezani, odvisni in delujejo na vseh ravneh družbenega življenja torej na politični, ekonomski, vojaški, gospodarski ravni, ravni notranje varnosti ipd. Med nevojaške vire ogrožanja notranje varnosti, s katerimi se tudi R. Slovenija neposredno ali posredno lahko sooča, danes uvrščamo organizirani kriminal, terorizem, asimetrične grožnje, ilegalne migracije, posedovanje, širjenje in trgovanje s sredstvi za množično uničevanje, trgovino z ljudmi, orožjem in mamili, pranje denarja, ogrožanje kritične infrastrukture države, naravne in druge nesreče ipd. Ogrožanje notranje varnosti pa predstavljajo tudi splošne, gospodarske in posebne oblike kriminalitete.

Skupni imenovalec omenjenih groženj je to, da jih povzročajo nedržavni, tako imenovani razpršeni dejavniki, katere podpirajo nekatere države iz tako imenovane svetovne periferije, usmerjene pa so predvsem na državne institucije, komunikacije, infrastrukturo, ozemlje ter prebivalstvo posameznih držav. Značilnost sodobnih varnostnih groženj pa je tudi njihova nadnacionalna narava, zato je za odzivanje nanje zelo pomembno medsebojno sodelovanje med državami v okviru sistemov kolektivne varnosti in obrambe.

Prav zaradi potencialnega ogrožanja je na območju EU v letu 2004/2005 nastal predlog programa za zaščito kritične infrastrukture, ki temelji na pristopu upoštevanja vseh nevarnosti s prednostno nalogo preprečevanja groženj terorizma. Skladno s tem je potrebno upoštevati tudi ostale dejavnike ogrožanja kot so človeški, tehnološki, naravne nesreče, prioriteta pa mora biti na grožnji terorizma.

2 KRITIČNA INFRASTRUKTURA

V okviru EU že od leta 2004, ko je Komisija EU posredovala Svetu in Parlamentu EU sporočilo o varovanju kritične infrastrukture v boju proti terorizmu v katerem je predlagala ukrepe za krepitev sposobnosti EU za zaščito kritične infrastrukture, intenzivno potekajo dejavnosti usmerjene v izboljšanje zaščite kritične infrastrukture zoper različne vire ogrožanja.

Svet je v sklepih o »preprečevanju, pripravljenosti in odzivu na teroristične napade« in o »solidarnostnem programu EU o posledicah terorističnih groženj in napadov«, ki jih sprejel konec leta 2004, podprl namero Komisije, da predlaga Evropski program za zaščito kritične infrastrukture (EPCIP), prav tako pa se je strinjal z vzpostavitvijo informacijskega omrežja za opozarjanje o kritični infrastrukturi (CIWIN) pri Komisiji.

S tem namenom je bila v okviru enotne politike EU oblikovana Zelena knjiga o Evropskem programu za zaščito kritične infrastrukture s katero želi EU medsektorsko in

interdisciplinarno, tako na nacionalnem kot tudi na meddržavnem evropskem nivoju, povezati aktivnosti za zaščito kritične infrastrukture. Cilj evropske politike v tej Zeleni knjigi je poenotiti kriterije za določanje, zagotoviti ustrezno in poenoteno stopnjo zaščite kritične infrastrukture, zagotoviti čim manj nezavarovanih točk ter vzpostaviti hitre in preverjene ukrepe za odpravo posledic.

Glede na veliko število potencialne kritične infrastrukture in njenih posebnih značilnosti jo je praktično nemogoče zaščititi samo z ukrepi na evropski ravni. Z uporabo načel subsidiarnosti[1], zaupnosti[2], sodelovanja zainteresiranih strani[3] ter sorazmernosti[4] mora EU svoja prizadevanja prvenstveno osredotočiti na zaščito kritične infrastrukture s čezmejnim učinkom, zaščito preostale kritične infrastrukture pa prepustiti v pristojnost držav članic, vendar v skupnem okviru.

Kritično infrastrukturo z nadnacionalnim vplivom in posledicami EU opredeljuje kot t.i. evropsko kritično infrastrukturo, ki jo definira kot skupek nacionalnih kritičnih infrastruktur katerih poškodovanje, uničenje ali okvara zaradi terorističnih napadov, naravnih nesreč, malomarnosti, nesreč ali vdorov hekerjev, kriminalne dejavnosti in zlonamernega vedenja lahko povzroči ogrožanje življenja ljudi ter lastnine in ovira gospodarske ter druge življenjsko pomembne funkcije na vseh ravneh življenja državljanov, držav članic in EU kot celote. Iz slednjega izhaja, da morajo biti takšne nacionalne kritične infrastrukture z nadnacionalno razsežnostjo prepoznane, ugotovljene in določene kot evropska kritična infrastruktura. To pa je mogoče le z izvedbo skupnega postopka na ravni EU ter z oceno potreb po izboljšanju zaščite teh infrastruktur.

Merila za določanje evropske kritične infrastrukture, katera veljajo tudi za določanje kritične infrastrukture znotraj držav članic, so določena glede na resnost posledic okvare ali uničenja določne kritične infrastrukture, ki jih ima le- ta na:
- javni vpliv (obseg in domet posledic ipd);
- ekonomski vpliv (vpliv na BDP, velikost gospodarske izgube in/ali poslabšanje proizvodov ali storitev ipd.);
- okoljski vpliv (vpliv na javnost in okolje ipd);
- politični vpliv (zaupanje v sposobnost vlade ipd);
- psihološki vpliv (časovni učinek posledic ipd);
- posledice za javno zdravje (število prizadetega prebivalstva, izguba življenj, bolezni, resne poškodbe, evakuacija ipd)

Zaradi nadnacionalne razsežnosti bi takšen integrirani pristop na ravni EU pri preiskovanju slabosti in šibkih točk[5] ter ugotavljanju pomanjkljivih varnostnih ukrepov ustrezno dopolnil

[1] Popolnoma razumljivo je, da je zaščita kritične infrastrukture predvsem v nacionalni pristojnosti. Prav tako pa je jasno, da je za varnost EU temeljnega pomena zagotoviti, da je infrastruktura, ki ima vpliv na dve ali več držav ali na eno članico, če se infrastruktura nahaja v drugi državi članici, ustrezno zaščitena ter da ena ali več držav ni ogroženih zaradi pomanjkljivosti ali znižanja standardov varovanja v drugih državah članicah EU.

[2] Izmenjevanje informacij povezanih z zaščito kritične infrastrukture mora potekati v okolju zaupanja in varnosti. To je nujno glede na to, da je mogoče z izkoriščanjem notranjih informacij, ki »nenamerno« odtekajo povzročiti škodo. Tako na nacionalni ravni kakor tudi na ravni EU bi bile posamezne informacije označene kot tajni podatek in opremljene z ustrezno stopnjo zaupnosti. Dostop in ravnanje s tajnimi podatki bi imele samo pooblaščene osebe.

[3] Za zagotavljanje ustrezne stopnje zaščite, ukrepov in postopkov pri zaščiti kritične infrastrukture je potrebno sodelovanje vseh zainteresiranih strani vključno z državami članicami EU, Komisijo, gospodarskimi in poslovnimi združenji, organi za standardizacijo ter lastniki, upravljavci in uporabniki, vsaka stran glede na svoje pristojnosti in strokovnost. Sodelovanje mora potekati tako znotraj države kot tudi na ravni EU, še posebej pa je pomembno medsektorsko sodelovanje.

[4] Glede na to, da vseh kritičnih infrastruktur ne možno zaščititi pred vsemi grožnjami morajo biti varnostne strategije in ukrepi sorazmerni s stopnjo ogroženosti.

[5] Pomeni značilnost elementa konstrukcije kritične infrastrukture, njenega izvajanja ali delovanja, ki predstavlja potencialno nevarnost za okvaro ali uničenje zaradi grožnje in vključuje odvisnost od drugih vrst infrastrukture. Grožnja pa pomeni vsak namig,

in dodal vrednost nacionalnim programom za zaščito kritične infrastrukture, ki se v državah članicah EU že izvajajo.

Pri nadnacionalnem pristopu je potrebno obvezno upoštevati tudi sektorske izkušnje, znanje in zahteve kakor tudi že obstoječe sektorske ukrepe za kritično infrastrukturo. Iz tega izhaja, da je potrebno določiti tudi seznam sektorjev kritične infrastrukture, ki bo olajšal izvajanje pristopa za zaščito kritične infrastrukture po posameznih sektorjih. Poleg javnega sektorja je nujno potrebno vključiti tudi zasebni sektor, saj je večina kritične infrastrukture v zasebnem lastništvu oziroma v upravljanju. Dejstvo je, da mora vsak upravljavec nadzorovati upravljanje svojih tveganj saj je odločitev o vrsti varnostnih ukrepov in načrtov za neprekinjeno delovanje ter ukrepov za obnovo po nesreči, ki se bodo izvajali, v njegovih rokah.

Na podlagi različnih parametrov izhaja, do so evropske kritične infrastrukture izredno povezane in visoko soodvisne. K takšnemu stanju so prispevali gospodarsko združevanje, industrijska racionalizacija, učinkovite poslovne prakse, koncentracija prebivalstva v urbanem območju, soodvisnost od skupnih informacijsko komunikacijskih tehnologij, vključno z internetom, satelitsko radijsko navigacijo in telekomunikacijami. Prav zaradi tega se lahko motnje širijo skozi te soodvisne infrastrukture ter pri tem povzročajo nepričakovane in vedno resnejše odpovedi delovanja temeljnih služb[6], največkrat z vplivom tudi na druge države članice EU.

Glede na različno opredeljevanje kaj dejansko obsega pojem kritična infrastruktura je EU pripravila predlog Direktive Sveta EU o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njenega varovanja (Tabela 1).

Tabela 1: Seznam sektorjev in podsektorjev kritične infrastrukture

SEKTOR	PODSEKTOR
I. ENERGETIKA	1. Proizvodnja, rafiniranje, predelava ter skladiščenje nafte in plina ter distribucija preko naftovodov in plinovodov 2. Proizvodnja in prenos električne energije
II. JEDRSKA INDUSTRIJA	3. Proizvodnja in skladiščenje/predelava jedrskih snovi
III. INFORMACIJSKE IN KOMUNIKACIJSKE TEHNOLOGIJE, IKT	4. Zaščita informacijskih sistemov in omrežij 5. Sistemi za avtomatizacijo in nadzor instrumentacije (SCADA ipd.) 6. Internet 7. Zagotavljanje fiksnih komunikacij 8. Zagotavljanje mobilnih komunikacij 9. Radijska komunikacija in navigacija 10. Satelitska komunikacija 11. Oddajanje
IV. VODA	12. Zagotavljanje pitne vode 13. Nadzor nad kakovostjo vode 14. Zajezitev in nadzor nad količino vode
V. HRANA	15. Zagotavljanje hrane in zaščita varne hrane

okoliščino ali dogodek, ki lahko potencialno okvari ali uniči kritični infrastrukturo ali kateri koli njen element. (predlog Direktive, 2006)

[6] Verižne reakcije, ki nastanejo zaradi medsebojnih sinergijskih učinkov infrastrukturnih industrij, so zelo škodljive in povzročajo obsežne izpade storitev kar lahko ponazorimo na primeru napada na službo za distribucijo električne energije, ki bi imel za posledico omejitev delovanja in distribucijo elektrike, kar bi povzročilo odpoved naprav za čiščenje odplak in vodovodov, saj bi se lahko zaustavile turbine in druge električne naprave v teh objektih.

VI.	ZDRAVJE	16. 17. 18.	Zdravniška in bolnišnična oskrba Zdravila, serumi, cepiva in farmacevtski proizvodi Biolaboratorij in bioagensi
VII.	FINANCE	19. 20.	Infrastruktura in sistemi za plačila in obračun ter poravnavo Regulirani trgi
VIII.	PROMET	21. 22. 23. 24. 25.	Cestni prevoz Železniški prevoz Letalski prevoz Prevoz po celinskih plovnih poteh Čezoceanski in pomorski prevoz na kratke razdalje
IX.	KEMIČNA INDUSTRIJA	26. 27.	Proizvodnja in skladiščenje/predelava kemičnih snovi Cevovodi za nevarne snovi (kemične snovi)
X.	VESOLJE	28.	Vesolje
XI.	RAZISKAVE	29.	Raziskovalne zmogljivosti

Vir: Predlog direktive Sveta o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njenega varovanja (2006)

Pri nazornem pregledu zgornje tabele in primerjave sporočila Komisije ter Zelene knjige pa je opaziti, da Direktiva ne določa področja državne/javne administracije, kot ga predlagata prej omenjena dokumenta. Razloge gre verjetno iskati v tem, da gre pri tej kritični infrastrukturi za izključno državno lastništvo in upravljanje, kjer zasebni sektor nima svoje vloge. Iz tega izhaja, da je dejansko breme vseh aktivnosti povezanih z zaščito te kritične infrastrukture izključno na javnem sektorju.

Mnenja sva, da bi področje državne/javne administracije moralo biti del kritične infrastrukture vsaj v tistem delu, ki zagotavlja življenjske in strateške interese posamezne države. V to področje bi sodili: določeni organi in organizacije javne in državne uprave, Vlada in njene službe, pravosodni organi, oborožene sile, reševalne službe, poštne in kurirske službe, informacijska omrežja, kulturna dediščina ipd.

Znano dejstvo je, da je pojem kritična infrastruktura relativno nov in je postal zanimiv predvsem zaradi odmevnih terorističnih aktivnosti v bližnje preteklosti. Pred tem se je o teh objektih oziroma sektorjih govorilo le kot o »infrastrukturi« pa čeprav se njihova pomembnost za delovanje države od takrat ni v veliki meri spremenila. Ključna razlika je predvsem v percepciji ogroženosti posameznika, skupnosti in države v celoti. Če sedaj glavna ogroženost izhaja iz terorističnih aktivnosti je bila v takratnem obdobju glavna skrb lastnikov oziroma upravljavcev usmerjena v tehnološki razvoj, širjenje proizvodnje, povečanje zmogljivosti predvsem z namenom zadovoljiti potrebe po povečanju oziroma je grožnjo predstavljala nezmožnost zadovoljevanja pričakovanih potreb.

Prav tako kot se je pojavila potreba po enotnem definiranju infrastrukture/kritične infrastrukture se je pojavila tudi potreba po metodološkem okvirju za zaščito te infrastrukture. Nedvomno je res, da je vsak lastnik oziroma upravljavec poskrbel, po svojih najboljših zmožnostih za ustrezno stopnjo zaščite svoje infrastrukture, pa kljub temu dejstvu obstaja nujnost po poenotenju stopnje zaščite in ukrepov v primeru različnih vrst ogrožanja.

Za učinkovito zaščito kritične infrastrukture so pomembni komunikacija, koordinacija ter sodelovanje tako na ravni države kakor tudi na ravni EU med vsemi zainteresiranimi stranmi,

lastniki in upravljavci[7], zakonodajno vejo oblasti, strokovnimi telesi in gospodarskimi združenji v sodelovanju z vsemi upravnimi ravnmi ter javnostjo. Zavedati se je potrebno, da stopnja zaščite ni nujno enaka za vso kritično infrastrukturo in je lahko odvisna od posledic omejitve njenega delovanja. Čeprav so ukrepi za odpravo posledic enaki ali podobni pri večini motenj delovanja, pa se lahko zaščitni ukrepi razlikujejo glede na vrsto grožnje. Med grožnje sodijo tudi namerni napadi in naravne nesreče. Prav slednji vrsti groženj določata različne vrste pristopov pri definiranju varnostnih ukrepov. Možnosti so naslednje: (Zelena knjiga, 2005:3)

- pristop z upoštevanjem vseh nevarnosti na vseh področjih predstavlja celosten pristop, ki upošteva vse vrste groženj, vendar poudarka ne namenja terorizmu;
- pristop z upoštevanjem vseh nevarnosti, pri katerem je v osredju terorizem predstavlja prilagodljiv pristop, ki zagotavlja povezavo z ostalimi vrstami groženj vendar pa je v ospredju terorizem;
- pristop z upoštevanjem nevarnosti terorizma predstavlja pristop usmerjen izključno v terorizem, ki ne upošteva možnosti ostalih groženj.

Samo za ilustracijo ter primerjavo navajava delitev groženj, kot jih opredeljujejo Združene države Amerike v svojem Nacionalnem načrtu zaščite infrastrukture: (National Infrastructure Protection Plan, 2006)

- naravne nesreče:
  - požari,
  - poplave,
  - neurja,
  - potresi
- nesreče, ki jih povzroči človek:
  - velike prometne nesreče,
  - razlitja in izpusti nevarnih snovi
- sociološke, kriminalne in teroristične aktivnosti:
  - vandalizem,
  - sabotaže,
  - neredi, demonstracije, stavke,
  - napadi z JRKB – orožjem ali eksplozivnimi napravami
- ostalo:
  - malomarnost pri vzdrževanju delovnih sredstev,
  - pomanjkanje energije in materialnih sredstev.

Ne glede na zgoraj navedene oblike ogrožanja, ki predstavljajo samo primer percepcije ogroženosti v ZDA, predstavlja ocenjevanje tveganja integracijo grožnje, ranljivosti in možnih posledic. Iz tega izhaja, da upravljanje s tveganjem sestavljajo potrebni ukrepi za zaščito, ki izhajajo iz načrtov za zmanjšanje tveganja oziroma iz načrtov za čim prejšnjo odpravo posledic.

Kljub velikemu število avtorjev in iz tega izhajajočih modelov oziroma metodoloških okvirjev za zagotavljanje ustrezne zaščite kritične infrastrukture je vsem, bolj ali manj, skupen metodološki okvir z naslednjimi pripadajočimi elementi: Critical Infrastructure Protection (Elements of Risk)

- Določanje zmogljivosti in določanje njihovih kritičnosti po prioriteti;
- Določanje, karakteriziranje in ocenjevanje ogroženosti;

[7] Kritično infrastrukturo imata v lasti in z njo upravljata tako javni kot tudi zasebni sektor. Kljub temu pa je mnenje Komisije, da mora biti krepitev določenih varnostnih ukrepov zoper napade, usmerjene proti družbi kot celoti in ne proti industrijskim subjektom, breme države. V tem pogledu mora javni sektor odigrati ključno vlogo (Sporočilo, 2004:2).

- Ocenjevanje ranljivosti šibkih točk glede na specifičnost groženj;
- Določanje tveganja (*pričakovane* posledice glede na specifično obliko ogrožanja);
- Prepoznavanje načinov na zmanjšanje tveganja;
- Določanje ukrepov za zmanjšanje tveganja, ki temeljijo na načrtih (po prioriteti).

Omenjeni okvir bi lahko lastniku oziroma upravljavcu predstavljal osnovo za načrtovanje zaščite kritične infrastrukture. Kljub vsemu pa obstaja potreba po enotnem skupnem metodološkem okvirju tako znotraj države kot tudi širše.

Glede na velikost in obseg kritične infrastrukture pa je popolnoma razumljivo in splošno sprejemljivo, da je ni mogoče popolnoma zaščititi. Z uporabo ustreznih metod obvladovanja tveganja se lahko tako pozornost usmeri na področja največjega tveganja glede na grožnjo, pomembnost infrastrukture, razmerja med stroški in koristmi, obstoječe stopnje varovanja ter učinkovitosti razpoložljivih strategij za ublažitev posledic omejitev delovanja ali uničenja kritične infrastrukture.

3 ZAKLJUČEK

Številna evropska podjetja poslujejo prek državnih meja in zato zanje veljajo različne obveznosti. V interesu držav članic in EU je, da se vzpostavijo enotni standardi ter ukrepi za zaščito kritične infrastrukture in da vsaka država članica ustrezno zaščiti svojo nacionalno kritično infrastrukturo vendar znotraj skupnega okvira, predvsem z namenom poenotenja in preglednosti ter s tem odprave velikega števila različnih metodologij in dodatnih stroškov, ki izhajajo prav iz nepreglednosti in nestandardiziranih postopkov. Države članice so, na podlagi ustreznih kriterijev in metodologije, dolžne določiti nacionalno kritično infrastrukturo ter opredeliti katera zaradi svoje dejavnosti lahko sodi tudi v okvir evropske kritične infrastrukture. Poleg določitve kritične infrastrukture je dolžnost vsake države članice tudi razviti nacionalne programe za njeno zaščito. Za vsako raven ogroženosti namreč obstaja določena stopnja pripravljenosti, po kateri je mogoče na splošno sprožiti dodatne varnostne ukrepe oziroma po potrebi uveljaviti stopnjevane varnostne ukrepe. Posamezne članice, ki ne bi želele sprožiti določenega ukrepa, bi lahko na določeno grožnjo odreagirale z alternativnimi ukrepi. Ukrepi katere izvaja država članica pa so lahko tudi strožji od tistih, ki bodo standardizirani in predvideni z Direktivo.

Nedvomno pa je potrebno preučiti tudi možnost skupne metodologije prepoznavanja in razvrščanja groženj, zmogljivosti, tveganj in šibkih točk ter sklepanja o možnosti, verjetnosti in resnosti tega, da bo grožnja povzročila motnjo oziroma okvaro na objektu kritične infrastrukture. To bi vključevalo oceno tveganja in določitev prioritet, po katerih bi bilo mogoče tvegane dogodke opredeliti glede na verjetnost njihovega pojava, vpliv in povezave z drugimi tveganimi območji oziroma procesi.

4 SEZNAM LITERATURE IN VIROV

Knjiga:

1. Anžič, A. (1997): Varnostni sistem Republike Slovenije, Uradni list RS, Ljubljana.
2. Bennett, B.T. (2007): Understanding, assessing, and responding to terrorism : protecting critical infrastructure and personnel, Wiley-Interscience, Chichester.
3. Bungert, H., Heitmann, J. (2003): Secret intelligence in the twentieth century, Frank Cass, London, Portland.

4. Dunn, M., Wigert, I. (2004): International CIIP Handbook, Swiss federal institute of technology, Zurich. Dostopno na: http://www.crn.ethz.ch/ z dne 28. 1. 2008.
5. Furlan, B. in drugi (2006): Vojaška doktrina, Defensor, Ljubljana.
6. Grizold, A.(2005): Slovenija v spremenjenem varnostnem okolju, FDV, Ljubljana.
7. Grizold, A., Ferfila, B. (2000): Varnostne politike velesil, FDV, Ljubljana.
8. Linkov, I., Wenning, J.R., Kiker, A.G. (2007): Managing Critical Infrastructure Risks, Springer, AA Dordrecht.
9. Lewis, T.G. (2006): Critical infrastructure protection in homeland security : defending a networked nation, Wiley-Interscience, Chichester.
10. McKnight, D., Aldrich, R. (2002): Espionage and the Roots of the Cold War, Frank Cass, London, Portland.
11. Prezelj, I. (2005): Nacionalni sistemi kriznega menedžmenta, knjižna zbirka Varnostne študije, FDV, Ljubljana.
12. Richelson, J. (1995): The U.S. Intelligence Community, Ballinger Publishing, Cambridge.
13. Sarkesian, S.C., Williams, J.A., Cimbala, S.J. (2002): US National Security: Policymakers, Process and politics, 3. izdaja, Lynne Rienner Publishers, London.
14. Scott, L.V., Jackson, P.D. (2004): Understanding Intelligence in the Twenty-first Century, Routledge, New York, London.
15. Sullivant, J. (2007): Strategies for protecting national critical infrastructure assets: a focus on problem-solving, Wiley-Interscience, Chichester.

Članek v reviji:

1. Dolenc, R. (2007): Glavni izzivi varnosti v današnjem mednarodnem okolju in v okviru Evropske unije s poudarkom na terorizmu, Dnevi varstvoslovja 2007, VPVŠ, Bled.
2. Prezelj, I. (2005): Skupna evropska varnostna in obrambna politika: dosežki, izzivi in dileme v luči učinkovitega kriznega menedžmenta. V: HAČEK, M., ZAJC, D.: Slovenija v EU: zmožnosti in priložnosti, Knjižna zbirka Politični procesi in institucije, FDV, Ljubljana.
3. Prezelj, I. (2006): Modeliranje celovitega ocenjevanja ogrožanja nacionalne varnosti, Dnevi varstvoslovja 2006, VPVŠ, Bled.
4. Prezelj, I. (2007): Nujnost medresorskega sodelovanja in koordiniranja v boju proti terorizmu: nekateri primeri iz Republike Slovenije, Bilten Slovenske vojske št. 2/9, GŠSV, Ljubljana.

Pravni viri Republike Slovenije:

1. Ustava Republike Slovenije (Ur.l.RS, št. 33/91-I, 42/97, 66/00, 24/03, 69/04 in 68/06)
2. Zakon o obrambi (Ur.l.RS, št. 103/04–ZObr–UPB1).
3. Zakon o parlamentarnem nadzoru obveščevalnih in varnostnih služb (Ur.l.RS, št. 26/03–ZPNOVS).
4. Zakon o vladi (Ur.l.RS, št. 24/05–ZVRS–UPB1).
5. Zakon o policiji (Ur.l.RS, št. 107/06–ZPol–UPB6).
6. Zakon o službi v Slovenski vojski (Ur.l.RS, št. 68/07–ZSSloV).
7. Zakon o varstvu pred naravnimi in drugimi nesrečami (Ur.l.RS, št. 51/06–ZVNDN–UPB1).
8. Resolucija o strategiji nacionalne varnosti Republike Slovenije (Ur.l.RS, št. 56/01–ReSNV).
9. Resolucija o splošnem dolgoročnem programu razvoja in opremljanja Slovenske vojske do 2015 (Ur.l.RS, št. 89/04).
10. Nacionalni program varstva pred naravnimi in drugimi nesrečami (Ur.l.RS, št. 44/02–NPVNDN).
11. Obrambna strategija Republike Slovenije (Vlada RS, št: 820-00/2001-1, z dne 20. 12. 2001).
12. Srednjeročni obrambni program 2007-2012 (Vlada RS, št: 803-2/2006-58, z dne 27. 11. 2006).

13. Doktrina zaščite, reševanja in pomoči (št: 807-00-5/2000-6, z dne 22. 5. 2002).
14. Odlok o svetu za nacionalno varnost (Ur.l.RS, št. 135/04).
15. Uredba o določitvi objektov in okolišev objektov, ki so posebnega pomena za obrambo in, ukrepih za njihovo varovanje (Ur.l.RS, št. 7/99 in 67/03).
16. Uredba o načinu izvajanja nadzora zračnega prostora (Ur.l.RS, št. 29/04).
17. Državni načrt zaščite in reševanja ob uporabi orožij ali sredstev za množično uničevanje v teroristične namene oziroma terorističnemu napadu s klasičnimi sredstvi (št: 214-00-167/2003-32, z dne 23. 2. 2005)

Pravni viri EU:

1. Council Framework Decision of 13 June 2002 on Combating Terrorism (2002), Official Journal of the European Communities, 22 Junij, Bruselj.
2. European Security Strategy – A Secure Europe in a Better World (2003), 12 December, Bruselj.
3. EU Plan of Action on Combating terrorism (2004), Council of the EU, 15 Junij, 10586/04, Bruselj.
4. Sporočilo Komisije Svetu in Evropskemu parlamentu o varovanju kritične infrastrukture v boju proti terorizmu (2004), 20 Oktober, 52004DC0702, Bruselj.
5. EU Strategy for Combating Radicalisation and Recruitment to Terrorism (2005), Council of the EU, 24 November, 14781/1, Bruselj.
6. Strategija EU za boj proti terorizmu (2005), Svet EU, 30 November, Bruselj.
7. Green Paper on a European nprogramme for Critical Infrastructure Protection (2005), 17 November, COM(2005) 576, Bruselj.
8. Predlog direktive Sveta o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njenega varovanja (2006), osnutek, December, Bruselj.
9. Implementation of the Strategy and Action Plan to Combat Terrorism (2007), Council of the EU, 23 November, 14306/3/04, Bruselj.

Internetni viri:

1. Critical infrastructure protection.
   Dostopno na: http://www.publicsafety.gc.ca/prg/em/cip-eng.aspx z dne 10. 2. 2008.
2. Critical Infrastructure Protection: Elements of Risk.
   Dostopno na: http://cipp.gmu.edu/archive/RiskMonograph_1207_r.pdf z dne 10. 2. 2008
3. Critical Infrastructure Protection: Shared Functions – Shared Vulnerability.
   Dostopno na: http://cipp.gmu.edu/archive/Sweden-US_CIP_30-Nov-2005.pdf z dne 11. 2. 2008
4. National Infrastructure Protection Plan 2006.
   Dostopno na: http://cipp.gmu.edu/archive/NIPP_Plan6-06.pdf z dne 13. 2. 2008

Ostalo:

1. Encyclopedia of the Central Intelligence Agency, Facts on File, New York, 2003
2. International Military and Defense Enciklopedy: Macmillan INC., Washington, 1993.
3. Leksikon Cankarjeve založbe - Družboslovje, Ljubljana, 1986.
4. Slovar slovenskega knjižnega jezika, Ljubljana, 1994.