# Grožnje in ranljivost kritične infrastrukture iz fizičnega in kibernetskega prostora

Aleš Kotnik, Ministrstvo za obrambo

**Namen prispevka:**
Prispevek je namenjen prepoznavanju groženj in ranljivosti, ki pretijo kritični infrastrukturi in pravočasen odgovor na le te, kar postaja vse bolj pomemben faktor varnostnega upravljanja. Cilj raziskave je, kako ugotoviti v primeru ogroženosti ali gre za eno ali več groženj kritični infrastrukturi.

**Metodologija:**
Doseženi cilji predstavljajo razumevanje pojmov in procesov, ki so se v zadnjih letih zgodili na področju zaščite kritične infrastrukture ter kako je lahko kritična infrastruktura ogrožena iz kibernetskega prostora. Prispevek je rezultat znanstvenih in neznanstvenih metod dela: analiza domače in tuje literature s področja zaščite kritične infrastrukture in varnosti kibernetskega prostora, študije primerov, izkustvene metode poznavanja sistemov in metoda avtoritete, kjer se bom skliceval na spoznanja določenih avtoritet s tega področja. Teoretični del prispevka bo podal osnovni vpogled v problematiko in omogočil nadaljnji razvoj in raziskave ter vpeljavo rešitev v prakso.

**Ugotovitve:**
Raziskava bo pokazala del stanja na področju zaščite kritične infrastrukture ter kibernetskega prostora, ki je neločljivo povezan z njo ter kako vpliva ogroženost in ranljivost kibernetske prostora na kritično infrastrukturo. Diskusija je namenjena iskanju rešitev na področju obvladovanja tveganj na osnovi analiz groženj in ranljivosti, ki pretijo kritični infrastrukturi iz fizičnega in kibernetskega prostora.

**Omejitve/uporabnost raziskave**
Omejitev predstavlja širina področja, zato v raziskavo ne bomo vključili podrobnih razčlenitev kritične infrastrukture po posameznih sektorjih in podsektorjih. Podrobneje se bo obravnavala kritična infrastruktura brez delitve na posamezne sektorje, razen informacijsko komunikacijske tehnologije, ki je vezana na kibernetski prostor. Prispevek bo osnova za izvedbo raziskave – ankete na področju kritične infrastrukture in stanja le te v republiki Sloveniji.

**Praktična uporabnost**
Prispevek bo omogočil poglobljeno teoretično razmišljanje in poznavanje problematike, ki vodi do praktičnih rešitev in služijo za nadaljnji razvoj obravnavane problematike.

**Izvirnost/pomembnost prispevka**
Prispevek predstavlja nadaljevanje pionirskega dela na tem področju in uvaja kot možne rešitve matematični in statistični vidik obravnavanja problematike. Prispevek je namenjen vsem strokovnjakom, ki se na kakršnikoli ravni ukvarjajo s problemom zaščite kritične infrastrukture v javnem in zasebnem sektorju.

**Ključne besede:** kritična infrastruktura, kibernetski prostor, ogroženost, ranljivost, obvladovanje tveganj

## 1 UVOD

Velike spremembe v mednarodnem okolju na političnem, varnostnem, obrambnem, socialnem in okoljskem področju ter globalizacija so v 21. stoletju prinesle nove priložnosti in izzive na varnostnem področju. Vse to postavlja odgovornost nacionalno varnostni politiki in nacionalno varnostnemu sistemu, da vzpostavi učinkovite odgovore na spremenjeno varnostno okolje. Značilnost sodobnih groženj je kompleksnost, grožnje so med seboj povezane in transnacionalne in zahtevajo takojšen odziv, da ne pride do t.i. domino efekta. Danes se soočamo z grožnjami v fizičnem in virtualnem

svetu, ki so dokaj realne, nevarne in lahko imajo potencialno smrtonosne posledice. Grožnje eni državi ali naciji pomenijo potencialno grožnjo tudi za druge, česar se premalo zavedamo. Prepoznavanje groženj in pravočasen odgovor na le te postaja vse bolj pomemben faktor varnostnega upravljanja. Grožnje varnosti kot so terorizem, informacijske, okoljske, gospodarske, kriminalitetne, zdravstvene, vojaške in druge grožnje, so v raziskovalnem in prakseološkem smislu pomembne zaradi njihovega potencialno smrtonosnega vpliva na ljudi in temeljno družbeno infrastrukturo (Prezelj, 2010: 5).
Kibernetskega prostora ne omejujejo meje, zato je potrebno sodelovanje in usklajevanje posameznih vlad na področju kibernetske obrambe, varnostni režimi pa se vedno bolj zanašajo na povezane in odvisne informacijsko komunikacijske sisteme. Hitrost kibernetskih napadov in posledično napačne politične odločitve lahko v javnem in zasebnem sektorju povzročijo veliko in nepopravljivo škodo na kritični infrastrukturi. Vse bolj naraščajo politično motivirani kibernetski incidenti in konflikti, kibernetska varnost pa vse bolj vpliva na nacionalno varnost. Še vedno se premalo zavedamo pomembnosti zaščite kritične infrastrukture, ki je bolj ali manj prepuščena posameznikom in posameznim organizacijam. Ali smo sploh varni in kako ugotoviti v primeru ogroženosti ali gre za eno ali več groženj, ki so potencialno nevarne, so glavna vprašanja, ki se zastavljajo ob reševanju tega problema.

# 2 KRITIČNA INFRASTRUKTURA, KIBERNETSKI PROSTOR IN KIBERNETSKE GROŽNJE

Danes je vse bolj potrebno razumevanje novega okolja, ki nas obdaja – t.i. kibernetsko okolje. Bistvene razlike med kibernetskim in nuklearnim okoljem postavljajo pred družbo nove izzive varnosti. V sodobnem času se pojavljajo nove grožnje kritični infrastrukturi in kibernetske grožnje, kar predstavlja veliko skrb in obveznost, da se zagotovi obstoj varnega in stabilnega okolja.

Tabela 1: Razlike med nuklearnim in kibernetskim okoljem (Vir: prirejeno po Williams, 2011)

| Nuklearno okolje | Kibernetsko okolje |
|---|---|
| Nevarno samemu sebi | Del vsakdanjega življenja |
| Računanje s tveganjem | Odsev in prispeva h globalizaciji |
| Pretežno samo vojaško politično zadeva | Zadeva javni in zasebni sektor |
| Hitro razvijanje strategij | Nejasen razvoj strategij |
| Odvračanje, prisila, krizno upravljanje in nadzor nad oborožitvijo | Nejasna opredelitev pojmov |

Pri obravnavi kritične infrastrukture in kibernetskega prostora lahko govorimo o njuni kompleksni soodvisnosti, kar bo predmet nadaljnje raziskave. Seveda pa moramo vzeti v obzir tudi različno gledanje in pojmovanje kritične infrastrukture, njene ogroženosti in ogroženosti iz kibernetskega prostora v posameznih državah, ki se med seboj lahko razlikuje predvsem po njeni pomembnosti in ogroženosti. Dayton opredeljuje vse večje grožnje z razvojem informacijsko komunikacijske tehnologije. S tem, ko je svet postal vse bolj povezan in države vse bolj odvisne od računalniške tehnologije in visoke hitrosti komunikacije, vidimo vse večje grožnje zasebnosti naših državljanov, celovitosti naših poslovnih transakcij, varnosti naše kritične infrastrukture in tudi pripravljenosti naših oboroženih sil. (Per Concordiam, 2011:4).
Kritična infrastruktura predstavlja občutljivo področje zaradi njene vloge v družbi in procesih, ki potekajo v njej. Zgodovinsko gledano se o kritični infrastrukturi pogovarjamo šele nekaj desetletij. Problem kritične infrastrukture se pojavi že na samem začetku, ko poskušamo identificirati kaj jo sploh predstavlja oziroma kaj sodi izven tega področja. Kritična infrastruktura predstavlja pojem, kateri ima več definicij, ki so odvisne od okolja v katerem se le ta nahaja. Danes poznamo več definicij, skupni imenovalec pa lahko najdemo v definiciji Prezlja, ki pravi, da sodobno pojmovanje kritične infrastrukture zajema vse tiste objekte in sisteme, katerih nedelovanje oziroma omejeno delovanje povzroča družbeno-krizne situacije ali celo ogroža varnost. Sem sodi širok spekter infrastruktur, kot so prometna, elektroenergetska, naftna, plinska, zdravstvena, jedrska, prehranjevalna, vodooskrbna, informacijska in podobna infrastruktura (Prezelj, 2010: 5-6).

Zapletenost procesov v fizičnem in kibernetskem prostoru predstavlja danes glavno težavo pri zagotavljanju varnosti. Dostop do elektronskih medijev in s tem prisotnost posameznika v virtualni skupnosti postaja vse pogostejše in tudi časovno vse dalj časa. Kibernetski prostor obsega tako globalne javne dobrine kot nacionalno politično področje, sredstva in obveznosti, je vir moči in šibkosti in tudi posrednik tako represije kot revolucije, kar predstavlja značilen paradoks in kompleksnost (Williams, 2011). Je domena, ki je povezana z ostalimi fizičnimi in vojaškimi domenami in predstavlja neodvisen in soodvisen sistem kritične infrastrukture, kar pomeni, da sam po sebi predstavlja kritično infrastrukturo in vpliva na ostale sektorje kritične infrastrukture. Danes lahko govorimo o prostoru na kopnem, morju, zraku, vesolju in novi »dimenziji, ki jo je v celoti ustvaril človek in jo poimenujemo kibernetski prostor (Wingfield, 2011). V teh domenah se hitro razvija tehnologija, ki ima veliko možnosti uporabe, izvaja se politika za doseganje boljšega stanja ter zakonodaja, ki nam to dopušča ali pa prepoveduje. Nazadnje se je razvil kibernetski prostor, kjer veljajo posebni varnostni in tehnološki režimi. Vsak incident v kibernetskem prostoru sproži vprašanje ali gre pri tem za kaznivo dejanje oziroma se bo izvajal kazenski pregon, ali gre morebiti za napad ali celo vojaško operacijo, kjer bo potrebno upoštevati pravo oboroženih konfliktov[1], ali pa gre za legalno zbiranje podatkov in v nekaterih primerih tudi za vohunjenje.

Kibernetski prostor ni omejen samo na internet s katerim ga največkrat povezujemo. V ta širok prostor vključujemo od signalov za daljinsko upravljanje, mobilnih telefonov, radijskih in televizijskih signalov, interneta do povezav za vodenje brezpilotnih letal, raznih nadzornih sistemov, električnih omrežij, navigacijskih sistemov, bankomatov, satelitskih povezav in podobno. Nadalje ta prostor sestavlja informacijsko okolje v katerem so prepletena soodvisna omrežja infrastrukture, informacijske tehnologije, vključno z internetom, telekomunikacijska omrežja, računalniški sistemi in vgrajeni procesorji in krmilniki (Department of Defence USA Army, 2010).

Kibernetske grožnje predstavljajo zapleten pojav, ki ga običajno posamezne vlade ne jemljejo dovolj resno. Kompleksnost sodobnih groženj vodi k vedno večjemu tveganju in s tem ranljivosti sodobne družbe. Organiziran kriminal, teroristične skupine, skrajneži in tudi v nekaterih primerih vojaške in obveščevalne službe so lahko vir kibernetskih groženj. Iz tabele je razvidno, da je varnost kritične infrastrukture iz kibernetskega prostora odvisna od simetričnih in asimetričnih groženj, ki pretijo iz narave ali pa so plod dela človeka kot posameznika ali skupine v fizičnem ali kibernetskem okolju.

Tabela 2: Razdelitev groženj, ki vplivajo na varnost kritične infrastrukture (vir: po Hanganu, 2011)

| Razdelitev groženj in nevarnosti | | |
|---|---|---|
| Izvor | Narava | Človek |
| Simetrične | Potres, poplava, suša, plazovi,… | Konvencionalno vojskovanje, incidenti, … |
| Simetrične kibernetske | | Programske napake, tehnične napake,… |
| Asimetrične | Ekstremni vremenski dogodki, padec meteorjev in drugih kozmičnih predmetov. | Terorizem, organiziran kriminal, napake pri oblikovanju, delovanju in vzdrževanju sistemov |
| Asimetrične kibernetske | | Informacijsko, omrežno vojskovanje,… |

Po mojem mnenju se do sedaj nismo preveč obremenjevali z asimetričnimi grožnjami, kjer izstopajo padci meteorjev in drugih kozmičnih predmetov ter informacijskim in omrežnim vojskovanjem, katere grožnje vse bolj prehajajo iz imaginarnosti v realnost. Ne glede na to za kakšno vrsto kritične infrastrukture gre in v kateri državi se nahaja, je le ta ogrožena od skupnih groženj, ki so lahko naravne nesreče, namernih groženj od kriminala do sabotaž in nenamernih groženj, kot so razne sistemske in druge napake.

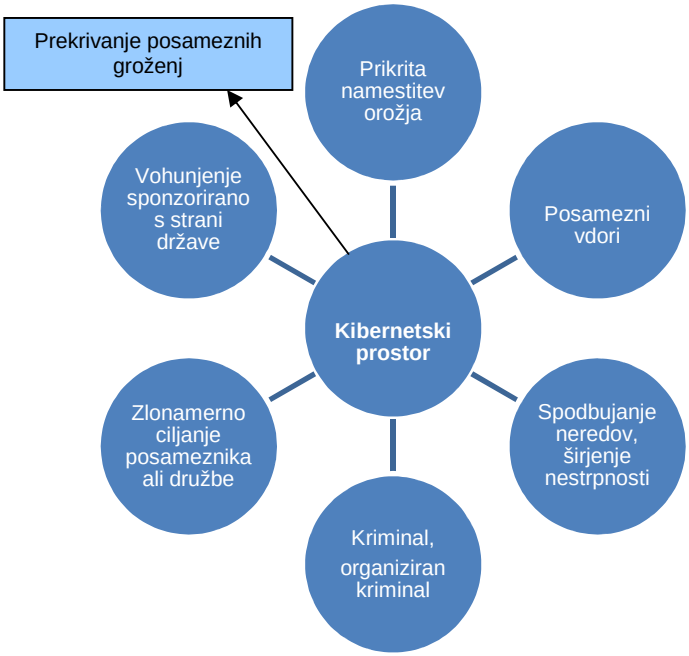
Delovanje v kibernetskem okolju omogoča anonimno in tudi lažno predstavljanje, kar seveda otežuje nadzor nad kibernetskimi operacijami. Sodobna družba postaja vse bolj odvisna od kibernetskega prostora, kar povečuje nevarnosti, ki zaenkrat še niso ustrezno definirane, kadar govorimo o

[1] Znano kot Mednarodno humanitarno pravo.

kibernetskem kriminalu ali kibernetskih napadih. Visoka hitrost izvajanja kibernetskih operacij pušča malo časa za:

- učinkovito preiskavo vdorov,
- učinkovito sodelovanje med prizadetimi državami ali organizacijami,
- učinkovit in hiter pregled vseh pravnih sredstev, ki so nam na voljo za obrambo.

Poleg kibernetskega kriminala ogrožajo varnost še kibernetsko industrijsko vohunjenje in spletni napadi, ki povzročajo na svetovnem nivoju milijardne stroške in ogrožajo narodna gospodarstva in nacionalno varnost. Spletni kriminal sodi med po nekaterih raziskavah med najhitreje rastoče in je celo prehitel do kriminal nezakonite uporabe drog. Kot primer porasta kibernetskega kriminala navajam poročilo Nacionalnega centra za gospodarski kriminal (kriminal belih ovratnikov)[2] iz ZDA, kjer so leta 2009 zaznali več kot 330.000 primerov kibernetskega kriminala, kar je bilo skoraj sedemkrat več kot leta 2001.




Slika 1: Različne vrste groženj iz kibernetskega prostora (Vir: lastnen)

Na sliki so prikazane grožnje, ki so lahko neznatne, lahko pa so tudi obsežne in kompleksne. Iz kibernetskega prostora nam pretijo različne grožnje, ki praktično nimajo omejitev in so odvisne od namena in domišljije napadalca, kar ga postavlja v prednost pred branilcem, ki mora zagotavljati varnost ter je omejen pri odkrivanju in preprečevanju tovrstnih napadov. Sliko bi lahko še razvejali, saj je različnih možnosti zlorabe kibernetskega prostora še veliko. Kibernetski kriminal vse bolj ogroža varnost omrežij, ki so nezaščitena, grožnje proti njim pa so vse bolj prefinjene.

Kibernetski terorizem pa se v splošnem razume kot nezakonit napad in grožnjo za napad na računalnike, omrežja in informacije shranjene na njih, da bi se ustrahovala ali prisilila vlada in njeni ljudi v izpolnjevanje političnih in družbenih ciljev (Kamal, 2005: 61). Kibernetski terorizem bi lahko bil le ena od oblik kibernetskega napada, kar pa lahko privede do napačnega razumevanja kibernetskih groženj na splošno in zavedanja nevarnosti kibernetskega terorizma. Primer kibernetskega terorizma bi bili politično motivirani kibernetski napadi, ki bi vodili v smrt ali telesne poškodbe, eksplozije ali hudo gospodarsko škodo (Kane, 2010). Posebno pozornost v kibernetskem prostoru je potrebno nameniti kriminalno teroristični povezavi, katera je lahko zavestno in namenoma, nevarno pa je nenamensko sodelovanje, ko se lahko kriminalci uporabijo kot orodje v rokah teroristov.

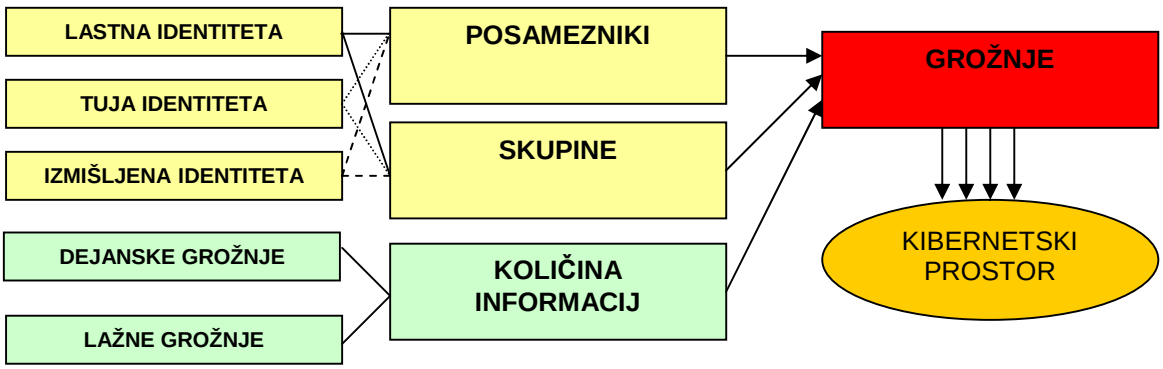
Kibernetski napadi naraščajo tako v smislu pogostosti kot tudi resnosti napadov. Dnevno je sproženo na tisoče kibernetskih napadov, ki povzročajo ogromno finančno škodo. Kibernetski napadi v osnovi

[2] U.S. National White Collar Crime Center.

ne povzročajo poškodb, smrti ali uničenja. Največja teža kibernetskega napada je uničenje podatkov, ki neposredno vplivajo na delovanje sistemov. Posledica nedelovanja sistemov pa lahko povzroči poškodbe, smrt ali uničenje. Glavne značilnosti kibernetskih napadov so:

- Napadalci ne rabijo fizičnega stika z objektom napada.
- Napadalec ima na voljo več oblik napada.
- Razvejano kibernetsko omrežje onemogoča takojšnjo identifikacijo napadalca.
- Po identifikaciji napadalca se pogosto pojavi vprašanje kako ukrepati naprej.

Kibernetski napadi po eni starani zagotavljajo anonimnost, saj se lahko na mnogo načinov zakrije identiteta napadalcev, napadalcem je zagotovljena varnost, saj lahko delujejo na velike razdalje in niso nikoli v takšni nevarnosti kot kriminalci, ki delujejo na »klasične« načine. Tudi kazni na področju kibernetskega kriminala so nižje. Za samo izvedbo, predvsem manjših napadov, pa ne potrebujemo večjih finančnih sredstev. S pomočjo komunikacijsko informacijskih sistemov se lahko dejansko povzroči tudi fizična škoda s pomočjo ukazov, ki povzročajo namerne napake pri delovanju krmiljenih sistemov. Na ta način je lahko ogrožena infrastruktura in v povezavi z njo življenja ljudi.




Slika 2: Različne možnosti ogrožanja v kibernetskem prostoru (vir: lasten)

Najtežje je odkrivati identiteto za katero stojijo ljudje, ki »živijo« v kibernetskem prostoru. Pri tem uporabljajo lastno, tujo ali izmišljeno identiteto. Po drugi strani pa se varnostni organi srečujejo s problemom, kako iz množice sovražnih informacij in groženj v kibernetskem prostoru odkriti tiste, ki dejansko pomenijo grožnjo.

# 3 OCENA GROŽENJ IN POSLEDIC NAPADA NA KRITIČNO INFRASTRUKTURO

Tveganja, nevarnosti in grožnje za kritično infrastrukturo so različne in so odvisne od velikosti in lege države. Na vsako državo vedno obstaja možnost (kibernetskega) napada na kritično infrastrukturo. Raziskava narejena v Srbiji (Gačić, 2010), je podala pregled ocene ogroženosti objektov kritične infrastrukture od potencialnih terorističnih napadov. Sama stopnja nevarnosti od potencialnih terorističnih delovanj na kritično infrastrukturo je nizka, za kar se je izreklo 63,16% vprašanih. Samo 5,26% vprašanih pa je ocenilo, da je stopnja ogroženosti zelo visoka in 15,79%, da je visoka. Nadalje je v raziskavi potekala ocena najbolj ogroženih objektov kritične infrastrukture, kjer so med te postavili energetske objekte, objekte vodne oskrbe, industrijske objekte, telekomunikacijske objekte, vojaške in državne objekte, letališča in verske objekte. Po oceni vprašanih so veliko manj ogroženi objekti ambasad, mednarodnih organizacij, tujih podjetij, kmetijskih objektov, objektov za javna zbiranja, izobraževalne institucije, prometna infrastruktura, športni objekti, železniške postaje in vlaki, plovni objekti (rečna plovila) ter avtobusne postaje in avtobusi.
Raziskava narejena v Indiji (Express Computer, Mumbai, 2011), je pokazala, da je njihova kritična infrastruktura ogrožena. Kritična infrastruktura v Indiji se je v zadnjih letih močno spremenila in se je

razširila predvsem na področju javnih podjetij v sektorjih telekomunikacij, energije, rafinerij nafte, plinovodov in obrambnega resorja. Kritična infrastruktura je v lasti podjetij, ki so z vidika narodnega gospodarstva zelo pomembni in bi napad preko kibernetskega omrežja na njih imel velik negativen ekonomski vpliv, ki bi lahko ogrozil nacionalno varnost. Ta ocena je nastala po napadih na posamezne elemente kritične infrastrukture v Indiji, ki so postali vse pogostejši in učinkoviti. Frekvenca napadov na kritično infrastrukturo je zabeležena na vsakih »nekaj« mesecev. Za indijsko vlado in industrijo je v primeru kritične infrastrukture prednostnega pomena postala informacijska varnost, ki ima največjo luknjo v uporabi ponarejene programske opreme. Raziskava je pokazala, da 43% indijskih podjetij poskuša »zapreti« svoja omrežja zaradi učinkovitih napadov na njih. Za izboljšanje situacije na prvo mesto navajajo varnostno usposabljanje za zaposlene in hiter odziv ter revizijo stanja ob napadu. Nadalje je raziskava pokazala, da 80% indijskih podjetij ceni načrte njihove vlade za zaščito kritične infrastrukture. Podjetja morajo prenehati uporabljati varnostne kopije za arhiviranje pravnih dokumentov in uporabljati tehnologije za preprečevanje izgube podatkov. 70% anketirancev je bilo zaskrbljenih zaradi izgube podatkov.

Kakšne bi bile posledice napadov na kritično infrastrukturo (fizično, iz kibernetskega prostora ali kombinirano), je težko oceniti. Napadi bi lahko bili življenjsko nevarni, ne glede na to, pa bi takšen napad pomenil napad na način življenja. V vsakem primeru bi bile posledice hude, tudi če se napad zgodil samo na enem področju kritične infrastrukture. Najtežji udarci bi povzročili:

- Pomanjkanje oskrbe z električno energijo, kot posledica napada na elektroenergetski sistem, ki ga tvorijo jedrske, termo in hidroelektrarne.
- Prekinjena ali omejena komunikacija na mobilnih, stacionarnih in internetnih omrežjih kot posledica napada na informacijsko komunikacijske sisteme.
- Prekinjen ali omejen cestni, železniški in letalski transport kot posledica napada na transportno omrežje.
- Zamrznjeno ali omejeno finančno poslovanje ali celo zlom borz, bank in ostalih finančnih inštitucij kot posledica napada na finančne in bančne centre.
- Prekinitev linij vodenja in poveljevanja vojaških in policijskih enot ter nacionalnih centrov za krizno upravljanje in pošiljanje ponarejenih ukazov in naročil.

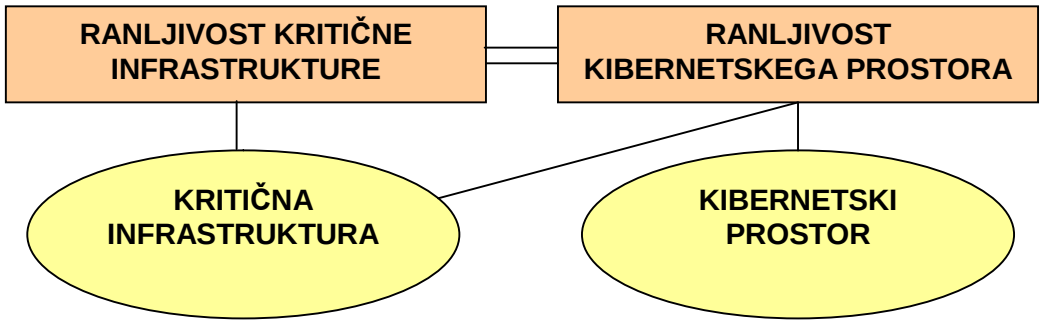
Pri napadih na sisteme kritične infrastrukture bi prišlo do težkih posledic, velike gospodarske škode in izgube podatkov in premoženja, ki bi lahko trajalo daljše časovno obdobje. Napadi bi povzročili začasno onesposobitev ali uničenje energetskih sistemov, prometa, finančnega sistema, informacijsko komunikacijskega sistema, nujnih in drugih storitev, katere bi lahko spremljale tudi poškodbe ali celo smrti večjega števila prebivalstva. Na mikro nivoju bi lahko bili primeri teh napadov povzročanje smrti ali telesnih poškodb s pomočjo eksplozij, napadov na masovna transportna sredstva, onesnaženje oziroma doziranje strupenih snovi v pitno vodo in podobno. Načinov in sredstev je veliko in je nemogoče predvideti vse možnosti. Resni napadi na kritično infrastrukturo bi lahko bili posledica terorizma, saj bi imele posledice tudi večji politični učinek. Napade, ki bi ovirali nebistvene storitve ali ne bi povzročali večje škode, ne moremo uvrstiti kot grožnjo kritični infrastrukturi. Odvisno od vrste motnje na kritični infrastrukturi bi lahko imele le te lokalne, regionalne ali širše svetovne posledice. Kritična točka je odvisna od stopnje šibkosti kritične infrastrukture, ki jo lahko izkoristijo posamezniki, skupine ali države pri napadu na kritično infrastrukturo. Zato lahko govorimo o t.i. kritični ranljivosti, ki jo bodo izkoristili naši sovražniki v kritičnem času v prihodnosti. Grožnje kritični infrastrukturi lahko povzročijo grožnjo celotni naciji, kaos, smrt, izgubo nadzora s strani vlade, spremembo razmerja moči in radikalizma ogroženih državljanov (Kane, 2011).

## 3.1 Ranljivost kritične infrastrukture in kibernetskega prostora

Napadi, nesreče, naravne katastrofe in druge oblike negativnih dogodkov nas občasno spomnijo na našo ranljivost, ki je lahko prisotna na vseh področjih družbenega in zasebnega življenja posameznikov. Po mnenju OVSE (Ohlsson, 2011) obstajajo trije dejavniki zaradi katerih je kritična infrastruktura ranljiva:

1. kompleksnost sistema kritične infrastrukture,
2. grožnje pred kibernetskimi napadi
3. globalizacija.

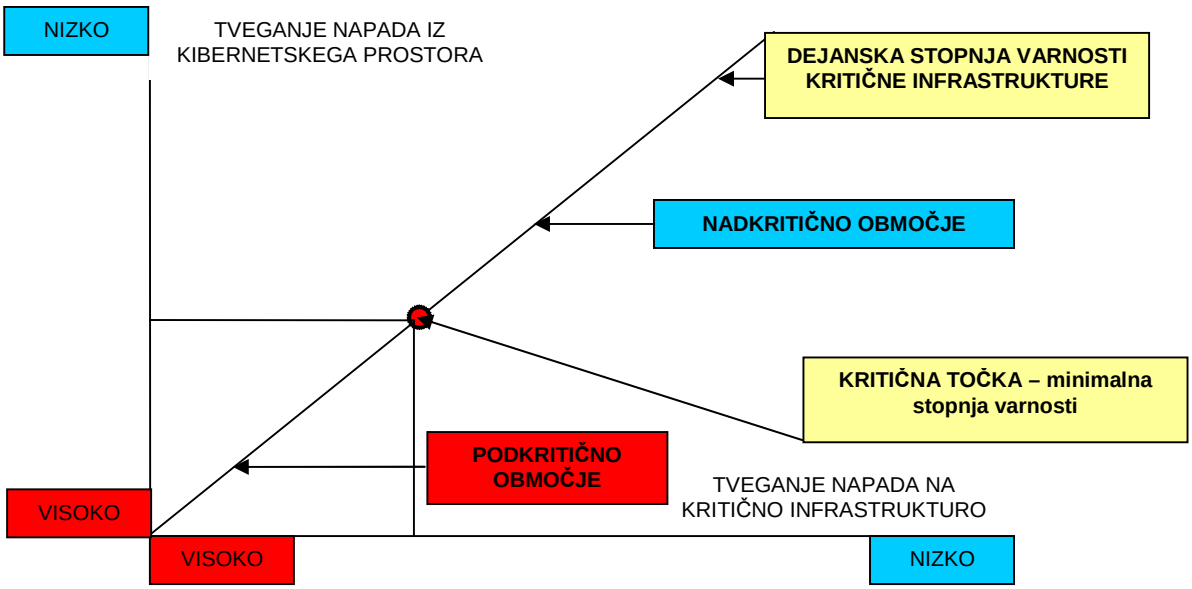
Ranljivost izvira iz nezmožnosti, da se zagotovi ustrezna zaščita in je ponavadi neposredno sorazmerna z vlogo, ki jo infrastruktura ima (Hanganu, 2011: 79). Ob tem pa se pojavlja tudi efekt domin, ko se pojavi kolateralna škoda tudi v direktno neprizadetih sektorjih. Takšni primeri kot je na primer električni mrk v ZDA leta 2003, ko je brez elektrike ostalo 55 milijonov ljudi. Ob tem pa je nastala tudi kolateralna škoda, saj se je ustavil tudi javni prevoz (vlak), čistilne naprave za zagotavljanje pitne vode niso delovale, baterije mobilnih telefonov so ostale izpraznjene, veliko podjetij je ostalo zaprti in tako naprej (Branscomb, 2011). Iz tega primera vidimo, da je kritična infrastruktura ranljiva ne samo v enem segmentu, ampak lahko pomeni izpad enega segmenta posledično izpad tudi drugih segmentov kritične infrastrukture.




Slika 3: Ranljivost kritične infrastrukture (vir: lasten)

Kritična infrastruktura bo vedno imela visoko stopnjo ranljivosti. Kadarkoli cilj predstavlja destabilizacijo ali uničenje, to postavlja kritično infrastrukturo na prvo mesto med tarčami. Ranljivost kritične infrastrukture je odvisna od več dejavnikov in je možna iz kopnega, morja, zraka, vesolja in kibernetskega prostora. Ranljivost kritične infrastrukture vpliva na kritično infrastrukturo, medtem ko ranljivost kibernetskega prostora vpliva na kibernetski prostor in kritično infrastrukturo. Iz te medsebojne povezave torej ne smemo zanemariti ranljivosti kritične infrastrukture iz kibernetskega prostora. Kritična infrastruktura je bila v preteklosti najbolj ranljiva tam, kjer je bila njena zaščita v smislu organizacijskih, tehničnih in drugih dejavnikov najslabša. Dejavnik ranljivosti iz kibernetskega prostora je bil pred desetletji povsem zanemarljiv, v sodobnem času in prihodnosti pa bo verjetno prevzel največji delež k skupni ranljivosti kritične infrastrukture. Iz navedenega lahko sklepamo, da je ranljivost kritične infrastrukture odvisna od ranljivosti kibernetskega prostora. Torej velja, bolj kot je ranljiv kibernetski prostor, bolj je ranljiva kritična infrastruktura. Iz tega lahko izpeljemo trditev, da je ranljivost kritične infrastrukture sorazmerna z ranljivostjo kibernetskega prostora.
Dejanska stopnja varnosti kritične infrastrukture je odvisna od stopnje tveganja napada na kritično infrastrukturo in stopnje tveganja napada na kritično infrastrukturo iz kibernetskega prostora. V kolikor sta stopnja tveganja napada na kritično infrastrukturo iz kibernetskega prostora in tveganje napada na kritično infrastrukturo pod kritično točko, pridemo v podkritično območje, kjer dejansko ne moremo govoriti o varnosti kritične infrastrukture oziroma je možnost napada na njo velika.
Dejansko je pomembno kakšna stopnja tveganja obstaja in kje se tveganja lahko razvijejo v negativno smer. Zaradi tega je potrebna ocena tveganja in analiza ogroženosti, ki nam dasta podlago za določitev dejanske stopnje varnosti kritične infrastrukture in kritične točke. Vrednosti dejanske stopnje varnosti kritične infrastrukture, ki so odvisne od obeh tveganj pa ne smejo biti pod kritično točko, ki ga opredeljujeta oba tveganja. Želeno stanje doseganja nadkritičnega območja pa v praksi pogosto ni enostavno ali včasih tudi dosegljivo
Dobra primera dokaza slike in diagrama je ranljivost kritične infrastrukture iz kibernetskega prostora, kjer je bila ogrožena jedrska infrastruktura in bi lahko imeli napadi zelo hude posledice:

- Iranski jedrski program, ki je bil leta 2010 s pomočjo črva Stuxnet napaden iz kibernetskega prostora, kar je povzročilo povečevanje hitrosti centrifug do kritične meje in izklop varnostnih sistemov.
- Nuklearna elektrarna Davis-Besse v Ohiu v ZDA je bila leta 2003 s pomočjo črva Slammer napadena iz kibernetskega prostora, kar je povzročilo večurno prekinitev delovanja nadzornega sistema jedrske elektrarne.




Slika 4: Stopnja varnosti kritične infrastrukture v odvisnosti od tveganj napada na kritično infrastrukturo in tveganj napada na kritično infrastrukturo iz kibernetskega prostora (vir: lasten)

Nizka stopnja tveganja napada na jedrsko kritično infrastrukturo, ki se zagotavlja z visokimi standardi, organizacijskimi, tehničnimi, fizičnimi in drugimi ukrepi, ki zagotavljajo varnost jedrskih programov oziroma objektov niso zagotovili minimalne stopnje varnosti, zaradi visoke stopnje tveganja napada iz kibernetskega prostora, kar je bila posledica pomanjkljivih varnostnih ukrepov pred napadi iz kibernetskega prostora.

## 3.2 Javno-zasebni interes na področju zaščite kritične infrastrukture

Večina strokovnjakov z varnostnega področja se strinja, da mora tako zasebni kot tudi javni sektor oziroma vlada enakopravno sodelovati in nositi svoj del odgovornosti pri zaščiti kritične infrastrukture in s tem tudi kibernetskega prostora. Določena stopnja sodelovanja postaja vse bolj nujna in nepogrešljiva. Zasebni sektor pa se med seboj vse bolj povezuje, zaradi česar postajajo družbe v rokah tako domačih kot tujih lastnikov. Ravno to pa postavlja pred državo pomembno vlogo, kako doseči visoko stopnjo zaščite kritične infrastrukture s tem da pomaga in tudi »prisili« domače in tuje lastnike kapitala, da bodo ustrezno zaščitili infrastrukturo s katero upravljajo. Pri sodelovanju pa pri sodelovanju seveda ne sme priti do slabljenja varnosti enega ali drugega sektorja. Zato je potrebno jasno razlikovanje med javnim in zasebnim sektorjem v zvezi z odgovornostjo na področju zaščite kritične infrastrukture, ki počasi a vztrajno izginja, vse do točke, kjer ni nihče v celoti odgovoren za določen segment, temveč je to skupna odgovornost (Čaleta, 2011: 20). Pri temu je potrebno doseči ravnovesje med odgovornostjo, ki jo imajo pri zagotavljanju zaščite na eni strani upravljavci kritične infrastrukture in na drugi strani država ter najti ustrezne rešitve pri razdelitvi nalog med državo na eni strani in npr. zasebnim podjetjem na drugi. Ena izmed težav, ki nastopajo na tem področju so varnostne naložbe, ki ne smejo biti zgolj strošek podjetja ampak investicija, ki pa ni nujno dobičkonosna. Zato se mora tukaj vključiti država, ki takšne investicije spodbuja z raznimi ukrepi in olajšavami, seveda pa tovrstni stroški ne morejo bremeniti samo države ampak morajo biti enakomerno porazdeljeni med oba subjekta.
To še posebej velja npr. za ZDA, kjer je 85% kritične infrastrukture v lasti zasebnega sektorja (Kane: 2011) in mora prihajati do sodelovanja med vlado in zasebnim sektorjem. Tudi ameriška Komisija NSPG[3], ki je naslednica Komisije 9/11 je ob 10 obletnici v svojem poročilu zapisala, da je varovanje

[3] National Security Preparedness Group

kritične infrastrukture, ki je v zasebni lasti postala nujna prednostna naloga, pri čemer morata javni in zasebni sektor izboljšati izmenjavo in pretok informacij (Tenth Anniversary Report Card, 2011: 6). Zasebni sektor v ZDA se mora prilagoditi na novo realnost in se osredotočiti na to, kako najboljše zaščititi infrastrukturo in osebje ter razvijati načrte pripravljenosti ob motnjah ter razvijati inovativne varnostne značilnosti po posameznih panogah (npr. celovitost ladijskih zabojnikov, ki prihajajo v državo, analize tveganj zavarovalnih družb odražajo nove razmere v podjetjih). Tudi napadi iz kibernetskega prostora po mnenju komisije niso nemogoči ali nerealni, zaradi česar morajo tudi temu področju posvetiti prednostno nalogo. Kibernetske grožnje so osredotočene na sisteme kritične infrastrukture, ki so po mnenju komisije sistemi z oskrbo električne energije, finančni sektor, sistemi za oskrbo z vodo, hrano in energijo ter vojaška in telekomunikacijska omrežja. Komisija je ugotovila (tudi na primeru japonske jedrske krize), kakšne uničujoče posledice za družbo imajo prekinitve električnih omrežij in druge osnovne infrastrukture.

Podoben procent lastništva kritične infrastrukture imajo tudi v ZRN, kjer se 80% kritične infrastrukture nahaja v zasebni lastnini. V ZRN je odgovornost porazdeljena med zasebni sektor in vlado. Naloga zasebnega sektorja je upravljanje infrastrukture in zagotavljanje varnosti. Podlaga za njihovo dejavnost je nemška ustava, zakoni, ekonomska logika in zasebni interesi. Nemška vlada na zveznem nivoju pa zagotavlja zaščito infrastrukture in državljanov v vojnem času, v miru pa skrbi za koordinacijo in podporo. 16 zveznih dežel pa je odgovorno za kontrolo nad uničenjem v mirnodobnem času. ZRN nima posebnega zakona za zaščito kritične infrastrukture, imajo pa izdelano strategijo, ki opredeljuje principe sodelovanja na zveznem in deželnem nivoju skozi njihovo zakonodajo in drugo organizacijo, kjer prihaja do sodelovanja med različnimi ministrstvi, ki pokrivajo posamezna sektorska področja kritične infrastrukture (Papsthart, 2011). Podporo pri zaščiti kritične infrastrukture nudi tudi zvezna vlada pod katero delujejo organizacijske enote Ministrstva za notranje zadeve in drugih ministrstev[4].

Dejstvo je, da so zasebna podjetja, ki upravljajo s kritično infrastrukturo v današnjem času preprosto prisiljena, da vlagajo v varnost. S tem zaščitijo sebe, svoje poslovanje in zagotovijo širšo družbeno varnost. V kolikor prihaja do sodelovanja z javnim sektorjem, lahko postane vlaganje v varnost še bolj učinkovito, razdelijo pa se tudi stroški in druge zmogljivosti, kar poveča stopnjo varnosti.

# 4 ZAKLJUČEK

Varnostne razmere v svetu in regiji se hitro spreminjajo. Dosežena varnostna stanja niso končna stanja. Zato je varnost dobila novo vlogo, opredeljene so nove naloge in načini zaščite kibernetskega prostora in kritične infrastrukture. Idealne varnosti ni, lahko samo dosežemo optimalno varnost v določenem času in prostoru. Zaradi tega se moramo zavedati, da so na tem področju potrebne spremembe v našem razmišljanju in strategiji, ki jo bomo ubrali. Grožnje kritični infrastrukturi iz kibernetskega prostora se v prihodnosti ne bodo zmanjševale, ampak bodo postajale vedno bolj kompleksne in povezane, zaradi česar bo potrebno izboljšati odzivnost vseh vpletenih subjektov, ki skrbijo za varnost. Dejstvo je, da smo nesporno odvisni in s tem ranljivi iz kibernetskega prostora in kritične infrastrukture, bolj kot si to sami želimo. Predvsem kibernetski prostor nam predstavlja šibko točko, na katero velikokrat ne moremo vplivati in bo v veliki meri predstavljala možnost potencialne katastrofe. Vnaprej načrtovani in pripravljeni napadi bodo vedno najbolj kritični in nevarni. Vprašanje zaščite kritične infrastrukture in kibernetskega prostora ni omejeno zgolj na tehnični del, ki v glavnem predstavlja zanašanje na tehnologijo oziroma ožje na fizično in tehnično varovanje, ampak predstavlja celotno politiko in iz nje izhajajočo strategijo. Vse to pa nas vodi do različnih razmerij med ranljivostjo na eni ter zaščito na drugi strani ter kontroliranega nadzora nad tem razmerjem.

Do nove dinamike razvoja prihaja na vseh področjih. Zaradi tega bo postalo obvezno sodelovanje na javno – zasebne sektorju v državah in sodelovanje med državami, zavezništvi in drugimi mednarodnimi inštitucijami. Tako javni kot zasebni sektor bosta morala biti v prihodnosti zelo fleksibilna in pripravljena na hitre prilagoditve.

[4] Counter-Terrorism (Federal Criminal Police Office (BKA), Federal Office for the Protection of the Constitution (BfV)), Information Security (Federal Office for Information Security (BSI)), Civil Protection (Federal Office for Civil Protection and Disaster Assistance (BBK), Technical Unit (THW)).

Po mojem mnenju se kritična infrastruktura in kibernetski prostor v Sloveniji obravnavata dokaj abstraktno v smislu njune nedotakljivosti in neranljivosti, saj zlasti kibernetski prostor predstavlja enega najbolj primernih in učinkovitih načinov za izvajanje asimetričnega bojevanja v bližnji prihodnosti s kibernetskimi napadi, ki so lahko samostojni ali kombinirani z različnimi oblikami fizičnih napadov. Zaradi tega se je potrebno na začetku vprašati kakšna je narava problema in ali je ta problem za nas dragocen v smislu zagotavljanja varnosti. Po rešitvi osnovnega problema je potrebno predvideti kaj nas čaka v prihodnosti, s kakšnimi grožnjami se bomo srečevali, katere grožnje bodo »napredovale« in kakšni bodo problemi kritične infrastrukture in kibernetskega prostora v prihodnosti, kjer bo potrebno podati dokaj kritičen pogled na obravnavano temo.
Absolutne varnosti v najširšem pomenu besede ni in ne obstaja, torej tudi absolutne varnosti kritične infrastrukture in kibernetskega prostora ni. Ali smo dejansko pripravljeni na nove izzive varnosti ali ne, pa bo pokazal čas oziroma dogodek, ki bo vplival na varnost kritične infrastrukture in kibernetskega prostora Slovenije. Do takrat pa je potrebno posvetiti čim večjo pozornost tem vprašanjem in izvajati preventivne ukrepe, ki morajo biti konstantni v daljšem časovnem obdobju, da se bomo približali idealni pripravljenosti pred napadi in nesrečami.

# VIRI


Branscomb, M. L. (2011). Still Vulnerable in 2011. Pridobljeno 1.10.2011 na http://www.proquest.co.uk

Čaleta, D. (Ed.), Shemella, P. (Ed.) (2011). Counter terrorism challenges regarding the process of critical infrastructure protection. Ljubljana.

Department of Defence USA Army (2010). Dictionary of Military and Associated Terms, Joint Publication.

Express Computer, Mumbai (2011). The intent of cyber criminals has changed. Pridobljeno 10.9.2011 na http://www.proquest.co.uk

Gačić, J. (2010). The management of the system of integrated protection in the function of eliminating the consequences of terrorist attacks. FSS, Belgrade.

Hanganu, M. (2011). Martime and Fluvial Critical Infrastructure Security, Pridobljeno 13.9.2011 na http://www.ceeol.com

Kamal, A. (2005). The Law of Cyber Space. United Nations Institute for Training and Research, Geneva, Switzerland.

Kane, J. J. (2011). Cyber Security and Cyber Terror, George C. Marshall European Centre for Security Studies. Garmisch-Partenkirchen, Germany.

Lukman, M., Bernik, I. (2009). Ogrožanje kritične infrastrukture iz kibernetskega prostora. 10. slovenski dnevi varstvoslovja. UM, Fakulteta za varnostne vede, Ljubljana.

National Security Preparedness Group, (2011). Tenth Anniverssary Report Card. Pridobljeno 8.9.2011 na http://www.bipartisanpolicy.org/sites/default/files/CommisionRecommendations.pdf

Papsthart, C. (2011). Critical Infrastructure Protection in Germany – Peculiarities and Complexities in a federal State with Private Operators. IRC, Maribor, 27 – 29.9.2011.

Per Concordiam, Volume 2, Issue 1 (2011). Securing Cyberspace (str. 4 – 41). Journal of European Security and Defence Issues.

Perrow, C. (2007). The Next Catastrophe: Reducing Our Vulnerabilities to Natural, Industrial, and Terrorist Disasters. Princeton University Press, ZDA.

Podbregar, I. (2011). Critical Infrastructure and Public-Private Partnership. IRC, Maribor, 27 – 29.9.2011.

Prezelj, Iztok (Ur.) (2010). Kritična infrastruktura v Sloveniji. Fakulteta za družbene vede.

Svete, U., Kolak, A. (2011). Defending Cyber Threats: What traditional national approach can Contribute? IRC, Maribor, 27 – 29.9.2011.

The Cyber Security Forum Initiative, (2010). Preliminary Stuxnet report ver. 1:16. Pridobljeno na http://www.csfi.us.

Williams, P. (2011). Strategy for Infrastructure Protection and Crisis management in the Cyber Age: An Elusive Quest? IRC, Maribor, 27 – 29.9.2011.

Wingfield, C. T. (2000). The Law of Information Conflict: National Security Law in Cyberspace. Aegis Research Corp.