UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Andreja Marinčič

Zaščita kritične infrastrukture v ZDA: primerjalni vidik

Diplomsko delo

Ljubljana, 2009

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Andreja Marinčič

Mentor: doc. dr. Iztok Prezelj

Zaščita kritične infrastrukture v ZDA: primerjalni vidik

Diplomsko delo

Ljubljana, 2009

Zahvala

Zahvalila bi se mojemu mentorju dr. Iztoku Prezlju za njegove strokovne usmeritve in nasvete pri izdelavi diplomske naloge. Posebej bi se zahvalila svojim najbližjim za razumevanje in podporo, še posebej očetu, dr. Dušanu Marinčiču, ki je s svojo strokovnostjo in predvsem z očetovskim čutom dodatno vplival na mojo vztrajnost in uspešnost pri izdelavi diplomske naloge. Preteklost in izkušnje so me pripeljale do naslednjega uspešnega koraka, kar mi brez družine ne bi uspelo, zato posvečam svojo diplomsko nalogo očetu dr. Dušanu Marinčiču in mami Jelki Marinčič.
HVALA.

ZAŠČITA KRITIČNE INFRASTRUKTURE V ZDA: PRIMERJALNI VIDIK

V današnjem času se z razvojem sodobne družbe pojavljajo tudi najrazličnejše oblike ogrožanja temeljnih družbenih razsežnosti, ki so pomembne za njen obstoj. Pričujoča diplomska naloga obravnava predvsem stopnjo zaščite kritične infrastrukture v ZDA, ki omogoča obstoj in razvoj tamkajšnje družbe ter s tem varnost prebivalstva. Kakovost zaščite je preverjena s pomočjo primerjalne analize razvitosti zaščite kritične infrastrukture v ZDA in izbranih evropskih državah. Z analizo definiranja kritičnih sektorjev, organizacijskih vidikov, normativnih podlag, pobud in iniciativ v Franciji, Nemčiji, na Nizozemskem, v Švici in Veliki Britaniji je ocenjena sistemska urejenost zaščite kritične infrastrukture v ZDA. Z razkrivanjem sistemskih razlik se pojavlja tudi zanimivo razmerje zagotavljanja zaščite med javnim in zasebnim sektorjem v posamezni državi. Analiza finančnega vlaganja v sistemske projekte zaščite kritične infrastrukture v ZDA in EU pa prikaže razliko med celostno obravnavo le-te na nacionalni ravni v ZDA in večnacionalnim pristopom v EU kot mednarodni organizaciji, ki je bolj usmerjena v raziskave in razvoj. Vsi našteti analitični elementi nakazujejo, da so ZDA celostno oblikovale in uskladile zaščitne ukrepe in instrumente, kar jim zagotavlja pravočasno ter učinkovito odzivanje na krizne razmere in s tem zaščito kritične infrastrukture.

Ključne besede: Kritična infrastruktura, krizne razmere, zaščita kritične infrastrukture in ZDA.

CRITICAL SECURITY INFRASTRUCTURE IN USA: COMPARATIVE ANALYSIS

Development of contemporary society has been confronted with different threats to its societal dimensions. The level of protection of critical infrastructure in USA is primary topic of this diploma, because it represents part of the society that enables existence and constant development and security for the population. Quality of protection was analyzed with the comparative analysis of developments in protection of critical infrastructure among USA and five chosen European countries. With the analysis of defined critical sectors, organizational views, normative basis, initiatives and comprehension of the concept in France, Germany, the Netherlands, Swiss and Great Britain, was possible to assess the system of critical infrastructure protection in USA. Different approach in financial investments for the critical infrastructure protection between USA and EU clearly shows holistic approach on a national level in USA and multinational approach in EU, which is more oriented toward researches and developments. All above mentioned analytical elements indicates that the USA have been protecting their critical infrastructure by defining and synchronizing protective measures and instruments in the holistic way, which is providing timely and efficient response in the crisis.

Key words: Critical infrastructure, crisis, system of critical infrastructure protection (CIP) and USA.

KAZALO

SEZNAM TABEL, GRAFOV IN SLIK

1. GRAFI

2. SLIKE

3. TABELE

SEZNAM KRATIC

AKSIS Working Group on Infrastructure Protection
(Delovna skupina zaščite KI)

BCS British Computer Society
(Britanska združba računalničarjev)

BKA The Federal Criminal Police Agency
(Federalna kriminalna policija)

BKK Federal Office for Civil Protection and Disaster Response
(Federalna divizija za civilno zaščito in odzivi na katastrofe)

BMI Federal Ministry of the Interior
(Federalno ministrstvo za notranje zadeve)

BSI The Federal Office for Information Security
(federalna divizija za zaščito informacijske tehnologije)

CIDDAC Cyber Incident Detection & Data Analysis Center
(neprofitna organizacija za zaščito omrežja pred cyber-kriminalom)

CIP Critical infrastructure protection
(Zaščita kritične infrastrukture)

CIWIN Critical Infrastructure Warning Information Network
(Krizno informacijsko omrežje KI)

CLUSIS Association Suisse de la Sécurité des Systèmes d'Information
(Švicarsko združenje sistema zaščite informacijske tehnologije)

CPNI Centre for the Protection of the National Infrastructure
(Center za zaščito KI)

CSS Center fo security studies
(Center za varnostne vede)

CSTI Strategic Advisory Board on Information Technologies
(Strateško posvetovalno telo za informacijsko tehnologijo)

DHS Department of homeland security
(Ministrstvo za domovinsko varnost)

ECI European critical infrastructure
(Evropska kritična infrastruktura)

ECP.NL Platform Electronic Commerce in the Netherlands

(Izboljšanje elektronske komerciale)

EPA U. S. Environmental protection agency
(agencija v ZDA za zaščito okolja)

EPCIP European Programme for CIP
(Evropski program za zaščito KI)

EU European Union
(Evropska unija)

FBI Federal Bureau of Investigation
(Federalna obveščevalna agencija)

FEMA Federal Emergency Management Agency
(Federalna agencija za nujno odzivanje)

FOCP Federal Office for Civil Protection
(Federalno ministrstvo za civilno zaščito in tudi šport ter obrambo)

HSPD-7 Homeland Security Presidential Directive
(Predsedniška direktiva domovinske varnosti)

I3P Institute for Information Infrastructure Protection
(Združenje vodilnih univerz, nacionalnih laboratorijev in neprofitnih institucij za zaščito informacijske KI)

IAAC Information Assurance Advisory Council
(Svetovalni organ informacijske tehnologije)

InfraGard Partnership between the FBI and the private sector
(predstavlja partnerstvo med FBI in zasebnim sektorjem)

ISAC Financial Services Information Sharing and Analysis Center
(Center za širjenje informacij in analizo – finančni, transportni, električni)

ISDF French Dependability Institute
(Forum predstavnikov zasebnega sektorja)

KI Kritična infrastruktura

KWINT Kwetsbaarheid op Internet – Samen werken aan meer veiligheid en betrouwbaarheid

MI5 The Security Service
(Varnostna služba VB)

MNZOK Ministrstvo za notranje zadeve in odnosi kraljestva

NACOTEL National Telecommunications Contingency Plan

(Nacionalni načrt razvoja telekomunikacij)

NCI National critical infrastructure
(Nacionalna kritična infrastruktura)

NCO-T National Continuity Consultation Platform Telecommunications
(Nacionalni načrt razvoja oplemenitenja telekomunikacij)

NCSA National Cyber Security Alliance
(Državno povezavo cyber-zaščite med industrijo in vladnimi organizacijami)

NCSP National Cyber Security Partnership
(Prostovoljna koalicija trgovskega združenja industrije za zaščito cyber-omrežja)

NES National economic supply
(Agencija za državne ekonomske zaloge)

NIPP National Infrastructure Protection Plan
(Nacionalni načrt za zaščito infrastrukture)

NISCC National Infrastructure Security Co-ordination Centre
(Nacionalni center za koordinacijo infrastrukturne varnosti)

NSAC National Security Advice Centre
(Nacionalni center za varnostno svetovanje)

PCCIP Presidential Commission on Critical Infrastructure Protection
(Predsedniška komisija za zaščito KI)

PCIS Partnership for Critical Infrastructure Security
(Partnerstvo za zaščito KI)

PDD Presidential Decision Directives
(Predsedniške odločilne direktive)

SGDN General Secretary of National Defense
(Generalni sekretariat državne obrambe)

SSP Sector-specific plan
(Sektorsko specifični načrt)

VB Velika Britanija

WG CIP Working group for criticial infrastructure protection
(Delovna skupina za zaščito KI)

ZDA Združene države Amerike

UVOD

Motiv za nastanek diplomske naloge je nastal z razmišljanjem, kaj je tisto, o čemer bi pisala, da bi imelo ne samo osebni, vendar tudi družbeni, širši pomen. Zavedanje, da vsako raziskovalno delo pripomore h kritičnemu razmišljanju, je prvi korak k spreminjanju družbe. Osebna želja in motiv je, da bi naloga podala jasno sliko o dejanski pripravljenosti ZDA, da zaščitijo temeljne varnostne, družbene razsežnosti in njihovo kritično infrastrukturo, v teoretičnem in praktičnem smislu.

Pričujoča diplomska naloga se je izoblikovala na podlagi številnih predhodnih razmišljanj in raziskovanj, tujih in domačih virov. Svoje razmišljanje sem usmerila v tisto, kar je za sodobno družbo vitalnega pomena. Ena od možnih tem je bila prav zaščita kritične infrastrukture (KI), ki predstavlja zaščito posameznih delov družbe, pomembnih za njen obstoj. Na poti raziskovanja sem prišla do ugotovitve, da ni veliko literature, ki bi opredeljevala kritično infrastrukturo. Tovrstno dejstvo je posledica premajhnega razmišljanja in vlaganja v zaščito najpomembnejših virov preživetja, vse od ravni zasebnega podjetja do širše družbene skupnosti. Kot pripadniki sodobne družbe bi se morali zavedati pomembnosti zaščite kritične infrastrukture ter posledic njenega razdejanja. Vsi se namreč spomnimo mogočnega orkana Katrina, ki je rušil številne domove v New Orleansu in za seboj puščal razdejanje, ki je spodbudilo nova vlaganja v razvoj zaščite kritične infrastrukture ZDA.

Ameriška družba se je ob omenjeni krizi soočila z varnostnim vprašanjem, kako zaščititi družbo in njene temeljne razsežnosti. Ljudje so bili brez vode, elektrike, skratka, brez pogojev za normalno bivanje. Tedanja družba je bila zgrožena nad delovanjem najmogočnejše države, ki se je po 11. septembru 2001 resnično usmerila v celostno zaščito države. Dejstva pričajo svoje in govorijo, da niti najmogočnejše države, kot so ZDA, niso bile sposobne uspešno reševati nepredvidljivih kriznih razmer.

Zaradi omenjenih dejstev sem se, po pregledu novejših virov, odločila za raziskovanje, kako pravzaprav deluje zaščita kritične infrastrukture v ZDA kot ekonomsko-politično najmočnejši državi na svetu v primerjavi z izbranimi evropskimi državami ter EU kot

mednarodno organizacijo. Skozi celotno diplomsko nalogo bom poskušala prikazati delovanje zaščite kritične infrastrukture dveh kontinentov, ki ju oblikujeta in zaznamujeta povsem različni tradiciji in s tem tudi vojaške izkušnje.

ZDA nosijo tradicijo politike izolacionizma; neposrednim vojaškim bojem svetovnega vidika se priključijo šele leta 1917 in s tem prvič potencialno ogrožajo svoje vitalne vire preživetja. Skozi zgodovinska obdobja vse od antike do modernega časa so se evropske države nenehno bojevale in tako vedno znova rušile pomembne družbene razsežnosti določenega zgodovinskega časa. Glede na vojaška udejstvovanja so imele ZDA (in Švica) večje možnosti razvoja in vlaganja v zaščito kritične infrastrukture kot ostale evropske države, ki so se nenehno bojevale. Veliki mejnik v zgodovini ZDA predstavlja 11. september 2001, ko so teroristi napadli simbol njihovega gospodarskega uspeha. Ameriško prebivalstvo in njegovi vitalni viri preživetja so bili prvič v zgodovini v neposredni nevarnosti, posledice pa katastrofalne: veliko žrtev in seveda najpomembnejše – rušenje ekonomske stabilnosti in varnosti v ZDA. Nastopil je čas velikih sprememb, ko je bilo med drugim opaziti pospešen razvoj zaščite kritične infrastrukture, kar dokazuje pomembnost njenega obstoja v nekoč najbolj razviti državi.

Na osnovi opisanega bi verjetno vsak bralec predvideval, da Evropa in tudi EU kot mednarodna organizacija bolj ali manj zaostajata za ZDA. A vendarle čas in tradicija nista edino merilo zagotavljanja varnosti zaščite družbeno najpomembnejših razsežnosti. S to ugotovitvijo sem se podala na pot raziskovanja, kjer se pojavljajo tudi druga merila, ki lahko vsako raziskovalno delo usmerijo v nepričakovano smer. Slednja misel je tisto, kar daje velik pečat nastalemu delu.

1 METODOLOŠKO-HIPOTETIČNI OKVIR

Metodološko-hipotetični okvir vsebuje glavne usmeritve pri obdelavi virov. S tem bom prišla do želenih raziskovalnih spoznanj. Ta del se nanaša zlasti na opredelitev predmeta in ciljev raziskave ter na hipoteze, ki bodo uporabljene kot povezovalni elementi. Za lažje razumevanje področja proučevanja bom definirala nekaj najpomembnejših pojmov.

1.1 Opredelitev predmeta in cilja proučevanja

Predmet proučevanja je primarno zaščita kritične infrastrukture v ZDA; v okviru tega bom opisala strukturne elemente, njihov pomen za stabilnost družbenega razvoja, načrtovane ukrepe za njihovo zaščito in subjekte zagotavljanja zaščite KI. *Sekundarni predmet proučevanja bo zaščita KI v Franciji, Veliki Britaniji, Nemčiji, Švici in na Nizozemskem ter na ravni EU kot mednarodne organizacije.* Do sedaj obdelani viri kažejo na povezanost mnogih akterjev, ki je vidna skozi številne odnose. Prav ti odnosi so osnova nastajajočega omrežja, vse od zasebnih agencij do institucij državne ravni. Če vse skupaj združimo, dobimo veliko število akterjev, povezanih v vrsto medsebojnih odnosov, ki tvorijo kompleksno omrežje zaščite kritične infrastrukture. V tem pomenu je kompleksnost razumljena kot število odnosov, ki jih je treba aktivirati v času ogrožanja KI. Potreba, da morajo za zaščito KI poskrbeti subjekti zasebne ravni (e. g. zasebne agencije) kot tudi državni organi, ki skrbijo za normalno delovanje celotne družbe, bo razložena v nadaljnjih poglavjih.

Celosten pristop vsekakor upošteva tudi cilj proučevanja diplomske naloge, ki je opredeljen v naslednjih točkah:

1. *Z izbranimi viri pridobiti vpogled v zaščito KI v ZDA, EU kot mednarodni organizaciji ter posebej v Franciji, Nemčiji, na Nizozemskem, Švici in Veliki Britaniji*. Za primerjavo sem izbrala EU kot mednarodno organizacijo, ki se nenehno primerja z ZDA na področju ekonomije, politike in varnosti. Gre za

pariteto obeh sil, kjer v tem primeru ZDA opredeljujemo kot organizacijo združenih držav[1] in EU kot organizacijo članic evropskih držav.[2]

Poudariti moram, da EU do danes še nima potrjenega sistema zaščite Evropske kritične infrastrukture. Torej celotna zaščita kritične infrastrukture temelji na direktivi, kjer je junija 2008 Svet za pravosodje in domovinske zadeve dosegel politično soglasje za izdajo direktive za identifikacijo KI EU (ECI) in izboljšanje njene zaščite. Direktiva vzpostavlja nujnost za identifikacijo in imenovanje ECI ter podaja splošen pristop ocenjevanja potrebe za izboljšanje zaščite KI, z namenom zaščititi ljudi. Direktiva se osredotoča na zaščito energije in transporta, kasneje pa bodo po potrebi dodani ostali kritični sektorji, kot je informacijska tehnologija (EU Council 2008, 1–3). Torej, kot vidimo, dosedanja zaščita KI v EU ne obsega vseh kritičnih sektorjev (le energijo in transport) in vsi obstoječi dokumenti, iz katerih sem črpala podatke, služijo zgolj kot predlogi, ki se bodo morda nekoč uveljavili. Skratka, zaščita KI v EU temelji na predlogu in nekoč morda lahko pričakujemo sistem, ki bo v celoti obravnaval vse pomembne kritične sektorje, ne samo transport in energijo.

Druga primerjava se nanaša na ZDA in izbrane evropske države. Vse države so bile izbrane na podlagi kriterija družbene razvitosti, ki se kaže tudi v zadostni razvitosti kritične infrastrukture posamezne države. Francija, Nemčija, Nizozemska in VB, vse članice EU, bodo z medsebojnimi razlikami služile kot merilo usklajenosti posameznih držav (nacionalna raven) kot tudi EU (mednarodna raven). Poleg članic EU je k seznamu držav dodana tudi Švica, ki predstavlja nevtralno državo skozi celoten zgodovinski razvoj modernih držav in mednarodnih odnosov. Švica kot država, ki je vodila politiko nevmešavanja in izolacionizma vse do danes, predstavlja edinstven primerek v sistemu zagotavljanja varnosti. Njeno mesto je postavljeno na podlagi zanimanja, ali je razvila primerljivo oziroma bolj razvito zaščito KI kot ZDA glede na podobno politiko vodenja ZDA vse do leta 1917.

2. *Analiziranje pojmovanja KI* v ZDA, EU in petih izbranih državah. Kako vsak izbrani subjekt opredeljuje KI in zakaj je temu tako.

[1] Konstitucionalna – federalna republika, ki predstavlja skupno 50 držav in 1 pokrajino (https://www.cia.gov/library/publications/the-world-factbook/geos/us.html#Govt (7. avgust 2008)).
[2] »Edinstveno« gospodarsko in politično partnerstvo med 27 demokratičnimi evropskimi državami (za podrobnejši opis glej http://europa.eu/abc/panorama/index_sl.htm (7.avgust 2008)).

3. *Predstaviti organizacijski vidik, normativne podlage, pobude in iniciative zaščite KI* v ZDA, EU in petih izbranih državah. Z interpretacijo bom ugotavljala podobnosti in razlike med izbranimi entitetami.
4. *Cilj proučevanja predstavljajo tudi nadaljnja finančna vlaganja na področju zaščite KI v ZDA in EU.* Po mojem mnenju so finančna vlaganja eden od pomembnejših kazalcev, ali država razvija in s tem tudi izboljšuje zaščito KI. Cilj je torej odgovoriti na vprašanje, ali ZDA in EU povečujejo/zmanjšujejo svoja finančna vlaganja v zaščito KI, na katerih področjih in kaj je vzrok takšne odločitve.

1.2 Hipoteze

Celotna diplomska naloga bo izhajala iz štirih hipotez, ki bodo vseskozi povezovale predmet in cilj proučevanja. Najpomembnejša bo vsekakor splošna hipoteza, kateri bodo sledile posebne.

a) Splošna hipoteza

»Zaščita kritične infrastrukture v ZDA je bolj razvita v primerjavi z izbranimi državami in EU kot mednarodno organizacijo.« Razvitost zaščite KI bom utemeljila na podlagi razlik določenih izbranih spremenljivk. Merilo bo razvejanost sistema, v smislu števila akterjev oziroma subjektov, ki so neposredno povezani na zasebni in javni ravni. Poleg tega bo pomemben kazalec razvitosti tudi čas, torej, kdaj je posamezna država pričela razvijati zaščito KI, normativni akti, ostali pomembni dokumenti ter finančna vlaganja v zaščito KI.

b) Posebne hipoteze

Iz splošne hipoteze sem izpeljala posebne hipoteze, in sicer:

1. Posebna hipoteza: ***»V ZDA je razumevanje fizične in virtualne družbene razsežnosti kritične infrastrukture bolj celostno opredeljeno v primerjavi s Francijo, Nemčijo, Nizozemsko, Švico in Veliko Britanijo.«*** Postavljeno domnevo bom skušala raziskati s primerjavo definicij kritičnih sektorjev predhodno

omenjenih držav. Kritični sektorji namreč opredeljujejo obseg družbenih razsežnosti, ki so bodisi fizične ali »navidezne« narave. Fizično bom obravnavala v smislu neposrednega ogrožanja sistema KI, katerega posledice so vidne človeškemu očesu. Pojem »navidezno« oziroma virtualno pa se bo vsekakor nanašal na neposredno ogrožanje sistema KI preko elektronsko-komunikacijskih omrežij. Gre torej za »nove oblike ogrožanja«, ki v prvi vrsti ogrožajo informacijske sisteme[3]. Glede na pridobljene vire ZDA v svoji zaščiti KI opredeljujejo tudi informacijski sistem, kar pomeni večji obseg zaščite vitalnih družbenih razsežnosti.

2. Posebna hipoteza: ***»V času novih oblik groženj družbi je vse bolj pomembna zaščita informacijske kritične infrastrukture, ki predstavlja vitalni del družbenega razvoja.«*** Zadnja hipoteza se navezuje na predhodno omenjeno hipotezo, kjer v veliki meri ugotavljam, ali ima zaščita informacijske KI vse bolj pomembno vlogo v celotnem sistemu zaščite KI. To bom ugotavljala na podlagi tega, kakšno zaščito imajo ZDA, v smislu poudarjanja pomena informacijske KI. Ali ZDA informacijsko KI obravnavajo kot sestavni element celotnega sistema KI, brez katerega sistema KI sploh ne bi bilo?

3. Posebna hipoteza: ***»Večja finančna vlaganja v zaščito kritične infrastrukture in tradicija opredeljevanja potrebnih ukrepov dajejo prednost ZDA pred EU.«*** Kot sem omenila že pri splošni hipotezi, bo zgodovinski čas eden od kazalcev prednosti oziroma razvitosti sistema zaščite KI. K temu bom dodala še ekonomski vidik, finančna vlaganja EU in ZDA. V smislu, koliko ZDA in EU pravzaprav vlagajo v razvoj sistemov KI. Iz tega bo razvidno, ali ZDA bolj poudarjajo zaščito KI kot EU in v kolikšni meri.

[3] Tu se srečamo s pojmom informacijsko bojevanje, digitalno bojevanje (ang. digital warfare), kibernetsko bojevanje (ang. cyber warfare) ali nebojno bojevanje (ang. non-cinetic warfare). Pri opredeljevanju informacijskega bojevanja naletimo na problem, kajti nekega splošno sprejetega in uveljavljenega pristopa, ki bi opredeljeval informacijsko bojevanje, ni. Skoraj vedno zajema uporabo informacijskih tehnologij, vključuje napade na informacije, informacijske procese in informacijsko infrastrukturo nasprotnika ter zavarovanje lastnih informacij, informacijskih procesov in informacijske infrastrukture. Izvaja ga neka organizirana skupina (izjemoma posameznik) za dosego svojih ciljev, ki so lahko vojaški, ekonomski, socialni, politični, ideološki ipd. Nasprotnik v informacijskem spopadu je navadno odvisen od informacijskih sistemov (Dovč 2005, 7–9).

1.3 Struktura naloge

Diplomska naloga bo poleg uvoda, metodološko-hipotetičnega okvira, vsebovala tudi zaključek z verifikacijo postavljenih hipotez, seznam uporabljene literature in naslednje vsebinske sklope:

a) **Opredeljevanje obsega kritičnih sektorjev ter definiranje različnih pojmovanj kritične infrastrukture** za posamezne izbrane države. Omenjeno bo vsebina *prvega poglavja*, kjer bom s primerjalno analizo med ZDA, EU in petimi izbranimi evropskimi državami prikazala obseg kritičnih sektorjev. Najpomembnejše bodo razlike posameznih držav, ki bodo služile kot kazalec razvitosti in razumevanje pomembnosti zaščite KI.

b) V *drugem poglavju* bom pojasnila **organizacijski vidik** zaščite KI posameznih izbranih držav. Torej, kateri subjekti so najpomembnejši v verigi odločanja, koliko je agencij, in podobno. V tem poglavju bo najpomembnejše ugotavljanje, ali poleg državne in zasebne ravni ločenega sodelovanja obstaja tudi sodelovanje javno - zasebno. Kazalec tega bo vsekakor število tovrstnih povezav in njihovo sodelovanje.

c) Sledila bosta opis in definiranje pomena zaščite KI posameznih izbranih držav v *tretjem poglavju*, preko obsega in števila **normativnih aktov, iniciativ in pobud**. Kdaj je posamezna država institucionalizirala zaščito KI, koliko dokumentov obstaja, ali so se dokumenti skozi čas »posodabljali« in zakaj je temu tako? V drugem in tretjem poglavju bom svoje raziskovanje usmerila tudi v primerjalno analizo sistemov zaščite *informacijske kritične infrastrukture*.

d) *Četrto poglavje* bo pojasnjevalo morebitna sedanja in prihodnja **finančna vlaganja** na področju zaščite KI, tako v ZDA kakor tudi v EU. Pojasnila bom dosedanje dosežke na omenjenem področju s primerjavo obeh entitet ter nato prikazala razvojne smernice.

Po končanem vsebinskem delu sledi sklepni del na podlagi primerjalne analize, kjer bom rezultate raziskovanja povezala v teorijo z verifikacijo postavljenih hipotez.

1.4 Uporabljene metode raziskovanja

Glede na problem proučevanja bom v svoji analizi uporabila logiko inverzne dedukcije. Na začetku bo analiza izhajala iz teoretičnih modelov razlage zaščite KI, sledila ji bo primerjalna analiza na podlagi empiričnih podatkov, kasneje pa se bodo ugotovitve ponovno preverile z osnovnim teoretičnim modelom. V zaključku bom z verifikacijo hipotez opisala vpliv empiričnih raziskovalnih rezultatov na znano teorijo. Pri analizi se bodo uporabile naslednje metode raziskovanja:

a) Z deskriptivno metodo bom pojasnila temeljne pojme zaščite KI na splošno in v posameznih izbranih državah. Tovrstno metodo bom uporabila tudi med posameznimi poglavji, kjer bo treba natančno opredeliti temeljne pojme za nadaljnjo razumevanje analize.
b) Z analizo primarnih in sekundarnih virov bom opisala do sedaj znano teorijo o zaščiti KI.
c) S študijo primera bom raziskala predvsem zaščito KI v ZDA, nato v Franciji, Nemčiji, Švici, na Nizozemskem in v Veliki Britaniji ter v EU kot mednarodni organizaciji.
d) Sledila bo metoda primerjalne analize zaščit KI posameznih držav (in EU) ter njihovih kazalcev. Ugotavljala bom razlike in podobnosti, njihove povezave in razmerja na transnacionalni ravni.

1.5 Opredelitev temeljnih pojmov

Diplomska naloga bo vseskozi povezovala štiri najpomembnejše temeljne pojme analize. Sprva bom definirala **kritično infrastrukturo,** sledil bo pojem **kritične informacijske infrastrukture**, **zaščita kritične infrastrukture** in nazadnje pojem **krize**.

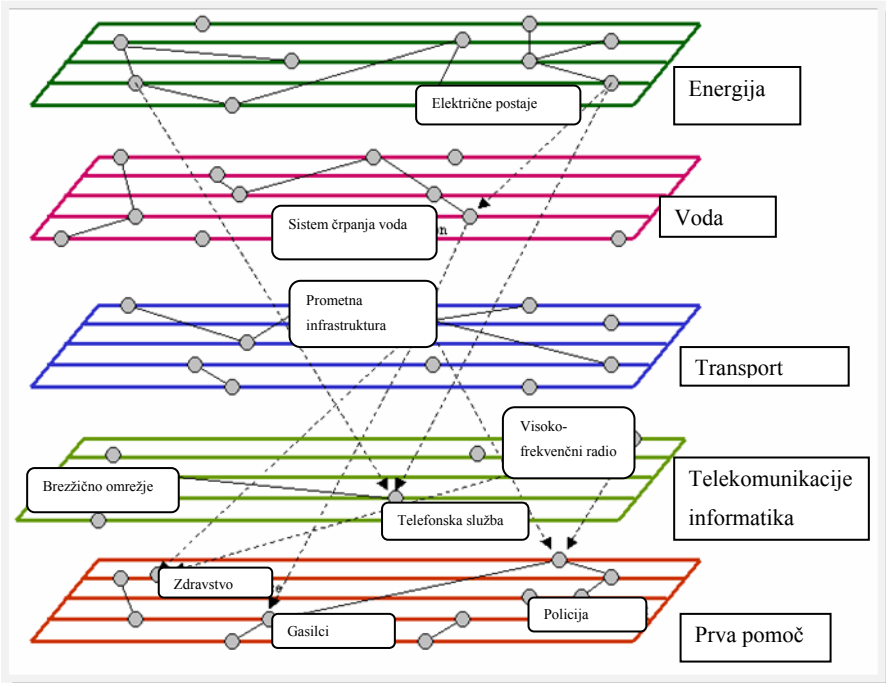
1.5.1 Kritična infrastruktura

Tako kot kriza ima tudi KI različna pojmovanja in opredelitve. Glede na to, da bom primerjala posamezne države, bom predhodno prikazala različne definicije KI v

izbranih državah. Identificiranje medsebojne odvisnosti in operatibilnosti posameznih sistemov kritičnih sektorjev (glej Sliko 1.1) nam pomaga razumeti, kateri so resnično kritični in potrebujejo največjo zaščito (What is CIP? Dostopno prek: http://cipp.gmu.edu/cip/ (11. avgust 2008)). Pojem kritičnosti nam predstavlja predpogoj za natančno opredelitev KI.

Vedeti moramo, da niso vse infrastrukture kritične, in vse KI imajo različno stopnjo kritičnosti. Da bi primerno obravnavali zaščito KI in opredelili, kaj je kritično, moramo razviti analitičen pristop. Omenjeni pristop naj bi opredelil kritične sisteme, identificiral »ranljivost«[4] in se osredotočil na povečanje možnosti preživetja kritičnih območij.

Slika 1.1: Medsebojna odvisnost kritičnih sektorjev oziroma sistemov infrastruktur



VIR: Pederson et al. (2006, 3).

Iz zgornje slike (Slika 1.1) lahko razberemo, kako so posamezni sistemi znotraj celotne kritične infrastrukture določene države med seboj povezani. Kot primer: če zaradi

[4] V kasnejših publikacijah je Haimes (2006) trdil, da je ranljivost *multidimenzionalni koncept*, ki je najbolje opisan preko variable posameznih držav. Variable opisujejo pomanjkljivosti sistema in interakcijo sistema, pri čemer sledi uničujoči pojav. Številni znanstveniki so analizirali pomen »ranljivosti« v različnih kontekstih (e. g. Villagrán de León 2006; Hellström 2005; McEntire 2005; Agarwal et al. 2003; Paton and Johnson 2001; Weichselgartner 2001; Einarsson and Rausand 1998) in prišli do zaključka, da ranljivost pomeni kakršenkoli vidik sistema, ki oslabi svoje sposobnosti preživetja v sovražnem/razdiralnem okolju (Abelle-Wigert and Dunn 2007, 25).

»razloga X« nastane škoda električne postaje, preneha delovati sistem črpanja vode. Če je kriza dolgotrajna, ljudje območja X nimajo dostopa do pitne vode. S tem pride do raznovrstnih posledic, med drugim tudi do večjih zdravstvenih težav ljudi območja X.

Posledice so lahko še večje, kajti izguba elektrike onesposobi delovanje cestnih operacij (e. g. semaforjev), kar prinaša zmedo na cesti in poveča zahteve prve pomoči.

V obeh primerih gre tudi za onesposobitev delovanja informacijskih in telekomunikacijskih sistemov, ki v sodobnem času predstavljajo enega od ključnih povezovalnih elementov kritičnih sektorjev.

Skratka, vsi kritični sektorji posameznih držav so medsebojno povezani kot tudi neodvisni. Zaradi tega se kritična infrastruktura obravnava kot zelo kompleksen in neodvisen **sistem, omrežje in bogastvo**, **ki omogoča obstoj in razvoj vitalnih družbenih** razsežnosti (What is CIP? Dostopno prek: http://cipp.gmu.edu/cip/ (7. avgust 2008)).

S primerjavo definicij pojma KI v posameznih državah pridemo do podobnosti in tudi do razlik. Za večino držav KI pomeni, da lahko njeno neposredno uničenje ali škodovanje le-tej pripelje do resnih negativnih posledic v zvezi s socialno in ekonomsko blaginjo ter državno varnostjo. Nekatere definicije uporabljajo bolj »močno« terminologijo, kjer namesto »resnih« problemov podajajo termin »slabitev«. Nekatere vključujejo vlado, ki predstavlja jedro nacionalne varnosti, druge razširijo socialno in ekonomsko blaginjo z javnim zdravstvom, varnostjo in zaščito. Kljub podobnim definicijam nekatere države podajajo natančnejše elemente definicij, kar služi kot argumentacija, da vse KI niso enako kritične (George Masons university 2007, 4–5). Za bolj celostni vpogled bomo podali definicije KI izbranih držav, in sicer Francije, Nemčije, Nizozemske, Švice, VB, ZDA, ter EU.

Prva, **Francija,** definira KI kot kritične sektorje, ki tvorijo *»vso infrastrukturo, ki je vitalnega pomena za vzdrževanje primarnih socialnih in ekonomskih procesov«* (Abelle-Wigert and Dunn 2006, 149).

»*Kritične infrastrukture so organizacije in institucije velikega pomena za družbo, katere propad ali oslabitev prinaša nenehno pomanjkanje dobrin, močno erozijo javnega reda in ostale dramatične posledice«* (Lenz 2006, 7), opredeljuje **Nemčija**, ki za razliko od Francije uporabi pojem organizacije in institucije. Torej poudarja pomen večjega sistema odnosov. **Nizozemska** *»sektorje razume kot 'kritične', če njihova slabitev ali uničenje lahko vodi do škode nacionalne ravni«* (Ministrstvo za notranje in državne odnose, 2003: 13). Veliko bolj skopa definicija v primerjavi z Nemčijo in skoraj enaka kot definicija Francije. Nikjer ne omenja vitalne oziroma pomembne družbene razsežnosti. **Švica** pojmuje *»kritične infrastrukture ... kot sisteme in bogastvo, katerega uničenje ali slabitev ima lahko velik vpliv na nacionalno varnost ter ekonomsko in socialno blaginjo države«* (Center za varnostne študije 2005, 3). Slednja definicija vključuje elemente definicij vseh prej naštetih držav. Poudarja KI kot sistem, opredeli blaginjo ter dodaja varnostno dimenzijo nacionalne države.

Velika Britanija KI opredeli kot *»kritično nacionalno infrastrukturo, ki je sestavljena iz tistih dobrin, služb in sistemov, ki podpirajo ekonomsko, politično in socialno življenje. Njihova pomembnost je tako velika, da izguba povzroča:*

- *veliko število žrtev,*
- *velik, resen vpliv na nacionalno ekonomijo,*
- *ostale resne socialne posledice za družbo in*
- *pomeni primarno skrb nacionalne vlade«.*

(CPNI. Dostopno prek: http://www.cpni.gov.uk/About/whatWeDo.aspx (11. avgust 2008)). Ta definicija že natančneje opredeli, kaj pomeni uničenje, škoda – tudi v smislu števila žrtev. Torej povezuje tako družbeno kot nacionalno raven. Poudarja KI, ki je omejena na nacionalne meje VB in ne sega preko njih, kar predstavlja negativno konotacijo dojemanja KI na mednarodni ravni. Bolj celosten pristop pri opredeljevanju KI najdemo v definiciji **ZDA**, kjer KI predstavlja *»premoženje, sistem in omrežje, fizično ali virtualno, ki je tako vitalnega pomena za Združene države Amerike, da bi njegovo uničenje ali oslabitev imelo velik negativen vpliv na varnost, državno ekonomsko varnost, javno zdravstvo ali zaščito ali kombinacijo naštetega«* (U. S. Department of Homeland Security 2006, 103). Zelo pomembno je, da tukaj prvič razmejujemo fizično in virtualno oziroma navidezno kritično infrastrukturo. Torej enak pomen pripisujemo KI, ki jo lahko zazna človekovo oko, kot tudi KI, ki je našemu

očesu nevidna. V to področje vključujemo predvsem informacijsko KI, ki jo bom obravnavala v nadaljevanju.

Ne nazadnje moram omeniti še pojmovanje KI **EU,**[5] ki se glasi: *»Evropska kritična infrastruktura – kritična infrastruktura ... če je oslabljena ali uničena, ima močne vplive na dve ali več držav članic ali na eno članico, če je KI locirana v drugi državi članici. Glede na obstoj kompetenc posameznih družb odgovornost za zaščito KI ostaja v rokah posameznih držav in operaterjev KI. Evropska komisija bo podprla državo članico le na njeno prošnjo«* (Commission of the European Communities 2006, 3). Sodeč po tem EU nastopa kot alternativna rešitev za posamezne države članice. V prvi vrsti mora država uporabiti svoje mehanizme in instrumente, če to ne deluje, sledi prošnja EU, ki rešuje nadaljnje probleme. Tu je poudarjen predvsem element odgovornosti. Podobno EU pojmuje Evropsko kritično infrastrukturo, kjer je KI locirana v članicah EU, *katere uničenje ali slabšanje bi imelo vidne posledice v vsaj dveh državah članicah EU. Vsaka določena ECI bo morala imeti operativni varnostni načrt (OSP), ki bo pokrival identifikacijo pomembnih dobrin, krizno analizo, ki temelji na večjih kriznih scenarijih, ter ranljivost vsake dobrine, identifikacijo, selekcijo in poudarjanje pomembnosti zaščitnih dejanj in postopkov*. Zvezni varnostni uslužbenec bo imel funkcijo povezovalca varnostnih vprašanj med ECI-lastniki/operaterji in avtoriteto relevantnih držav članic. Vsaki dve leti bo vsaka država članica Komisiji podala informacije v zvezi z grožnjami in krizami v vsakem ECI-sektorju. Na podlagi teh poročil bodo Komisija in države članice ocenile, ali je potrebna nadaljnja zaščita KI na ravni EU (Europe moves ahead on critical infrastructure protection. Dostopno prek: http://www.continuitycentral.com/news03978.htm (20. septembra 2008)).

Pri analiziranju pojmovanja kritične infrastrukture je videti podobnosti in razlike med posameznimi državami in EU. Najbolj vidna podobnost KI je tisti del družbe, katerega uničenje/slabitev posledično prinaša negativen razvoj vseh pomembnih družbenih razsežnosti. Razlike so vidne predvsem zaradi uporabe različnih terminov. Menim, da najbolj celostno definicijo KI podajo ZDA in EU, ki zajemajo vse elemente definicij ostalih držav in k temu dodajajo virtualno KI, ki je razložena v nadaljevanju.

[7] KI je sestavljena iz fizične in informacijske tehnologije, ustanov, omrežij, služb in dobrin, katerih uničenje ali oslabitev ima lahko resne posledice za zdravje, varnost, zaščito ali ekonomijo vseh državljanov ali funkcije vlad v državah članicah (Commission of European communities 2004, 3).

1.5.2 Kritična informacijska infrastruktura

Ena od mnogih vrst virtualne, navidezne KI je tudi informacijska kritična infrastruktura. V času moderne družbe računalnikov je v splošnem vredno omeniti, da morajo navidezno nenehne serije majhnih elementov delovati pravilno in med seboj sodelovati. Z namenom, da bi ohranili številne procese, ki jih v večini jemljemo za samoumevne.

Le en računalniški virus, majhno odstopanje, tako iznajdljivo, da je za človeško oko nevidno, lahko teoretično sproži kompleksno verigo dogodkov, katere posledice so vidne bodisi na nacionalni ali globalni ravni (Westrin 2001, 67–79). Opisana značilnost loči podatke komunikacije in računalnikov v širšem smislu besede kot tudi omrežja od ostalih elementov KI. Termin »informacijska infrastruktura« se običajno opisuje kot neokrnjenost tovrstne povezave računalnikov in omrežij kot tudi pomembnih informacij, ki potujejo prek njih. Razlika med KI in informacijsko KI je v tem, da informacijska KI zajema vse, kar povezuje ostale kritične sektorje (Dunn 2006, 7).

Ameriški pravni akt CIIA (2002, 7) opredeljuje informacijsko KI kot informacijo, ki ni običajna na javnem področju in se povezuje z varnostjo kritične infrastrukture ali varnostnega sistema. Torej je zaščita informacijske KI v podrejenem položaju glede na zaščito KI. Informacijska KI se osredotoča na zaščito informacijske tehnologije, vključujoč elemente telekomunikacije, računalnike, internet, satelite itd., in na povezave računalnikov ter omrežij.

Če povzamemo, informacijska KI povezuje vse elemente KI, kar priča, da ima zelo velik pomen za stabilnost in zaščito družbenih razsežnosti. Glede na to, da informacijska KI predstavlja eno od družbenih razsežnosti, jo štejemo v podkategorijo KI. Po mojem mnenju, tako kot opredeljuje tudi Dunn (2006, 7), je informacijska KI tista, ki povezuje ostale kritične sektorje. Prav zaradi tega mislim, da je zaščita informacijske KI primarnega pomena. Če preneha delovati informacijska tehnologija, ki predstavlja sestavni del vseh kritičnih sektorjev, preneha delovati celotna zaščita kritične infrastrukture. S tega vidika sem vseskozi obravnavala zaščito informacijske KI.

1.5.3 Zaščita kritične infrastrukture – sistemski vidik

Obstajata dve univerzalni, svetovno veljavni trditvi glede zaščite kritične infrastrukture: preprosto *je nemogoče doseči 100-odstotno varnost kritične infrastrukture in idealna pot reševanja problemov ne obstaja v nobeni državi.* Čeprav ima vsaka država različne (sisteme) zaščite KI, lahko oblikujemo tri glavne kategorije:

Prva kategorija je predhodno omenjena zaščita informacijske KI. Vsebinsko se nanaša neposredno na varnost in zaščito informacijskih povezav in rešitev, znotraj in med individualnimi infrastrukturnimi sektorji. Zaščita fizičnih sestavin je zagotovljena v ločenih organizacijskih okvirih. Funkcije in kompetence, povezane z zaščito KI, so razpršene med različnimi organi. Še več, poskuša se integrirati zasebni sektor na vseh ravneh zaščite KI.

Druga kategorija zajema zaščito informacijske KI in tudi fizično zaščito KI. Na tem mestu je fizična zaščita del nacionalno-civilnega obrambnega modela, centralni ter strateški organi so istočasno center kompetenc v informacijski varnosti, civilni obrambi in nadzorih katastrof. Jasna razmejitev med individualnimi elementi ne obstaja. Pa tudi pomembna vloga nacionalnih ministrstev za obrambo, glede na koordinacijsko vlogo, mora biti poudarjena. Opisani kategoriji rečemo tudi pristop »Vse vrste tveganj«.[6] Oba zgoraj opredeljena pristopa poskušata v nacionalni organizacijski sistem integrirati tako državne kot zasebne akterje. Vendar je sodelovanje med zasebnimi in javnimi sektorji na strateški ravni velikokrat popolnoma odsotno oziroma obstaja v elementarni obliki.

Tretji pristop je poseben primer, ker obstaja samo v kitajskem modelu zaščite KI. Tu ni nobenega sodelovanja med zasebnimi in javnimi sektorji. Model služi bolj za ohranitev vlade in tistih organov, ki predstavljajo interes države, kot pa za zaščito KI. Eden od kazalcev, ki merijo pristop različnih držav, je vprašanje, ali obstaja *nacionalna, nepremagljiva strategija* za zaščito KI. Nekateri verjamejo, da taka strategija obstaja le v ZDA, v ostalih državah pa je popolnoma odsotna (Ritter et al. 2003, 1–2).

[6] Dobesedno mu rečemo pristop »All Hazards«.

1.5.4 Kriza

Kriza je dokaj pogosto uporabljena oznaka za težavne, nevarne in za prihodnost odločilne položaje, saj se nanaša na izredno široko področje naravnih, družbenih, ekonomskih in duševnih procesov (e. g. politična kriza, gospodarska kriza, finančna kriza, naftna kriza, ekološka kriza itd.). V vsakdanjem življenju ima kriza negativno konotacijo, saj jo povezujemo z najrazličnejšimi neprijetnostmi in težavami (Dubrovski 2004, 13).

Zavedati se moramo, da zaradi različnih pojavnih oblike krize in s tem povezanih pristopov obdelave poznamo različne oblike definicij »krize«. Če izhajamo iz začetkov, je Sruk (1980, 189) zapisal, da izraz kriza izvira iz grške besede *krinein*, kar pomeni odločiti kaj, soditi; *krisis* – presoja, prepir. Pri analizi me bo zanimala kriza družbenih razsežnosti oziroma najpomembnejših temeljnih razsežnosti sodobne družbe. Kot bomo videli v nadaljevanju vsebinskega dela, družbene razsežnosti skupaj tvorijo področja kritičnih sektorjev in tudi celotnega sistema zaščite KI. Sprva si bomo ogledali različne definicije priznanih strokovnjakov različnih področij ter na koncu opredelili kazalce krize, ki so pomembni za raziskovanje zaščite KI.

C. F. Hermann (1972, 13) krizo opredeli kot: »... situacijo, ki ogroža visoko prioritetne cilje odločevalca, omejuje količino časa, ki je na voljo za obdelavo odločitve, in že s svojim pojavom preseneti odločevalca.«

Raziskovalci projekta International Crisis Behavior opredeljujejo mednarodno krizo, gledano s perspektive države, kot situacijo, v kateri: (1) so ogrožene temeljne vrednote, (2) je omejen čas za ukrepanje in (3) obstaja visoka verjetnost prisotnosti vojaške sovražnosti.

Podobno opisuje tudi Holsti (1990), ki pravi, da krizo označujeta resno ogrožanje pomembnih vrednot in omejen čas za ukrepanje. Značilno je tudi, da kriza povečuje stres med tistimi, ki se z njo ukvarjajo.

Verjetno najvidnejšo in prepoznavno definicijo krize opredeljujejo Rosenthal, t' Hart in Charles (1989, 10). Pravijo, da je kriza resna grožnja ključnim strukturam ter temeljnim

vrednotam in normam družbenega sistema, ki – pod časovnim pritiskom in v zelo negotovih razmerah – zahteva sprejemanje kritičnih odločitev.

Ne nazadnje je tudi Stern (2001, 8) zapisal: »Kriza odločanja je situacija, ki izhaja iz spremembe zunanjega ali notranjega okolja določene kolektivitete in jo označujejo tri nujne in zadostne zaznave dela odgovornih odločevalcev: ogroženost temeljnih vrednot, nujnost (v smislu časovnega pritiska, množični mediji) in negotovost.«

Iz naštetih definicij krize je razvidno, da je Stern podal najbolj sintetično opredelitev. S to definicijo poskuša zajeti vse oblike kriz in se ne omejuje samo na eno izmed njih. Definicija temelji na vse večji dojemljivosti sodobnih družb za krize in vse večjo nevarnost, ki jo te predstavljajo za sodobne družbe (Grošelj 2004, 21).

Pri svojem raziskovanju bom zaščito KI obravnavala v povezavi z manjšimi krizami, kot je nekajurna izguba električnega toka, pa tudi druge primere vse do sodobnih oblik krize. Boin in Lagadec (2000, 186) menita, da so ključne značilnosti sodobnih kriz naslednje:

- imajo velik vpliv na velik delež prebivalstva posamezne države,
- prinašajo visoke ekonomske stroške, ki presegajo običajne zavarovalniške zmogljivosti,
- povzročijo učinek »snežne kepe«,
- sistemi kriznega upravljanja in vodenja/odločanja[7] sprejemajo napačne in nepotrebne ukrepe,
- povzročajo izjemno visoko stopnjo negotovosti,
- trajajo daljše obdobje, pri čemer se viri ogrožanja spreminjajo,
- pritegnejo veliko število akterjev na kraju dogajanja,
- prinašajo raznovrstna tveganja in

[7] Na krizo se tesno navezuje fenomen kriznega upravljanja in vodenja, pri čemer slednje lahko opredelimo kot oblikovanje postopkov, dogovorov in odločitev, ki vplivajo na potek krize, obsega pa organizacijo, priprave, ukrepe in razporeditev virov za njeno obvladovanje. Krizno upravljanje in vodenje se običajno odvija v organizacijskem kaosu, pod pritiskom množičnih občil, v stresnih razmerah in ob pomanjkanju natančnih informacij, če naštejemo le nekatere ključne značilnosti. Spremembe vrste in zasnove sodobnih kriz krizno upravljanje in vodenje še otežujejo, saj so sodobne krize izjemno zapletene, imajo mednarodne posledice, se širijo z enega na druga družbena področja, povezujejo z drugimi družbenimi problemi in so praviloma dolgotrajne (Malešič 2004, 14).

- razkrijejo probleme komuniciranja, in sicer med odgovornimi akterji in množičnimi občili, z javnostjo, z žrtvami in celo z javnostjo, ki je časovno in prostorsko precej oddaljena od kraja dogajanja.

Zaščito KI lahko prizadene kriza, ki ima naslednje pomembnejše značilnosti:

1. Ogroža vitalne družbene razsežnosti (od koder izhaja kritična infrastruktura), kjer v prvi vrsti mislimo na socialo, politiko, informacijske sisteme, ekonomijo ter okolje.
2. Lahko je kratkotrajna, traja nekaj sekund, ali dolgotrajna, traja nekaj let.
3. Zahteva krizno odločanje in sodelovanje akterjev zaščite KI, tako na nacionalni kot mednarodni ravni.
4. Stopnje intenzitete so različne; obsega bodisi uničenje komunikacijskega sistema določenega dela države ali pa uničenje informacijskega sistema celotnega kontinenta.
5. Posledice krize so prav tako različne, odvisno od uspešnosti in razvitosti sistema zaščite KI.

Poleg vidnejših značilnosti ima kriza, ki jo bom opredelila kot **krizo zaščite KI nacionalne in mednarodne ravni**, tudi ostale psihološke in značajske značilnosti. Pomembno je, da to krizo razumem kot situacijsko stanje.

2 ZAŠČITA KRITIČNE INFRASTRUKTURE V ZDA

> *Napadi 11. septembra 2001 so demonstrirali širino naše ranljivosti ob terorističnih grožnjah. Posledično smo kot narod pokazali trdno rešitev in zaščito naše kritične infrastrukture ter pomembnih dobrin pred nadaljnjim izkoriščevanjem teroristov. V ta namen so vlada na vseh ravneh, zasebni sektorji in državljani preko celotne države začeli pomembne korake k razvoju partnerstva in zaobljube akciji (George Bush, 2003).*

Za ameriško javnost je bil teroristični napad 11. septembra 2001 največji kazalec, kako težko je zagotoviti varnost neskončnemu številu žrtev z omejenimi viri zaščite. Po dogodku se je pričel proces nastajanja številnih dokumentov, predvsem nacionalnih strategij, ki naj bi bolje opredelile ter povezale posamezne elemente zaščite KI in pomembnih dobrin (CIP 2007, 9). Svojo pozornost so ZDA popolnoma usmerile v zaščito pred katerokoli obliko terorističnih napadov, kot pravi George Bush (2002, 3):

> *Oblikovali smo globalno koalicijo, ki je premagala teroriste*[8] *in njihove nasprotnike v Afganistanu in ostalih delih sveta. Več kot 60.000 ameriških vojakov je bilo deportiranih okoli sveta v vojni z terorizmom. Utrdili smo našo letalsko varnost in meje na zemlji. Nakopičili smo si medicinska sredstva za obrambo proti bioterorizmu in izboljšali naše sposobnosti bojevanja proti orožjem množičnega uničevanja. Izboljšali smo način komuniciranja med obveščevalnimi agencijami in naredili smo pomembne korake za zaščito kritične infrastrukture. Vlada ZDA nima nobene druge naloge kot zaščititi državo pred prihodnjimi terorističnimi napadi.*

Zaščita ameriške KI in pomembnih dobrin je velik izziv. Njihov sistem je odprt in tehnološko zapleten, družba pa predstavlja skoraj neskončne možnosti potencialnih tarč.

[8] Strokovnjaki si niso enotni, kaj je terorizem, kakšna je njegova definicija in kako ga ločevati od uporništva ali kriminalnega nasilja. Dr. Rudi Rizman je oblikoval dve definiciji terorizma. Po prvi naj bi bil terorizem *»načrtovana uporaba ali grožnja z uporabo nasilja z namenom povzročiti strah in na ta način pritiskati ali groziti vladam in družbam«*. V drugi definiciji razmišlja, da naj bi bil terorizem *»uporaba nasilja ali grožnje z namenom doseči določene politične, verske ali ideološke cilje oziroma uporabo nasilnih sredstev proti posameznikom, skupinam ali lastnini«* (Rizman v Škrjanc 2004, 5). Prezelj (2006, 20) opredeljuje terorizem kot »načrtovanje, organiziranje, izvajanje in podpiranje nasilnih dejavnosti večinoma proti nedolžnim civilnim ciljem (predvsem v smeri vplivanja na vlade, da sprejmejo ali ne sprejmejo določenih ukrepov)« (Sagadin 2007, 14–15).

Prav tako se ameriška KI, kot je značilno v ekonomskem svetu, zelo hitro spreminja. Vse tarče je nemogoče zaščititi kjerkoli in ob kateremkoli času. Na drugi strani pa so zmožni pomagati pri zastraševanju oz. odklanjanju napadov ali zmanjševanju vplivov z oblikovanjem strateških izboljšanj in zaščite ter varnosti. Vsi elementi ameriške družbe predstavljajo odločilen vložek v zmanjšanje njihove ranljivosti, kjer ima prav vsak pomembno vlogo v zaščiti pred terorizmom. Zaščita ameriške KI in pomembnih dobrin zahteva sodelovanje na vseh ravneh, od vlade do zasebne industrije in institucij, ter ne nazadnje tudi z državljani ZDA. Federalna vlada ima tako pomembno nalogo vzdrževanja okolja sodelovanja in spodbujanja, da vse naštete entitete med seboj sodelujejo pri zagotavljanju varnosti ZDA (Nacionalna strategija 2002, 29–39).

Sodeč s tega vidika lahko rečemo, da so ZDA začetnik razvoja »zaščite KI«.[9] Termin »zaščita KI« se predvsem nanaša na zaščito ljudi, fizičnih dobrin, komunikacij/cyber-sistemov, ki so nujno potrebni za državno varnost, ekonomsko stabilnost in varnost družbe. Metode sistema zaščite KI služijo kot vir zastraševanja ali zmanjševanja vplivov terorističnih napadov proti KI, od človeka povzročenih dejanj (e. g. teroristi, kriminal, hekerstvo itd.), od narave (e. g. orkani, tornadi, potresi, poplave itd.) in tudi od ostalih incidentov, kamor prištevamo nuklearne, radiološke, biološke ali kemične substance (i. e. »vseobsegajoči« pojavi). Na splošno bi lahko rekli, da zaščita KI predstavlja zaščito tistih dragocenih dobrin, ki omogočajo življenje, svobodo in ne nazadnje tudi prinašajo blaginjo. Vse to je ameriška nacionalna realnost (Dostopno prek: http://www.usfa.dhs.gov/fireservice/subjects/emr-isac/what_is.shtm (22. avgusta 2008)).

Za doseganje nacionalne varnosti je potrebno vzpostaviti relativno uspešno in delujočo zaščito KI. Obstajati mora vsestranska organizacija, ki jasno opredeljuje vloge in odgovornosti. Omogočati mora sodelovanje na vseh vladnih ravneh in tudi na ravneh zasebnega sektorja. Ob kompleksni zbirki izzivov, ki jih s seboj prinaša zaščita KI v ZDA in tudi po svetu, mora biti odgovornost jasno porazdeljena na federalni, državni, lokalni, občinski in zasebni ravni. Poleg tega je pomembno, da je zaščita KI sposobna učinkovito prerazporediti zaščitene vire, glede na grožnjo in potrebe družbe (NIPP 2006, 17).

[9] V literaturi najdemo ime CIP – critical infrastructure protection.

Iz napisanega lahko sklepamo, da je ameriška vlada zelo hitro po terorističnem napadu 11. septembra 2001 začela razvijati in vlagati v zaščito KI na vseh ravneh. Razvila je celosten, analitičen model, katerega razvitost bom prikazala s študijo primera odpravljanja posledic orkana Katrina, s primerjavo ključnih elementov sistema KI z ostalimi izbranimi državami in EU ter ostalimi kazalci, kot je na primer proračunsko vlaganje v razvoj zaščite KI v ZDA in EU.

Da bi v celoti razumeli delovanje zaščite KI v ZDA, moramo najprej predstaviti posamezne segmente, ki jo sestavljajo.

Vse našteto bom raziskala, predstavila in opisala v nadaljnjih podpoglavjih diplomske naloge. Sprva bom predstavila **kritične sektorje**, sledil bo **organizacijski vidik zaščite KI**, **normativna podlaga, pobude in iniciative** ter nazadnje še **finančni vidik zaščite KI**. Podpoglavje se bo vsakokrat začelo z analizo ZDA, sledil bo krajši opis izbranih evropskih držav, primerjalna analiza EU in ZDA določenega vsebinskega dela ter ob koncu še primerjalna analiza ZDA z izbranimi evropskimi državami določenega vsebinskega dela.

2.1 KRITIČNI SEKTORJI

Kritične sektorje opredeljujemo kot posamezne panoge oziroma področja, ki sestavljajo kritično infrastrukturo. Kritični sektorji torej oblikujejo celotno kritično infrastrukturo posamezne države.

2.1.1 Kritična infrastruktura v ZDA

Sistem KI v Ameriki sestavljajo številni povezani kritični sektorji. Leta 2007 je DHS[10] opredelil 17 najpomembnejših kritičnih sektorjev, to so: informacijska tehnologija, telekomunikacije, kemične snovi, transportni sistem (vključuje množične tranzicije, letalstvo, mornarico, zemeljsko površje, železnice in cevovodni sistem), prva pomoč,

[10] DHS – Department of Homeland Security (Ministrstvo za domovinsko varnost)

pošta in ekspedicija, kmetijstvo, hrana (meso, perutnina, jajčni proizvodi), javno zdravstvo, oskrba in hrana (drugo od mesa, perutnine in jajčnih proizvodov), pitna voda in sistem odpadne vode, energija, nuklearni reaktorji, materiali in odpadki, bančništvo in finance, državni spomeniki in ikone, obramba industrijske osnove, komercialne ustanove, vladne ustanove, zajezitvena voda – jezovi (Critical infrastructure and Key assets. Dostopno prek: http://www.dhs.gov/xprevprot/programs/gc_1189168948944.shtm (23. avgusta 2008), (glej Tabelo 2.1).

Omenjeni seznam kritičnih sektorjev se je skozi ameriško zgodovino zelo spreminjal (Slika 2.2). Že od leta 1983 so v ZDA opredelili šest kritičnih sektorjev, in sicer transport, zaloge voda, izobraževanje, javno zdravstvo, zapore in industrijske kapacitete. Do leta 2003 se je seznam kritičnih sektorjev močno razširil in do danes zaobsegel 17 ključnih kritičnih sektorjev. Pomembno je poudariti, kot je zapisano v Nacionalni strategiji (2002, 39), da je »transport vitalnega pomena, vendar ni vsak most kritičen za državo v celoti«. Torej, opredeljeni so resnično tisti sektorji, ki v celoti predstavljajo kritičnost države v ZDA.

Slika 2.1: Kritična infrastruktura skozi ameriško zgodovino

Table 3. Critical Infrastructure and Key Assets Over Time

Infrastructure	U.S. Government Reports and Executive Orders							
	CBO (1983)	NCPWI (1988)	E.O. 13010 (1996)	PDD-63 (1998)	E.O. 13228 (2001)	NSHS (2002)	NSPP (2003)	HSPD-7 (2003)
Transportation	X	X	X	X	X	X	X	X
Water supply /waste water treatment	X	X	X	X	X	X	X	X
Education	X							
Public health	X			X		X	X	X
Prisons	X							
Industrial capacity	X							
Waste services		X						
Telecommunications			X	X	X	X	X	X
Energy			X	X	X	X	X	X
Banking and finance			X	X		X	X	X
Emergency services			X	X		X	X	X
Government continuity			X	X		X	X	
Information systems				X	X	X	X	X
Nuclear facilities					X			
Special events					X			
Agriculture/food supply					X	X	X	X
Defense industrial base						X	X	X
Chemical industry						X	X	X
Postal / shipping services						X	X	X
Monuments and icons							X	X
Key industry / tech. sites							X	
Large gathering sites							X	

Source: CRS compilation. See earlier footnotes. Note that the cross-referencing marks, "X", in Table 3 are meant to be illustrative, and generally correspond to the specific mention

VIR: Moteff et al. (2004, 18).

Zaradi obširnega seznama sektorjev so se v ZDA na podlagi normativnega akta HSPD-7 (Homeland Security Presidential Directive 7)[11] odločili, da bodo podelili odgovornosti agencijam (Tabela 2.1). Oblikoval se je tako imenovani Sektorsko specifični načrt agencij.[12] SSP podpira nacionalni infrastrukturni načrt zaščite[13] tako, da vzpostavlja koordinacijski pristop k uresničevanju nacionalnih prioritet, ciljev, ter zahtev po zaščiti KI in pomembnih dobrin. SSP prispeva sredstva, ki omogočajo celostno implementacijo nacionalnega načrta zaščite infrastrukture skozi vse sektorje KI, kot tudi nacionalni okvir za posamezni sektor, ki ima svoje edinstvene lastnosti in krizne razsežnosti (Sector-Specific Plans. Dostopno prek: http://www.dhs.gov/xprevprot/programs/gc_117986619760.shtm#content (24. avgust 2008)).

Tabela 2.1: Kritični sektorji in odgovornost agencij posameznih sektorjev v ZDA

Kritični sektor	Federalna agencija kritičnih
Kmetijstvo, hrana (meso, perutnina, jajčni proizvodi)	**Ministrstvo za kmetijstvo, hrano in administracijo**
Bančništvo in finance	**Ministrstvo za finance**
Kemične snovi	**Ministrstvo za domovinsko varnost**
Komercialne ustanove	**Ministrstvo za domovinsko varnost**
Telekomunikacije	**Ministrstvo za domovinsko varnost**
Zajezitve voda – jezovi	**Ministrstvo za domovinsko varnost**
Obramba industrijske osnove	**Ministrstvo za obrambo**
Nujna pomoč	**Ministrstvo za domovinsko varnost**
Energija	**Ministrstvo za energijo**
Vladne ustanove	**Ministrstvo za domovinsko varnost**
Informacijska tehnologija	**Ministrstvo za domovinsko varnost**
Državni spomeniki in ikone (svete podobe)	**Ministrstvo za notranje zadeve**
Nuklearni reaktorji, materiali in odpadki	**Ministrstvo za domovinsko varnost**
Pošta in ekspedicija	**Ministrstvo za domovinsko varnost**
Javno zdravstvo, oskrba in hrana (drugo od mesa, perutnine in jajčnih proizvodov)	**Ministrstvo za zdravstvo in pomoč**
Transportni sistem	**Ministrstvo za domovinsko varnost**
Voda	**Agencija za okoljsko zaščito**

VIR: HSPD-7 (2003).

Večina kritičnih sektorjev je v rokah DHS, znotraj katerega so posamezni oddelki, ki skrbijo za določena področja KI. Zanimivo je, da se na seznamu pojavlja le ena agencija, ki skrbi za kritični sektor voda. Ostali sektorji so porazdeljeni med ministrstvi

[11] Podrobneje opredeljen v podpoglavju Normativne podlage in pobude.
[12] Krajše SSP.
[13] Podrobneje opisan v podpoglavju Normativne podlage in pobude.

in znotraj teh med posameznimi uradi, oddelki in podobno, kar bomo videli v podpoglavju Organizacijski vidik.

2.1.2 Kritična infrastruktura v evropskih državah

V nadaljevanju bom naštela kritične sektorje petih evropskih držav, in sicer Francije, Nemčije, Velike Britanije, Švice in Nizozemske.

a) Francija

Francija ima skupaj 9 kritičnih sektorjev, to so: bančništvo in finance, kemična in biotehnološka industrija, energija in elektrika, nuklearne postaje, javno zdravstvo, javna varnost in red, telekomunikacije, transport in zaloge vode.

Tabela 2.2: Kritični sektorji v Franciji

Kritični sektorji	Število sektorjev
Bančništvo in finance	
Kemična in biotehnološka industrija	
Energija in elektrika	
Nuklearne postaje	9
Javno zdravstvo	
Javna varnost in red	
Telekomunikacije	
Transportni sistem	
Zaloga vode	

VIR: Abelle-Wigert in Dunn (2006, 97).

Iz Tabele 2.2 je razvidno, da Francija nima tako obširnega seznama opredeljenih kritičnih sektorjev kot ZDA. Abelle-Wigert in Dunn (2006) sta zapisali, da je Francija usmerjena v vzdrževanje kritičnih sektorjev, ki poudarjajo zaščito primarnih socialnih in ekonomskih procesov. Iz tega vzroka pri Franciji ne zasledimo specifičnih sektorjev, kot so državni spomeniki in ikone (svete podobe) ter vedno bolj poudarjena vloga informacijske tehnologije. Poleg tega Francija v nasprotju z ZDA ne omenja kritičnega sektorja pošte in ekspedicije, ker ju najverjetneje šteje v skupino sekundarnih

ekonomskih procesov. Prav tako nikjer ne zasledimo kritičnega sektorja, ki bi vključeval kmetijske izdelke, čeprav po mojem mnenju sodi med primarne procese obstoja vseh družb, tudi družbe v Franciji. Menim, da Francija v primerjavi z ZDA kljub opredelitvi, da upošteva le primarne socialne in ekonomske procese, ne zajema vseh kritičnih sektorjev, pomembnih za normalno delovanje družbe. Vsekakor na prvo mesto spadajo kmetijski izdelki, hrana, česar Francija ne omenja in ne opredeljuje kot poseben kritični sektor. Zanimivo je, da Francija kljub temu obravnava poseben kritični sektor javnega reda in miru, česar pri ZDA nisem zasledila. ZDA veliko bolj poudarjajo pomen vladnih ustanov in zaščite komercialnih delov družbe kot pa javnega reda in miru. Na splošno ZDA v primerjavi z Francijo opredeljujejo več kritičnih sektorjev, ki so pomembni za obstoj družbe. Imajo tudi daljšo zgodovino opredeljevanja pomembnih kritičnih sektorjev (glej Sliko 2.1), česar pri Franciji nisem zasledila.

b) Nemčija

Nemčija ima 8 ključnih kritičnih sektorjev in 32 podsektorjev. Med ključne sektorje uvršča: transport in promet, energijo, pomembne materiale, telekomunikacije in informacijsko tehnologijo, finance in zavarovanje, različne službe, javno administracijo in pravni sistem ter nazadnje še kritični sektor ostalo (mediji itd.).

Tabela 2.3: Kritični sektorji v Nemčiji

Kritični sektorji	Kritični sektorji	Število sektorjev
Transport in promet (letalstvo, morsko, železnice, lokalno, notranji rečni promet, cestni sistem, poštni sistem)	**Finance in zavarovanje (bančništvo, finance, finančna služba, delničarstvo)**	**8 sektorjev** **32 podsektorjev**
Energija (elektrika, mineralno olje, plin, nuklearne postaje)	**Usluge (prva pomoč, zdravstvena oskrba, civilna zaščita, zaloge hrane in vode, menedžment odpadkov)**	
Pomembni materiali (kemične in biološke substance, materiali transporta, obrambna industrija)	**Javna administracija in legalni sistem(vlada, vladne agencije, javna administracija, policija, navade in oborožene sile države)**	
Telekomunikacije in informacijska tehnologija	**Ostalo (mediji, večje raziskave, posebnosti oziroma simbolika, kulturna dediščina)**	

VIR: Office for Security in the Information Technology. Dostopno prek: http://www.bsi.bund.de/fachthem/kritis/index.htm (26. avgust 2008).

Iz zgornje tabele (Tabela 2.3) razberemo, da ima Nemčija že v listi potrjenih kritičnih sektorjev tudi 32 podsektorjev, česar ZDA nimajo. Dejstvo je, da ZDA znotraj ključnih kritičnih sektorjev opredeljujejo pomembne podsektorje v nacionalnem načrtu in ostalih dokumentih vsakega kritičnega sektorja posebej. Kljub temu lahko vidimo, da ima Nemčija zelo podoben seznam kritičnih sektorjev kot ZDA. Nemčija opredeljuje vse kritične sektorje, ki so primarno pomembni za njeno socialo in ekonomijo. Torej – javno zdravstvo oziroma usluge, hrano, vodo, transport, energijo, telekomunikacije, industrijo in tudi vladni ter legalni sistem. Opazimo prav tako, da informacijsko tehnologijo skupaj z telekomunikacijami uvršča v poseben kritični sektor. Nemčija in ZDA menijo, da postaja informacijska tehnologija vse bolj pomembna v moderni družbi, in na podlagi tega jo obravnavajo kot poseben kritični sektor. Nemčija ima tako kot ZDA specifične kritične sektorje in državni ter simbolni dediščini dodaja še medije in raziskave. Zelo zanimiv podatek, kajti ZDA posebej ne omenjajo raziskav ali medijev, ki bi bili tako pomembni, da bi jih uvrstili v okvir specifičnih sektorjev kot državne simbole in ikone. Po mojem mnenju imajo ZDA in Nemčija zelo podoben seznam opredeljenih kritičnih sektorjev. Če vemo, da so ZDA prve (že leta 1983) pričele oblikovati kritične sektorje, je najverjetneje Nemčija tista, ki se zgleduje po seznamu opredeljenih kritičnih sektorjev v ZDA.

c) Nizozemska

Nizozemska opredeljuje 12 ključnih sektorjev in 33 podsektorjev. Zaradi primerjave ključnih sektorjev bom naštela le te, ki so naslednji: zaloga pitne vode, energija, finance, hrana, zdravje, zakonski red, javni red in varnost, zadržanje in vodenje nadgladinskih voda, telekomunikacije, javna administracija, transport ter kemična in nuklearna industrija.

V spodnji tabeli (Tabela 2.4) vidimo, da Nizozemska tako kot ZDA opredeljuje kritične sektorje, kot so hrana, energija, finance in podobno. Torej opredeljuje primarne kritične sektorje, ki so pomembni za obstoj družbe na Nizozemskem. Na seznamu kritičnih sektorjev Nizozemska nima opredeljenih specifičnih kritičnih sektorjev in tudi informacijske tehnologije ne opredeljuje posebej tako kot ZDA. Nizozemska je kot ostale severne države znana po zelo naprednem razvoju informacijske tehnologije. Zato menim, da informacijske tehnologije ne obravnava kot samostojnega kritičnega

sektorja, ker informacijska tehnologija povezuje vse kritične sektorje med seboj. Torej ima informacijska tehnologija najpomembnejše mesto, ker so od njenega delovanja odvisni vsi ostali kritični sektorji. Poleg tega je zelo zanimivo dejstvo, da Nizozemska razcepi politično in javno okolje na več kritičnih sektorjev, in sicer na javno administracijo, javni red in varnost ter zakonski red. Tega ZDA ne uvrščajo med kritične sektorje oziroma omenjajo kritični sektor vladnih ustanov. Iz tega lahko sklepamo, da Nizozemska loči izvršno in sodno vejo oblasti, kjer vsaka predstavlja svoj kritični sektor. Predvsem je izvršna veja posebnost, česar ne opredeljuje niti Nemčija niti ZDA. Posebnost je tudi kritični sektor vodenja nadgladinskih voda, čemur najverjetneje botruje hidrografski položaj Nizozemske; ima namreč zelo razvit transportni rečni in morski sistem. Podobno bi lahko rekli za Nemčijo, a ta kljub temu ne omenja kritičnega sektorja vodenja nadgladinskih voda kot Nizozemska, zato omenjeni kritični sektor uvrščam med specifične kritične sektorje.

Tabela 2.4: Kritični sektorji na Nizozemskem

Kritični sektorji	Kritični sektorji	Število sektorjev
Zaloga pitne vode	**Upravljanje površinskih voda (vodenje kvalitetne vode, zadržanje in vodenje količine voda)**	**12 sektorjev** **33 podsektorjev**
Energija (elektrika, naravni plin in nafta)	**Telekomunikacije (internet, mobilni operaterji, radio, navigacija, satelitsko, širše, poštna in kurirska služba)**	
Finance (finančna služba, infrastruktura, javna in zasebna)	**Javna administracija (diplomatska komunikacija, informacijski nadzor vlade, oborožene sile, obramba, odločanje javne administracije)**	
Hrana (zaloga hrane in varnost hrane)	**Transport (glavna pristanišča, glavne ceste, vodovodi, železnica)**	
Zdravje (nujna zdravstvena oskrba, zdravila, nuklearna medicina)	**Kemična in nuklearna industrija (transport, skladiščenje, proizvodnja)**	
Zakonski red (administracija za uvajanje zakonov)	**Javni red in varnost (vzdrževanje reda in varnosti)**	

VIR: Ministry of interior and kingdom relations (2003, 7).

d) Švica

Švica je letos natančno opredelila 10 kritičnih sektorjev in 31 podsektorjev, ki jih morajo v prihodnje bolje definirati, zato jih nisem vpisala v spodnjo tabelo (Tabela 2.5). Njeni ključni sektorji so: javna administracija, splošna varnost, reševanje in prva pomoč, informacijska in telekomunikacijska tehnologija, energija, finančna služba, kemijska industrija, odlaganje odpadkov, splošno zdravstvo, transport ter hrana in voda.

Tabela 2.5: Kritični sektorji v Švici

Kritični sektorji	Kritični sektorji	Število sektorjev
Javna administracija	**Finančna služba**	**10 sektorjev** **31 podsektorjev**
Splošna varnost, reševanje in prva pomoč	**Kemična industrija**	
Informacijska in telekomunikacijska tehnologija	**Odlaganje odpadkov**	
Energija	**Splošno zdravstvo**	
Voda in hrana	**Transport**	

VIR: The Swiss Programme on Critical Infrastructure Protection (2008, 4).

Iz Tabele 2.5 lahko razberemo, da je Švica prva od sedanjih držav, ki hrano in vodo združuje v skupni kritični sektor. Enako kot Nemčija in ZDA tudi Švica opredeljuje informacijsko tehnologijo kot kritični sektor. V seznamu kritičnih sektorjev Švica nikjer ne opredeljuje javne administracije, ustanov, reda in miru ali zakonskega reda. Torej izključuje politično-državno okolje iz seznama kritičnih sektorjev za razliko od ZDA, Nemčije in Nizozemske. Zelo zanimivo je, da Švica posebej opredeljuje kritični sektor odlaganja odpadkov, kar ZDA uvrščajo v kritični sektor nuklearnih reaktorjev in materialov. Dejstvo je, da imajo ZDA bolj razčlenjen seznam kritičnih sektorjev, saj je Švica svoj nedokončani seznam uradno izdala šele letos. Verjetno lahko v prihodnje s strani Švice pričakujemo natančneje opredeljen seznam kritičnih sektorjev in podsektorjev.

e) Velika Britanija

Velika Britanija enako kot Švica opredeljuje 10 ključnih kritičnih sektorjev in 39 podsektorjev. Ključni kritični sektorji VB so naslednji: komunikacije, prva pomoč, energija, finance, hrana, vlada in javne službe, varnost javnosti, zdravje, transport in voda.

Tabela 2.6: Kritični sektorji v VB

Kritični sektorji	Kritični sektorji	Število sektorjev
Komunikacije (podatki, glasovni podatki, e-pošta, javne informacije, brezžična komunikacija)	Vlada in javne službe (državno, regionalno, lokalno, parlament, pravo, zakoni, državna varnost)	10 sektorjev 39 podsektorjev
Prva pomoč (ambulanta, požar in reševanje, obalna straža, policija)	Varnost javnosti (kemično, biološko, radiološko in nuklearno (CBRN), terorizem, javni in množični dogodki)	
Energija (elektrika, naravni plin, petrolej)	Zdravje (oskrba, zdravstvo)	
Finance (menedžment imetja, finančne ustanove, investiranje, tržišče, lokalno bančništvo)	Transport (zračni, morski, železniški in cestni)	
Hrana (proizvod, uvoz, procesiranje, razdeljevanje, maloprodaja)	Voda (vodovod, odtok)	

VIR: Home Office Security (2003). Dostopno prek: http://security.homeoffice.gov.uk/ (27. avgust 2008).

V zgornji tabeli (Tabela 2.6) vidimo, da VB v primerjavi z ZDA podobno opredeljuje pomembne kritične sektorje, kot so voda, hrana, energija, finance, zdravstvo, transport in podobno. Zanimivo je, da VB informacijsko tehnologijo uvršča v kritični sektor komunikacij in ne v poseben kritični sektor tako kot ZDA. VB tudi nima specifičnih kritičnih sektorjev, kot so državni spomeniki, kulturna dediščina, na primer v seznamih Nemčije in ZDA. Kot Francija in Nizozemska ima VB prav tako posebej opredeljen kritični sektor varovanja javnosti. Znotraj tega izpostavlja pomen terorizma, v smislu javnih in množičnih dogodkov. ZDA posebej ne obravnavajo kritičnega sektorja, ki bi zajemal vsebino varovanja javnosti oziroma ohranjanja reda in miru. Zanimiv podatek, kajti ZDA nenehno poudarjajo, da je njihov primarni cilj prav zaščita državljanov.

Menim, da ZDA veliko bolj poudarjajo kritičnost tistih delov družbe, ki zagotavljajo ekonomski razvoj in stabilnost družbe, slednje v smislu zdravja in ne nadzorovanja kot v Franciji, na Nizozemskem in v Veliki Britaniji.

V nadaljevanju bom opredelila kritične sektorje EU in jih primerjala s kritičnimi sektorji v ZDA.

2.1.3 Kritični sektorji v EU

Z namenom, da bi zaščitili KI v Evropski uniji, je Evropski svet leta 2004 podal predlog za razvoj Evropskega programa za zaščito KI.[14] EPCIP poudarja, da imajo različni sektorji različne izkušnje, strokovne podlage in zahteve glede zaščite KI, in se bo razvijal na osnovi identifikacije posameznih kritičnih sektorjev. Tako bo implementiral dogovorjen seznam sistema zaščite kritičnih sektorjev. S tega vidika ima EU 11 ključnih sektorjev (EPCIP 2006, 1–9). Že leta 2005 so v EU z izdajo Zelenega lista na CIP[15] razčlenili seznam ključnih sektorjev v podsektorje, kot vidimo v spodnji tabeli (Tabela 2.7). Unija torej predlaga naslednje ključne kritične sektorje: energijo, informacijsko in komunikacijsko tehnologijo, vodo, hrano, zdravje, finance, javnost in legalni red ter varnost, civilno administracijo, transport, kemično in nuklearno industrijo ter vesolje in raziskave.

Iz spodnje tabele (Tabela 2.7) razberemo, da je bil v EU predlagan seznam najpomembnejših kritičnih sektorjev, kot so voda, hrana, zdravje, finance, energija in ostalo. Unija najbolj razčlenjuje kritični sektor energije ter informacijske in telekomunikacijske komunikacije. Torej opredeljuje informacijsko tehnologijo kot samostojen kritični sektor, k temu pa dodaja tudi specifičen kritični sektor vesolja in raziskav. Slednjega ne omenja nobena država razen Nemčije, ki navaja večje raziskave. Skratka, vesolje se tu prvič omenja kot kritični sektor.

[14] V literaturi imenovan s kratico EPCIP – več v podpoglavju normativnih aktov.
[15] »Zeleni list« služi kot možnost reakcije Komisije na pobudo Evropskega sveta za ustanovitev EPCIP (Green paper 2005, 2–3).

Tabela 2.7: Kritični sektorji v EU

Kritični sektor	Kritični sektor	Število sektorjev
Energija (nafta, plini, rafinerija, zaloga, postopki, plinovodi, električni generatorji, transmisija elektrike, proizvodnja nafte in plina, distribucija elektrike, nafte in plina)	Finance (plačilni sistem, zasebni plačilni sistem, vladne finančne storitve)	11 sektorjev 38 podsektorjev
Informacijske in komunikacijske tehnologije (informacijski sistem in zaščita omrežja, instrumentacija avtomatizma in kontrole sistema (SCADA itd.), internet, mobilniki, radio, navigacije, satelitsko komuniciranje in oddajanje)	Vesolje in raziskave	
	Red in varnost v družbi (vzdrževanje, administracija)	
Voda (pitna voda, nadzor količine vode, mašenje in kontrola kvalitete vode)	Civilna administracija (vlada, vojska, civilne službe, nujna pomoč, pošta in kurirska služba)	
Hrana (nadzor nad hrano in varnost ter zaščita hrane)	Transport (cesta, železnica, zrak, zemlja, oceani)	
Zdravje (zdravstvo, oskrba, medicina, zdravila, cepiva, laboratoriji, bioagenti, farmacija)	Kemična in nuklearna industrija (zaloge, skladiščenje, proizvodnja)	

VIR: Green paper on CIP (2005, 24).

Morda bi se morali vprašati, ali vesolje spada med kritične družbene dele oziroma med tiste dele, ki so nujni za obstoj družbe. Po mojem mnenju je vesolje tisti del družbe, ki ni tako pomemben za njen stabilen obstoj, omogoča pa njen napredek. Verjetno ga prav iz tega razloga kot kritični sektor ne omenja nobena druga država, niti ZDA. Poleg tega EU predlaga, tako kot Nizozemska in VB, kritične sektorje javnega reda in miru ter civilne administracije. Več kritičnih sektorjev torej zajema socialni del družbe, kar ZDA opredelijo z enim kritičnim sektorjem vladnih ustanov.

2.1.4 Primerjalna analiza kritične infrastrukture

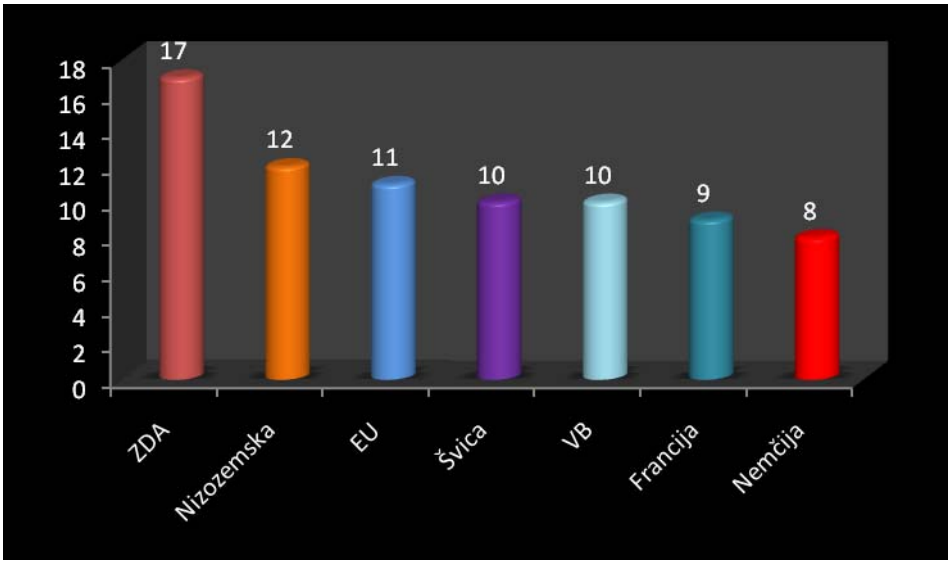
Kot vidimo, se nenehno pojavljajo razlike in podobnosti med seznami kritičnih sektorjev ZDA, izbranih evropskih držav ter EU. Prav zaradi tega sem obstoječim primerjavam med posameznimi državami, EU in ZDA na podlagi seznama kritičnih sektorjev in podsektorjev dodala še primerjalno analizo naslednjih spremenljivk:

a) Število kritičnih sektorjev

Tu me bo zanimalo število kritičnih sektorjev posamezne države (EU) v primerjavi z ZDA. S tem bom ugotovila, ali imajo posamezne države glede na ZDA enake/drugačne kritične sektorje.

Spodnji graf (Graf 2.1) kaže, da imajo največ kritičnih sektorjev ZDA (17). Sledi jim Nizozemska (12), EU (11), Švica (10), Velika Britanija (10), Francija (9) in nazadnje Nemčija (8). Sodeč po pridobljenih podatkih bi lahko rekli, da imajo ZDA največ opredeljenih kritičnih sektorjev glede na ostale države in EU. To pomeni, da ZDA opredeljujejo več področij, ki so ključnega pomena za obstoj in normalno delovanje družbe. Kljub temu poleg ključnih kritičnih sektorjev nekatere države opredeljujejo svoje podsektorje, kar pomeni, da kritične sektorje bolj razčlenjujejo v primerjavi z ZDA, kar bomo videli v nadaljevanju.

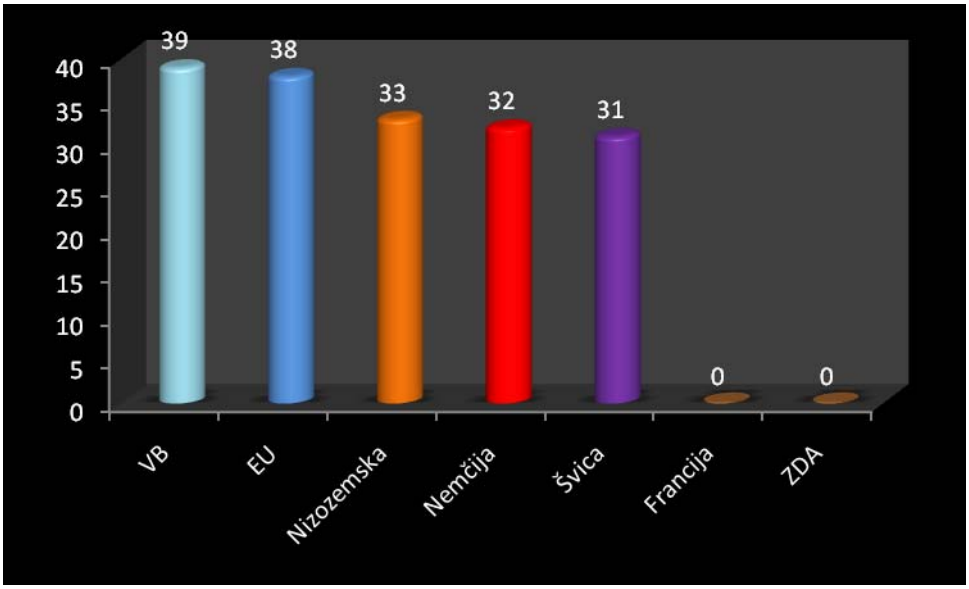
Graf 2.1: Primerjava števila kritičnih sektorjev izbranih evropskih držav, EU in ZDA



b) Število kritičnih podsektorjev

S to spremenljivko bom ugotavljala število podsektorjev posamezne države (EU) v primerjavi z ZDA. Tako bom primerjala, ali imajo posamezne države in ZDA enake/različne kritične podsektorje.

Graf 2.2: Primerjava števila kritičnih podsektorjev izbranih evropskih držav, EU in ZDA



Iz zgornjega grafa (Graf 2.2) je razvidno, da ima največ kritičnih podsektorjev VB (39), sledi EU (38), Nizozemska (33), Nemčija (32), Švica (31) in nato še Francija in ZDA (vse 0). Prve štiri države in EU imajo številčno zelo podobne sezname kritičnih sektorjev in podsektorjev, kar lahko navezujemo tudi na možno mednarodno sodelovanje in zgledovanje na področju kritične infrastrukture. Ne glede na to, kaj je vzrok, je dejstvo, da se vse prve štiri države in EU nahajajo v istem evropskem prostoru. Zanimivo je, da ZDA ne omenjajo in uradno ne potrjujejo seznama kritičnih podsektorjev tako kot kritične sektorje. Res je, da v različni literaturi lahko zasledimo, kako preko podrobnih in natančnih dokumentacij razlagajo in razčlenjujejo posamezen kritični sektor. Če pa upoštevamo uradno potrjene sezname, imajo VB, Nizozemska, Nemčija in Švica natančneje opredeljene in razčlenjene sezname kritičnih sektorjev v primerjavi z ZDA in Francijo (EU ne sodi zraven, ker nima uradno potrjenega seznama kritičnih sektorjev, seznam temelji na predlogu). Kljub temu menim, da natančneje opredeljen in razčlenjen seznam kritičnih sektorjev nosi potencial za boljše oblikovanje zaščite kritične infrastrukture. Večje število ključnih kritičnih sektorjev pomeni, da posamezna država obravnava več področij družbenega obstoja in normalnega delovanja, na primer ZDA. Če država razčleni ključne sektorje v podsektorje, še ne pomeni, da opredeljuje več pomembnih področij družbe, temveč natančneje opredeli posamezen kritični sektor. Vsekakor je najboljša kombinacija takšna, da kritični sektorji zajemajo

kar največje število področij družbenega obstoja in normalnega delovanja posameznih držav, poleg tega pa so natančno opredeljeni s pomočjo podsektorjev.

c) Obstoj posebnega kritičnega sektorja

Ugotavljala bom, ali imajo izbrane države (EU) posebej opredeljen kritični sektor informacijske tehnologije, ki v današnjem času zaseda najpomembnejše mesto na skoraj vseh področjih družbe, v ekonomiji, politiki itd.

Iz spodnje tabele (Tabela 2.8) je razvidno, da le ZDA opredeljujejo informacijsko tehnologijo kot samostojen kritični sektor. Nemčija, Švica in EU jo v kritični sektor uvrščajo skupaj z telekomunikacijami, VB pa informacijsko tehnologijo umešča v kritični sektor komunikacije. Francija in Nizozemska je kot posebnega kritičnega sektorja sploh ne omenjata.

Tabela 2.8: Ali imajo izbrane države EU in ZDA poseben kritični sektor informacijske tehnologije?

Država (subjekt)	Kritični sektor informacijske tehnologije
ZDA	da
Francija	ne
Nemčija	da + telekomunikacije
Nizozemska	ne
Švica	da + telekomunikacije
VB	ne/da
EU	da + telekomunikacije

Po pregledovanju literature sem prišla do zaključka, da obe državi – Francija, sploh pa Nizozemska – najbolj vrednotita informacijsko tehnologijo. Prav zaradi tega informacijske tehnologije ne uvrščata v poseben kritični sektor, ker povezuje vse kritične sektorje med seboj. Torej je zaščita kritične infrastrukture odvisna od relativno stabilnega obstoja informacijske tehnologije. Popolnoma drugače je z ZDA, ki uvrščajo informacijsko tehnologijo v poseben kritični sektor, čeprav jo enako kot Nizozemska in Francija obravnavajo kot tisti del družbe, ki povezuje vse dele družbe v neko celoto.

Videti je, da imajo države in EU različne pristope pri obravnavanju informacijske tehnologije. Dejstvo je, da se ta pojavlja v vseh kritičnih sektorjih, v manjši ali večji meri. Prav zaradi tega mislim, da se je smiselno vprašati, ali informacijska tehnologija spada med kritične sektorje, ali je tako pomembna, da je pravzaprav ne moremo obravnavati kot enega od kritičnih sektorjev, saj povezuje vse ostale.

Podobno je s specifičnimi sektorji, ki si jih bomo ogledali v nadaljevanju.

d) Obstoj specifičnih kritičnih sektorjev

Ugotavljala bom, ali imajo izbrane države (EU) v primerjavi z ZDA specifične kritične sektorje, kot so raziskave, vesolje, mediji, kulturna dediščina in podobno. Vsi specifični sektorji nekako tudi prikazujejo, kaj je za določeno državo kritično. Potemtakem država, ki posebej opredeli kritični sektor državnih spomenikov, najverjetneje resneje obravnava zaščito zgodovinske kulture kot tista država, ki tega kritičnega sektorja ne opredeljuje.

Tabela 2.9: Primerjava števila specifičnih kritičnih sektorjev/podsektorjev izbranih držav EU in ZDA

Država (subjekt)	Vrsta specifičnega kritičnega sektorja/podsektorja	Število posebnih kritičnih sektorjev in podsektorjev
ZDA	Državni spomeniki in ikone (svete podobe)	2
Francija	Nima	0
Nemčija	Mediji, večje raziskave, posebnosti oziroma simbolika, kulturna dediščina	4
Nizozemska	Upravljanje površinskih voda	1
Švica	Odlaganje odpadkov	1
VB	Nima	0
EU	Vesolje in raziskave	2

Zgornja tabela (Tabela 2.9) kaže, da ima največ opredeljenih specifičnih sektorjev/podsektorjev Nemčija, in sicer opredeljuje medije, večje raziskave, posebnosti oziroma simboliko in kulturno dediščino. Torej enako kot ZDA tudi Nemčija kot specifični kritični sektor/podsektor opredeljuje simboliko, kulturno dediščino, kamor

spadajo državni spomeniki in tudi ikone (v smislu svetih podob). Podobno velja za raziskave, ki jih omenjata Nemčija in EU, ostale države pa teh ne uvrščajo med kritične sektorje/podsektorje. Nizozemska izpostavlja že omenjeno upravljanje površinskih voda ter Švica kritični sektor odlaganja odpadkov. Torej se obe državi bolj nagibata k okoljevarstvenemu vidiku specifičnih kritičnih sektorjev, medtem ko Nemčija, ZDA in EU bolj upoštevajo socialni vidik. VB in Francija presenetljivo ne omenjata nikakršnih posebnih kritičnih sektorjev/podsektorjev. Vzrokov za to je verjetno veliko. Državi morda preprosto menita, da specifični sektorji ne sodijo med tiste dele družbe, katerih ogrožanje/slabitev bi povzročila rušenje stabilnosti v družbi, s čimer se strinjam. Kulturna dediščina, mediji in drugi prej omenjeni specifični sektorji nikakor nimajo tolikšnega vpliva na vitalni družbeni obstoj. Če pride do uničenja kulturne dediščine ali večjih raziskovalnih centrov, posledice gotovo niso tako obsežne kot ob uničenju elektrarne ali zdravstvene ustanove. Vsekakor pa imajo tudi specifični kritični sektorji nek družbeni pomen, če ne primarni, pa vsaj sekundarni, bolj čustven.

2.2 ZAŠČITA KRITIČNE INFRASTRUKTURE: ORGANIZACIJSKI VIDIK

Zgornja analiza je pokazala, da ZDA le nimajo tako natančno razčlenjene zaščite KI. Morda je vzrok tudi v razdelitvi kritičnih sektorjev med nosilce odgovornosti, morda v sami organizacijski strukturi celotne zaščite KI. V tem poglavju bom opisala in opredelila le najpomembnejše akterje nacionalnega sistema KI v celotni organizacijski mreži, t. j. nosilce odgovornosti posameznih kritičnih sektorjev in celotnega sistema KI na državni ravni, kot so ministrstva, agencije, koordinacijske skupine itd. Zelo pomembno pa bo tudi vprašanje, ali znotraj zaščite KI posameznih izbranih držav in EU obstaja povezava javno - zasebno in koliko je teh povezav. Opredelila bom tiste, ki so zasnovane na podlagi zaščite informacijske KI, kjer gre razvoj zaščite KI vse bolj v smer informacijske tehnologije.

2.2.3 Organizacijski vidik zaščite kritične infrastrukture v ZDA

Novembra 2002 je kongres izdal Homeland Security Act[16] (2002, 107–296), ki je vzpostavil Ministrstvo za domovinsko varnost (DHS). Akt je novemu ministrstvu dal novo nalogo, ki vključuje zaščito pred terorističnimi napadi, zmanjšanje ranljivosti države in hitro odzivanje na omenjene napade. Specifično poudarja združenje številnih agencij v eno, ki opravlja državno-varnostne funkcije (e. g. patrulja na mejah, transport ...). V okviru sistema zaščite KI je akt prenesel naslednje agencije in službe v novo ministrstvo: NIPC (razen oddelka za raziskave računalništva), CIAO,[17] FedCIRC,[18] NISAC,[19] ostale varnostne strukture in aktivnosti znotraj ministrstva za energijo in nazadnje Nacionalni komunikacijski sistem (NCS).[20] Omenjene agencije so bile združene znotraj Direktorata za informacijsko analizo in zaščito infrastrukture (IA/IP) (eden od štirih direktoratov znotraj omenjenega akta) (Moteff 2007, 13–14).

2.2.3.1 Ministrstvo za domovinsko varnost

Predhodno sem prikazala (glej Tabelo 2.1), da ima vsak kritičen sektor svojo agencijo, ki je zanj odgovorna. ZDA imajo zelo razvejan sistem agencij in organov, ki skrbijo za varnost države (Slika 2.3). Tako ima kritična infrastruktura 17 kritičnih sektorjev, za deset od teh pa je odgovoren DHS, kar znaša 59 % odgovornosti vseh kritičnih sektorjev. Rezultat ne pomeni, da ostale agencije niso pomembne pri zaščiti kritične infrastrukture v ZDA, temveč ravno obratno: številne agencije so tiste, ki tvorijo DHS in ščitijo kritično infrastrukturo. Kljub temu bom pri raziskovanju upoštevala DHS, saj je ne nazadnje organ, ki nosi največjo odgovornost, koordinira in nadzira delovanje zaščite KI.

---

[16] Akt, ki je v veljavi od leta 2002. Dostopno prek: http://www.whitehouse.gov/deptofhomeland/bill/.

[17] Služba za zaščito KI je bila ustanovljena na podlagi predsedniške direktive 63, leta 1998. Bila je del ministrstva za komercialo (DOC), njene naloge pa obsegajo zagotavljanje varnosti energije, finančnih storitev, transporta, telekomunikacij in ostalih sistemov na federalni ravni (CIAO. Dostopno prek: http://www.espionageinfo.com/Cou-De/Critical-Infrastructure-Assurance-Office-CIAO-United-States.html (26. avgusta 2008)).

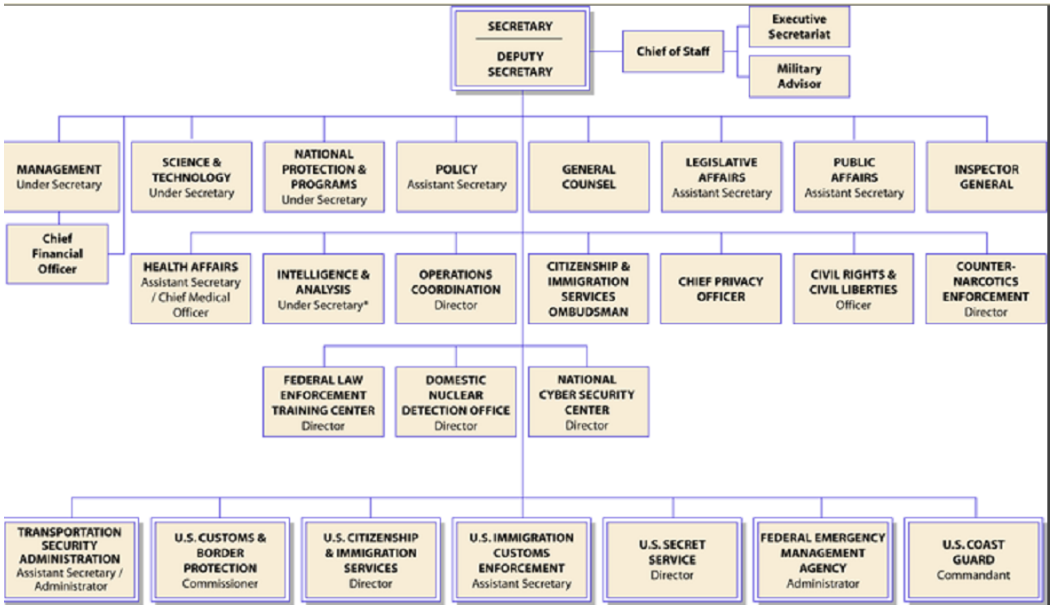
[18] Federalno računalniške sposobnosti kriznega odzivanja (dostopno prek: http://csrc.nist.gov/topics/incidentNIST/jan97-news.htm (23. avgusta 2008)).

[19] Nacionalni infrastrukturni simulacijski in analitični center ima znanje in strokovnost na področju medsebojne neodvisnosti in posledičnega uničenja KI. Nekoč je bil državni prvenstveni medministrski in medagencijski akter modeliranja, simulacij in analiz, ki je pripomogel k ublažitvi in taktiki načrtovanja (NISAC. Dostopno prek: http://www.sandia.gov/nisac/ (23.avgust 2008)).

[20] Več na http://www.ncs.gov/ (23. avgust 2008).

Dejstvo je, da od leta 1947 v ZDA ni bilo večje federalne reorganizacije – vse do nastanka DHS leta 2002. Od tedaj je ta doživljal številne reorganizacije. Do jeseni 2005 je bil razdeljen v 5 večjih oddelkov/divizij, ki so bili naslednji: varnost meja in transporta, priprave na nujno odzivanje, znanost in tehnologija, informacijska analiza in zaščita infrastrukture[21] ter menedžment (Abelle-Wigert in Dunn 2006, vol. 1, 321–322). Kasneje, jeseni leta 2005, so bili ustanovljeni štirje direktorati, in sicer: politika, operacijska koordinacija, pripravljenost in oddelek za obveščanje in analizo (Department of six-point agenda. Dostopno prek: http://www.dhs.gov/xabout/history (23. avgust 2008)). Na sliki (Slika 2.3) lahko vidimo sedanjo strukturo DHS, ki je sestavljen iz 16 pomembnejših direktoratov in služb. Sistem je zelo razvejan in kompleksen, kajti največja naloga vlade ZDA je bila združitev vseh funkcionalnih elementov zaščite in varnosti v eno samo ministrstvo.

Slika 2.2: Sedanja struktura Ministrstva za domovinsko varnost



VIR: www.dhs.com (23. avgust 2008).

[21] Direktorat se preimenuje v direktorat pripravljenosti (Moteff 2007, 15).

2.2.3.2 Povezovanje na ravni javno - zasebno

Spoznali smo, da ima federalna vlada nalogo vodstva in koordinacije za zaščito in blaženje ranljivosti državne KI, vsi akterji domovinske varnosti pa morajo odigrati pomembno vlogo, četudi je ta neuspešna. Omenjeno še posebno velja za zasebni sektor, ki ima v lasti in operira s kar 85 % državne KI. S tem predstavlja prvo bojno črto KI, ki si jo lastijo (Office of homeland security 2007, 28). Nenehna privatizacija vitalne infrastrukture, kot je voda, energija ali transport, je že v osemdesetih vodila v rast lastništva zasebnega sektorja in s tem upad vladnega lastništva KI (Henriksen in Stein 2004, 60–63). Posledično je zaščita KI večinoma v rokah zasebnega sektorja, ki vodi sistem KI. Medtem ko vlada nudi državno varnost ter pospešuje pretok informacij in komunikacijskih procesov, nudi zasebni sektor podrobno znanje o svoji KI, zato da bi implementacija uspešne zaščite večinoma ostala med njimi (Bundesministerium des Innern 2005, 6). Zaradi dinamike ogrožanja KI in informacijske KI ter možnosti posledičnih uspešnih napadov zasebni sektor lahko išče pomoč in dodatne informacije pri vladi in obratno (The White House (2003). Dostopno prek: http://www.whitehouse.gov/pcipb/physical.html (3. september 2008)).

V nadaljnji analizi bom navedla samo ključne povezave javno - zasebno na osnovi zaščite informacijske KI. Odločitev temelji preprosto na vedno bolj poudarjeni vlogi informacijske tehnologije, ki prekriva celotno mrežo zaščite KI v katerikoli sodobni državi. V analizo ne bom zajela povezovanja javno - zasebno, ki se dogaja na lokalni ali še nižji ravni. Zanimala me bodo izključno povezovanja na državnih in mednarodnih ravneh, omenjena v zborniku CIIP (2006, vol. 1).

Zaščita KI v ZDA obsega osem najpomembnejših povezav javno - zasebno za zaščito informacijske KI (glej Tabelo 2.10). Večinoma so partnerstva nastala v 21. stoletju; izjema je finančni ISAC, ki se je oblikoval že leta 1999, ter InfraGard (leta 1996). Partnerstva javno - zasebno v večini zajemajo področja informacijske tehnologije, kjer se industrijska združenja, neprofitne organizacije, centri in druga združenja povezujejo z javnim sektorjem določenega področja.

Danes imajo navadno vsi industrijski sektorji KI center za širjenje informacij in analizo (ISAC) (finančni, transportni, električni itd.) (Abelle-Wigert in Dunn 2006, 329–330).

InfraGard predstavlja partnerstvo med federalnim oddelkom za raziskovanje (FBI) in zasebnim sektorjem (dostopno prek: http://www.infragard.net/ (30. avgust 2008)). NCSA je državna povezava cyber-zaščite med industrijo in vladnimi organizacijami (dostopno prek: http://www.staysafeonline.info/ (30. avgust 2008)). Naslednja povezava, PCIS, je partnerstvo za zaščito KI; koordinira medsektorske iniciative, ki promovirajo javne in zasebne želje po zaščiti, varnosti in zanesljivosti sistema KI (dostopno prek: http://www.pcis.org/ (30. avgust 2008)). CIDDAC je prva neprofitna organizacija za zaščito omrežja pred cyber-kriminalom, ki povezuje javne, zasebne in vladne akterje (dostopno prek: http://www.ciddac.org (30. avgust 2008)). NCSP je prostovoljna koalicija trgovskega združenja industrije za zaščito cyber-omrežja (dostopno prek: http://www.cyberpartnership.org/init.html (30. avgust 2008)). I3P pa tvori združenje vodilnih univerz, nacionalnih laboratorijev in neprofitnih institucij za zaščito informacijske KI v ZDA (dostopno prek: http://www.thei3p.org/ (30. avgust 2008)).

Tabel 2.10: Partnerstvo javno - zasebno v ZDA

Povezava javno - zasebno	Število	Leto nastanka
DHS – oddelek za zasebni sektor[22]	8	2002
ISAC		1999
InfraGard		1996
NCSA		/
PCIS		2002
CIDDAC		2005
NCSP		2003
I3P		2001

VIR: Abelle-Wigert and Dunn (2006, vol. 1, 228–332).

Kot vidimo, odnosi javno - zasebno v ZDA obsegajo resnično vsa področja partnerstva, združenj, sodelovanja in povezovanja v okviru zaščite KI in posebej v okviru zaščite informacijske KI. V nadaljevanju bom ugotavljala, ali izbrane evropske države in tudi EU v enakem merilu ustvarjajo sodelovanje z zasebnim sektorjem kot v ZDA in kdaj so se posamezna partnerstva javno - zasebno oblikovala.

[22] Več na http://www.dhs.gov/dhspublic/display?theme=37 (24. avgust 2008).

2.2.4 Organizacijski vidik zaščite kritične infrastrukture v evropskih državah

a) Francija

V Franciji je najpomembnejši organ za zaščito sistema KI generalni sekretariat državne obrambe (SGDN). Med-ministrski sekretariat se osredotoča na raziskave, priprave odločitev in nadzor njihove implementacije. Koordinira in vodi delovne skupine, vzpostavljene v sodelovanju z vsemi ministrstvi. Med njimi so najpomembnejša ministrstvo za obrambo, ministrstvo za zunanje zadeve, ekonomijo, finance in industrijo, zdravstvo, razvoj in transport. SGDN pomaga predsedniku vlade izpolniti njegove odgovornosti v splošnem menedžmentu obrambe (2. odstavek dekreta 25. januarja 1978) in opravlja tudi naslednje naloge:

1. Deluje kot sekretariat za obrambne svetove in skupščine,
2. deluje kot sekretariat za medministrski komite za obveščevalne dejavnosti,
3. pripomore k varnosti države pred grožnjami napada na nacionalno ozemlje,
4. nadzoruje krize, ki prizadenejo varnostno okolje,
5. izboljšuje varnost državnega omrežja in informacijskega sistema ter tistih v javnem sektorju,
6. nadzira izvoz orožja in transferjev občutljive tehnologije,[23]
7. podpira študij in izobraževanje o obrambi (dostopno prek: http://www.sgdn.gouv.fr/rubrique.php?id_rubrique=20#6 (31. avgust 2008)).

Ob raziskovanju organizacijskega sistema KI v Franciji sem ugotovila, da ni veliko literature, ki bi natančno opredelila, kdo nosi odgovornosti določenega kritičnega sektorja. Vemo, da je SGDN tisti, ki se najbolj osredotoča na zaščito KI in sodeluje z ostalimi ministrstvi. Menim, da so za posamezne kritične sektorje odgovorna ministrstva specifičnih področij (za zdravstvo je na primer zadolženo ministrstvo za zdravstvo). Veliko bolj kot k zaščiti samega sistema KI pa se nagibajo k zaščiti informacijske KI, kot bomo videli kasneje pri normativnih aktih. Na podlagi tega so nastali tudi naslednji odnosi javno - zasebno (Tabela 2.11).

[23] V smislu orožja za množično uničevanje, nuklearnega, radiološkega itd.

Tabela 2.11: Partnerstvo javno - zasebno v Franciji

Odnos javno - zasebno	Število	Leto nastanka
Strateški posvetovalni svet za informacijsko tehnologijo (CSTI)	2	2000
Francoski institut zanesljivosti (ISDF)		1990

VIR: Abelle-Wigert and Dunn (2006, vol. 1, 103–104).

CSTI je strateško posvetovalno telo za informacijsko tehnologijo, ki se je oblikovalo leta 2000 in na čelu katerega je predsednik vlade. Sestavljajo ga vodilni iz sveta industrije ter raziskav in razvoja. Njegova odgovornost je, da vladi predstavi rešitve pri zaščiti informacijske KI (dostopno prek: http://www.csti.pm.gouv.fr/uk/home-uk.html (30. avgust 2008)). ISDF predstavlja forum predstavnikov zasebnega sektorja, ki je nastal že leta 1990 (Abelle-Wigert and Dunn 2006, vol. 1., 103). Če primerjamo z ZDA, vidimo, da do leta 1996 ZDA še niso imele partnerstva javno - zasebno za zaščito informacijske KI na državni ali mednarodni ravni tako kot Francija. Francija ima torej daljšo tradicijo obstoja in razvoja sodelovanja zasebnega sektorja z javnim na področju informacijske KI.

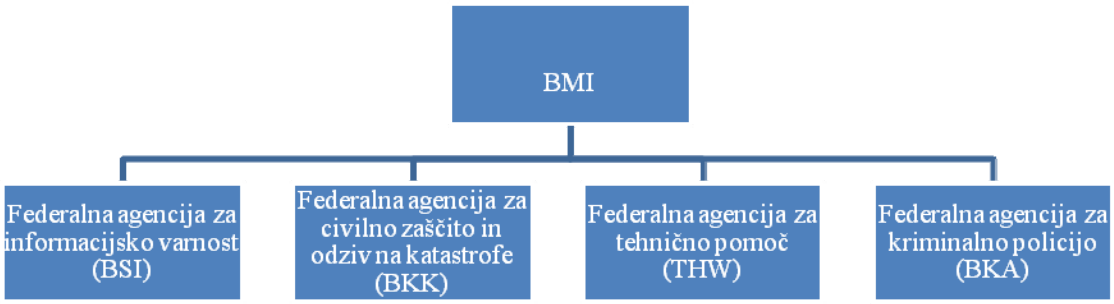
b) Nemčija

Kot so vladne agencije zadolžene za notranjo varnost v Nemčiji, je Federalno ministrstvo za notranje zadeve (BMI) odgovorno za zaščito sistema KI. Med-ministrske aktivnosti so se pričele že leta 1997 na pobudo BMI, ki ga je zmotivirala ameriška študija predsedniške komisije na temo zaščite KI. Leta 1999 je BMI oblikoval delovno skupino, imenovano AG Kritis. Strokovnjaki iz treh divizij so se združili, in sicer federalna divizija za civilno zaščito in odzivi na katastrofe (BKK), federalna kriminalna policija (BKA) ter federalna divizija za zaščito informacijske tehnologije (BSI). Srečanja omenjene skupine se izvajajo letno, za razvoj skupnih pristopov in za optimiziranje pretoka informacij znotraj treh divizij. Znotraj BMI so pomembne agencije[24] (glej Graf 2.4), ki so zadolžene za svoja področja odgovornosti (v našem primeru kritični sektorji). Poleg omenjenih agencij imajo pomembno vlogo pri zaščiti KI tudi ostala ministrstva, kot so ministrstvo za ekonomijo in delo, ministrstvo za

[24] Nekateri vključujejo še četrto agencijo, in sicer federalno agencijo za tehnično pomoč (THW) (dostopno prek: http://www.bmi.bund.de/cln_012/nn_148164/Internet/Content/Themen/Terrorism/DataAndFacts/Protection__of__critical__infrastructures.html (30. avgust 2008)).

pravosodje, ministrstvo za obrambo in ostala ministrstva, odgovorna za posebna področja (Critical infrastructure protection in Germany. Dostopno prek: http://www.bsi.bund.de/english/topics/kritis/Abelle-Wigert in Dunn _en.pdf (30. avgust 2008)).

Graf 2.3: BMI in podrejene agencije



VIR: Federal ministry of interior (2007, 51).

Javno - zasebno partnerstvo za Nemčijo predstavlja nujnost,[25] saj to prispeva k iskanju ciljnih skupin, specifičnih rešitev in njihovih implementacij (dostopno prek: http://cipp.gmu.edu/archive/8_CIPinGermany_2005.pdf (30. avgust 2008)).

Tabela 2.12: Partnerstvo javno - zasebno v Nemčiji

Odnos javno - zasebno	Število	Leto nastanka
Iniciativa D21	2	1999
AKSIS		1999

VIR: Abelle-Wigert and Dunn (2006, vol. 1, 119-120).

Iniciativa D21 je največje partnerstvo javno - zasebno v Nemčiji. Sestavlja jo več kot 200 predstavnikov podjetij, asociacij, političnih institucij in ostalih organizacij, ki so trenutno povezani. Vključuje tudi najvišje predstavnike podjetij, kot so Alcatel, AOL, Cisco sistemi, Debitel, IBM, Microsoft in Siemens (Iniciative D12. Dostopno prek: http://www.initiatived21.de/en/English.104.0.html (30. avgust 2008)). AKSIS je delovna skupina, ki je nastala na pobudo centra za strateške študije v Nemčiji. Torej je neformalni, prostovoljni forum za izmenjavo informacij javnega in zasebnega sektorja, ki dvakrat na leto organizira strokovna srečanja (Abelle-Wigert and Dunn 2006, vol. 1,

[25] Več kot 90 % kritične infrastrukture je v zasebnem lastništvu (dostopno prek: http://www.bsi.bund.de/english/topics/kritis/Abelle-wigert and Dunn _en.pdf,2008 (30. avgust 2008)).

120). Tako kot Francija ima tudi Nemčija dve pomembnejši partnerstvi javno - zasebno, torej šest manj kot ZDA. Zanimivo je, da je Nemčija v zaščito KI začela vlagati in jo razvijati istočasno kot ZDA (1997), a kljub temu ji ni uspelo doseči več povezav med zasebnim in javnim sektorjem, čeprav je kar 90 % njene KI v zasebnem lastništvu.

c) Nizozemska

Na Nizozemskem so Ministrstvo za notranje zadeve in odnosi kraljestva (MNZOK) odgovorni za koordinacijo sistema zaščite KI. Sestavljajo jih štiri glavne divizije, in sicer javni menedžment, odnosi kraljestva in vladavine, javni red in varnost ter obveščevalne in varnostne dejavnosti (dostopno prek: http://www.minbzk.nl/bzk2006uk/organisation/organisation-of-the (31. avgust 2008)). Poleg tega sta na Nizozemskem za zaščito KI odgovorna tudi nacionalni koordinacijski center ter direktorat kriznega menedžmenta, oba znotraj Ministrstva za notranje zadeve in odnosov kraljestva. Njuna naloga je predvsem koordinacija različnih projektov in splošnega delovanja zaščite KI (Abelle-Wigert and Dunn 2006, vol. 1, 204). Obe koordinacijski telesi sta nastali okoli leta 2004, približno istočasno kot povezave javno - zasebno (Tabela 2.13). Vse tri tovrstne povezave (ECP.NL, NACOTEL in NCO-T) govorijo o razvoju e-Nizozemske na podlagi študije in programa KWINT.[26] Nizozemska ima skupno dve partnerstvi javno - zasebno, tako kot Francija in Nemčija. Razlog je ta, da je NACOTEL prenehal delovati leta 2006, njegovo vlogo pa je prevzel NCO-T (Abelle-Wigert and Dunn 2006, vol. 1, 207–209). S tega vidika imajo ZDA še vedno največ povezav javno - zasebno na področju zaščite informacijske KI.

Tabela 2.13: Partnerstvo javno - zasebno na Nizozemskem

Odnosi javno - zasebno	Število	Leto nastanka
Izboljšanje elektronske komerciale (ECP.NL)	3 (2)	2002
Nacionalni načrt razvoja telekomunikacij (NACOTEL)		2002–2005
Nacionalni načrt razvoja izboljšanja telekomunikacij (NCO-T)		2006

VIR: Abelle-Wigert and Dunn (2006, vol. 1, 207–209).

[26] Glej podpoglavje Normativne podlage, iniciative in pobude.

d) Švica

V Švici je več različnih organizacij, ki se ukvarjajo z zaščito KI. Centralni organ, kakršnega imajo ZDA, Nemčija in Nizozemska, torej ne obstaja. Poleg tega predstavlja partnerstvo javno - zasebno enega od temeljev sistema zaščite KI (International telecommunication union 2005, 16). Leta 2006 je federalni svet dal mandat federalnemu ministrstvu za obrambo, civilno zaščito in šport (FOCP), da koordinira zaščito sistema KI med vsemi agencijami. Omenjeno ministrstvo ima nalogo do leta 2009 oddati poročilo o stanju zaščite KI v Švici (dostopno prek: http://www.admin.ch/aktuell/00089/index.html?lang=en&msg-id=13516 (31. avgust 2008)). Poleg tega se pri študijah Centra za varnostne vede (CSS) v Švici pri posameznih projektih vključujeta še federalna agencija za civilno zaščito in federalna agencija za državne ekonomske zaloge (NES) (dostopno prek: http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=46118 (31. avgust 2008)). Skratka, za posamezen kritični sektor skrbi federalno ministrstvo določenega področja. Podoben sistem najdemo v Franciji, torej necentraliziran, z nespecifično opredelitvijo in zelo poudarjenim pomenom zaščite informacijske tehnologije. Poleg tega je še posebej poudarjena vloga partnerstva javno - zasebno, ki temelji na tradiciji (Tabela 2.14).

Tabela 2.14: Partnerstvo javno - zasebno v Švici

Odnos javno - zasebno	Število	Leto nastanka
Infosurance zveza	3	1999
NES		/
CLUSIS		1989

VIR: Abelle-Wigert and Dunn (2006, vol. 1, 287–289).

Številna podjetja so ustanovila Infosurance zvezo, ki predstavlja skupnost za povečanje informacijske varnosti in sodelovanja med različnimi akterji KI (dostopno prek: http://www.infosurance.ch/de/verein.htm (31. avgust 2008)). NES (federalna agencija za ekonomske zaloge) deluje zelo tesno z zasebno industrijo, z akterji federalne, kantonske in komunalne ravni. Njena glavna naloga je osredotočenje na sektorsko uničenje na področju osnovnih zalog (hrana, energija, terapevtski produkti) ter ostala področja infrastrukture (transport, industrija in informacijska KI) (Federal Office for National Economic Supply 2006, 1–12). Nazadnje je tu še CLUSIS, ki predstavlja neprofitno organizacijo in združuje več kot 230 članov iz bank, industrije itd. (dostopno prek: http://www.clusis.ch/francais/presentation.htm# (31. avgust 2008)).

e) Velika Britanija

CPNI (center za zaščito KI) svetuje vladi VB, kako najbolje zaščititi nacionalno KI (CNI), ki je ključni element za nenehen razvoj pomembnih služb (dostopno prek: http://security.homeoffice.gov.uk/counter-terrorism-strategy/working-withpartners/protect-national-infrastructure/ (31. avgust 2008)). CPNI se je izoblikoval februarja 2007 z združitvijo Nacionalnega centra za koordinacijo infrastrukturne varnosti (NISCC) in dela MI5 (varnostna služba VB) ter Nacionalnega centra za varnostno svetovanje (NSAC) (omenjeni so bili predhodno pomembni za zaščito KI). To je torej medministrska agencija, ki dobi sredstva od številnih vladnih in nevladnih agencij, ki se ukvarjajo z zaščito KI (dostopno prek: http://www.cpni.gov.uk/aboutcpni188.aspx (31. avgust 2008)). Drugače pa za vsak kritični sektor skrbi eno (pri prvi pomoči 4 akterji in pri hrani 2 akterja) ministrstvo določenega področja (dostopno prek: http://www.cpni.gov.uk/About/work.aspx (31. avgust 2008)).

CPNI je prevzel vlogo NISCC, ki se je povezoval z zasebnim sektorjem, in ima v lasti KI. CPNI se povezuje na periodičnih industrijskih forumih in z medmrežnimi povezavami, kjer si delijo informacije o stanju KI (prirejeno po Abelle-Wigert and Dunn 2006, vol. 1, 302–303). Svetovalni organ informacijske tehnologije (IAAC) je unikatno partnerstvo, ki povezuje korporativne voditelje, javne uslužbence, zakonske akterje in raziskovalne skupine (dostopno prek: http://www.iaac.org.uk/ (31. avgust 2008)). Ostale povezave temeljijo na zaščiti informacijske KI, zadnja (konfederacija Britanske industrije) pa predstavlja lobistično organizacijo, ki se povezuje z vlado VB (dostopno prek: http://www.cbi.org.uk/ndbs/staticpages.nsf/StaticPages/home.html/?OpenDocument (31. avgust 2008)).

Tabela 2.15: Partnerstvo javno - zasebno v Veliki Britaniji

Odnos javno - zasebno	Število	Leto nastanka
CPNI (prej NISCC)	6	2007
IAAC		2000
BCS		1957[27]
Internetni varnostni forum		Okoli leta 2002
Opazovalna fundacija interneta		1996[28]
Konfederacija Britanske industrije		1965[29]

VIR: Abelle-Wigert and Dunn (2006, vol. 1, 302–303).

Iz zgornje tabele (Tabela 2.15) je razvidno, da ima VB en ključni organ, ki bolj koordinira celotni sistem KI in svetuje vladi (Home Office security[30]). Torej nima centraliziranega sistema kot ZDA, saj za vsak sektor skrbi določeno ministrstvo posebnega področja, ki je neodvisno od glavnega ministrstva v VB (Home Office security). Pri partnerstvu javno - zasebno že nekoliko dosega ZDA, saj obsega skupno 6 povezav, kar predstavlja 75 % partnerstva v ZDA. Zanimivo je predvsem, da so nekatera partnerstva v VB nastala že v 16. (BCS) in 17. stoletju (konfederacija Britanske industrije), kar morda pomeni večji napredek razvoja tovrstnih povezav zaradi tradicije.

Po krajšem pregledu organizacijskega vidika zaščite KI (in informacijske KI na področju partnerstva javno - zasebno) bom v nadaljevanju analizirala organizacijski vidik zaščite KI v EU.

2.2.5 Organizacijski vidik zaščite kritične infrastrukture v EU

Evropski svet je leta 2004 zahteval razvoj že omenjenega Evropskega programa za zaščito KI (EPCIP). Od takrat se izvaja splošno pripravljalno delo, ki vključuje organizacijo relevantnih seminarjev, publiciranje »Zelenega papirja« in diskusije z

[27] Več na http://www.bcs.org/server.php?show=nav.5651 (31. avgust 2008).
[28] Več na http://www.iwf.org.uk/ (31. avgust 2008).
[29] http://www.cbi.org.uk/ndbs/content.nsf/802737aed3e3420580256706005390ae/63a0c3fc22c7478e80257026004e0ba4? OpenDocument (31. avgust 2008)
[30] Več na http://security.homeoffice.gov.uk/ (31. avgust 2008).

javnimi in zasebnimi lastniki. Upoštevajoč slednje, je nastal EPCIP Komunikacije, ki je ustvaril horizontalni okvir za zaščito KI v Evropi. Okvir predvideva naslednje (najpomembnejše):

1. ukrepe za utrjevanje implementacije EPCIP, kamor spadajo tudi EPCIP-delovni načrt, opozorilni informacijski sistem KI (CIWIN),[31] uporaba strokovnih skupin na področju zaščite KI v Evropi, širjenje CIP-informacij ter identifikacija in analiza medsebojne neodvisnosti;
2. podporo državam članicam glede na državne sisteme zaščite KI (NCI), ki bi jih lahko optimalno uporabljale države članice;
3. k temu dodano finančno dimenzijo in delno tudi predlog programa EU na temo Odvrnitev, pripravljenost in menedžment posledic terorističnih in drugih oblik varnostnih ogrožanj za obdobje od 2007 do 2013. To naj bi prispevalo k večjim priložnostim investiranja v zaščito KI (EPCIP 2006, 1).

Kot vidimo, EU nima nekega organa ali telesa, ki bi bil odgovoren za zaščito KI v EU. Namesto tega so oblikovali program (EPCIP), ki je prevzel nalogo razvoja sistema zaščite KI v EU. Resnično gre za projekt, ki je usmerjen v prihodnje stanje in povezave z državami članicami. Zaradi tega CIP EU ne moremo primerjati s CIP v ZDA in izbranimi evropskimi državami. Z menoj se ne strinja Abro (2006, 3), ki pravi, da EPCIP predstavlja model centralne agencije, kjer so združene moči različnih narodov, ideologij in agencij. Po njegovem mnenju bo EPCIP uspešen, ker bodo številne agencije interesnih skupin prispevale finančna sredstva, vključujoč nevladne poslovne akterje, kot so Telekom in energetska podjetja v Evropi.

Enako velja za področje partnerstva javno - zasebno, kjer nisem zasledila niti enega. Kljub temu je Evropska komisija v EPCIP Komunikacije zapisala: *»Okrepitev določenih varnostnih ukrepov s strani javne avtoritete, v času neposrednih napadov na družbo v celoti in ne na industrijske akterje, mora oblikovati Država. Zasebni sektor je torej tisti, ki igra ključno vlogo.«* To so zapisali z vedenjem, da je večina KI v lasti zasebnega sektorja EU (Commision of european communities 2004, 4). Iz citata

[31] Sistem, ki združuje specialiste držav članic CIP z namenom sodelovanja z Evropsko komisijo, da bi oblikovali programe izmenjav informacij na podlagi groženj in ranljivosti. Poleg tega bi oblikovali primerne protiukrepe in strategije. ZDA imajo podoben sistem, znan kot Krizno informacijsko omrežje KI (CIWIN), ki deluje od leta 2003 (dostopno prek: http://www.euractiv.com/en/security/critical-infrastructure/article-140597 (2. september 2008)).

razberemo, da daje EU večji poudarek pomenu zasebnega sektorja. Resnična moč načrtov EU glede zaščite KI je v popolnosti odvisna od lastnikov KI. V ZDA pa so mnenja, da je odgovornost zaščite KI v rokah tako zasebnega kakor tudi državnega sektorja, kar je verjetno posledica terorističnih napadov. Za primerjavo: ZDA predvidevajo porabo 63 milijard dolarjev za zaščito KI, EU pa predlaga 140 milijonov dolarjev. Magnus Ovilius, višji administrator v Evropski komisiji, je dejal, da *»bo odgovornost za krizni menedžment ležala v rokah lastnikov in operaterjev«* (Abro 2006, 3). Torej je tu EU, ki je sestavljena iz 27 držav, kjer ima vsaka svoje zakone in normativne podlage glede zaščite KI, na drugi strani pa ZDA, kohezivna enota številnih držav, ki so podrejene le eni zakonski podlagi zaščite KI.

V nadaljevanju bom primerjala organizacijski vidik zaščite KI (in informacijske KI na področju partnerstva javno - zasebno) ZDA z izbranimi evropskimi državami. EU torej ne morem primerjati z ZDA, ker nima nikakršnega organizacijskega modela zaščite KI.

2.2.6 Primerjalna analiza organizacijskega vidika zaščite kritične infrastrukture

Zdaj ko sem naštela najpomembnejše organe vodenja zaščite KI in tudi povezave javno - zasebno zaščite informacijske KI, bom nadalje (Tabela 2.16) primerjala nacionalne pristope sistemov zaščite KI (centraliziran/necentraliziran), ključne vladne agencije sistema KI, števila ključnih povezav med javnim in zasebnim sektorjem informacijske KI in tradicije nastanka. Na tem mestu bi še enkrat poudarila, da sem upoštevala le pomembnejše državne oziroma mednarodne povezave zasebnega in javnega sektorja zaščite informacijske KI. Po mojem mnenju je informacijska tehnologija oz. zaščita informacijske KI najpomembnejša, saj omogoča obstoj vseh ostalih kritičnih sektorjev, ker predstavlja njihovo jedro. Govorim predvsem z vidika razvitejših modernih družb oziroma držav, kot so Francija, Nemčija, Nizozemska, Švica, VB in ZDA. Potemtakem ne morem primerjati povezave zasebnega in javnega sektorja ZDA z EU, ker v EU zaščita KI (in informacijske KI) organizacijsko ni definirana in ostaja v rokah posameznih evropskih držav.

Tabela 2.16: Primerjalna tabela organizacijskega vidika zaščite KI

	Centraliziran/ decentraliziran	Glavni nosilec zaščite KI	Število partnerstev javno - zasebno	Leto nastanka partnerstva javno - zasebno (povprečje)
ZDA	Centraliziran	DHS	8	2001
Francija	Decentraliziran	SGDN	2	1995
Nemčija	Decentraliziran	BMI	2	1999
Nizozemska	Decentraliziran	MNZOK	2	2003
Švica	Decentraliziran	FMOCŠ	3	1994
VB	Decentraliziran	CPNI	6	1987

a) Centralizirana/decentralizirana zaščita kritične infrastrukture

V zgornji tabeli (Tabela 2.16) vidimo, da imajo ZDA glede na druge države zelo centralizirano zaščito KI. Kar 59 % kritičnih sektorjev je pod nadzorom DHS, za ostalo pa skrbijo pristojna ministrstva določenega področja. Druge države po mojem mnenju nimajo centralizirane zaščite KI, ker zanjo skrbijo posamezna ministrstva in ne določen ključni akter kot v ZDA. Tam ima DHS glavno vlogo koordinatorja, nadzornika in nosilca odgovornosti. Znotraj tega se zaščita KI razporedi med posameznimi oddelki, ki skrbijo za izbrane kritične sektorje. Torej je večina odgovornosti zaščite sistema KI na državni ravni združena v eno telo, medtem ko v ostalih državah tega ne zasledimo. Te imajo namreč posebna koordinacijska telesa in telesa, ki skrbijo za svoj del odgovornosti pri zaščiti posameznih kritičnih sektorjev.

b) Glavni nosilec zaščite kritične infrastrukture

Kot sem že omenila, je v ZDA DHS tisti, ki koordinira, nosi največ odgovornosti zaščite KI, in znotraj njega so vsi organi (59 %), ki skrbijo za zaščito KI. V Franciji je SGDN organ, ki koordinira, vendar znotraj njega ni organov/teles, ki bi skrbeli za zaščito KI. Zaščito KI v Franciji torej omogočajo ločena ministrstva, ki so neodvisna od SGDN. Glede Nemčije smo povedali, da je BMI tisti, ki primarno skrbi za koordinirano vodenje zaščite KI. Znotraj tega so štiri glavne divizije, ki so odgovorne za svoja področja (informacijska tehnologija, civilna zaščita ...). Poleg štirih agencij pa za vsako področje kritičnih sektorjev poskrbijo pristojna ministrstva, neodvisna od BMI.

Podobno je na Nizozemskem, kjer ima ključno vlogo v zaščiti KI MNZOK, ministrstvo, znotraj katerega najdemo štiri agencije, koordinacijsko telo in direktorat kriznega odzivanja. MNZOK ima enako kot DHS bolj nadzorno funkcijo, saj koordinacijo in vodenje zaščite KI opravljajo telesa znotraj MNZOK. Za razliko od Nizozemske in ZDA v Švici za večino kritičnih sektorjev skrbijo pristojna ministrstva, tako kot v Franciji. Obstaja federalni organ FMOCŠ, vendar ima zgolj koordinacijsko funkcijo vodenja zaščite KI. Zelo podobno je v VB, kjer medministrska agencija CPNI skrbi za koordinacijo zaščite KI, medtem ko so za posamezne kritične sektorje odgovorna pristojna ministrstva.

Na splošno lahko trdim, da imajo organizacijsko podobno zaščito KI v ZDA, Nemčiji in na Nizozemskem. Vse tri naštete države imajo znotraj glavnega telesa zaščite KI posamezne oddelke, agencije, divizije ipd. Res je, da tudi med ZDA, Nemčijo in Nizozemsko obstajajo razlike, saj DHS nosi odgovornost, koordinira in vodi, BMI bolj koordinira in MNZOK bolj nadzira zaščito KI. Popolnoma drugače je v Franciji, Švici in VB, kjer imajo ključna telesa izključno koordinacijsko vlogo glede na ločena in neodvisna pristojna ministrstva oz. posamezna področja kritičnih sektorjev.

c) Število partnerskih povezav javnega in zasebnega sektorja zaščite informacijske kritične infrastrukture

Po podatkih zbornika CIIP (2006, vol. 1) imajo ZDA 8 povezav javno - zasebno na državni in mednarodni ravni. To pomeni, da je tam glede na ostale izbrane države največ tovrstnih povezav. Sledi VB, ki jih ima 6, Švica 3 in druge države vsaka po 2 povezavi javno - zasebno zaščite informacijske KI. To število nam pove, da ZDA največ vlagajo v razvoj sodelovanja zasebnega in javnega sektorja zaščite informacijske tehnologije na državni in tudi mednarodni ravni. Ker tu nisem upoštevala povezovanja javno - zasebno na nižjih ravneh, pomeni, da imajo lahko izbrane države v skupnem številu (državno, mednarodno, lokalno ...) več takšnih povezav kot ZDA. Vseeno menim, da je državna (in mednarodna) raven tista, ki je ključna za uspešno vodenje zaščite KI. S tega vidika so ZDA tiste, ki trenutno največ vlagajo (glede na število) v skupno sodelovanje zasebnega in javnega sektorja zaščite informacijske tehnologije, v primerjavi z ostalimi državami.

d) Letnica nastanka/oblikovanja partnerstva javnega in zasebnega sektorja zaščite informacijske KI

Seštela sem letnice nastankov vseh povezav javno - zasebno posamezne države in dobljeno število delila s številom povezav javno - zasebno v posamezni državi. Tako sem izračunala povprečno letnico nastanka partnerstva zasebnega in javnega sektorja posamezne države. Povprečna letnica nastanka parnerstva javno - zasebno zaščite informacijske KI v Švici je 1994 in v Franciji 1995. Kot sem že prej omenila, viri nakazujejo, da obe državi veliko bolj vlagata v zaščito informacijske KI kot v zaščito KI v celoti. Vsekakor nam pridobljen rezultat služi kot eden od kazalcev predhodnega vlaganja Švice in Francije v zaščito informacijske KI v primerjavi z ostalimi državami. Bolj presenetljiv je podatek, da je povprečna letnica nastanka partnerstva javno - zasebno v VB že 1987. Vsekakor to nakazuje dejstvo, da je bila VB med prvimi državami, ki so se zavedale pomena sodelovanja zasebnega in javnega sektorja informacijske KI, tako kot Švica in Francija. Nekoliko drugače je v Nemčiji, ZDA in na Nizozemskem, ki so v povprečju pričele razvijati partnerstva javno - zasebno okoli leta 2000. Če upoštevamo število zgoraj navedenih povezav javno - zasebno posameznih držav, opazimo neko korelacijo s povprečno letnico nastanka tovrstnih povezav. VB torej zaseda prvo mesto glede na povprečno leto nastanka povezav javno - zasebno in je druga po številu tovrstnih povezav. Švica zaseda drugo mesto glede na povprečno letnico nastanka povezav in je tretja glede na njihovo število. Zanimivo je, da za ZDA takšna korelacija ne velja, saj ima največ povezav javno - zasebno in zaseda predzadnje mesto po povprečnem letu njihovega nastanka. Slednji podatek nam služi kot dejstvo, da tradicija ni tista, ki pogojuje uspešnejši razvoj in obstoj zaščite KI ter informacijske KI. Vsekakor pa tradicija nakazuje, kdaj se je posamezna država začela ukvarjati z zaščito KI in se zavedati njene pomembnosti, v našem primeru pomembnosti sodelovanja zasebnega in javnega sektorja na področju zaščite informacijske KI.

Kot vidimo, je tradicija eden od kazalcev, kdaj se je posamezna država pričela ukvarjati z vprašanjem zaščite KI. V nadaljevanju si bomo ogledali tradicijo razvoja normativnih podlag, pobud in iniciativ posameznih izbranih držav in tudi EU.

2.3 ZAŠČITA KRITIČNE INFRASTRUKTURE: NORMATIVNE PODLAGE, POBUDE IN INICIATIVE

Že leta 1949, sicer na področju vojaških groženj, je protokol Ženevske konvencije v 52. členu spregovoril o splošni zaščiti civilnih objektov, v 53. členu o zaščiti kulturnih objektov in institucij ter v 54. členu o splošni zaščiti tistih objektov, ki so ključni za preživetje celotne populacije (dostopno prek: http://www.unhchr.ch/html/menu3/b/93.htm (9. september 2008)). Torej so nekatere države (tiste, ki so podpisale protokol) že leta 1949 poudarile pomembnost zaščite objektov v primeru vojaških groženj. Do danes so se oblikovale različne vrste groženj, ne samo vojaške, ki imajo lahko velik vpliv na obstoj kritične infrastrukture. S tega vidika bodo v nadaljevanju razčlenjene normativne podlage, pobude in iniciative nastanka zaščite kritične infrastrukture v ZDA, EU kot mednarodni organizaciji in izbranih petih državah.

2.3.1 Normativne podlage, pobude in iniciative zaščite kritične infrastrukture v ZDA

V poglavju o normativnih podlagah, pobudah in iniciativah v ZDA bom analizirala naslednje:

- Predsedniško komisijo za zaščito KI (PCCIP),
- Predsedniški direktivi 62 in 63,
- nacionalni načrt za zaščito informacijskega sistema,
- izvršne akte,
- Predsedniško direktivo domovinske varnosti 7 (HSPD-7),
- Nacionalni načrt za zaščito infrastrukture (NIPP),
- nacionalne strategije.

2.3.1.1 Predsedniška komisija za zaščito kritične infrastrukture

Predsednik Clinton je oblikoval Predsedniško komisijo za zaščito KI z namenom, da bi svetovala in pomagala predsedniku ZDA. Pomoč PCCIP se kaže predvsem skozi predlaganja nacionalnih strategij za zaščito in varnost KI pred fizičnimi in cyber-grožnjami (dostopno prek: http://www.usdoj.gov/criminal/cybercrime/critinfr.htm#Vc (9. september 2008)). Poleg tega je predlagala tudi splošne nacionalne normativne okvire in implementacijo načrtov za zaščito KI, določanje legalnih in strateških vprašanj s predlogom povečanja zaščite, ustavne in regulativne spremembe, nujne za delovanje zaščite. PCCIP je tako leta 1997 izdala poročilo predsedniku Clintonu, kjer je bila ocenjena fizična in cyber-ranljivost. Komisija ni našla nobene nujne kritične izpostavljenosti na državni ravni infrastrukture. Kljub temu pa je našla dovolj vzrokov za neposredno akcijo, posebej na področju cyber-varnosti.

Le-ti so naslednji: hiter razvoj in rast računalniške pismenosti populacije (z ozirom na računalniške hekerje[32]), svojstvena ranljivost skupnih protokolov v računalniškem omrežju, lahek dostop do osnovnih orodij hekerjev (dostopno na mnogih spletnih straneh) in nazadnje tudi dejstvo, da osnovna orodja hekerjev predstavljajo osnovna orodja večine populacije. Poleg tega je komisija predlagala sodelovanje in komunikacijo med zasebnim in javnim sektorjem. Zasebni sektor ima v lasti in operira z večino državne KI. Kot je zaznala komisija, je primarna vloga vlade (poleg varovanja lastne infrastrukture) zbiranje in širjenje zadnjih informacij o morebitnem motenju tehnike, analiza groženj in tudi poti za obrambo pred hekerji (Moteff 2007, 3–4). Pooblastila komisije niso več v veljavi, saj so prenesena na HSPD-7, ki je opredeljen v nadaljevanju.

[32] Obstaja približno 20.000 različnih definicij *hekerja*, od katerih lahko povzamem najpomembnejše:
a) oseba, ki preživi veliko časa v stiku z informacijskimi sistemi, z bolj fetišističnim pristopom; torej se spozna na računalnike, četudi ni programer,
b) oseba, ki pogosto uporablja in izrablja online-usluge,
c) programer,
d) oseba, ki uporablja računalnik v ilegalne namene, ne glede na zadevo, večinoma za vdor v drugi sistem preko omrežja itd. (dostopno prek: http://insecure.org/stf/hackenc.txt (10. avgust 2008)).

2.3.1.2 Predsedniški direktivi 62 in 63

Predsedniško direktivo[33] 62 (zaščita pred nekonvencionalnimi grožnjami domovinskemu in prekomorskemu ozemlju ZDA) je oblikoval predsednik Clinton maja 1998. Direktiva 62 govori o vzpostavitvi integracijskega programa za povečanje uspešnosti ZDA proti terorističnim grožnjam in tudi v pripravi na posledice takšnih napadov na državljane in infrastrukturo. Vodilne agencije so odgovorne za podporo programa, kot je agencija v ZDA za zaščito okolja (EPA). EPA naj služi kot primer, kjer ima Direktiva 62 naslednje zahteve:

- podpora posledic menedžmenta aktivnosti FEMA, ki vključujejo vse oblike materialnih in okoljskih problemov,
- pomoč DHS in usposabljanje ljudi državne in lokalne ravni za nujno odzivanje,
- usposabljanje kadrov,
- pomoč ministrstvu za pravosodje v smislu oskrbe kadrov z zaščitno opremo, preventivnimi instrumenti, na državni in lokalni ravni agencij.

Direktiva 62 poleg tega zahteva od vsake agencije, da razvija in vzdržuje operativni načrt, kot je zapisano v izvršilnem aktu 12656. Operativni načrt zagotavlja operativnost najpomembnejših funkcij agencij v primeru napada, ki onemogoči štab ustanov in vodstvenih vrhov (dostopno prek: http://www.epa.gov/rpdweb00/rert/presidential directives.html# pdd62 (11. september 2008)).

Istega leta je bila izdana tudi Predsedniška direktiva 63 (zaščita KI), kjer so bili postavljeni nacionalni cilji, ki naj bi se uresničili do leta 2000 in najkasneje 5 let od dneva podpisa direktive. Direktiva 63 opredeljuje zmožnost zaščite KI v ZDA pred namernimi napadi, ki bi lahko zelo oslabili:

1. delovanje federalne vlade za zaščito pomembnih državnih varnostnih nalog in za zagotavljanje splošnega zdravstva ter varnosti,

[33] Odločitev o zunanji politiki in državni varnosti (dostopno prek: http://www.epa.gov/rpdweb00/rert/presidentialdirectives.html#pdd62 (10. september 2008)).

2. državno in lokalno vlado pri vzdrževanju reda in omogočanju minimalne javne službe,
3. zasebni sektor pri zagotavljanju funkcije ekonomije in omogočanju delovanja telekomunikacij, energije, finančne in transportne službe (PDD-63. Dostopno prek: http://www.fas.org/irp/offdocs/paper598 (10. september 2008)).

Direktiva torej na splošno govori o težnji države k zagotavljanju varnosti ob naraščajoči ranljivosti in notranje povezanosti infrastrukture v ZDA. Pojem infrastrukture tu zajema telekomunikacije, finance in bančništvo, energijo, transport in druge pomembne vladne službe. Direktiva prav tako zahteva neposredno delovanje federalne vlade, ki vključuje krizno načrtovanje in načrtiranje za zmanjšanje izpostavljenosti napadom. Poudarja kritično pomembnost sodelovanja med državnimi in zasebnimi sektorji, tako da povežejo določene agencije s predstavniki zasebnega sektorja (PDD on infrastructure. Dostopno prek: http://www.uhuh.com/laws/pdd63.htm#PDD%2062%20and%2063%20Fact%20Sheet%20-%20Summary (10. september 2008)).

2.3.1.3 Nacionalni načrt za zaščito informacijskega sistema

Nacionalni načrt za zaščito informacijskega sistema (leta 2000) v ZDA predstavlja prvi poskus katerekoli države v obrambi lastne informacijske tehnologije. Predsednik Clinton je v Predsedniški direktivi 63 poudaril njegov razvoj in ga imenuje Verzija 1.0. Prvotna verzija načrta se osredotoča na domače pobude, ki jih izvaja federalna vlada za zaščito nacionalne kritične informacijske infrastrukture. Posledično načrt zajema širok seznam skrbi pod PDD-63, vključujoč specifične vloge industrije in državne ter lokalne vladne vloge, samostojno ali v obliki partnerstva z vlado. Gre torej tudi za zaščito zasebne KI, potrebo po fizični kot tudi po informacijski zaščiti pred nenehnimi napadi (The White house 2000, 9).

2.3.1.4 Izvršni akti

Po 11. septembru 2001 je tedanji predsednik Bush podpisal dva izvršna akta, ki sta vplivala na zaščito KI. Prvi akt 13228 se imenuje Vpostavitev ministrstva za domovinsko varnost in sveta domovinske varnosti. Istega leta, 8. oktobra 2001, so, kot sem že omenila, ustanovili DHS. Ena od funkcij DHS je koordinacija vseh moči za zaščito države in njene KI pred terorističnimi napadi. Omenjeni akt 13228 je vzpostavil tudi svet za domovinsko zaščito, ki svetuje in asistira predsedniku na vseh področjih domovinske varnosti. Drugi izvršni akt 13231, ki se imenuje tudi Zaščita KI v informacijski dobi, je ustanovil predsedniško komisijo za zaščito KI. Komisija ima nalogo »predlaganja politike in koordinira programe za zaščito informacijskih sistemov KI«. Ne nazadnje je akt 13231 vzpostavil tudi svetovalni svet nacionalne infrastrukture (NIAC), predsedniški svetovalni odbor, sestavljen iz lastnikov in operaterjev nacionalne KI (Abelle-Wigert and Dunn 2006, vol. 1, 316).

2.3.1.5 Predsedniška direktiva domovinske varnosti 7

Slednja direktiva je verjetno najpomembnejša, saj je bila vzpostavljena kot državni okvir za federalna ministrstva in agencije za identificiranje in dajanje prednosti KI ZDA in ključnih dobrin ter za zaščito KI pred terorističnimi napadi (Homeland security presidental directive/HSPD-7 2003, 1–8). HSPD-7 torej primarno posodablja politiko ZDA in vlogo ter odgovornost različnih agencij glede zaščite KI. Poleg tega izpostavlja tudi sektor-specifične agencije, med katerimi posamezna agencija določi svoj sektor zaščite, koordiniranja in dajanja prednosti (Moteff 2007, 14). Edina novost direktive je, da morajo vsa federalna ministrstva in agencije do leta 2004 pripraviti načrt za zaščito fizične in informacijske KI, ki je v zasebnih rokah ali samo vodena s strani zasebnikov (Executive Office of the president, Office of management and budget 2004, 1).

2.3.1.6 Nacionalni načrt za zaščito infrastrukture

Nacionalni načrt za zaščito infrastrukture (NIPP), izdan leta 2006, prinaša unificirano strukturo integracije zaščite KI in ključnih dobrin, v edinstven nacionalni program.

NIPP predstavlja celostno podobo programov in aktivnosti, ki se odvijajo prav v tem času med različnimi sektorji, kot tudi nove in razvijajoče se zaščite KI. Na splošno gre za sodelovanje med zasebnim sektorjem, državo, teritorialnimi in lokalnimi oblastmi ter nevladnimi organizacijami ter federalno vlado. Federalna vlada ima nalogo dajanja prednosti tistim zaščitnim ukrepom in investicijam, ki se dogajajo med sektorji. Poleg tega bo razporejala vire tako, da bodo prinašali največ ugodnosti za zmanjšanje groženj. To bo storila z zmanjšanjem ranljivosti, groženj in minimaliziranjem posledic terorističnih napadov in drugih nesreč. Sektor-specifične agencije in ostala federalna ministrstva ter agencije (opredeljeni v HSPD-7) se zavezujejo k naslednjemu (najvidnejše):

- podpori NIPP-koncepta, okvira, lastne funkcije v sistemu zaščite KI,
- sodelovanju s sekretariatom domovinske varnosti,
- oddajanju letnih poročil v skladu z zahtevami HSPD-7, sekretariatu domovinske varnosti,
- koordiniranju razvoja sektor-specifičnega načrta (SSP) z ostalimi partnerji, ki je potrjen s strani DHS (vsak sektor-specifični načrt bo v skladu z okvirom NIPP),
- razvoju ali modificiranju medagencijskega in agencijsko specifičnega načrta KI, ki je v skladu z NIPP in SSP,
- razvoju in utrjevanju partnerstva zaščite KI z državnimi, regionalnimi, lokalnimi, rodovnimi in mednarodnimi entitetami, zasebnim sektorjem, nevladnimi organizacijami,
- ne nazadnje tudi k zaščiti informacijske KI – poudarjeno v predhodnih normativnih okvirih (U. S. Department of Homeland Security 2006, III–IV).

2.3.1.7 Nacionalne strategije

Do sedaj je vlada ZDA izdala štiri pomembnejše nacionalne strategije področja zaščite KI, in sicer:

- Nacionalno strategijo domovinske varnosti (leta 2002),
- Nacionalno strategijo za varnost cyber-prostora (2003),
- Nacionalno strategijo za fizično zaščito KI in ključnih dobrin (2003) ter
- Nacionalno strategijo domovinske varnosti (oktobra 2007).

Glede na temo diplomske naloge bom analizirala nacionalno strategijo za domovinsko varnost (2007) in nacionalno strategijo za fizično zaščito KI in ključnih dobrin (2003).

a) Nacionalna strategija za fizično zaščito KI in ključnih dobrin

Omenjena nacionalna strategija je naslednica nacionalne strategije domovinske varnosti iz leta 2002. Torej predstavlja širšo perspektivo jedra zmanjšanja ranljivosti pred terorizmom z zaščito KI in ključnih dobrin pred fizičnimi napadi. Poleg tega identificira nacionalne cilje in argumente ter poudarja vodilne principe, ki bodo podprli KI in dobrine, vitalne za nacionalno varnost, vlado, zdravstvo in varnost javnosti, ekonomije in zaupanja ljudi. Najpomembnejše, strategija vzpostavlja fundacijo za gradnjo in spodbujanje okolja sodelovanja med vlado, industrijo in državljani (zasebniki). Skratka, strategija je vodilo za akterje na vseh ravneh, ki kolektivno prispevajo k večji varnosti KI. Navaja naslednje pomembne strateške argumente:

- identificiranje in zagotavljanje zaščite KI, pomembne za življenje ljudi,
- pravočasno opozarjanje in zagotavljanje zaščite specifične KI,
- zagotavljanje zaščite KI, ki postaja glavni cilj terorističnih napadov (Office of homeland security 2003, VII–VIII).

b) Nacionalna strategija domovinske varnosti

Najnovejša nacionalna strategija domovinske varnosti je bila izdana oktobra 2007. Nasledila in posodobila je nacionalno strategijo domovinske varnosti iz leta 2002. Ključna novost te različice je zavedanje vlade ZDA, da mora poleg zaščite države pred terorističnimi napadi poudariti zaščito države pred naravnimi nesrečami, ki jih povzroči človek ali narava sama. Glavno pobudo za nastanek strategije ZDA pripisujejo »življenjski vaji« ter katastrofi orkana Katrina. Zaradi tega so bili že opredeljeni cilji prejšnje strategije posodobljeni z naslednjimi zahtevami:

- zaščita pred terorističnimi napadi in onemogočanje le-teh,
- zaščita državljanov ZDA, KI in ključnih dobrin,

- odzivanje na in ponovno vzpostavljanje stanja pred nesrečo, ki se zgodi,
- nadaljevanje fundacije za zagotavljanje dolgoročnega uspeha.

Prvi trije cilji pomagajo organizirati državne pobude, zadnji cilj pa pomaga oblikovati in transformirati načela domovinske varnosti, sisteme, strukture in institucije. To vključuje tudi obširen pristop k razvoju kriznega upravljanja in kulture pripravljenosti, izboljšanju menedžmenta incidentov, uporabljanju znanosti in tehnologije ter mobiliziranju vseh instrumentov nacionalnega vpliva in moči. Strategija poudarja sodelovanje na vseh državnih ravneh, izraža pa tudi zavedanje, da grožnje segajo prek geografskih meja, zato poudarja sodelovanje z mednarodnimi partnerji.

Skratka, strategija domovinske varnosti iz leta 2007 kaže razumevanje pomena terorističnih napadov, zavedanje o posledicah naravnih nesreč (primer orkana Katrina leta 2004) in predlaga nove iniciative ter pristope, ki bodo povečali varnost ZDA. Prav tako dopolnjuje Nacionalno strategijo varnosti ter Nacionalno strategijo za bojevanje proti terorizmu, obe iz leta 2006 (Office of homeland security 2007, 1).

Iz vseh opredeljenih normativnih aktov, pobud in iniciativ razvoja zaščite sistema KI lahko sklepamo, da so se spreminjali v skladu s časovno aktualnimi grožnjami. Sprva je vlada ZDA opredelila pomen zaščite KI, temu dodala poziv k širšemu sodelovanju akterjev državne in nazadnje tudi mednarodne ravni. Najvidnejše je seveda poudarjanje zaščite KI pred terorističnimi napadi, čemur se kasneje (2007) doda tudi vedno večji pomen naravnih ali od človeka povzročenih nesreč. Iz preprostih aktov in direktiv so se torej sčasoma začele oblikovati nacionalne strategije, ki resnično identificirajo vlogo in odgovornost posameznih akterjev na različnih ravneh. Po mojem mnenju nacionalne strategije predstavljajo kazalec sodobne zaščite KI in zagotavljanja varnosti na najvišji integracijski stopnji povezovanja akterjev. Gre za unificiranje različnih metod, pristopov v en sam dokument, ki jasno opredeljuje svoje cilje in naloge.

V nadaljevanju bom z analizo izbranih evropskih držav in EU ugotavljala, ali tam obstajajo dokumenti oziroma nacionalne strategije tako kot v ZDA. V podporo temi diplomske naloge bom raziskala obstoj najpomembnejših normativnih aktov, pobud in iniciativ. Namen tega je ugotavljanje, ali imajo izbrane države in EU v primerjavi z ZDA nacionalno strategijo na področju zaščite KI, ali je v morebitnih dokumentih

poudarjena vloga sodelovanja javno - zasebno, pomembnost zaščite KI; nazadnje pa bom prikazala tudi transparentnost zaščite KI.[34]

2.3.2 Normativne podlage, pobude in iniciative zaščite kritične infrastrukture v evropskih državah

a) Francija

Ob analiziranju Francije nisem zasledila skoraj nobenega pravnega okvira, le pobude in iniciative, in sicer:

- Državni načrt okrepitve varnosti informacijskega sistema (2004–2007),
- Poročilo francoske civilne zaščite leta 2008.[35]

Prvi poudarja varnost glavnih in lokalnih vladnih omrežij ter tistih, ki so pomembna za menedžment vitalne infrastrukture. Francija je tako prvič nastopila s strateškim načrtom reševanja vedno večjih napadov na informacijske sisteme (Republice of France 2004–2007, 1–2). Poročilo civilne zaščite pa je bilo izdano letos in poudarja zaščito infrastrukture, ki je vitalnega pomena za družbo (SAIV). Obstaja namreč tudi dekret, ki je bil izdan na podlagi zaščite KI v letu 2006. Skratka, poročilo obravnava pomembnost integracije zasebnega in javnega sektorja ter državne in lokalne ravni pa tudi pomen identificiranja vlog akterjev sistema zaščite KI in nazadnje podaja konkretne rešitve, kot so priprave, nadzor in podobno (Livre blanc Haut comite Francais pour la defense civile 2008, 69–79).

V primerjavi z ZDA Francija nima nacionalne strategije niti večjega pravnega okvira, ki bi jasno identificiral in opredeljeval vlogo akterjev pri zaščiti KI. Oba dokumenta, poročilo in okrepitveni načrt v Franciji, zajemata zelo skope obrazložitve v primerjavi z ZDA. Vseeno je pomembno poudariti, da Francija napreduje v smeri zaščite informacijske tehnologije in tudi zaščite KI nasploh. Poglejmo, kako je to urejeno v Nemčiji.

[34] V smislu dostopnosti pomembnih informacij na internetu in v ostali literaturi – odprtost sistema kot kazalec demokracije, ki prispeva k razvoju družbe.
[35] Dostopno samo v francoskem jeziku.

b) Nemčija

Pri analiziranju Nemčije sem odkrila veliko dokumentov, iniciativ in pobud, torej mnogo aktivnosti na področju zaščite KI v zadnjih desetih letih. Med njimi so najpomembnejše naslednje:

- že omenjena AG Kritis skupina (1997),
- osnovni koncept za zaščito KI (2005),
- Nacionalni načrt za zaščito informacijske KI (2005),
- Nacionalna strategija za zaščito KI pred naravnimi nesrečami (2007).

Nemčija je za svoje vodilo izbrala rezultate ameriške študije predsedniške komisije ZDA (omenjena v poglavju 2.3.1.1). Ima zelo podoben, skorajda enak pristop k zaščiti KI kot ZDA. Upošteva zaščito KI na vseh ravneh in vse grožnje od naravnih nesreč do tehničnih napak informacijskega sistema. Poleg tega identificira naloge in vloge akterjev sistema zaščite KI, sodelovanje na vseh ravneh ter podaja osnovne ukrepe priprav in minimaliziranja posledic KI (osnovni koncept za zaščito iz leta 2005). Glede na vedno bolj številčna in ogrožajoča dejanja naravnih nesreč je to tudi v Nemčiji pripomoglo k razmišljanju o nacionalni strategiji zaščite KI pred naravnimi nesrečami. Nastala naj bi do leta 2009, do tedaj pa so se in se bodo odvijali številni s tem povezani projekti. S projekti so si zastavili številne vaje, ki temeljijo na izmišljenih scenarijih ogrožajočih neviht v povezavi z morjem, ki posledično lahko vplivajo na energijo, plinovod, železnice in ostalo KI. V obdobju 2007–2009 naj bi že razvili prilagodljive koncepte, v tretjem delu pa nacionalni načrt oziroma nacionalno strategijo, kamor bodo umestili tudi sodelovanje države z zasebnim sektorjem (dostopno prek: http://www.dkkv.org/upload/editor/Orkane2007/Vortrag_BBK_Lauwe.pdf (15. september 2008)).

Kot vidimo, je razvoj pravnega okvira, pobud in iniciativ v Nemčiji zelo podoben kot v ZDA, saj so jih jemali kot zgled pri razvoju zaščite KI. Torej poudarjajo vedno večji pomen povezovanja vseh akterjev na vseh ravneh (država, lokalno, zasebno itd.), terorizem obravnavajo kot enega od večjih kazalcev groženj sodobne družbe, k temu pa prištevajo vedno bolj ogrožajoča dejanja narave v obliki katastrofalnih poplav, neviht in podobnega.

Nadalje bom obravnavala razmere na Nizozemskem in preverila, ali obstajajo podobnosti oziroma razlike v primerjavi z ZDA.

c) Nizozemska

Na Nizozemskem predstavlja zaščita KI pomembno vprašanje v povezavi z nacionalno varnostjo. Tako se že od leta 1990 pojavljajo številna prizadevanja za boljše delovanje in vodenje sistema zaščite KI (Abelle-Wigert and Dunn 2006, vol .1, 198). Naštela jih bom nekaj in opredelila le najpomembnejše:

- Digitalna delta (1999),
- nizozemski »Beli papir 2000«,
- »Biti in delčki« (2000),
- KWINT poročilo in memorandum (2001),
- »Quick scan« (2003).

Prvi trije projekti/dokumenti se nanašajo izključno na zaščito informacijske KI, zato jih ne bom podrobneje razlagala. Naslednji, KWINT poročilo, se tudi nanaša na zaščito informacijske KI, vključuje pa tudi sodelovanje vlade z zasebnim sektorjem. Torej predstavlja izboljšanje pozicije industrije znotraj elektronske ekonomije, kjer ima pomembno mesto internet. Pri tem ima vlada izključno koordinacijsko in pospeševalno vlogo, torej se neposredno ne vmešava (De Bruin, 2002).

Verjetno najpomembnejšo študijo s področja zaščite KI predstavlja prav raziskovalno delo »Quick scan« vprašalnik, s katerim so znotraj javnega in zasebnega sektorja ugotavljali celoten pregled kritičnih sektorjev in služb, njihovo neodvisnost ter vlogo pri potencialni škodi kot rezultat ločenega porušenja sistema. Omenjeno študijo je izvajal nacionalni koordinacijski center v sodelovanju z organizacijo znanstvenih raziskovanj in je predstavljala prvo fazo nizozemskega projekta za zaščito KI. Naslednja točka projekta je bilo analiziranje posameznih kritičnih sektorjev v obliki scenarijev in podobnega. Torej je Nizozemska izvedla obsežne študije številnih faz, prvi »Quick scan« vprašalnik, nato podrobnejše analize in kasneje se je oblikoval akcijski načrt 10

točk, kjer natančno opredeljujejo stanje zaščite KI in njeno izboljšanje ter zaščito pred terorističnimi napadi (Ministry of the Interior and Kingdom Relations 2003, 1–23).

V primerjavi z ZDA se je Nizozemska v letih 2002–2003 odločila za večfazno študijo, ki je temeljila na celovitem raziskovanju področja zaščite KI. Gre za popolnoma drugačen pristop kot v ZDA, ki so nacionalno strategijo večinoma oblikovale znotraj političnega in strokovnega kroga vlade. Po mojem mnenju je Nizozemska uporabila dolgoročno boljšo zaščito KI, v kateri so bili pri študiji vključeni prav vsi akterji zasebnega in javnega sektorja. Nizozemska potemtakem kot država bolj zaupa v kompetence človeških virov v primerjavi z ZDA. Dejstvo je, da imajo ZDA številne nacionalne strategije, česar Nizozemska še ni dosegla (nacionalna strategija v procesu nastajanja).

V nadaljevanju bom ugotavljala, kakšen pristop so razvili v Švici, ali je bolj podoben nizozemskemu ali tistemu v ZDA.

d) Švica

Zaradi pomembnosti infrastrukture moderne družbe je tako kot veliko držav tudi Švica pričela identificirati KI ter razvijati strategije za njeno zaščito. Zato so v zadnjih letih izvedli nekaj s tem povezanih ukrepov. Še več, leta 2005 so ustanovili program zaščite KI, ki cilja na koordinacijo vseh aktivnosti in posledično tudi na oblikovanje nacionalne strategije KI v Švici (Federal Office for Civil Protection FOCP 2008, 1). Odgovornost programa zaščite KI nosi federalno ministrstvo za civilno zaščito, ki koordinira vse federalne aktivnosti s področja KI. Ustanovilo je delovno skupino (WG CIP), sestavljeno iz 23 oddelkov vseh sedmih federalnih vladnih ministrstev in tudi federalnega sodišča. Kantoni in zasebni sektorji se bodo v raziskovanje vključili v kasnejšem obdobju. Julija 2007 je federalni svet podprl prvo poročilo programa zaščite KI, ki ga je izdelala delovna skupina WG CIP. Poročilo je natančno opredelilo kritične sektorje in tudi poudarilo načrt za prihodnje delo, ki se bo kazalo v razvoju strategije KI do leta 2012. Do tedaj pa se odvijajo številni projekti, na primer analiza vpliva velikega potresa na KI in podobno. Do leta 2009 pričakujejo drugo poročilo, ki bo analiziralo napredek in ugotovitve različnih projektov s področja zaščite KI (Critical infrastructure protection. Dostopno prek:

http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski.html (16. september 2008)).

V primerjavi z ZDA je tudi Švica na poti oblikovanja nacionalne strategije za zaščito svoje KI. Da bi dosegla omenjeno, je enako kot Nizozemska izvedla številne fazne procese oziroma projekte, katerih ugotovitve se bodo odražale v nacionalni strategiji. Zanimivo, da sta se obe državi, tako Nizozemska kot Švica, lotili bolj raziskovalnega dolgoročnega pristopa, za razliko od ZDA. Kateri pristop je boljši, bo vsekakor pokazala praksa resničnih scenarijev, različnih stopenj kriz.

V nadaljevanju je tu še VB: ugotavljala bom, ali se bolj nagiba k načinu zaščite KI Švice in Nizozemske (obe evropski državi) ali bolj k pristopu ZDA.

e) Velika Britanija

Številne aktivnosti se izvajajo na področju informacijske tehnologije, zato je zaščita informacijske KI primarna naloga VB. Poleg tega sem zasledila, da VB svojo definicijo kritične infrastrukture podaja znotraj nacionalne strategije za boj proti terorizmu. Terorizem je v VB označen kot največji sovražnik nacionalne varnosti, kateremu sledijo napadi na informacijsko tehnologijo. Torej zaščita KI predstavlja podkategorijo zaščite v sklopu širše teme protiterorističnega delovanja (dostopno prek: http://security.homeoffice.gov.uk/counter-terrorism-strategy/working-with-partners/protect-national-infrastructure/ (16. avgust 2008)). V primerjavi z ZDA Velika Britanija terorizem obravnava kot primarnega sovražnika države, medtem ko ZDA sem uvrščajo še naravne nesreče. VB ima tako kot ZDA nacionalno strategijo, ki pa ne obsega celotne zaščite nacionalnega ozemlja kot v ZDA.

Ogledali si bomo še normativne podlage, pobude in iniciative zaščite KI v EU, ki jih bom poskušala primerjati z ZDA.

2.3.3 Normativne podlage, pobude in iniciative zaščite kritične infrastrukture v EU

Po terorističnem napadu na železniški postaji v Madridu (marca 2004) je Evropski svet dal pobudo Svetu za pravosodje in domovinske zadeve, da pripravi strategijo za

povečanje zaščite kritične infrastrukture v EU. Komisija je tako oktobra 2004 sprejela dokument Komunikacije za zaščito KI v boju proti terorizmu, ki je bil prvi korak za povečanje zaščite, pripravljenosti in odzivnosti EU ob terorističnih napadih, ki vključujejo KI (EU Council 2008, 1–3). Novembra 2005 je Komisija izdala »Green paper« na Evropski program za zaščito KI (EPCIP). »Green paper« navaja možnosti, kako lahko Komisija odgovarja na pobudo Sveta za vzpostavitev EPCIP in CIWIN (glej poglavje 2.2.5). Možnosti, ki jih predstavlja »Green paper« EPCIP, so kombinacije dejanj in jih moramo pojmovati kot dopolnilo trenutnim nacionalnim naporom (Protect infrastructure. Dostopno prek: http://ec.europa.eu/justice_home/fsj/terrorism/protection/fsj_terrorism_protection_infrastruct_en.htm (20. avgust 2008)). Decembra 2006 je tako Komisija izdala EPCIP, junija 2008 pa je Svet za pravosodje in domovinske zadeve dosegel politično soglasje za izdajo direktive za identifikacijo KI EU (ECI) in izboljšanje njene zaščite. Direktiva vzpostavlja nujnost za identifikacijo in imenovanje ECI ter podaja splošen pristop ocenjevanja potrebe za izboljšanje zaščite KI, z namenom zaščite ljudi. Direktiva se osredotoča na zaščito energije in transporta, kasneje pa bodo po potrebi dodani ostali kritični sektorji, na primer informacijska tehnologija (EU Council 2008, 1–3).

Kot vidimo, je EU začela razvijati zaščito KI po terorističnem napadu leta 2004. Bolj se je usmerila v razvoj programov in direktiv, ki nekako skušajo oblikovati evropsko zaščito KI. Po mojem mnenju EU poudarja razvoj zaščite KI v posameznih državah članicah, kjer ima bolj posredovalno funkcijo kot funkcijo odgovornosti. Ne glede na to se EU zaveda pomembnosti sodelovanja zasebnih lastnikov EU z nosilci odgovornosti političnih in strokovnih krogov države. Vsekakor EU poudarja pomembnost zaščite KI, tudi z vidika zaščite svojih prebivalcev. Torej je sistem zelo odprt, ker nudi državam članicam dostopnost informacij na internetu, konferencah in podobnih javnih srečanjih. Z zadnjo direktivo, ki naj bi prišla v veljavo do konca leta 2008, EU poudarja koncept ocenjevanja, kjer ima vsaka država članica pomembno vlogo. Pri uporabljenem konceptu EU dopušča možnosti dajanja prednosti zaščiti določenih kritičnih sektorjev za določeno obdobje in tudi dopušča možnost, da zaščite KI v EU sploh ne bi bilo. Tega pri ostalih državah nismo zasledili, kajti vse se nagibajo k razvoju strategij (razen Francije), ki ščitijo nacionalno KI, četudi v določenih obdobjih ne pride do krize.

EU se je torej na nek način pripravljena odreči zaščiti KI, če je ne potrebuje. Celotna zaščita KI v EU temelji na številnih predlogih, ki niso uradno potrjeni. Ne nazadnje EU meni, da zaščita KI morda sploh ni potrebna. Takega razmišljanja v drugih državah nisem zasledila. ZDA nenehno poudarjajo pomen zaščite KI, saj omogoča obstoj in normalno delovanje družbenih procesov. Poleg tega v primerjavi z ZDA koncept zaščite KI v EU tvorijo številni segmenti (države članice), medtem ko zaščita KI v ZDA predstavlja en večji segment. Torej sta si koncepta EU in ZDA popolnoma nasprotna, vsaj glede sprejemanja odgovornosti zaščite KI. Če izhajamo iz različnega definiranja pomembnosti obstoja koncepta zaščite KI ter dejstva, da EU nenehno predlaga in še vedno nima uradne dokumentacije, ki bi jasno definirala zaščito kritične infrastrukture, EU ne moremo primerjati z ZDA. Zaradi tega naslednja primerjalna analiza normativnih podlag, pobud in iniciativ zajema samo izbrane evropske države in ZDA.

2.3.3 Primerjalna analiza normativnih podlag, pobud in iniciativ zaščite kritične infrastrukture

Sedaj ko smo predstavili najpomembnejše normativne dokumente, iniciative in pobude ZDA in izbranih evropskih držav, bom v nadaljevanju s primerjalno tabelo pokazala podobnosti in razlike omenjenega raziskovalnega področja.

Iz spodnje tabele (Tabela 2.17) je razvidno, da sem države primerjala na podlagi štirih kazalcev.

Tabela 2.17: Primerjalna tabela normativnih aktov, pobud in iniciativ ZDA in ostalih držav

DRŽAVA	Nacionalna strategija (K1)	Omenjeno sodelovanje države z zasebnim sektorjem (K2)	Pomembnost zaščite KI (K3)	Transparentnost (K4)
ZDA	DA	DA/DA	Visoka	Zelo
Francija	NE	DA/DA	Posredovalna	Malo
Nemčija	DA	DA/DA	Visoka	Zelo
Nizozemska	V nastajanju	DA/DA	Visoka	Zelo
Švica	V nastajanju	DA/DA	Visoka	Zelo
VB	DA	DA/DA	Posredovalna	Vedno bolj

a) Ali ima posamezna država nacionalno strategijo, kjer je umeščena tudi zaščita KI?

Največ nacionalnih strategij, ki so vsebinsko najobsežnejše in v katere je umeščena tudi zaščita KI, imajo ZDA. Zelo podobno nacionalno strategijo je razvila tudi Nemčija, ki se je zgledovala po ameriški študiji (omenjena v poglavju 2.3.1.1). Obe državi sta terorizem omenili kot enega od pomembnejših dejavnikov, ki lahko ogrozijo zaščito KI. Nasprotno VB sicer obravnava terorizem kot del nacionalne strategije, znotraj katere je opredeljena zaščita KI, ne upošteva pa ostalih dejavnikov ogrožanja, kot so naravne nesreče. Torej ZDA in Nemčija veliko bolj celostno obravnavajo koncept zaščite sistema KI kot VB. Enako bi lahko rekli za Švico in Nizozemsko, ki resnično izvajata številne projekte in delavnice na temo zaščite KI. Obe državi šele razvijata nacionalne strategije, ki bodo zajemale celostni pristop sistema zaščite KI. Po mojem mnenju imata Švica in Nizozemska bolj analitičen in instrumentalen pristop k ugotavljanju, kako najbolje zaščititi sistem nacionalne KI in ugotovitve zapisati kot dolgoročnejše strategije države. Predvsem ZDA so se lotile oblikovanja nacionalnih strategij po nenadnih kriznih dogodkih (npr. teroristični napad 11. septembra 2001), kjer niso toliko upoštevali mnenja strokovnjakov na državni in javni ravni, kot sta to storili Švica in Nizozemska. Tudi Francija je država, ki ne upošteva strokovnega mnenja vseh ravni, kar se kaže tudi v pomanjkanju zanimanja za razvoj nacionalne strategije. Šele letošnje leto so v manjšem poročilu opredelili pomembnost KI v okviru civilne zaščite in ne v okviru vitalnih sistemov države, kljub temu da je bila Francija sama deležna terorističnih napadov, velikih protestov in drugih oblik družbenih deliktov.

b) Ali se v navedenih dokumentih posredno/neposredno omenja sodelovanje države z zasebnim sektorjem?

Na splošno bi lahko rekla, da vse države, ZDA, Francija, Nemčija, Nizozemska, Švica in VB, razumejo pomen sodelovanja države z zasebnim sektorjem. Torej se zavedajo, da so zasebni lastniki odgovorni za večinski del KI, medtem ko je država tista, ki zasebnim lastnikom pomaga v smislu informiranja o varnostnem stanju sistema KI. Po mojem mnenju je tako razmišljanje zelo pozitivno, saj spodbuja razvoj družbenih projektov na različnih forumih, konferencah, delavnicah in podobno. S tem se lahko oblikuje uspešnejša zaščita KI, saj te ne ščiti samo država ali samo zasebni lastniki KI.

Edino slabost omenjenega sodelovanja lahko morda povzroči linija odgovornosti, torej, za kaj je kdo odgovoren. To bi morala vsaka država jasno opredeliti, da ne bi prišlo do zapletov v resničnem kriznem položaju.

c) Ali posamezna država poudarja pomembnost zaščite KI?

Pomembnost zaščite KI se najbolj izraža v politiki ZDA, Nemčije, Švice in Nizozemske. Vse naštete države imajo več uradne dokumentacije, iniciativ ali pobud v smislu pomembnosti zaščite KI in njenega vrednotenja v družbi. Največ prednosti dajejo zaščiti splošne KI, nato sledi zaščita informacijske KI, ki postaja vedno pomembnejša za obstoj splošne KI.

Za razliko od naštetih dajeta Francija in VB večjo prednost informacijski KI in ne splošni KI, kar se kaže v njunih uradnih dokumentih, iniciativah in pobudah. Torej imata obe državi bolj posredovalno vlogo pri zagotavljanju delovanja sistema KI. To pomeni, da se Francija in VB kot državi pojavljata kot koordinacijsko telo in ne kot primarni organ izvajanja odgovornih faznih procesov zaščite KI, tako kot to izvajajo ZDA, Nemčija, Švica in Nizozemska.

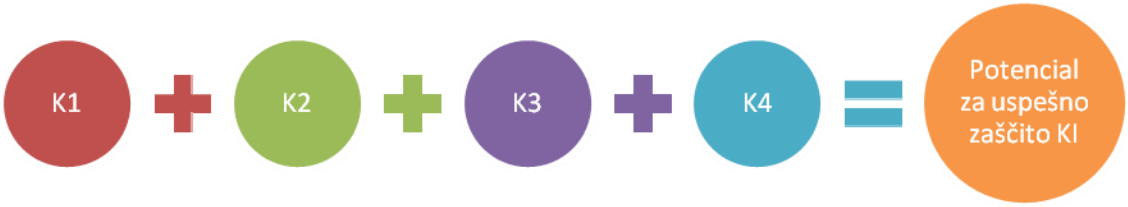
d) Če obstaja zaščita KI, ali je ta zaščita transparentna v smislu dostopnosti informacij na vseh ravneh (državni, javni, lokalni, mednarodni itd.)?

Menim, da imajo ZDA, Nemčija, Švica in Nizozemska zelo transparentno zaščito KI, v smislu dostopnosti informacij za širšo javnost. Tako sem sklepala predvsem na osnovi informacij, ki jih lahko pridobimo na njihovih spletnih straneh, dostopnosti uradnih in drugih dokumentov ter ne nazadnje tudi neposrednih rezultatov izvedenih študij (Švica in Nizozemska). Tega pri Franciji in VB nisem zasledila, saj nisem našla veliko oziroma skoraj ničesar v povezavi z zaščito KI. Podatki so bili zelo pomanjkljivi v primerjavi z ostalimi štirimi državami. Vsekakor mislim, da je transparentnost eden od kazalcev odprtega sistema in s tem tudi demokratične države. Po mojem mnenju je vsak državljan v času krize pomemben dejavnik zaščite KI, zato bi morala biti obveščena širša javnost na nacionalni in tudi mednarodni ravni, saj ponavadi krize ne poznajo geografskih meja. Verjetno bi se našli tudi ljudje, ki bi nasprotovali popolni transparentnosti zaščite KI, saj so nekatere informacije samo za vodstveni krog ljudi, ki

odloča o usodi KI na nacionalni in mednarodni ravni. Kateri sistem je boljši, transparentni ali netransparentni, verjetno lahko vsaka država in mednarodna skupnost presodi po preteklih izkušnjah (naravne nesreče, terorizem ipd.).

Kaže, da so izkušnje vseh držav sveta največji kazalec razvoja vedno bolj uspešne zaščite KI. Vsi vemo, da se na izkušnjah učimo in posledično postajamo vedno močnejši ter s tem odpornejši. Vsaj tako naj bi bilo po nekem racionalnem postopku, tudi pri razvoju in opredeljevanju zaščite KI. Če povzamem, vse zgoraj naštete države stremijo k nadgradnji obstoječe (predvsem ZDA) ali pa k izgradnji še neobstoječe/slabe zaščite KI (predvsem Francija). Dejstvo pa je, da se vse bolj zavedajo pomembnosti KI, katere uničenje ali slabšanje ima lahko resne posledice za obstoj ali nadaljnji razvoj družbe na lokalni, državni ali mednarodni ravni in v prihodnosti tudi na ravni vesolja (EU).

Po mojem mnenju je treba za uspešno zaščito KI upoštevati vse štiri temeljne kazalce, in sicer: nacionalno strategijo kot kazalec natančne opredelitve KI (*K1*), njeno umeščanje v širši okvir varnosti države (*K2*) ter obravnavanje kot enega od ciljev strategije varnosti države. Sledi sodelovanje države z zasebnimi lastniki KI (*K3*) kot kazalec fleksibilnosti in prilagodljivosti sistema zaščite KI v vedno bolj kompleksnih odnosih odgovornosti. Če temu dodam še transparentnost (*K4*) kot kazalec najvišje stopnje odgovornosti in zaupanja v javnost, dobimo sistem, ki je za državo primarni cilj delovanja. Vsi štirje kazalci torej skupaj tvorijo potencial za uspešno zaščito KI v sodobnih družbenih tvorbah, kakor prikazuje preprosta formula:



Vemo, da je za uspešno zaščito kakršnegakoli sistema, v našem primeru kritične infrastrukture, potrebna določena mera finančne injekcije. Potemtakem mora vsaka država presoditi, koliko bo vložila v zaščito posameznih kritičnih sektorjev in zakaj je temu tako. V nadaljevanju si bomo ogledali pretekla in sedanja finančna vlaganja ZDA in EU.

2.4 ZAŠČITA KRITIČNE INFRASTRUKTURE: EKONOMSKI VIDIK

Pri zbiranju in pregledovanju različnih virov sem pridobila zlasti podatke o finančnih vlaganjih v zaščito kritične infrastrukture ZDA in EU. Tovrstnih podatkov v povezavi z ostalimi državami nisem zasledila, zato sem te izključila iz nadaljnje analize. Sprva bom torej posebej obravnavala finančna vlaganja v zaščito KI v ZDA in nato še v EU, za konec pa bom finančna vlaganja na področju zaščite KI v ZDA in EU še primerjala.

2.4.1 Finančna vlaganja v zaščito kritične infrastrukture ZDA

V času od leta 2002 je DHS državi namenil skoraj 3 milijarde dolarjev subvencije za KI, z namenom povečanja moči države proti grožnjam, ki so povezane s terorističnimi napadi, naravnimi nesrečami in drugim. Leta 2005 je država prejela več kot 344 milijonov dolarjev subvencij, za leti 2006 in 2007 pa več kot 171 milijonov dolarjev. Letos je bilo temu namenjenih več kot 848 milijonov dolarjev, kar je tudi več kot katerokoli leto prej (DHS: Fact Sheet: Critical Infrastructure and Homeland Security Protection Accomplishments. Dostopno prek: http://news.tradingcharts.com/futures/7/4/113338447. Html (21. september 2008)).

Letos je DHS subvencije namenil za zaščito KI pristanišč, tranzitnih sistemov[36] in ostalih sestavin nacionalne KI.

Subvencijski programi so se za zaščito KI za fiskalno leto 2008 povečali za 29 %, in sicer je DHS pristaniščem namenil 388,6 milijona dolarjev, podpira vzdržljive sisteme dostopnosti, ščiti pred improviziranimi eksplozivnimi napravami in ostalimi nekonvencionalnimi napadi ter organizira vaje s scenariji kriznega odzivanja. Skoraj 221 milijonov dolarjev pripada pristaniščem visoke stopnje ogrožanja, sledi 138 milijonov dolarjev za 40 sekundarnih položajnih območij ter 17 milijonov dolarjev za 16 terciarnih položajnih pristanišč. Torej so pristanišča od leta 2003 prejela že skoraj 1,5 milijarde dolarjev subvencijske pomoči od države.

[36] Sem vključujemo mostove, ceste, avtoceste, vodni promet, kot so trajekti in podobno.

DHS je razdelil 380,1 milijona dolarjev za tranzitne varnostne sisteme, katerih cilj je boj proti grožnjam, ki lahko povzročijo veliko škodo komerciali in tudi povzročijo izgubo življenj. Več kot 333 milijonov dolarjev je bilo namenjenih osmim velemestnim območjem visoke stopnje ogrožanja. Približno 5 milijonov dolarjev je namenjenih varnostnim železniškim sistemom tovora in 25 milijonov dolarjev za medmestni železniški potniški sistem. Od leta 2005 je DHS subvencioniral tranzitne sisteme za približno 921 milijonov dolarjev.

Nekaj več, okoli 11,2 milijona dolarjev je namenjenih operacijam določenih medmestnih in »čarterskih« avtobusnih podjetij, ki služijo eni ali več definiranim sodnim vejam. Torej gre za zaščito visokostopenjskih posledic tveganja, antiteroristična usposabljanja, pripravljenost na vaje itd.

Približno 48,5 milijona dolarjev gre nevtralnim conam, ki podpirajo državno in lokalno varnost ter krizni menedžment za zaščito kemičnih tovarn, jedrskih elektrarn in drugih predelov visoke stopnje tveganja. Od leta 2005 je bilo nevtralnim conam namenjenih 236 milijonov dolarjev.

Nazadnje je tu še prevozništvo (špedicija), kateremu je namenjenih 15,5 milijona dolarjev, kjer subvencijski program obsega identifikacijo in usposabljanje sodelujočih, načrtiranje, komunikacijo in analizo informacij ter distribucijo. Od leta 2003 je bilo varnosti prevozništva namenjenih 78 milijonov dolarjev (dostopno prek: http://govexec.com/story_page.cfm?articleid=40050&ref=rellink (21. september 2008)).

Tabela 2.18: Primerjava subvencij DHS, namenjenih zaščiti KI za leto 2006, 2007 in 2008

Subvencijski program za KI	Leto 2006	Leto 2007	Leto 2008
Tranzitni sistem	$ 143.240.948	$ 171.780.000	**$ 380.100.000**
Pristanišča	$ 168.052.500	$ 201.170.000	**$ 388.600.000**
Medmestni avtobusni sistem	$ 9.503.000	$ 11.640.000	**$ 11.200.000**
Prevoznički sistem	$ 4.801.500	$ 11.640.000	**$ 15.500.000**
Nevtralne cone	$ 72.965.000	$ 48.500.000	**$ 48.500.000**

VIR: U. S. Department of homeland security, Office of grants and training (2007, 2).

Tabela 2.19: Primerjava subvencijskih razlik programov zaščite KI DHS med posameznimi leti

Razlike med leti	Δ 06/07 v %	Razlika 06/07 v $	Δ 07/08 v %	Razlika 07/08 v $	Δ 06/08 v %
Tranzitni sistem	+16,6 %	28.539.052	+ 54,8 %	208.320.000	+62,3 %
Pristanišča	+16,5 %	33.118.000	+48,2 %	187.430.000	+56,7 %
Medmestni avtobusni sistem	+18,35 %	2.137.000	-3,7 %	-444.000	+15,15 %
Prevozniški sistem	+58,75 %	6.838.500	+24,9 %	3.860.000	+69 %
Nevtralne cone	-33,52 %	-24.465.000	0,0 %	enako	-33,52 %

Iz zgornjih tabel (Tabeli 2.18 in 2.19) lahko razberemo, da so se subvencije DHS iz leta v leto skoraj na vseh področjih večale. Subvencije za tranzitni sistem so se od leta 2006 do 2007 povečale za 16,6 %, od leta 2007 do 2008 pa kar za 54,8 %.

ZDA svoje tranzitne sisteme postavljajo na drugo mesto zaščite s 380.100.000 dolarjev subvencijske pomoči. Najpomembnejše, vlada ZDA poudarja zaščito vseh pristanišč, in sicer se je delež subvencij zanje od leta 2006 do 2008 povečal za 56,7 %, kar je 5,6 % manj kot za tranzitni sistem enakega obdobja. Tretje mesto po višini subvencij pripada nevtralnim conam, kljub temu da se je delež od leta 2006 zmanjšal za 33,52 %. Pri prepisovanju podatkov so kot opombo navedli, da so leta 2006 prišteli zaščitni program nevtralne cone v vrednosti 25.000.000 dolarjev. Če to odštejemo, dobimo 47.965.000 dolarjev, kar je približno enako kot za leto 2007 in 2008.

Zgornja tabela (Tabela 2.19) kaže, da se je od 2006 do 2008 največ subvencij povečalo na področju prevozniških/tovornih sistemov, kar nam da vedeti, da ZDA vedno bolj vlagajo v zaščito ekonomskega transferja in posledično v stabilno gospodarsko rast. Ne nazadnje je tu še medmestni avtobusni sistem, kateremu je namenjeno najmanj subvencij; delež se je od leta 2006 do danes povečal le za 15,15 %.

Posebej moram omeniti še, da je DHS prvič za leto 2008 namenil dodatnih 4,9 milijona dolarjev za operaterje železniškega sistema ter 25 milijonov dolarjev za medmestni program potnikov železnic (obstaja od leta 2005, vendar za 2006 in 2007 nisem zasledila podatkov), kjer gre v obeh primerih za usposabljanje zaposlenih, utrjevanje območij delovanja in podobno (Chunovic 2008).

Videti je torej, da DHS iz leta v leto namenja več subvencij za programe zaščite KI, ki po mnenju države dosega najvišjo stopnjo tveganja posledic morebitne grožnje. Vsekakor je to eden od kazalcev, da se ZDA zavedajo kritičnosti svoje infrastrukture ter posledic, ki lahko sledijo po napadu na tovrstno KI. V nadaljevanju bom analizirala, ali financiranje EU na področju zaščite KI daje enake oziroma podobne rezultate kot subvencioniranje zaščite KI v ZDA.

2.4.2.1 Finančna vlaganja v zaščito kritične infrastrukture EU

2.4.2.2 Financiranje Evropskega programa za zaščito kritične infrastrukture

»Green paper« EPCIP jasno poudarja vire financiranja za aktivnosti, ki so povezane z zaščito KI v Evropi. Komisija EU je pripravljena sodelovati pri financiranju KI, kot so relevantne študije in razvoj specifičnih metod. Informacijskih posodabljanj komisija ne bo financirala in je potrebno poiskati druge vire fundacij.

Program EPCIP se torej lahko enako financira kot letni program Prevention, Preparedness and Consequence management of Terrorism – v povezavi s tem bom predstavila rezultate za leto 2007 in 2008.

Zaveza financiranja Komisije za povečanje varnosti evropske KI je bila demonstrirana preko pilotskega projekta z imenom Boj proti terorizmu leta 2005, s subvencijami v vrednosti 3,7 milijona evrov.

2.4.2.3 Financiranje Evropskega programa za zaščito kritične infrastrukture preko pilotskega projekta

Splošne trditve pilotskega projekta so za leto 2006 v prvi vrsti poudarjale splošni proračun EU, ki bi omogočal boj proti terorizmu in povečanju aktivnosti družbe za varnost državljanov. Eno od pomembnejših točk v pilotskem projektu programa za zaščito KI predstavlja podpora aktivnosti, povezanih s specifičnimi trditvami za povečanje zaščite KI. V letu 2007 je bilo predlaganih 3 milijone € subvencij za zaščito KI v EU, leta 2008 pa 15,2 milijona €, torej 12,2 milijona več (dostopno prek: http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm (23. september 2008)).

2.4.2.4 Proračun za letni program Prevention, Preparedness and Consequence management of Terrorism

Proračun zgoraj omenjenega programa obsega štiri skupine zaščite (glej Tabelo 2.20), in sicer: nacionalne in transnacionalne projekte, subvencije stalnih teles, subvencije skupnega raziskovalnega centra in javno preskrbo s strani komisije. Za leto 2007 je bilo za program Prevention, Preparedness and Consequence management of Terrorism skupno namenjenih 12,7 milijona evrov in ne 3 milijoni, kot so v začetku predlagali. Za razliko od leta 2008 je bilo za zaščito KI namenjenih za 2,5 milijona evrov manj. Katera področja so dobila več denarja in katera manj, bom prikazala v nadaljevanju.

Tabela 2.20: Primerjava proračuna programa Prevention, Preparedness and Consequence management of Terrorism za leto 2007 in 2008

Skupina zaščite	Predviden proračun za leto 2007	Predviden proračun za leto 2008	Δ 07/08 v €
Nacionalni in transnacionalni projekti (s predlogom)	€ 10,4 milijona	€ 11,8 milijona	€ 1,4 milijona
Subvencije stalnih teles (brez predloga)	€ 0	€ 0,3 milijona	€ 0,3 milijona
Subvencija skupnega raziskovalnega centra	€ 0	€ 1,8 milijona	€ 1,8 milijona
Javna preskrba s strani Komisije	€ 2,3 milijona	€ 1,3 milijona	€ -1 milijon
Skupaj	**€ 12,7 milijona**	**€ 15,2 milijona**	**€ 2,5 milijona**

VIR: Justice and home afairs 2007 in 2008.

a) Subvencije, namenjene nacionalnim ali transnacionalnim projektom

Za leto 2007 je bilo temu področju namenjenih 10,4 milijona € in za leto 2008 11,8 milijona € subvencij, ki so se razporedile med posameznimi področji (Tabela 2.21).

Poleg namenjenih subvencij je pomembno, da je Komisija za posamezne projekte pripravljena nameniti 70 % vrednosti projekta, ne odobri pa projektov, ki stanejo manj kot 50.000 € (obe leti enaka vsota) in stanejo več kot 750.000 € (za leto 2007) oz. 1,1 milijona € (za leto 2008). Torej so za leto 2008 povečali zgornjo mejo za kar 350.000 evrov. Po mojem mnenju subvencijske meje zelo omejujejo dejansko izvedbo nekaterih projektov, saj ni nikjer zagotovljeno, da bodo dobili subvencije kje drugje. Tega pri subvencioniranju v ZDA nisem zasledila, kar predstavlja večjo odgovornost in zaupanje države v projekte za zaščito KI. Mislim, da se EU vse bolj zanaša na posamezne države članice, namesto da bi pristopala bolj kot vodilna entiteta, ki usmerja članice na vseh področjih in jim tudi ustrezno pomaga na področju financiranja ter same zaščite KI, ker same morda tega niso sposobne.

Tabela 2.21: Primerjalna tabela subvencij EU za leto 2007 in 2008, namenjenih za zaščito KI

SEKTORJI	LETO 2007 v €	LETO 2008 v €	Δ 07/08 v €
Energija	2 milijona	3,2 milijona	+1 milijon
Nuklearna industrija	600.000	Ni subvencij	-600.000
Informacijska tehnologija	1,6 milijona	3 milijoni	+1,4 milijona
Voda	800.000	450.000	-350.000
Hrana	500.000	450.000	-50.000
Zdravje	400.000	700.000	-300.000
Finance	600.000	500.000	-100.000
Transport	900.000	1,5 milijona	+600.000
Kemična industrija	500.000	1 milijon	+500.000
Vesolje	500.000	Ni subvencij	-500.000
Raziskovalne institucije	400.000	400.000	0
Splošni projekti (komunikacija, sodelovanje med članicami itd.)	1,6 milijona	600.000	-1 milijon

VIR: Justice and home afairs 2007 in 2008.

Ne glede na finančne omejitve subvencij je EU vseeno določila subvencije za 12 posameznih področij, ki so se od leta 2007 do 2008 spremenile. Zanimivo je, da za leto 2008 ni namenjene nobene subvencije za nuklearno industrijo in vesolje. Nuklearna industrija se vse bolj ukinja in nadomešča z ostalimi alternativami, vesolje pa je glede na izbrane evropske države (omenjene v diplomski nalogi) in ZDA le EU opredelila kot enega od kritičnih sektorjev. Torej je zelo verjetno EU prišla do zaključka, da vesolje vseeno ni področje zaščite KI in trenutno spada bolj v razvoj in raziskave v znanosti. Na račun zmanjšanja subvencij na področju vode, hrane, zdravja, financ in splošnih projektov se je v letu 2008 povečal proračun za zaščito informacijske tehnologije, kar dokazuje vse večjo pomembnost le-te. Tega pri ZDA ne opazimo, ker se znotraj petih področij namenja denar tudi za informacijsko tehnologijo, ne vemo pa, kolikšen znesek v celoti gre dejansko v ta namen (Justice and home afairs 2007 in 2008).

b) Subvencije, namenjene javni preskrbi s strani Komisije

Omenjenih subvencij medsebojno ne morem primerjati, ker se spreminjajo vsako leto posebej, zato bom navedla le celotno vsoto, ki za leto 2007 znaša 2,3 milijona € in za leto 2008 1,3 milijona €, torej milijon manj v primerjavi s prejšnjim letom. Iz tabele (Tabela 2.20) razberemo, da je EU na račun manjšega vlaganja v navedena področja za leto 2008 namenila več subvencij stalnih teles in subvencij skupnega raziskovalnega telesa, kar v letu 2007 sploh ni bilo opredeljeno.

c) Subvencije stalnih teles (CEN) in skupnega raziskovalnega centra (JRC)

Na tem mestu gre za subvencije Evropskega komiteja v zvezi s standardizacijo (CEN) aktivnosti na področju zaščite KI, čemur se namenja 300.000 €. S subvencijami skupnega raziskovalnega centra (JRC) pa so financirana naslednja področja:

- študija za identificiranje racionalnega in predlogi za kriterije imenovanja evropskega kritičnega komuniciranja in informacijske infrastrukture v podsektorju instrumentov in kontrole sistema – 350.000 €,
- študija radiofrekvence, ki ogroža telekomunikacije in kontrole sistema informacijske tehnologije – 400.000 €,
- tehnična znanja in podpora proti boju različnim grožnjam in odpravljanja ranljivosti skladiščenja različnih eksplozivnih sredstev – 400.000 €,

- zaznavanje visoko prioritetnih kemičnih in bioloških agentov – 350.000 €,
- podpora mehanizma izmenjave informacij na področju zaščite KI – 300.000 €.

EU namenja 1,8 milijona € raziskovalnemu področju in 300.000 € za standardizacijo področja zaščite KI, skupaj 2,1 milijona €. Zgoraj naštetih pet študij kaže, da program resnično zaščito KI opredeljuje kot del programa za zaščito pred terorističnimi grožnjami. Torej se zaščita KI subvencionira v sklopu varnosti celotne EU pred tovrstnimi grožnjami. V naslednjem poglavju bom s primerjalno analizo subvencij za zaščito KI ugotavljala podobnosti in razlike med EU in ZDA.

2.4.2 Primerjalna analiza finančnih vlaganj zaščite kritične infrastrukture ZDA in EU

Zaradi lažje predstave bom sistema primerjala po naslednjih točkah, in sicer:

1. Oba sistema, tako ZDA kot EU, povečujeta subvencije za zaščito KI.
2. ZDA obravnavajo zaščito KI kot samostojen sistem subvencij, medtem ko EU obravnava zaščito KI kot del sistema subvencij za zaščito pred terorističnimi grožnjami.
3. EU se pri subvenciji zaščite KI usmerja bolj v subvencioniranje projektov, ki so podobni področju R & D (raziskav in razvoja), kateremu ZDA posebej namenjajo denar, ločeno od sistema subvencij zaščite KI.
4. Oba sistema subvencioniranja imata finančne omejitve, s tem da EU omejuje tudi minimalno in maksimalno raven subvencioniranja, ki predstavlja problem izvedbe nekega določenega projekta.
5. ZDA opredeljujejo 5 glavnih področij subvencioniranja zaščite KI, medtem ko ima EU v letu 2007 dva področji in v letu 2008 štiri področja subvencij zaščite pred terorističnimi grožnjami.

Ugotovitve nakazujejo, da sistemov ZDA in EU ne moremo enako obravnavati, saj imata obe entiteti različne pristope identificiranja zaščite KI in njenega vrednotenja. V ZDA zaščito KI obravnavajo kot samostojen sistem, ki si zasluži celostno obravnavo in tudi ločeno subvencioniranje, česar za EU ne moremo trditi. Vsekakor je finančni vidik pokazal, kako pravzaprav narašča oziroma upada pomen zaščite KI v celoti. V začetku

so bile teroristične grožnje tiste, ki so pospešile celoten razvoj zaščite KI v ZDA in kasneje tudi v EU. Danes so teroristične grožnje zamenjale naravne katastrofe, ki velikokrat s seboj prinašajo večjo škodo in uničenje zaščite KI, kar iz leta v leto zahteva večja finančna vlaganja; o tem priča primer ZDA in tudi EU.

Vsi kazalci, našteti in opredeljeni v diplomski nalogi, tvorijo neko celoto raziskovalnega problema, kar bom nadalje pokazala z verifikacijo hipotez. S tem sem pridobila željeni odgovor na zastavljene hipoteze v začetku naloge, ki so služile kot vodila pri raziskovanju in analiziranju.

3 SKLEP

Že v času ženevskih konvencij v letu 1949 so se nekatere države (države podpisnice) pričele zavedati, kako pomembno je zaščititi človeška življenja in tudi druge dobrine, ko potekajo različne oblike vojaških bojevanj. Do danes sta se seznam groženj in njihova intenziteta tako povečala, da se države zavedajo potrebe po zaščiti čim širšega spektra tistih delov družbe, ki so nujni za njeno preživetje in obstoj. Iz tega izhaja pričujoča diplomska naloga, ki poudarja vse večji pomen zaščite tiste infrastrukture, katere uničenje ali poslabšanje vodi v začasno ali trajno nestabilnost celotne družbe. V kritično infrastrukturo prištevamo finančne sisteme, kmetijstvo, prvo pomoč, transportni sistem, energijo, telekomunikacije, informacijski sistem in podobno. Našteto predstavlja osnovni model, ki ga vsaka država definira posebej, glede na lastno videnje elementov kritične infrastrukture. Ne glede na različna pojmovanja kritične infrastrukture velja, da le-ta zajema posamezne sisteme, ki skupaj tvorijo omrežja odnosov. Prav zaradi tega je zaščita kritične infrastrukture svojevrsten izziv, saj so ti odnosi številni, med seboj odvisni in kompleksni.

Zanimalo me je, kako se nekoč ekonomsko in vojaško najmočnejša država, ZDA, sooči z zagotavljanjem zaščite tako kompleksnega sistema, kot je kritična infrastruktura. Verjetno največja preizkušnja ZDA je bil prav mejnik 11. septembra 2001, ko so porušili simbol njihove ekonomske in varnostne stabilnosti. Od takrat naprej so ZDA začele intenzivno vlagati v zaščito kritične infrastrukture v primeru terorističnih groženj in vse pogostejših naravnih katastrof. S primerjalno analizo ZDA in EU kot mednarodne organizacije ter Francije, Nemčije, Nizozemske, Švice in Velike Britanije sem ugotavljala, ali imajo ZDA razvito zaščito kritične infrastrukture. Razvitost sem merila s številnimi indikatorji in prišla do zaključkov, opisanih v nadaljevanju.

V začetku sem raziskovala, kako posamezna država ali EU pojmuje kritično infrastrukturo. Odkrila sem – navkljub različnim definicijam – skupno značilnost, in sicer, da je po pojmovanjih kritična infrastruktura tista, katere uničenje/slabitev posledično prinaša negativen razvoj vseh pomembnih družbenih razsežnosti (okolja, sociale, informacijske tehnologije, politike, ekonomije, demografije in podobnega). Menim, da kritično infrastrukturo najbolj celostno definirajo ZDA in EU, ki zajemajo

vse elemente definicij ostalih držav in k temu dodajajo še virtualno pojmovanje kritične infrastrukture. Zaradi tega lahko potrdim prvo posebno hipotezo: ***»V ZDA je razumevanje fizične in virtualne družbene razsežnosti kritične infrastrukture bolj celostno opredeljeno v primerjavi s Francijo, Nemčijo, Nizozemsko, Švico in Veliko Britanijo.«*** ZDA opredeljujejo in omenjajo tako fizično kot virtualno kritično infrastrukturo, česar Francija, Nemčija, Nizozemska, Švica in Velika Britanija ne storijo. Torej se ZDA zavedajo, da je današnji čas prepleten s številnimi grožnjami, ki v prvi vrsti ogrožajo informacijsko tehnologijo. Pri raziskovanju pojma kritične informacijske infrastrukture sem ugotovila, da analitiki različno pojmujejo informacijsko infrastrukturo. Nekateri strokovnjaki menijo, da je podrejena zaščiti kritične infrastrukture, drugi pa menijo, da kritična informacijska infrastruktura povezuje vse kritične sektorje. Ne glede na strokovna neskladja velja, da živimo v obdobju hitrega razvoja informacijske tehnologije. Vemo, da prav ta povezuje vse sisteme od osebnega bančništva do vodenja kompleksnih transportnih sistemov. Informacijska tehnologija torej povezuje vse kritične sektorje, ki tvorijo celotno kritično infrastrukturo. Če preneha delovati informacijska tehnologija, ki predstavlja sestavni del vseh kritičnih sektorjev, preneha delovati celotna mreža zaščite kritične infrastrukture.

Omenjeno pritrjuje naslednjemu raziskovalnemu vprašanju, in sicer: ***»V času novih oblik groženj družbi je vse bolj pomembna zaščita informacijske kritične infrastrukture, ki predstavlja vitalni del družbenega razvoja.«*** Zanimivo, da ZDA in EU priznavajo in upoštevajo virtualne grožnje, medtem ko ostale izbrane države tega ne omenjajo. Vsi vemo, da ima vsaka družba svoje tako imenovane hekerje, ki le z eno potezo lahko uničijo ali začasno oslabijo delovanje enega in s tem številnih ostalih sistemov. »Domino-efekt« je lahko še večji, če ga povzroči organizirana skupina, kjer poteka dolgotrajno kibernetsko bojevanje. Dejstvo je, da so ZDA med prvimi državami, ki so začele raziskovati informacijsko omrežje in zaradi tega bolje razumejo posledice njegovega razdejanja. Kljub temu menim, da bi morale tudi vse ostale države bolje razumeti posledice uničenja ali slabitve informacijske infrastrukture na ta način, da jo priznajo kot potencialno grožnjo pri zaščiti celotne kritične infrastrukture.

ZDA in EU torej priznavajo vse oblike groženj, fizične in virtualne, ki lahko ogrozijo obstoj zaščite kritične infrastrukture. Da bi zagotovili relativno uspešno zaščito kritične infrastrukutre, so potrebna nenehna finančna vlaganja. Na splošno tako ZDA kot EU

povečujejo svoja finančna vlaganja v zaščito kritične infrastrukture. Razlika je ta, da ZDA kritično infrastrukturo obravnavajo kot samostojen sistem, medtem ko jo EU obravnava kot del sistema subvencij za zaščito pred terorističnimi grožnjami. Menim, da so ZDA z zgodnjim razumevanjem pomena zaščite kritične infrastrukture (leta 1983) in z oblikovanjem potrebnih zaščitnih ukrepov v prednosti pred EU, ki se je s tem šele pričela ukvarjati. EU pravzaprav še danes nima potrjenega sistema zaščite kritične infrastrukture in vsa omenjena dokumentacija zluži zgolj kot predlog, ki se bo morda nekoč uveljavil. Zato lahko potrdim zadnjo posebno hipotezo, ki pravi: ***»Večja finančna vlaganja v zaščito kritične infrastrukture in tradicija opredeljevanja potrebnih ukrepov dajejo prednost ZDA pred EU.«***

Do sedaj raziskano me je vodilo do splošnega raziskovalnega vprašanja, ki je utemeljeno skozi naslednje vsebinske sklope: kritični sektorji, organizacijski vidik, normativne podlage, pobude in iniciative ter nazadnje že omenjeni ekonomski vidik zaščite kritične infrastrukture, ki sem ga uvrstila v posebno, predhodno navedeno raziskovalno vprašanje.

V prvem sklopu kritičnih sektorjev sem ugotavljala, koliko kritičnih sektorjev posamezna država in EU kot mednarodna organizacija pravzaprav opredeljuje. Od vseh naštetih jih največ opredeljujejo ZDA. Kljub temu ima večina izbranih držav in EU svoje kritične podsektorje, česar Francija in ZDA nimajo. Menim, da bolj razčlenjen in natančno opredeljen seznam kritičnih sektorjev s podsektorji nosi potencial za boljše oblikovanje zaščite kritične infrastrukture. Poleg tega sem raziskala tudi obstoj posebnega kritičnega sektorja informacijske tehnologije in ostalih specifičnih sektorjev. ZDA edine posebej opredelijo kritični sektor informacijske tehnologije, medtem ko jo ostale države in EU združujejo s telekomunikacijami ali pa je sploh ne opredeljujejo. Na področju specifičnih sektorjev je v ospredju Nemčija, sledijo ZDA in EU, druge države omenjajo en specifični sektor ali pa nobenega. Vsi izbrani vsebinski sklopi nakazujejo, da ZDA na področju kritičnih sektorjev niso nič bolj razvite v primerjavi z izbranimi evropskimi državami in EU kot mednarodno organizacijo.

Z organizacijskega vidika zaščite kritične infrastrukture sem raziskovala naslednje vprašanje: ali ima izbrana država centralizirano/decentralizirano zaščito kritične infrastrukture, kdo je glavni nosilec zaščite kritične infrastrukture, kakšno je število

partnerskih povezav javnega in zasebnega sektorja zaščite informacijske kritične infrastrukture ter letnica nastanka/oblikovanja partnerstva javnega in zasebnega sektorja zaščite informacijske kritične infrastrukture. Analiza je pokazala, da so ZDA edine, ki imajo centralizirano zaščito kritične infrastrukture, katere glavni nosilec je Ministrstvo za domovinsko varnost. Slednje je odgovorno za večino zaščite kritične infrastrukture v ZDA in ima vlogo koordinatorja, nadzornika in nosilca odgovornosti. V ostalih državah imajo glavni nosilci odgovornosti samo eno od treh vlog, bodisi nadzirajo, koordinirajo ali so delno odgovorni.

Pri državni organizaciji zaščite kritične infrastrukture sem upoštevala in vključila tudi organizacijsko povezovanje javnega in zasebnega sektorja na področju zaščite kritične infrastrukture, ker nosi večinski delež lastništva (v ZDA 85 %). Predvsem so me zanimala pomembnejša državna partnerstva javno - zasebno na področju informacijske KI, ki so vse bolj pomembna. Ugotovila sem, da imajo teh največ v ZDA, k čemur ni prispevala povprečna letnica nastanka vseh povezav javno - zasebno v ZDA, saj so glede na to od vseh držav na predzadnjem mestu. Slednje nam služi kot dejstvo, da tradicija ni tista, ki pogojuje uspešnejši razvoj in obstoj zaščite kritične infrastrukture ter informacijske kritične infrastrukture. Vsekakor pa tradicija nakazuje, kdaj se je posamezna država pričela s tem ukvarjati in se zavedati pomembnosti zaščite kritične infrastrukture ob sodelovanju zasebnega in javnega sektorja na področju zaščite informacijske kritične infrastrukture. Glede na ugotovitve trdim, da imajo ZDA bolj razvito zaščito kritične infrastrukture z organizacijskega vidika, saj imajo zelo centralizirano zaščito, največ povezav javnega sektorja z zasebnim, čeprav so se v povprečju od vseh izbranih držav (razen Nizozemske) najkasneje pričele ukvarjati z vprašanjem sodelovanja države z zasebnimi lastniki na področju informacijske kritične infrastrukture.

Po analizi organizacijskega vidika sem se usmerila na raziskovanje temeljev definiranja zaščite kritične infrastrukture. Raziskala sem normativne podlage, pobude in iniciative zaščite kritičnih sektorjev izbranih držav in EU kot mednarodne organizacije. V tem vsebinskem sklopu me je zanimalo, ali ima posamezna država nacionalno strategijo, uradno potrjeno sodelovanje javnega in zasebnega sektorja, ali je za državo pomembna zaščita kritične infrastrukture in nazadnje, ali je sistem zaščite kritične infrastrukture transparenten. Skoraj vse države imajo oziroma razvijajo nacionalno strategijo zaščite

kritične infrastrukture (razen Francije). Vse države in EU priznavajo pomembnost sodelovanja privatnega z zasebnim sektorjem, kjer je poudarjen tudi pomen zaščite celotne kritične infrastrukture. V korelaciji z naštetim je tudi transparentnost zaščite kritične infrastrukture, ki je v večini držav zelo velika. Torej obstaja veliko podatkov o zaščiti kritične infrastrukture, ki so dostopni širši javnosti. Če opazujemo sedanje stanje (upoštevamo, da Švica in Nizozemska še nimata nacionalne strategije), ZDA in Nemčija nosijo potencial za uspešno zaščito kritične infrastrukture, saj zagotavljajo vse štiri omenjene vsebinske sklope. Iz tega izhaja, da je zaščita kritične infrastrukture ZDA na področju normativnih aktov, pobud in iniciativ bolj razvita kot v večini izbranih držav (razen Nemčije) in EU kot mednarodni organizaciji.

Tako sem potrdila splošno raziskovalno hipotezo, ki se glasi: ***»Zaščita kritične infrastrukture v ZDA je bolj razvita v primerjavi z izbranimi državami in EU kot mednarodno organizacijo.«*** ZDA so glede na štiri raziskane vsebinske sklope v treh bolj razvite, in sicer na področju finančnih vlaganj, z organizacijskega vidika in nazadnje pri normativnih podlagah, pobudah in iniciativah, glede na kritične sektorje pa so enakovredne. Zaščita kritične infrastrukture zajema številne elemente, ki jih je za uspešno in stabilno delovanje potrebno povezati v celoto. Ključni elementi, ki jih posamezna država mora imeti, so naslednji: dobro uzakonjena in uradno potrjena zaščita kritične infrastrukture, organizacija številnih med seboj povezanih subjektov, nenehna finančna vlaganja in še mnogo drugih pomembnih segmentov zaščite kritične infrastrukture. Menim, da so ZDA uspešno povezale vse pomembne elemente, kar se v sedanjem času kaže v relativno uspešnem odzivanju na naravne katastrofe in s tem v zaščiti kritične infrastrukture. Kot pravi Ritter (2003, 1–2), pa je nemogoče doseči 100-odstotno varnost kritične infrastrukture in nobena država ne pozna idealne poti reševanja problemov.

Ker človek nenehno teži k raziskovanju neznanega in razvijanju še boljšega načina odkrivanja ter odpravljanja problemov, sem prepričana, da bomo v prihodnje razvili boljše in uspešnejše načine zaščite kritične infrastrukture.

4 LITERATURA

1. Abelle-Wigert, Isabelle in Myriam Dunn, ur. 2006. *International CIIP hand book 1*. Center for Security Studies: ETH Zurich.
2. Abelle-Wigert, Isabelle in Myriam Dunn, ur. 2006. *International CIIP hand book 2*. Center for Security Studies: ETH Zurich.
3. Abro, Lateef. 2006. *EU Plans for the Fight against Terrorism: A Review.*Dostopno prek:http://www.gummyprint.com/blog/downloads/EU_Individual_Paper_Lateef_Abro.pdf (30.avgust 2008).
4. *BCS*. Dostopno prek: http.//www.bcs.org/server.php?show=nav.5651 (31. avgust 2008).
5. Boin, A. in P. Lagadec. 2000. Preparing for the Future. Critical Challenges for the Future. *Journal of Contingencies and Crisis Management* 8 (4):186.
6. BSI KRITIS. 2004. Critical Infrastructure Protection. *Survey of World-Wide Activities*. Dostopno prek: http://www.bsi.bund.de/english/topics/kritis/paper_studie_en.pdf (3.september 2008).
7. Bundesministerium des Innern. 2005. Schutz Kritischer Infrastrukturen. *Basisschutzkonzept*. Dostopno prek: http://www.bbk.bund.de (28.avgust 2008).
8. Center for security studies. 2005. *A comparative analysis of cybersecurity initiatives worlwide*. Swiss: Swiss federal institut of technology.
9. *Center for the protection of national infrastructure (CPNI)*. Dostopno prek:http.//www.cpni.gov.uk/About/whatWeDo.aspx (11. avgust 2008).
10. Chunovic, Louise. 2008. DHS announces $844 million critical infrastructure grants. Government security news. Dostopno prek:http.//www.gsnmagazine.com/cms/features/news-analysis/767.html (22. september 2008).
11. *CIA*. Dostopno prek: https.//www.cia.gov/library/publications/the-world-factbook/geos/us.html#Govt (7. avgusta 2008).
12. *CIAO*. Dostopno prek: http.//www.espionageinfo.com/Cou-De/Critical-Infrastructure-Assurance-Office-CIAO-United-States (26. avgust 2008).
13. Commision of European communities. 2004. *Critical Infrastructure Protection in the fight against terrorism*. Dostopno prek:

http://ec.europa.eu/justice_home/doc_centre/criminal/terrorism/doc/com_2004_702_en.pdf (3.september).

14. Commission of the European communities. 2005. *Green paper on a European programm for critical infrastructure protection*. Dostopno prek:http://www.libertysecurity.org/IMG/pdf/EC__Green_Paper_on_CI__17.11.2005.pdf (3.september 2008).
15. Commission of the European Communities. 2006. *The European Programme for Critical Infrastructure Protection (EPCIP)*. Dostopno prek: http://ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm (4.september 2008).
16. *Confederation of Britain industry*. Dostopno prek:http.//www.cbi.org.uk/ndbs/staticpages.nsf/StaticPages/home.html/?OpenDocument (31. avgust 2008).
17. *Conseil strategique des technologies de information*. Dostopno prek:http.//www.csti.pm.gouv.fr/uk/home-uk.html (30. avgust 2008).
18. Councile of the European Union. 2008. *Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection*. Brussels: European union.
19. *CPNI*. Dostopno prek: http.//www.cpni.gov.uk/aboutcpni188.aspx (31. avgust 2008).
20. *Crisis and risk network*. Dostopno prek: http.//www.crn.ethz.ch/ (31. avgust 2008).
21. *Critical Infrastructure and Homeland Security Protection Accomplishments*. Dostopno prek:http.//news.tradingcharts.com/futures/7/4/113338447.html (21. september 2008).
22. *Critical Infrastructure and Key Resources*. Dostopno prek:http.//www.dhs.gov/xprevprot/programs/gc_1189168948944.shtm (23. avgust 2008).
23. *Critical infrastructure protection*. Dostopno prek:http.//www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski.html (16. september 2008).
24. *Critical infrastructure*. Dostopno prek:http.//www.euractiv.com/en/security/critical-infrastructure/article-140597 (2. september 2008).

25. De Bruin, Ronald. 2002. *From Research to Practice. A Public-Private Partnership Approach in the Netherlands on Information Infrastructure Dependability*. Netherlands: Workshop (28.februar 2002).
26. *Department of Justice*. Dostopno prek:http.//www.usdoj.gov/criminal/cybercrime/critinfr.htm#Vc (9. september 2008).
27. *Department of six-point agenda*. Dostopno prek:http.//www.dhs.gov/xabout/history (23. avgust 2008).
28. *DHS*. Dostopno prek: http.//www.dhs.gov/dhspublic/display?theme=37 (24. avgust 2008).
29. *Die neue InfoSurance – Unterstützung für die Basis der Schweizer Wirtschaft*.Dostopno prek: http.//www.infosurance.ch/de/verein.htm (31. avgust 2008).
30. Dovč, Danica. 2005. *Uporaba oblik informacijskega bojevanja v sodobnem terorizmu: Primer teroristične organizacije PKK*. Diplomsko delo. Ljubljana: FDV.
31. Dubrovski, Drago. 2004. *Krizni management in prenova podjetja*.Koper: Fakulteta za management.
32. EU Councile, Justice and home affair councile. 2008. *European critical infrastructure*. Luxembourg: European union. Dostopno prek:http://www.eurunion.org/partner/euusterror/EUCritInfrastructFactsheet-6-5-08.pdf (4.september 2008).
33. *Europe moves ahead on critical infrastructure protection*. Dostopno prek:http.//www.continuitycentral.com/news03978.htm (20. september 2008).
34. *European Programme for Critical Infrastructure Protection*. Dostopno prek:http.//ec.europa.eu/justice_home/funding/2004_2007/epcip/funding_epcip_en.htm (23. september 2008).
35. Executive Office of the president, Office of management and budget. 2004. *Memorandum for the heads of executive departments and agencies*. Washington:White house.
36. *FedCIRC quartely summary report*. Dostopno prek:http.//csrc.nist.gov/topics/incidentNIST/jan97-news.htm (26. avgust 2008).
37. Federal ministry of interior. 2007. *Protection of Critical Infrastructures – Baseline Protection Concept*. Dostopno prek:

http://www.bmi.bund.de/Internet/Content/Common/Anlagen/Broschueren/2007/Basisschutzkonzept__kritische__Infrastrukturen__en,templateId=raw,property=publicationFile.pdf/Basisschutzkonzept_kritische_Infrastrukturen_en.pdf (30.avgust 2008).

38. *Federal ministry of interior*. Dostopno prek:http.//www.bmi.bund.de/cln_012/nn_148164/Internet/Content/Themen/Terrorism/DataAndFacts/Protection__of__critical__infrastructures.html (30. avgust 2008).
39. Federal Office for Civil Protection. 2008. *The Swiss Programme on Critical Infrastructure Protection*. Switzerland. Dostopno prek:http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski.parsysrelated1.82246.downloadList.93673.DownloadFile.tmp/factsheete.pdf (1.december 2008).
40. Federal Office for Information Security. 2005. Critical infrastructure protection in Germany. Dostopno prek:http://cipp.gmu.edu/archive/8_CIPinGermany_2005.pdf (25.oktober 2008).
41. Federal Office for National Economic Supply. 2006. *National economic supply strategy*. Dostopno prek: http://www.bwl.admin.ch/themen/00506/index.html?lang=en (15.oktober 2008).
42. Glad, Betty. 1990. *Psychological Dimensions of War*. *Crisis Management*, ur.Holsti, 116- 142. Newbary Park: Sage Publications.
43. *Global security newsfire*. 2008. Homeland Security Department provides $844 million in critical infrastructure protection grants, (20.maj).
44. Grošelj, Klemen. 2004. *Kognitivno-institucionalna analiza kriznega upravljanja in vodenja (primer nesreče v Sloveniji)*. Magistrsko delo. Ljubljana: FDV.
45. *Hacker's Encyclopedia*. Dostopno prek: http.//insecure.org/stf/hackenc.txt (10. avgust 2008).
46. Henriksen, Stein. 2004. *The Shift of Responsibilities within Government and Society*. Stockholm: CRN Workshop Report.
47. Herman, C.F. 1972. *International Crises. Insight From Behavioral Research*. New York: The Free.
48. Home Office Security. 2003. *Counter-terrorism strategy: Protecting the critical national infrastructure*. Dostopno prek: http.//security.homeoffice.gov.uk/ (27. avgust 2008).

49. *Homeland Security Act* (107–296), 107 kongres. Dostopno prek:http://www.whitehouse.gov/deptofhomeland/bill/hsl-bill.pdf (1.oktober 2008).
50. Homeland security. 2006. *National infrastructure protection program*. USA:Department of homeland security.
51. *Improving the protection of critical infrastructure*. Dostopno prek:http.//www.admin.ch/aktuell/00089/index.html?lang=en&msg-id=13516(31. avgust 2008).
52. *Information assurance advisory councile*. Dostopno prek:http.//www.iaac.org.uk/(31. avgust 2008).
53. *InfraGard*. Dostopno prek: http.//www.infragard.net/ (30. avgust 2008).
54. *Insight the index*. Dostopno prek:http.//www.cgdev.org/section/initiatives/_active/cdi/ inside (22. avgust 2008).
55. International telecommunication union. 2005. *Comparative Analysis of Cybersecurity Initiatives Worldwide*. Geneva: WSIS Thematic Meeting on Cybersecurity.
56. *IWF*. Dostopno prek: http.//www.iwf.org.uk/ (31. avgust 2008).
57. Justice and home afairs. 2007. *Annual work programm 2007 – Prevention, prepardness and consequence management of terrorism and other security related risks.* Dostopno prek: http://ec.europa.eu/justice_home/funding/cips/doc/awp_cips_en.pdf(15.septembe r 2008).
58. Justice and home afairs. 2008. *Annual work programm 2008 – Prevention, prepardness and consequence management of terrorism and other security related risks.* Dostopno prek: http://ec.europa.eu/justice_home/funding/cips/doc/awp_cips_2008_en.pdf (15.september 2008).
59. Kouzmin, Alexander in Alan Jarman. 1989. Crisis Decision making. Towards a Contingent Decision Path Perspective. *Crime, law and social changes* 14 (4): 399-433.
60. L. McGill, William in Bilal M. Ayyub. 2007. *The Meaning of Vulnerability in the Context of Critical Infrastructure Protection*.Arlington: George Mason university.

61. Lenz, Suzanne. 2006. *Critical infrastructure protection in disaster reduction*. Federal office of civil protection and disaster assistance. Center for critical infrastructure protection. Dostopno prek: http://davos2006.idrc.info/Presentations/Lenz_S_Pres.pdf (16.september 2008).
62. *Livre blanc Haut comite Francais pour la defense civile*. 2008. Rapport Défense civile. Dostopno prek: http://www.hcfdc.org/rapport_defciv_HCFDC2008.pdf(30.avgust 2008).
63. Malešič, Marjan. 2004. *Krizno upravljanje in vodenje v Sloveniji*.Ljubljana: FDV.
64. Malešič, Marjan. 2008. *O kriznem upravljanju in vodenju*. Ljubljana: FDV
65. Mednarodno humnitarno pravo. *Protocol Additional to the Geneva Conventions of 12 August 1949 and in relation to Protection of Victims of International Armed Conflicts (Protocol 1)*- Dopolnilni protokol Ženevske konvencije iz leta 1949 in v povezavi z protokolom o žrtvah mednarodnih oboroženih konfliktov, sprejeta 12. avgusta 1949. Dostopno prek:http://www.unhchr.ch/html/menu3/b/93.htm (3.oktober 2008).
66. Ministry of interior and kingdom relations. 2003. *Critical infrastructure protection in Netherlands*. Netherlands: Ministry of the Interior and Kingdom relations.
67. *Ministry of interior and kingdom relations*. Dostopno prek:http.//www.minbzk.nl/bzk2006uk/organisation/organisation-of-the (31. avgust 2008).
68. Moteff, John. 2007. *Critical Infrastructures: Background, Policy, and Implementation*. Congressional research service. Dostopno prek: http://www.fas.org/sgp/crs/homesec/RL30153.pdf (28.avgust 2008).
69. *National cyber security alliance*. Dostopno prek: http.//www.staysafeonline.info/(30. avgust 2008).
70. *National cyber security partnership*. Dostopno prek:http.//www.cyberpartnership.org/init.html (30. avgust 2008).
71. *NCS*. Dostopno prek: http.//www.ncs.gov/ (26. avgust 2008).
72. *Netzwrk fur die zukunft*. Dostopno prek:http.//www.initiatived21.de/en/English.104.0.html (30. avgust 2008).
73. *NISAC*. Dostopno prek: http.//www.sandia.gov/nisac/ (26. avgust 2008).

74. *Non-profit organization for the protection from cyber-criminal*. Dostopno prek:http.//www.ciddac.org (30. avgust 2008).
75. Office for Security in the Information Technology (Bundesamt für Sicherheit in der Informationstechnik). 2007. *Protection of critical infrastructures in Germany*. Dostopno prek: http.//www.bsi.bund.de/fachthem/kritis/index.htm (26. avgust 2008).
76. Office of homeland security. 2002. *National strategy for homeland security*. USA: Homeland security councile. Dostopno prek: http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf (28.avgust 2008).
77. Office of homeland security. 2003. *The Physical Protection of Critical Infrastructures and Key Assets*. USA: The white house. Dostopno prek:http://www.whitehouse.gov/pcipb/physical_strategy.pdf (28.avgust 2008).
78. Office of homeland security. 2007. *National strategy for homeland security*. USA: Homeland security councile. Dostopno prek:http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf (27.avgust 2008).
79. Office of the Press Secretary. 2003. *Homeland Security Presidential Directive/Hspd-7*. Dostopno prek:http.//www.whitehouse.gov/news/releases/2003/12/20031217-5.html (25. avgust 2008).
80. *Panorama Evropske unije*. Dostopno prek:http.//europa.eu/abc/panorama/index_sl.htm (7. avgust 2008).
81. *Partnership for critical infrastructure security*. Dostopno prek:http.//www.pcis.org (30. avgust 2008).
82. *PDD on infrastructure*. Dostopno prek:http.//www.uhuh.com/laws/pdd63.htm#PDD%2062%20and%2063%20Fact%20Sheet%20-%20Summary (10. September 2008).
83. *PDD-63*. Dostopno prek: http.//www.fas.org/irp/offdocs/paper598.htm (10. september 2008).
84. Pederson, P., D. Dudenhoeffer, S. Hartley in M. Permannet. 2006. *Critical Infrastructure Interdependency Modeling. A Survey of U. S. and International Research*.Idaho Falls:Idaho national laboratory.
85. *Présentation générale de l'Association*. Dostopno prek:http.//www.clusis.ch/francais/presentation.htm# (31. avgust 2008).

86. *Presidential Decision Directives*. Dostopno prek:http.//www.epa.gov/rpdweb00/rert/presidentialdirectives.html#pdd62 (10. september 2008).
87. Prezelj, Iztok. 2006. *Teroristično ogrožanje nacionalne in mednarodne varnosti* 1 (8): 20.
88. *Protect infrastructure*. Dostopno prek:http.//ec.europa.eu/justice_home/fsj/terrorism/protection/fsj_terrorism_protection_infrastruct_en.htm (20. avgust 2008).
89. *Protecting the critical infrastructure.* Dostopno prek:http.//security.homeoffice.gov.uk/counter-terrorism-strategy/working-with partners/protect-national-infrastructure/ (31. avgust 2008).
90. Republice of France. 2004–2007. *State Information System Security Reinforcement Plan*. Dostopno prek:http://www.ssi.gouv.fr/site_documents/PRSSI/PRSSI-en.pdf (1.september 2008).
91. Sagadin, Klavdija. 2007. *Teroristični napadi v Beslanu*. Diplomsko delo. Ljubljana:FDV.
92. School of law, George Mason university. 2007. *International Definitions of Critical Infrastructure* 5 (12): 4-7.
93. *Secretariat general de la defense nationale*. Dostopno prek:http.//www.sgdn.gouv.fr/rubrique.php?id_rubrique=20#6 (31. avgust 2008).
94. *Sector-Specific Plan*. Dostopno prek:http.//www.dhs.gov/xprevprot/programs/gc_117986619760shtm#content (24. avgust 2008).
95. Søby, Kristensen Kristian. 2006. *Critical infrastructure protection*. Dostopno prek: http.//www.libertysecurity.org/article734.html (29. avgust 2008).
96. Sruk, Vladimir. 1980. *Filozofsko izrazje in repertoarji*. Murska Sobota: Pomurska založba.
97. Stein Wille, Bernhard Hämmerli, Hartmut Pohl, & Reinhard Posch, ur 2003. *Critical infrastructure protection (CIP)*. Frankfurt: CI Workshop on CIP.
98. Stern, E. 2001. *Crisis Decisin making: A Cognitive-Institutional Approach.A Publication of the Crisis management Europe Research Program* 6 (2):8
99. Škrjanc, Robert. 2004. Terorizem – daleč, a vendar tako blizu. *Obramba* 36:(*10*).

100. *The European Programme for Critical Infrastructure Protection (EPCIP*). 2006. Dostopno prek:http.//europa.eu/rapid/pressReleasesAction.do?reference=MEMO/06/477&format=HTML&aged=0&language=EN&guiLanguage=en (12. avgust 2008).

101. *The institute for information infrastructure protection.* Dostopno prek: http.//www.thei3p.org/ (30. avgust 2008).

102. The White house. 2000. *National plan for Information Systems Protection Version – An invitation to dialogue.* Dostopno prek:http://www.fas.org/irp/offdocs/pdd/CIP-plan.pdf (31.avgust 2008).

103. *The White house*. 2003. Dostopno prek:http.//www.whitehouse.gov/pcipb/physical.html (3. september 2008).

104. U. S. Department of homeland security, Office of grants and training. 2007. *Overwiev – FY 2007 Infrastructure protection program*. Dostopno prek: http://www.akprepared.com/grant_forms/acrobat_docs/FY07%20HSGP%20Guidance%20FINAL.pdf (1.september 2008).

105. U. S. Department of Homeland Security. 2006. *National infrastructure protection program (NIPP)*. Dostopno prek:http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (1.september 2008).

106. *U. S. Fire Administration (FEMA)*. Dostopno prek:http.//www.usfa.dhs.gov/fireservice/subjects/emr-isac/what_is.shtm (22. avgust 2008).

107. Westrin, Peter. 2001. Critical Information Infrastructure Protection. V The *Internet and the Changing Face of International Relations and Security*, ur. Andreas Wenger. Information & Security. *An International Journal* 7(1):67-79.

108. *What is CIP?* Dostopno prek: http.//cipp.gmu.edu/cip/ (11. avgusta 2008).