UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

BOGDAN KRES

ZAŠČITA KRITIČNE INFORMACIJSKE INFRASTRUKTURE V REPUBLIKI ITALIJI – ŠTUDIJA PRIMERA

DIPLOMSKO DELO

Ljubljana, 2006

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

BOGDAN KRES

Mentor: red. prof. dr. Marjan Malešič
Somentor: asist. dr. Uroš Svete

ZAŠČITA KRITIČNE INFORMACIJSKE INFRASTRUKTURE V REPUBLIKI ITALIJI – ŠTUDIJA PRIMERA

DIPLOMSKO DELO

Ljubljana, 2006

ZAHVALA

Mentorju red. prof. dr. Marjanu Malešiču in somentorju asist. dr. Urošu Svetetu se iskreno zahvaljujem za njuno podporo, pomoč in vodenje od odločitve o izbiri teme do končnega cilja

Staršem, sorodnikom in prijateljem, ker so verjeli vame, me podpirali in spodbujali

Najdražji osebi, prijateljici in življenjski sopotnici - ženi Vilmi!

KAZALO

1. UVOD

»Ogroženi smo. Amerika je vedno bolj odvisna od računalnikov …
Jutrišnji teroristi bi lahko bili sposobni narediti več škode
s tipkovnico kakor z bombo.«
National Academy of Sciences, 1990:7 (V: Dunn, 2004)

Te misli, izrečene že leta 1990, so se izkazale za še kako preroške in realne, saj sodobne družbe postajajo vedno bolj odvisne od informacijsko-komunikacijske tehnologije (IKT) in zapletenih ter kompleksnih infrastruktur, ki slonijo na upravljanju preko takšnih tehnologij. Infrastrukture postajajo pomemben dejavnik varnosti na najrazličnejših področjih družbe in se je zato za njih uveljavilo ime kritične nacionalne infrastrukture (CNI – Critical National Infrastructures), njihovo pravilno in nemoteno delovanje pa je vitalnega pomena za delovanje neke države in njeno varnost.
Tovrstne infrastrukture prežemajo vsa temeljna področja modernih družb (zdravstvo, gospodarstvo, energetiko, transport, telekomunikacije, javni red in mir, obrambo, vse sektorje javne uprave…) in so podvržene kriznim dogodkom v najrazličnejših oblikah (namernim napadom, pa tudi nenamernim človeškim napakam ter naravnim nesrečam), ki lahko ogrozijo njihovo učinkovitost in pravilno delovanje.
Nacionalne kritične infrastrukture se za svoje delovanje vse bolj naslanjajo na informacijsko-komunikacijsko tehnologijo (ki s tem postaja tudi sama kritična; CII – Critical Information Infrastructure) in mora biti sposobna delovati v normalnih pogojih, še posebej pa ob kriznih dogodkih, zato je še kako pomembno, da se nepravilnosti oz. okvare ne pojavijo celo znotraj samih kritičnih nacionalnih infrastruktur ali celo kritičnih informacijskih infrastruktur.
Z razvojem se hkrati pojavlja tudi vedno večja soodvisnost teh infrastruktur, kar po eni strani pomeni večjo povezanost in učinkovitost v delovanju, po drugi strani pa večjo ranljivost in posledično večjo, lahko tudi katastrofalno škodo v primeru odpovedi enega sistema, ki lahko povzroči motnje ali odpoved drugih sistemov oz. infrastruktur. Vsa področja razvitih družb so že v osnovi odvisna od energije in informacijsko-komunikacijske tehnologije, za kateri lahko rečemo, da sta temeljni infrastrukturi modernih (informacijskih) družb.

Prvi zametki tega zavedanja segajo približno 50 let nazaj (pojav prvih računalnikov, ki pa še niso bili sposobni medsebojne komunikacije), v začetku 90-ih let prejšnjega stoletja pa začne postajati informacijsko-komunikacijska tehnologija tako pomembna in vpletena tudi v

življenje vsakega posameznika ter v vse sfere družb, da se je izkazala potreba po normativnem urejanju tega pojava, in ena prvih držav, ki je začela dopolnjevati svojo zakonodajo tudi na tem področju, je Italija, država z bogato zgodovinsko, kulturno, politično, ekonomsko, državotvorno, nenazadnje tudi pravno oz. zakonodajno tradicijo (ne smemo pozabiti, da večina modernih zakonov izhaja ravno iz rimskega prava).

Ko so se mednarodne institucije in integracije (Organizacija združenih narodov, skupina G8, Organizacija za ekonomsko sodelovanje in razvoj, Evropska unija…), katerih članica je tudi Italija, začele zavedati tega problema oziroma potrebe, je leta 1992 OECD izdala prve smernice za varnost informacijskih sistemov in omrežij. Italija jih je (prilagojeno) takoj v naslednjem letu začela vključevati v svojo zakonodajo. Večkrat v naslednjih letih je bila ta država (v povezavi z informacijsko-komunikacijsko tehnologijo in CIIP – Critical Information Infrastructure Protection; zaščito kritične informacijske infrastrukture) zelo aktivna, celo pobudnica sprememb in dopolnil normativov za področje informacijsko-komunikacijske tehnologije v mednarodnih integracijah, njeni strokovnjaki so avtorji mnogih raziskav, člankov, člani komisij v mednarodnih integracijah, vodje delovnih teles…

Za enega temeljnih ciljev si je Italija postavila hitrejši razvoj na področju informacijsko-komunikacijske tehnologije in informatizacije družbe v primerjavi z drugimi članicami Evropske unije in v to vlaga veliko finančnih in drugih sredstev. Pri tem je še posebej v zadnjih nekaj letih zelo uspešna.

To dejstvo se bo pokazalo in potrdilo tudi v raziskovalni nalogi, ki je predstavljena v nadaljevanju.

2. METODOLOŠKO-HIPOTETIČNI OKVIR

2.1. Opredelitev predmeta proučevanja in cilji diplomske naloge

Predmet proučevanja v moji diplomski nalogi se nanaša na povezavo med kritično informacijsko infrastrukturo (v nadaljevanju CII – critical information infrastructure) in njeno zaščito v Republiki Italiji, s ciljem proučiti in primerjati normativno ureditev tega področja v Italiji z normativno ureditvijo tega področja v mednarodnih integracijah, katerih članica je, in nakazati trende razvoja zaščite kritične informacijske infrastrukture v omenjeni državi.

CIIP (critical information infrastructure protection) oz. zaščita kritične informacijske infrastrukture je v številnih državah razumljena kot ključna naloga sistema nacionalne varnosti, še posebej se ta tendenca kaže po terorističnem napadu 11. 9. 2001 v ZDA. CI (critical infrastructure) oz. kritična infrastruktura se opredeljuje kot skupek posebnih segmentov družbe, katerih onesposobitev ali celo uničenje bi imelo za posledico oslabitev funkcioniranja družbe tako na ekonomskem kot socialnem področju.

Velik zagon v sprejemanju smernic za zaščito CII je pomenila tako imenovana informacijska revolucija in razvoj informacijsko-komunikacijske tehnologije (IKT) ter izredna dostopnost le-te najrazličnejšim uporabnikom. Vzporedno s tem pa so se enako hitro razvijali in širili tudi načini in orodja za zlorabo IKT, od katere postajajo razvite družbe vedno bolj odvisne.

2.2. Hipoteze

V nalogi bom pokušal potrditi oziroma ovreči tri hipoteze:

- Razvoj CIIP v Italiji gre v smeri približevanja zakonodaji EU in smernicam OECD glede varnosti informacijskih sistemov in omrežij (nazadnje spremenjenih in dopolnjenih l. 2002).
- Razvoj CIIP v Italiji poteka v obdobju zadnjih nekaj let zelo pospešeno (spreminjanje zakonodaje, povečana vlaganja v infrastrukturo, oblikovanje novih varnostnih mehanizmov…).
- Glede na postavljene cilje mora Italija posvečati več pozornosti izobraževanju in usposabljanju kadrov na tem področju, saj le-ti predstavljajo najšibkejšo točko v razvoju CIIP.

2.3. Metodologija

Pri pisanju diplomskega dela se bom opiral na *metodo zbiranja virov*; predvsem internetnih, saj je ustrezna literatura, ki obstaja le v pretežno italijanskem in nekaj v angleškem ter (predvsem za prvi del) tudi v slovenskem jeziku, dostopna večinoma preko internetnih virov.

Z analizo in interpretacijo primarnih in sekundarnih virov bom predstavil temeljne dokumente s področja CIIP, ki so povezani tudi z mednarodnimi integracijami in Republiko Italijo. Ti dokumenti niso nikjer zbrani v enem delu, zato sem jih moral poiskati in zbirati posamezno, kar je bilo dolgotrajno in precej zamudno. Velikokrat pa me je odkriti dokument pripeljal do naslednjega pomembnega besedila.
Težko sem dostopal do določenih spletnih strani CLUSIT-a (italijanskega združenja za informacijsko varnost), pa tudi italijanske policije za pošto in komunikacije; večkrat so bili dostopi do teh strani pogojeni s tem, da sem moral dati npr. osebne podatke in razlog za dostop (registracija je pogojevala vpogled v določene dokumente in sem tako še pred začetkom pisanja mojega diplomskega dela naletel na izvajanje in učinkovitost CIIP v Italiji).

Z zgodovinsko analizo bom kronološko prikazal normativni razvoj CIIP v Italiji in tudi v mednarodnih integracijah tako, da bom predstavil povzetke, po mojem mnenju, najpomembnejših dokumentov s tega področja.

Na podlagi *študije primera in primerjalnega raziskovanja* bom poskušal podati zaključke in nakazati trende nadaljnjega razvoja tega področja v Italiji.
Prav tako bo predvsem na tej metodi slonelo preverjanje hipotez v zaključku.

2.4. Opredelitev temeljnih pojmov

2.4.1. Varnost in IKT

O percepciji varnosti lahko govorimo z več vidikov: z vidika posameznika, družbe, države, mednarodne skupnosti in celo sveta kot celote ter predstavlja ravnotežje v odnosih med njimi, zaradi česar se v zavesti posameznika oblikuje občutek stabilnosti, homeostatičnosti, torej tudi zagotovljenih pogojev za življenje in preživetje (Jelušič, 1997:70).

Grizold opredeli varnost kot stanje, v katerem je zagotovljen fizični, duhovni, duševni ter gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov (Grizold, 1999:23).

Uresničevanje nacionalne varnosti države je neločljivo povezano z zagotavljanjem mednarodne varnosti, saj učinki negativnih varnostnih procesov v okolju države neposredno in posredno zadevajo tudi njeno varnost. Mednarodna skupnost živi v obdobju, ki je polno iskanja, negotovosti, novih zamisli in tudi napak. Zaznamujeta ga velika soodvisnost držav, katerih sposobnost delovanja se z vključevanjem v različne mreže, ki jih omogoča sodobna tehnologija, povečuje, in erozija nacionalne države, h kateri prispevajo tudi viri ogrožanja, ki učinkujejo čezmejno in se ne zmenijo za koncept suverenosti nacionalnih držav (Malešič, 2002: 138).

Obravnavanje varnosti se ne omejuje več na vojaške vire ogrožanja, katerih cilj je predvsem (nacionalna) država, vedno bolj se varnost obravnava kompleksno tako v smislu virov ogrožanja, referenčnih objektov, na katere se varnost nanaša, kot mehanizmov za njeno zagotavljanje.

Pojmovanje varnosti se spreminja vzporedno s spremenjenimi (novimi) viri ogrožanja, kot tudi novimi akterji zagotavljanja varnosti, saj predstavlja tehnološka odvisnost od splošno družbeno prisotne IKT v informacijskih družbah osnovo za razpravo o informacijskem bojevanju, po drugi strani pa naj bi njena razširjenost pomenila tako vir moči kot vir ranljivosti in s tem povezanih varnostnih izzivov, tveganj in groženj (Svete, 2005:17).

Ko je govora o IKT sistemih, lahko ob pojmu varnosti dodam tudi pojem **zanesljivosti**, s katerim so se teoretično ukvarjali: Algirdas Avižienis (UCLA Computer Science Dept., USA), Jean-Claude Laprie (LAAS-CNRS, France) in Brian Randell (Dept. of Computing Science, Univ. of Newcastle, U.K.), in je predstavljen v njihovem skupnem delu z naslovom **Fundamental Concepts of Dependability (Temeljni koncepti zanesljivosti)**.

Tudi ti avtorji že v uvodu izpostavijo, da je skrb za preživetje kompleksnih informacijskih sistemov, ki podpirajo infrastrukturo razvitih družb, med najpomembnejšimi nacionalnimi in celo svetovnimi nalogami.

Zanesljivost je opredeljena **kot lastnost nekega sistema**, ki vključuje naslednje atribute:

- *razpoložljivost oz. dostopnost,*
- *trdnost,*
- *varnost oz. zaščito,*
- *zaupnost,*

- *neokrnjenost,*
- *vzdržljivost.*

Struktura pojma zanesljivost se poleg atributov navezuje še na:

- grožnje (*napake, pomote, razpadi*)
- sredstva oz. načine za doseganje zanesljivosti (*preprečevanje, toleranco, predvidevanje, odstranitev napak*).

Avtorji pravijo, da bi lahko bila najpreprostejša definicija varnosti sistemov kombinacija treh že omenjenih atributov:

1. zaupnosti (preprečitve nepooblaščenih razkritij informacij),
2. neokrnjenosti oz. integritete (preprečitve nepooblaščenih sprememb ali izbrisov informacij) in
3. razpoložljivosti (preprečitve nepooblaščenih zadrževanj informacij).

Torej je lahko varnost opredeljena tudi kot odsotnost nepooblaščenih dostopov ali spreminjanja stanja sistemov.
(Avižienis, Laprie, Randell: 2000, 1-12)

Ob upadanju pomena vojaških virov ogrožanja se vedno jasneje kažejo nevojaški viri ogrožanja, ki lahko prav tako kot vojna, močno ogrozijo sodobne države in družbe. Pogosto so med seboj povezani in soodvisni, delujejo in učinkujejo transnacionalno.
Varnost oziroma zaščita informacij, ki je za nek sistem in njegovo nemoteno delovanje (pa naj si bo to transport, bančništvo, (tele-)komunikacije, javno zdravstvo, civilna zaščita, javna uprava itn. ali pa skupek le-teh na nekem državnem teritoriju – v moji nalogi bo to Republika Italija) vitalnega pomena, je torej kritična.

2.4.2. Informacijska in kritična infrastruktura

V tej luči so opredeljeni temeljni pojmi, ki se pojavljajo v nadaljevanju diplomskega dela, potrebno je najprej postaviti ločnico med CI in CII (CI – Critical Infrastructure; kritično infrastrukturo in CII – Critical Information Infrastructure; kritično informacijsko infrastrukturo), ki sicer zvenita podobno, vendar je prva širši pojem od druge, saj vključuje vse sisteme in imetje, čigar nezmožnost ali uničenje bi lahko oslabilo nacionalno oz. državno varnost ter njeno ekonomsko in socialno blaginjo, druga pa vsebuje komponente, kot so telekomunikacije, računalniki in njihovo programsko okolje, internet, sateliti, optična vlakna itn. Ta termin se uporablja tudi za sistem med seboj povezanih računalnikov in računalniških

mrež ter (kritičnih) informacijskih tokov, ki med njimi potekajo, kakor tudi za tisti del globalne oz. nacionalne informacijske infrastrukture, ki je posebej pomembna za nepretrgano oz. neokrnjeno delovanje kritičnih infrastrukturnih služb.

Zaščita kritične informacijske infrastrukture (CIIP) je postala še posebej pomembna zaradi dveh razlogov; prvi razlog je naraščajoča neprecenljiva vloga na ekonomskem področju, drugi razlog pa je povezovalna vloga med različnimi infrastrukturnimi sektorji in osnovnimi zahtevami za njihovo nemoteno in neprekinjeno delovanje. Prav tako je potrebno pri razlikovanju med CI in CII biti pozoren na različne posebnosti oz. značilnosti, ki se razlikujejo od tradicionalnih in uveljavljenih struktur, vključujoč zgodnje informacijske infrastrukture. Razlikujejo se tako z vidika razsežnosti kot tudi medsebojnega povezovanja in soodvisnosti. Narašča pa tudi število kibernetičnih napadov, ki se vse bolj kažejo v povečani zmožnosti povzročanja škode, to pa posledično zahteva konstantne tehnološke izboljšave in nove pristope, soočamo se tudi z dinamično globalizacijo informacijskih služb, ki v povezavi s tehnološkimi izboljšavami (npr. lokalnimi brezžičnimi povezavami) povečujejo možnosti medsebojnega povezovanja, kar lahko vodi po eni strani v boljše poznavanje obnašanja takšnih sistemov in povezav, po drugi strani pa v premajhno poznavanje njihove ogroženosti (povzeto po Dunn in Wigert, 2004).

Iz povedanega lahko sklepam, da se preveč pozornosti posveča razvoju takšnih sistemov, premalo pa zaščiti, ki tako hitrim razvojnim tendencam ne sledi. Vzrok za to lahko najdemo v dejstvu, da se skrajšuje čas uvajanja in operacionalizacije v tržnem segmentu, pa tudi povečevanju deleža kritičnih infrastruktur v privatnem sektorju in celo drugih držav (distribucija električne energije, telekomunikacije…), zato lahko posledično pričakujemo povečanje števila nestabilnih infrastruktur, kritičnih točk razpada in povečane soodvisnosti.
Tako se lahko znajdemo v škripcih različnih stališč in težavah pri umestitvi odgovornosti v izvajanju zaščite CII ter določanju primernih političnih orodij za to.

Meja med različnimi pogledi in pojmovanji CIIP je precej zabrisana, navedel bom nekaj najbolj tipičnih (povzetih po Dunn in Wigert, 2004):

- *Sistemsko-tehnična perspektiva:* na CIIP gleda kot na zaščito informacijske tehnologije z velikim poudarkom na internetni varnosti. Pri tem uporablja tehnična sredstva, kot so npr. protivirusni programi, programi za ugotavljanje in preprečevanje vdorov, požarni zidovi … Kot posledica takšnega gledišča se v mnogih državah

ustanavljajo ti. CERT-i (Computer Emergency Response Teams) in podobne institucije oz. službe. [1]

- *Poslovna (ekonomska) perspektiva:* pojmuje CIIP kot bistveno vprašanje »poslovne kontinuitete«, še posebej v primeru e-poslovanja. To zahteva ne le permanenten dostop do IT infrastruktur, temveč tudi stalne poslovne procese za zagotovitev uspešnih poslovnih učinkov. To gledišče se v veliki meri navezuje na prej navedene ideje o tehnični družbi, vendar poleg tega vključuje še organizacijski in človeški faktor, zato se pojavlja največkrat v državah, ki dajejo ključni pomen informacijski družbi.
- *Zakonodajno-upravna perspektiva:* pojmuje CIIP kot ključno sredstvo za zaščito družbe pred kibernetskim kriminalom, ki je zelo široko področje, saj zajema vse od samega tehničnega uničenja računalniških sistemov do kriminala, povzročenega na posameznih računalnikih, prav tako to gledišče pokriva kršitve avtorskih pravic, računalniških prevar, otroške pornografije in kršitve varnosti omrežja. Proti kibernetskemu kriminalu se še vedno borijo z bolj ali manj tradicionalnimi zakonodajno-pravnimi strategijami, posebej z uvajanjem primerne zakonodaje in spodbujanjem mednarodnega sodelovanja.
- *Nacionalno-varnostna perspektiva:* Predstavlja najbolj obširno pojmovanje CIIP-a, saj izhaja iz predpostavke, da je celotna družba potencialno ogrožena, zato se zaščitni ukrepi izvajajo na najrazličnejših nivojih in vključujejo vse akterje, ki lahko prispevajo k zaščiti družbe (vladne uradnike in agencije, predstavnike privatnega sektorja ter posameznike).

Obe pojmovni kategoriji (CI in CII) se močno navezujeta na IKT (informacijsko-komunikacijsko tehnologijo), ki je sestavni del obeh komponent, še bolj slednje, in predstavlja osnovo delovanja – to je posredovanje in sprejemanje najrazličnejših informacij. Problem, ki se ob tem lahko pojavi, je nenadzorovano in neželeno širjenje teh informacij v svetovni splet oz. omrežje ter njihovo varovanje.

2.4.3. Mednarodne integracije in sodobna varnost

Izredno hiter razvoj IKT v zadnjem obdobju in njena dostopnost ter uporaba so omogočili

---

[1] V Sloveniji obstaja SI-CERT; http://www.arnes.si/si-cert/, ki deluje v okviru ARNES-a, Akademske in raziskovalne mreže Slovenije. SI-CERT (Slovenian Computer Emergency Response Team) je center za posredovanje pri internetnih incidentih, ki koordinira obveščanje in reševanje varnostnih problemov v računalniških omrežjih v Sloveniji. Glavna naloga, ki jo SI-CERT opravlja, je sprejem in posredovanje obvestil o zlorabah in vdorih v računalniške sisteme. Predstavlja znano kontaktno točko, ki opravlja posredniško in svetovalno vlogo (http://www.arnes.si/si-cert/opis.html).

velike možnosti disperzije v sodobnih družbah. Telekomunikacije, satelitske povezave in računalniška omrežja so velik del sveta povezali v prepleteno celoto – informacijsko družbo (Svete, 2005: 5).

Ta prepletenost povezav ne glede na državne meje pa ne pomeni le prednosti, ampak tudi večjo ranljivost, kajti varnosti ni več mogoče zagotavljati na mejah držav niti na mejah skupnosti držav, zato so države postavljene pred drugačne vloge, saj je za mnoge povezovanje v mednarodne organizacije, preko meja nacionalnih držav, zaenkrat edina možna strategija učinkovitega preprečevanja oz. odpravljanja vzrokov, posledic in virov ogrožanja v sodobnem času. [2]

Takšno sodelovanje poteka na več nivojih, od usklajevanja zakonodaje oz. zakonskih aktov, izmenjave podatkov do združenega delovanja na celotnem področju (npr. geografskem, političnem, ekonomskem, nacionalno-varnostnem…).

Glede na ta področja bom omenil le mednarodne integracije (z vidika CIIP), ki se neposredno dotikajo teme moje diplomske naloge in katerih članica je tudi Republika Italija.

2.4.3.1. Organizacija združenih narodov (OZN)

OZN je največja mednarodna organizacija, saj so njene članice skoraj vse države sveta. Cilji, za katere se zavzema, so: ohranjanje mednarodnega miru in varnosti, razvoj prijateljskih odnosov med državami, pospeševanje (med)narodnega gospodarstva, prepoved uporabe sile, obveznost mirnega reševanja sporov; države članice pa naj upoštevajo še naslednja načela: načelo suverene enakosti, načelo nevmešavanja v notranje zadeve držav in aktivno sodelovanje držav članic. Njihovo uresničevanje ima temeljni pomen v sodobnem mednarodnem pravu in se zagotavlja zlasti z mirnim mednarodnim sodelovanjem in sistemom kolektivne varnosti. [3]

Najpomembnejša organa OZN sta Generalna skupščina (GS), katere članice so vse države, ki so včlanjene v OZN, in Varnostni svet (VS), ki ima le pet stalnih članic in deset članic z dvoletnim mandatom ter predstavlja udejanjanje sistema kolektivne varnosti. [4]

---

[2] Značilnost sistemov je v soodvisnosti. Kompleksni sistemi torej ne morejo obstajati v izolaciji, vsaka sprememba znotraj sistema se odraža širše (Dunn, 2004).

[3] V zadnjem času se pojavljajo močne težnje po spremembah v ureditvi nekaterih organov OZN, posebej varnostnega sveta (VS), predvsem po terorističnih napadih Al Kaide v ZDA in posredovanju ZDA v Iraku. Za te spremembe se v veliki meri zavzema tudi Italija.

[4] Slovenija je postala članica OZN 22. 5. 1992, leta 1998 in 1999 je bila tudi članica VS.

V zvezi s CIP in CIIP je OZN v zadnjih nekaj letih sprejela naslednje resolucije:
- boj proti zlorabi informacijske tehnologije (55/63, 2001),
- ustvarjanje globalne kulture kibernetske varnosti in zaščita CII (58/199, 2003),
- ustvarjanje globalne kulture kibernetske varnosti (57/239, 2003).

Te resolucije povečujejo globalno zavedanje in nudijo skupno začetno točko za soočanje vseh narodov/držav s problemi kibernetske varnosti (The CIP Report, Maj 2004: 14).

Druga omenjena resolucija (58/199, 2003) je za mojo diplomsko nalogo najpomembnejša, saj najbolj neposredno zadeva obravnavano temo. Članice OZN poziva k upoštevanju **11 elementov za zaščito kritične informacijske infrastrukture**, usmerjenih v:

1. vzpostavitev podpornih opozorilnih omrežij v primerih nastanka kibernetskih šibkih točk, ogrožanja ali incidentov,
2. ozaveščenost članic za poglabljanje razumevanja narave in obsega njihovih kritičnih infrastruktur ter zaščitne vloge, ki jo morajo pri tem opraviti,
3. proučitev infrastruktur, prepoznavanje njihove medsebojne odvisnosti in posledično okrepitev njihove zaščite,
4. spodbujanje partnerstva med članicami, tako na javnem kot zasebnem področju, posredovanje in analiziranje informacij, ki se nanašajo na kritično informacijsko infrastrukturo, in s tem preprečevanje, raziskovanje in odzivanje na škodo ali napade na takšne infrastrukture,
5. izdelava in vzdrževanje kriznih komunikacijskih omrežij in s tem zagotovitev, da bodo v kriznih situacijah ostala varna in stabilna,
6. zagotavljanje politike dostopnosti podatkov, ki upošteva potrebo po zaščiti kritičnih informacijskih infrastruktur,
7. omogočanje sledenja napadom na kritične informacijske infrastrukture in kjer je to primerno, razkrivanje pridobljenih informacij drugim državam,
8. izobraževanje in usposabljanje za namene povečevanja reakcijskih sposobnosti in testiranje pripravljalnih načrtov za primer napada na informacijsko infrastrukturo in vzpodbujanje držav članic, da izvedejo te aktivnosti,
9. sprejemanje ustreznih temeljnih in proceduralnih zakonov ter zagotovitev usposobljenega osebja, ki državam omogoča preiskovanje in zakonsko preganjanje napadov na kritično infrastrukturo, in v koordiniranje teh preiskav z drugimi državami,

10. vključevanje v mednarodno sodelovanje, kadar je to primerno, da se zaščiti kritična informacijska infrastruktura, vključno z razvijanjem in koordiniranjem podpornih opozorilnih sistemov, posredovanjem in analizo podatkov, ki zadevajo šibke točke, grožnje in incidente ter koordiniranje preiskav napadov na take infrastrukture v skladu z domačo zakonodajo,
11. promoviranje nacionalnih in mednarodnih raziskav, razvoj in vzpodbujanje uporabe varnostnih tehnologij, ki so v skladu z mednarodnimi standardi (The United Nations Resolution on CIIP (2004), NISCC Quarterly 02/04: 15).

2.4.3.2. Skupina držav G8

G8 (članice: Velika Britanija, Francija, Italija, Japonska, Kanada, Nemčija, ZDA in Rusija) je nastala z razlogom, da bi voditelji sedmerice (najprej se je imenovala G7) razpravljali o trgovini in ekonomskih vprašanjih, zdaj pa že kar nekaj let voditelji držav članic enkrat letno obravnavajo vsa aktualna svetovna vprašanja, tudi politična.

Marca 2003 je skupina **G8 sprejela enajst elementov CIIP**, ki jih je še v istem letu soglasno sprejela OZN v resoluciji 58/199, in sem jo podrobneje že povzel.

Teh enajst elementov CIIP je v bistvu proizvod High Tech Crime Sub Group (podskupine za boj proti visokotehnološkemu kriminalu), primarno namenjene zakonodajno-pravnemu iniciativnemu oddelku (The United Nations Resolution on CIIP, 2004, NISCC Quarterly 02/04:14).

2.4.3.3. Organizacija za ekonomsko sodelovanje in razvoj (OECD)

Ta Organizacija za ekonomsko sodelovanje in razvoj vključuje 30 večinoma evropskih držav (vključujoč še Avstralijo, Japonsko, Kanado, Južno Korejo, Mehiko, Novo Zelandijo in ZDA; Slovenija ima status opazovalke – je podpisnica smernic OECD).

Leta 2002 je na 1037. seji Sveta OECD sprejela Smernice za varnost informacijskih sistemov in omrežij: H kulturi varnosti. [5] Vzroki za sprejetje teh smernic so nenehne spremembe na področju informacijske tehnologije, ki omogočajo veliko prednosti, hkrati pa zahtevajo, da se namenja veliko več pozornosti varovanju na vseh nivojih; od vlad, podjetij in drugih organizacij do posameznikov, ki posedujejo, razvijajo, nudijo storitve in z njimi upravljajo ter

[5] Leta 1992 je OECD podala prve smernice na to temo, ki jih je sprejela tudi Italija. Prvi rezultat uvajanja teh smernic v Italiji je bilo sprejetje Zakona 547 (Legge 547) v letu 1993, ki je sicer imel nalogo predvsem zaščititi privatno lastnino in nepooblaščen dostop do osebnih in drugih podatkov v IKT sistemih, je pa tudi postavil uspešna merila in postopke za boj proti tovrstnemu kriminalu.

pri tem uporabljajo informacijske sisteme in omrežja (OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002).

Te smernice imajo veliko skupnega z 11 elementi za zaščito CII, ki so podani v resoluciji OZN, pomembna razlika pa je v tem, da resolucija OZN usmerjena na države oz. njihove vlade, smernice OECD pa pokrivajo vse nivoje, od vlad pa do vsakega posameznika, ki uporablja IKT.

Cilji, ki jih te smernice zasledujejo:

- Povečati kulturo varnosti med vsemi udeleženci s ciljem zaščite informacijskih sistemov in omrežij.
- Dvigniti zavedanje glede tveganj v zvezi z informacijskimi sistemi in omrežji ter pri soočanju s temi tveganji pokazati pripravljenost za implementacijo zaščitnih metod tako na ravni politike, prakse, ukrepov kot postopkov z namenom reševanja (odpravljanja) teh tveganj.
- Poglobiti zaupanje med udeleženci v informacijskih sistemih in omrežjih ter vzpostaviti načine posredovanja in uporabe.
- Ustvariti splošna priporočila, ki bodo udeležencem pomagala pri razumevanju bistvenih varnostnih zadev in spoštovanju etičnih vrednot pri razvoju in implementaciji usklajenosti politik, praks, ukrepov in postopkov.
- Spodbujati sodelovanje in posredovanje informacij, kadar je to primerno, med vsemi udeleženci v procesu razvoja politik, praks, ukrepov in postopkov.
- Poudariti pomen upoštevanja varnosti kot pomembnega dejavnika med vsemi udeleženci tako glede razvoja kot implementacije standardov.

Pri uresničevanju ciljev naj se upošteva naslednjih **9 načel**:

1. Ozaveščenost

Udeleženci se morajo zavedati potrebe po zavarovanju informacijskih sistemov in omrežij ter po svojih močeh prispevati k temu.

2. Odgovornost

Vsi udeleženci so odgovorni za varnost informacijskih sistemov in omrežij.

3. Odzivanje

Udeleženci naj reagirajo hitro in kooperativno, da preprečijo, zaznajo in se odzovejo na varnostne incidente.

4. Etičnost

Udeleženci naj spoštujejo legitimnost interesov drugih.

5. Demokratičnost

Varnost informacijskih sistemov in omrežij naj bo kompatibilna s temeljnimi vrednotami demokratične družbe.

6. Ocena tveganja

Izvaja naj se neprenehoma pri vseh udeležencih.

7. Zasnova varnosti in implementacija

Varnost naj se pojmuje kot bistven element informacijskih sistemov in omrežij.

8. Varnostno upravljanje

Udeleženci naj sprejmejo poenoten sistem varnosti.

9. Ponovno preverjanje in ocena

Udeleženci naj preverijo in ponovno ocenijo varnost informacijskih sistemov in omrežij ter sprejmejo primerne prilagoditve v varnostni politiki, praksi, ukrepih in postopkih.

Priporočila Sveta OECD državam članicam:

- Ustanovite nove ali dopolnite obstoječe politike, prakse, ukrepe in postopke, upoštevajoč Smernice za varnost informacijskih sistemov in omrežij: H kulturi varnosti, in s tem usvojite in poglabljajte kulturo varnosti, kot je predlagano v smernicah.
- Posvetujte in usklajujte se ter sodelujte na nacionalnih in mednarodnih ravneh, da implementirate te smernice.
- Posredujte te smernice vsem javnim in zasebnim sektorjem, tudi vladam, podjetjem, raznim organizacijam in posameznim uporabnikom, s ciljem dviganja kulture varnosti in opogumljanja vseh strani, ki jih to zadeva, da so odgovorne in sprejmejo potrebne korake za implementacijo smernic na primeren način glede na njihovo vlogo.
- Omogočite čimprejšnjo dostopnost smernic na primeren način državam, ki niso članice OECD.
- Ponovno ocenite smernice vsakih pet let, zaradi lažjega mednarodnega sodelovanja glede temeljnih vprašanj, ki se nanašajo na varnost oz. zaščito informacijskih sistemov in omrežij (OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, 2002: 8).

2.4.3.4. Svet Evrope

Prvi cilj Sveta Evrope (Councile of Europe) je doseči večjo enotnost med 46 članicami pri varovanju osebne svobode, politične neodvisnosti in vladavine prava na načelih, ki so podlaga demokracije in se na različne načine dotikajo življenja vseh Evropejcev. Vse države članice

Sveta Evrope so pri vsem svojem ravnanju zavezane trdno spoštovati načela svobode, človekovega dostojanstva in blaginje vsakega posameznika. Zdaj organizacija vključuje že okrog 800 milijonov Evropejcev. Vse od ustanovitve leta 1949 je bil Svet Evrope sila miru in sodelovanja, zasidrana v naši skupni dediščini, človekovih pravicah in demokraciji. S padcem berlinskega zidu leta 1989 in širitvijo demokratičnih vrednot po vsej Evropi je organizacija dobila novo politično razsežnost. Dejansko je širitev Sveta Evrope zdaj že skoraj do konca uresničena (http://www.coe.int/si/portal/default.asp?L=SI).
23. novembra 2001 je Svet Evrope na zasedanju v Budimpešti sprejel konvencijo št. 185 z naslovom Convention on Cybercrime (Konvencija o kibernetskem kriminalu), ki predstavlja prvi mednarodni sporazum, in se ukvarja s hudodelstvi (zločini) v internetu in drugih računalniških omrežjih, še posebej s kršitvami na področju avtorskih pravic, računalniških prevar, otroške pornografije ter kršitvami omrežne varnosti (http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm). Vsebuje tudi veliko polnomočij oz. pooblastil in postopkov, med drugimi tudi iskanje ter prestrezanje oz. preprečevanje škodljivih računalniških omrežij in povezav.

Glavni cilj te konvencije, ki je opredeljen že v njeni preambuli, je zaščititi človeško družbo pred kibernetskim kriminalom, ga zasledovati in preganjati, pospešiti mednarodno sodelovanje in kar je po mojem mnenju najpomembneje, **ustvariti in sprejeti primerno zakonodajo**, ki bo omogočila ustrezne sankcije ob kršitvah. Ta konvencija je plod štiriletnega dela strokovnjakov Sveta Evrope, kakor tudi ZDA, Kanade, Japonske in drugih držav, ki niso članice te organizacije, in je v veljavo stopila 1. julija 2004.

28. 1. 2003 je Svet Evrope v Strasbourgu sprejel še dodatek k tej konvenciji z zaporedno številko 189, protokol (http://conventions.coe.int/Treaty/en/Summaries/Html/189.htm), v katerem poleg vzpostavitve usklajene zakonodaje, sredstev in dejanj na tem področju uvaja še kategorijo boja proti ksenofobiji in rasistični propagandi, ki se lahko širita preko interneta. Omenjeni protokol naj bi končno uredil in vzpostavil učinkovit in usklajen notranjepolitični in mednarodni odgovor kibernetskemu kriminalu.

2.4.3.5. Evropska unija (EU)

Ta integracija je skupnost petindvajset demokratičnih evropskih držav, ki si prizadevajo za mir in blaginjo, vendar se od drugih mednarodnih organizacij razlikuje v tem, da so države članice ustanovile skupne institucije, na katere so prenesle del svoje suverenosti, tako da na

evropski ravni lahko demokratično sprejemajo odločitve o vprašanjih skupnega interesa. Načelo pravne države je za Evropsko unijo temeljnega pomena.
Institucije EU so: evropski parlament, Svet Evropske unije, evropska komisija, sodišče evropskih skupnosti in računsko sodišče; ob teh institucijah pa obstaja še več teles (najvišje telo je Evropski svet) in agencij. EU se poleg trgovine in gospodarstva ukvarja še s številnimi drugimi zadevami, kot so: človekove pravice, zagotavljanje svobode, regionalni razvoj, varstvo okolja, globalizacija, pravice in varnost (http://europa.eu.int/abc/index_sl.htm).

V okviru varnostne politike EU pokriva tudi področje informacijske družbe in je na tem področju ena vodilnih. V svojih aktih, dokumentih, smernicah, direktivah, nenazadnje **sprejetih zakonih** predstavlja informacijska družba in informacijska varnost oz. zaščita eno najpomembnejših področij razvoja in raziskav EU. Upošteva različne vplive na državljanstvo, izobraževanje, poslovanje, zdravstvo in komunikacije.
Prav tako podpira in razvija najrazličnejše programe, kot so npr. razni akcijski načrti: e-Evropa, e-vsebine, e-varnost, akcijski načrt Internet, raziskave tehnologij informacijske družbe in drugo.
Ključno iniciativo v strategiji EU za modernizacijo njene ekonomije predstavlja program »eEurope 2002 - informacijska družba za vse in vsakogar«, ki je bila sprožena 8. decembra 1999. V tej strategiji EU spoznava in priznava ogromen ekonomski in socialni potencial, ki ga imajo nove informacijsko-komunikacijske tehnologije (IKT), od tega pa naj bi imeli koristi vsi Evropejci.
V tem programu je predstavljenih enajst najpomembnejših smeri razvoja, razdeljenih v tri večje skupine (http://www.e-europestandards.org/action_lines.htm#2002) :

- cenejši, hitrejši, varnejši internet
    - cenejši in hitrejši internetni dostop
    - hitrejši internet za raziskovalce in študente
    - **varna omrežja** in pametne kartice (e-varnost)

- vlaganje v ljudi in njihovo usposabljanje
    - evropska mladina v digitalni dobi (e-izobraževanje)
    - delo v na znanju temelječem gospodarstvu (e-delo)
    - participacija za vse v na znanju temelječem gospodarstvu (e-dostopnost/udeležba)

- vzpodbujanje uporabe interneta
    - pospeševanje e-trgovanja (e-poslovanje)
    - vlada on-line: elektronski dostop do javnih služb (e-vlada in e-uprava)
    - zdravstvo on-line (e-zdravstvo)
    - evropske digitalne vsebine za globalna omrežja (e-vsebine)
    - inteligentni transportni sistemi (e-transport)

EU vseskozi poudarja, da mora biti internet dostopen oz. na voljo vsem, v vsakem času in brez prekinitev, zaščiten mora biti pred napadi hekerjev in virusov. Kot je razvidno iz dokumenta (programa), predstavlja varnost oz. zaščita CI/CII za to integracijo eno pomembnih smeri razvoja (e-varnost). Dokler se ne rešijo vprašanja varnosti na tem področju, se informacijska družba ne bo mogla uspešno razvijati. Informacijska varnost, ki vključuje tudi CIIP, je postala ključna komponenta v tako imenovani viziji »Internet naslednje generacije« in je vključena v politične prioritete programa »e-Evropa 2005«, v katerega so med drugim vključeni še e-izobraževanje, dinamično e-poslovno okolje, sodobne e-vladne službe, široko dostopna in poceni linijska dostopnost in nenazadnje varna informacijska infrastruktura. Akcijski načrt »e-Evropa 2005 – informacijska družba za vse in vsakogar« je bil sprejet junija 2002 in predstavlja razširitev uspešne programske iniciative »e-Evrope 2002«. Poudarjeno je, da je informacijska varnost odvisna od človeškega odnosa oz. obnašanja, poznavanja ogroženosti in reševanja ter odpravljanja te ogroženosti. Poudarjen je tudi socialni in politični aspekt informacijske varnosti. Ker zajema informacijska varnost veliko političnih področij, kot so npr. zasebnost, državljanske pravice, zakonodaja, mednarodno poslovanje in obramba, lahko učinkovit pristop v izvajanju CIIP predstavlja samo vključevanje vseh vpletenih akterjev (tako javnega, zasebnega sektorja kot posameznikov) pri vzpostavljanju in izvajanju zaščitnih ukrepov, ki potekajo na več področjih (vključujejo vprašanja tehnične narave in družbene, politične ter zakonske okvire).

Za izpolnitev ciljev teh akcijskih načrtov je EU sprožila in podprla različne aktivnosti, ena teh je bila vzpostavitev posebnega foruma, ti. *foruma o kibernetskem kriminalu*, (http://cybercrime-forum.jrc.it/default), v katerem se velika pozornost posveča promoviranju uspešnih postopkov in orodij, ki obdelujejo področje kibernetskega kriminala in ga preprečujejo, razvijajo se sistemi zgodnjega obveščanja in kriznega upravljanja.

V juniju 2001 je *Evropska komisija* izdala sporočilo z naslovom: »Omrežna in informacijska varnost; predlog k pristopu evropske politike«, vključujoč priporočila evropskim standardizacijskim telesom za nadaljnje razvijanje njihovih dejavnosti. Oktobra istega leta sta

bila tako ustanovljena *Evropski komite za standardizacijo (CEN)* in *Evropski inštitut za telekomunikacijske standarde (ETSI)*, z izdajo priporočil o omrežni in informacijski varnosti. Ta priporočila so dobila dokončno obliko in bila sprejeta v juliju 2003.
Na pobudo *Evropske komisije* je bila v začetku leta 2004 ustanovljena *Evropska agencija za omrežno in informacijsko varnost (ENISA)*, ki pomeni zakonsko osnovo in koordiniran pristop EU k vprašanjem informacijske varnosti. Agencija ima posvetovalno in koordinacijsko funkcijo pri zbiranju in analizi podatkov o informacijski varnosti, predstavlja pa tudi neke vrste izvedensko središče institucij in članic EU. Vzpostavlja sodelovanje med ključnimi akterji, interoperabilnost omrežij in informacijskih sistemov ter promovira varnostne standarde. Predstavlja velik korak v izboljšanju CIIP na mednarodnem nivoju (Dunn in Wigert, 2004: 305 - 308).

Omeniti pa je treba **še nekaj pomembnih dokumentov, ki se navezujejo na področje CIP-a in CIIP-a**, in jih bom kronološko na kratko predstavil:

- **Resolucija Sveta EU** in predstavnikov vlad držav članic 97/C 70/01 (http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:41997X0306:EN:HTML) **o ilegalni in škodljivi vsebini na internetu**, ki države članice poziva k takojšnjemu sprejemu ukrepov, s katerimi se vzpodbuja in lajša izgrajevanje samoregulacijskih sistemov, učinkovitih postopkov obnašanja in mehanizmov za takojšnje poročanje, dosegljivih javnosti, in vzpostavitev sistemov za ocenjevanje vsebin s poudarkom na tehničnem razvoju sistemov za filtriranje, ocenjevanje, sledenje, omogočanje zasebnosti z upoštevanjem evropskih kulturnih in jezikovnih razlik, kar bo porok za stalno preverjanje legalnih internetnih vsebin.
- **Odločba Evropskega parlamenta in Sveta** št. 1336/97/ES (http://europa.eu.int/eur-lex/LexUriServ/LexUriServ.do?uri=CELEX:31997D1336:SL:HTML), ki določa smernice z že izdelanimi cilji, prednostnimi nalogami in ukrepi **za vzpostavitev vseevropskih omrežij za telekomunikacijsko infrastrukturo**, ki naj bi omogočila lažji prehod v informacijsko družbo, izboljšala konkurenčnost podjetij, okrepila notranji trg, omogočila večjo kohezijo (tako gospodarsko kot socialno), pospeševala razvoj dejavnosti, ki prispevajo k ustvarjanju novih delovnih mest.

  Med drugim ta odločba govori tudi o uvajanju nelastniških digitalnih podpisov (elektronskih imen) kot podlagi za odprto zagotavljanje storitev in mobilnost uporabe, ki omogoča primerno varstvo zasebnosti, splošno dostopnost in priznanost.

- **Odločba Evropskega parlamenta in Sveta** št. 276/1999/ES (http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31999DO276:EN:HTML), s katero se sprejema **večletni akcijski načrt Skupnosti pri promoviranju varnejše rabe interneta in boju proti ilegalni ter škodljivi vsebini v globalnih omrežjih**. Po tej odločbi naj bi industrija (internetna) postavila samoregulativne in vsebinsko-nadzorne sheme, ki bi ustvarile varnejše internetno okolje in pomagale pri odkrivanju vsebin, kot so otroška pornografija, razna sovraštva na osnovi rasnih, spolnih, verskih, nacionalnih in etničnih razlik ipd. Spodbujala naj bi se izdelava filtrirnih orodij in kategorialnih sistemov, ki naj bi učiteljem in staršem pomagali pri izbiri primernih vsebin za otroke z upoštevanjem lingvističnih in kulturnih razlik, omogočilo bi se širše spoznavanje novih možnosti in prednosti, ki jih internet nudi. Uporabniki in internetna industrija naj bi torej razvili primerne samoregulacijske sisteme, nove tehnične rešitve in aplikacije, gojili sodelovanje, izmenjavo izkušenj in rešitev tako na evropskem kot mednarodnem področju, kar bi v končni fazi privedlo do kompatibilnosti v pristopih in dejanjih tako v Evropi kot tudi drugod po svetu.
- **Uredba Evropskega parlamenta in Sveta** št. 43/2001 (http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:SL:HTML) **o varstvu posameznikov pri obdelavi osebnih podatkov** v institucijah in organih Skupnosti in o prostem pretoku takih podatkov, s katero se posameznikom zagotovijo pravno izvršljive pravice, da se določijo dolžnosti upravljavcev pri obdelavi osebnih podatkov znotraj organov in institucij Skupnosti in da se ustanovi neodvisni nadzorni organ, odgovoren za spremljanje obdelave osebnih podatkov. Na ta način bi se popolnoma razvil sistem varstva osebnih podatkov, ki ne zahteva le določitve pravic posameznikov in dolžnosti obdelovalcev podatkov, ampak tudi ustrezne sankcije za kršitelje in nadzor neodvisnih nadzornih organov.
- **Direktiva Evropskega parlamenta in Sveta** 2002/58/ES (http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:SL:HTML) **o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij**, v kateri sta za področje CIIP še posebej pomembna dva člena: **4. člen**, ki narekuje ponudnikom javno razpoložljive elektronske komunikacijske storitve, da sprejmejo ustrezne tehnične in organizacijske ukrepe in s tem zagotovijo **varnost** svojih storitev, in **5. člen,** v katerem je točneje opredeljena **zaupnost sporočil** in izvedba le-te, saj prepoveduje poslušanje, prisluškovanje, shranjevanje ali prestrezanje in nadzorovanje komunikacij (sporočil) brez privolitve uporabnikov, razen v zakonsko dovoljenih izjemah.

- **Resolucija Sveta EU** 2003/C 48/01 (http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32003G0228(01):EN:HTML) **o evropskem pristopu h kulturi omrežne in informacijske varnosti**, v kateri se promovira oz. poudarja varnost kot ena bistvenih sestavin javnega ali zasebnega nadzora tako, da se vzpodbuja dodeljevanje oz. širjenje odgovornosti, omogoča primerno izobraževanje in urjenje, še posebej pa osveščanje o varnostnih problemih med mladimi uporabniki IKT, uvaja primerne ukrepe kot odgovor na varnostne nezgode in vzpodbuja sodelovanje med akademskimi krogi ter podjetji za izdelavo in zagotovitev varnih tehnologij in naborov ter razvoj splošno priznanih standardov. Hkrati pozdravlja namero Evropske komisije o ustanovitvi posebne kibernetsko-varnostne enote in uporabnike informacijskih sistemov poziva k bolj holističnemu pogledu na nevarnosti, do katerih prihaja tako zaradi fizičnih elementov, človeških napak, kot tudi tehnoloških ranljivosti ali namernih napadov.

Z razvojem služb informacijske družbe postaja omrežna in informacijska varnost pomemben dejavnik v vsakdanjem življenju, zato morajo države članice še naprej razvijati in krepiti vseobsežno strategijo evropske omrežne in informacijske varnosti ter mednarodnega sodelovanja na tem področju. Ob tem pa ne smejo pozabiti na posameznikove pravice do zasebnosti, treba je doseči transparentnost, izmenjavo informacij in sodelovanje med državami članicami, evropskimi institucijami in privatnim sektorjem.

- **Uredba Evropskega parlamenta in Sveta** št. 460/2004/ES (http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:SL:HTML) **o ustanovitvi Evropske agencije za varnost omrežij in informacij (ENISA)**, ki sem jo že predstavil.
- **Sporočilo Komisije Svetu in Evropskemu parlamentu** KOM/2004/702 (http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0702:SL:HTML) **o varovanju kritične infrastrukture v boju proti terorizmu**, ki vsebuje pregled dejavnosti Komisije pri izvajanju varovanja kritične infrastrukture (CI), obenem pa predlaga dodatne ukrepe za krepitev obstoječih instrumentov, izpolnitev nalog in pooblastil, naloženih s strani Evropskega sveta. V tem dokumentu kritično infrastrukturo predstavljajo tisti obrati, omrežja, storitve in premoženja fizične ter informacijske tehnologije, katerih okvara oz. uničenje bi resno vplivalo na zdravje, varnost ali gospodarsko blaginjo državljanov in učinkovito delovanje vlad držav članic. Kritične infrastrukture zajemajo številne sektorje gospodarstva, tudi bančništvo in finance, promet in dostavo, energetiko, komunalne

storitve, zdravstvo, oskrbo s hrano in komunikacijami, kot tudi ključne državne službe. Nekateri **kritični elementi** v teh sektorjih, strogo rečeno, niso „infrastruktura“, temveč so dejansko **omrežja ali dobavne verige**, ki podpirajo oskrbo s ključnimi proizvodi ali storitvami.[6]

Kritična infrastruktura vključuje:

- energetske naprave in omrežja,
- komunikacijsko in informacijsko tehnologijo,
- finance,
- zdravstvo,
- hrano,
- vodo,
- prevoz,
- proizvodnjo, skladiščenje in prevoz nevarnih snovi,
-vlado.

Te infrastrukture imata v lasti in z njimi upravljata tako zasebni kot javni sektor. Evropske kritične infrastrukture so izredno povezane in visoko soodvisne. Postale so bolj odvisne od skupnih informacijskih tehnologij, zaradi medsebojne povezanosti in soodvisnosti so te infrastrukture bolj ranljive za motnje ali uničenje. Raziskovati je potrebno merila za določanje faktorjev, zaradi katerih je določena infrastruktura ali njen element kritičen.

Za ugotavljanje te kritičnosti se predlaga naslednje **faktorje**:

- domet (geografski obseg – mednarodni, državni, pokrajinski/teritorialni ali lokalni),

– obseg (stopnja vpliva ali izgube – nična, zmerna ali velika; merila pa npr.: posledice za prebivalstvo, gospodarstvo, okolje, soodvisnost med elementi CI in politične posledice),

– časovni učinek (to merilo ugotavlja, na kateri točki naj bi se pokazale resne posledice, npr. takoj, v 24-ih do 48-ih urah, po enem tednu…).

Ne sme se zanemariti psiholoških učinkov, ki lahko poslabšajo dogodke. Varovanje kritične infrastrukture (CIP) zahteva dosledno partnerstvo na temelju sodelovanja med lastniki in upravljavci kritične infrastrukture ter organi držav članic. Za upravljanje s tveganjem znotraj fizičnih obratov, dobavnih verig, informacijskih tehnologij in

[6] Na primer: oskrba s hrano ali vodo v naših večjih mestnih središčih je odvisna od nekaj ključnih obratov, toda tudi od kompleksne mreže proizvajalcev, predelovalcev, izdelovalcev, distributerjev in trgovcev na drobno.

komunikacijskih mrež so odgovorni predvsem lastniki in upravljavci. Občasno lahko pride do določenih tveganj ali groženj terorističnega napada, ki zahtevajo takojšnje ukrepanje. V teh primerih bo od držav članic, vlad in industrije potreben dobro usklajen in operativno naravnan odziv.

Glede na veliko število potencialno kritičnih infrastruktur in njihovih posebnih značilnosti je nemogoče vse varovati z ukrepi na evropski ravni. Z uporabo načela subsidiarnosti mora Evropa osredotočiti svoja prizadevanja na varovanje infrastruktur s čezmejnim učinkom in prepustiti ostale v pristojnost držav članic, toda v skupnem okviru.

Komisija bo vsako koledarsko leto ostalim ustanovam s sporočilom poročala o napredku. Nadalje bo Komisija v tem sporočilu po potrebi predlagala posodobitve in horizontalne organizacijske ukrepe, za katere obstaja potreba po uskladitvi ali sodelovanju. *To sporočilo, ki bo združevalo vse sektorske analize in ukrepe, bo predstavljalo podlago za Evropski program za varovanje kritične infrastrukture (EPCIP).* Ta program bo poskušal pomagati industriji in vladam držav članic na vseh ravneh EU, ob upoštevanju njihovih individualnih nalog in pooblastil ter odgovornosti.

Pri sestavljanju programa lahko pomaga mreža, ki bi združevala strokovnjake programa pobud Skupnosti iz držav članic EU – ta Informacijska mreža za opozorila o kritični infrastrukturi (CIWIN) bi se morala vzpostaviti čim prej v letu 2005. Cilj EPCIP in naloga Komisije bi bila v celotni Uniji zagotoviti ustrezne in enake stopnje zaščitne varnosti na kritični infrastrukturi, čim manj nezavarovanih točk odpovedi ter hitre in preverjene ukrepe za odpravo posledic, EPCIP bi pomenil stalen proces.

- **Okvirni sklep Sveta** 2005/222/PNZ (http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:SL:HTML) **o napadih na informacijske sisteme**, s ciljem poenotenja določb kazenskega prava in izboljšanja sodelovanja med pravosodnimi in drugimi specializiranimi organi službenega pregona držav članic na področju napadov na informacijske sisteme. Velike vrzeli in razlike v zakonodaji držav članic na tem področju lahko ovirajo boj proti organiziranemu kriminalu in terorizmu ter otežijo učinkovito policijsko in pravosodno sodelovanje na področju napadov na informacijske sisteme.

Z zagotovitvijo skupnega pristopa do tega področja v Evropski uniji je treba dopolniti delo, ki so ga opravile mednarodne organizacije, zlasti delo Sveta Evrope na področju približevanja kazenske zakonodaje in delo skupine G8 o transnacionalnem sodelovanju glede kriminala na področju visokih tehnologij.

Kazensko zakonodajo na področju napadov na informacijske sisteme je treba približati, da se zagotovi največje možno policijsko in pravosodno sodelovanje na področju kaznivih dejanj, povezanih z napadi na informacijske sisteme, ter s tem pripomore k boju proti organiziranemu kriminalu in terorizmu.

Z zagotovitvijo skupnih opredelitev kaznivega dejanja nezakonitega dostopa do informacijskega sistema, nezakonitega poseganja v sistem in nezakonitega poseganja v podatke je treba doseči skupni pristop k sestavnim elementom kaznivih dejanj in doseči, da so za napade na informacijske sisteme v vseh državah članicah predpisane učinkovite, sorazmerne in odvračalne kazenske sankcije.

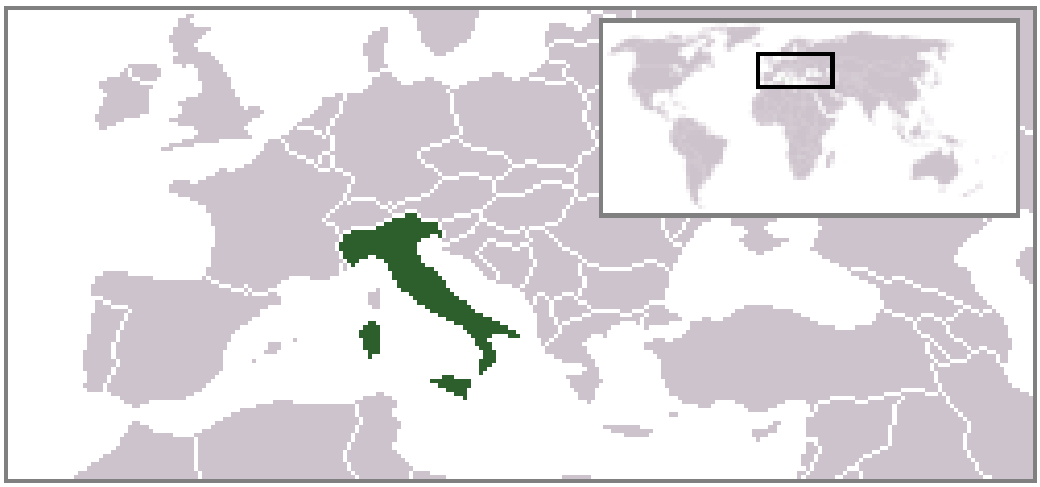
V ta namen so v okvirnem sklepu izdelani in opredeljeni naslednji pojmi: informacijski sistem, računalniški podatki, pravna oseba, neupravičen dostop ali poseganje, nezakonit dostop do informacijskih sistemov, nezakonito poseganje v sistem, nezakonito poseganje v podatke, napeljevanje ter pomoč in podpiranje ali poskus, poleg tega pa so opisane tudi odgovornosti in kazni za pravne osebe ter sodne pristojnosti držav članic kot tudi Unije. Za izpolnitev določb tega sklepa je določen 16. marec 2007.

3. ZAŠČITA KRITIČNE INFORMACIJSKE INFRASTRUKTURE – ŠTUDIJA PRIMERA ITALIJE

Kratka predstavitev italijanske države:

Slika 1: Geografska umestitev

Repubblica Italiana:



Vir: http://sl.wikipedia.org/wiki/Italija

Republika Italija je južnoevropska obmorska država z dvema velikima otokoma v Sredozemskem morju, Sicilijo in Sardinijo, z glavnim mestom Rim. San Marino in Vatikan sta neodvisni državi znotraj italijanskega ozemlja.

Uradni jeziki so italijanščina, nemščina na južnem Tirolskem in francoščina v dolini Aoste. Na kopnem meji na Francijo, Švico, Avstrijo in Slovenijo.

Po površini je z nekaj več kot 300.000 km^2 69. na svetu, po prebivalstvu pa z nekaj manj kot 58 milijoni 22. v svetovnem merilu.

Upravno je razdeljena na 20 dežel, od katerih jih 5 uživa poseben avtonomen status: Aosta, Furlanija – Julijska krajina, Sardinija, Sicilija in Trentinsko – Južna Tirolska (http://sl.wikipedia.org/wiki/Italija).

3.1. Opredelitev CIIP (konceptualna in vsebinska analiza)

Glavna premisa, ki se pojavlja v italijanski politiki CIIP, je, da je javna blaginja države vse bolj odvisna od informacijsko-telekomunikacijsko-tehnoloških (IKT) sistemov. IKT ima pomembno vlogo v številnih kritičnih sektorjih v italijanski družbi. V Italiji ni uradnih definicij, ki bi opredeljevale **kritične sektorje**, vendar pa se večjo pozornost posveča predvsem tem sektorjem:

- bančništvu in financam,
- civilni obrambi,
- e-vladi,
- energiji,
- javni upravi
- (tele-) komunikacijam,
- javnemu zdravstvu,
- plinskim omrežjem,
- transportnim sistemom na kopnem in v zraku,
- vodam

(Dunn in Wigert, 2004: 113, 114).

Prvič se je CIIP kot termin uradno pojavil v diskusijah na sestanku, ki se je odvijal na Ministrstvu za zunanje zadeve, organiziran s strani Generalnega direktorata za ekonomsko sodelovanje, v marcu 2000, veljal pa je kot pripravljalno srečanje med Italijo in ZDA z namenom določitve potencialnega sodelovanja na znanstvenem in tehnološkem področju. Drugi tak dogodek in priložnost za nadaljnje spoznavanje in reševanje problema CIIP je bilo delovno srečanje med kabinetom italijanskega ministrskega predsednika in ambasado ZDA meseca maja 2002 v Rimu.

Temu je sledila **ustanovitev delovne skupine za zaščito kritične informacijske infrastrukture** na **Ministrstvu za inovacije in tehnologijo** v marcu **2003**. V to delovno skupino so vključena vsa ministrstva, ki upravljajo kritične infrastrukture, skupaj z lastniki in operaterji teh infrastruktur, kot tudi nekateri raziskovalni inštituti. Cilj te delovne skupine je bil pomagati italijanski vladi v boljšem razumevanju problemov, povezanih s CIIP, še posebej naključnih ali namernih hib oz. napak, po drugi strani pa pripraviti osnove za identifikacijo organizacijskih zahtev in pobud za povečanje čvrstosti kritičnih infrastruktur (Dunn in Wigert, 2004: 113).

3.2. Zgodovinski razvoj CIIP v Italiji

Italija je že v zgodnjih 90-ih letih prejšnjega stoletja začela uvajati specifično zakonodajo in ministrske dekrete, ki se nanašajo na področje CIP in CIIP. Od takrat je nastala množica dekretov in zakonov, ki se posredno ali neposredno dotikajo teme moje diplomske naloge, zato se bom omejil le na tiste, ki po mojem mnenju najbolj neposredno zadevajo to temo.

3.2.1. Prvi pomembnejši italijanski zakoni s področja CIIP

Prvi tak zakon je bil sprejet decembra 1993 **(Zakon 547)** in daje večjo moč in pooblastila preiskovalcem v fazi priprave dokazov kakor tudi za prestrezanje in prisluškovanje računalniških telekomunikacij. S tem zakonom je Italija postala **ena prvih evropskih držav, ki je začela sistematično pravno urejati to področje**, predvsem zaradi pojava novih oblik kriminala s področja računalniških prevar, goljufij, uničevanja ali spreminjanja podatkov, računalniških zlorab, nepooblaščenega prestrezanja računalniških komunikacij in sabotaž. Velika pozornost tem zločinom je posvečena predvsem zaradi dejstva, da so **računalniški vdori opredeljeni kot kršitve zoper privatno lastnino**. Inovativnost tega zakona se kaže tudi v konceptu »High Tech Crime«, ki je že bil uveljavljen v italijanski kazenski zakonodaji (člen 420), saj že samo namere ali poskuse omenjenih kriminalnih dejanj pojmuje kot kaznive.

Naslednji zakon iz decembra 1996 **(Zakon 675)** se nanaša na zaščito osebnih podatkov.

Sledi **zakon št. 248** o piratstvu, povezanem z IKT iz leta 2000.[7]

Leta 2001 pa je bil sprejet **zakon št. 438**, namenjen izboljšanju zakonodajnih instrumentov in zatiranju terorizma, ob katerem je treba posebej poudariti, da se kriminalna dejanja, zagrešena v Italiji, sodno preganjajo in obravnavajo tudi, če so usmerjena v druge države ali multilateralne inštitucije (Dunn in Wigert, 2004: 325).

3.2.2. Vladne smernice za razvoj informacijske družbe

Ministrstvo za inovacije in tehnologijo je junija 2002 izdalo obsežen dokument (124 strani) z naslovom **»Linee guida del Governo per lo sviluppo della Societa dell'Informazione nella legislatura«** (Vladne (zakonodajne) smernice za razvoj informacijske družbe). S tem

[7] Ta zakon ima podlago v dekretu št. 518 že iz leta 1992.

dokumentom se italijanska vlada zavezuje postaviti Italijo kot eno vodilnih držav v digitalni dobi, še posebej se posveča modernizaciji države z uvajanjem in uporabo novih IKT, tako v zasebnem kot tudi v javnem sektorju, s pospeševanjem in izboljševanjem e-vlade in e-poslovanja, skratka z uporabo novih tehnologij na vseh državnih nivojih in področjih. Prav tako vladne smernice urejajo omrežno varnost in v ta namen vpeljujejo nacionalni plan za zaščito in zasebnost IKT sistemov, s tem želijo vzpostaviti varnostni sistem, ki bi povečal zaupanje uporabnikov v internet, tako zasebnih kot poslovnih, še posebej v komunikaciji in poslovanju z vlado oz. vladnimi inštitucijami.

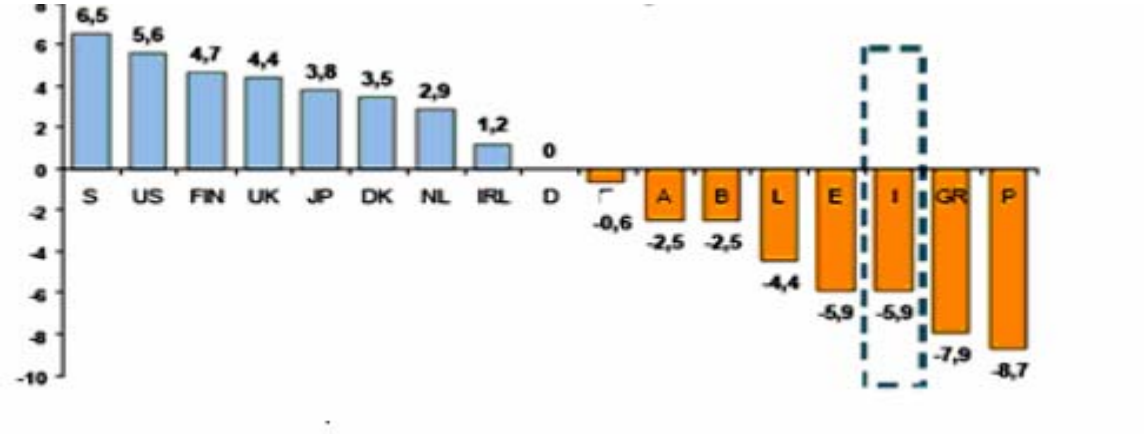
Dokument[8] (Linee guida del Governo per lo sviluppo della Societa dell'Informazione nella legislatura, 2002) je zgrajen **iz štirih vsebinskih delov:**

3.2.2.1. Scenariji in politike za informacijsko družbo

Prvi del opisuje scenarije v novem socialno-ekonomskem kontekstu, povezane z inovacijami, evolucijo IKT tehnologij in primerjavo z EU, kako se to odraža v Italiji (razvoj podobnih sistemov), in kakšno politiko mora Italija voditi na inovacijsko-tehnološkem področju (programske smernice).

Na grafih, ki sledijo, je viden zaostanek Italije v 90-ih letih na področju inovacij in investicij v IKT (grafa 1, 2), IKT pismenosti in v razpoložljivih vladnih on-line službah (grafa 3, 4), torej zaostajanje italijanske informacijske družbe v celoti.

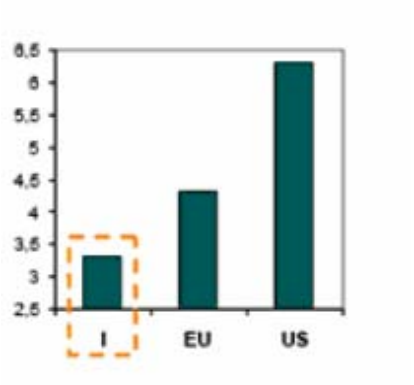
Graf 1: Sintetični indeks inovacij



Vir: Linee guida del Governo per lo sviluppo della Societa dell'Informazione nella legislatura (2002: 16).

[8] http://www.innovazione.gov.it/ita/documenti/socinfo11_06_02.pdf

Graf 2: Delež IKT v % v PIL (svežem investicijskem kapitalu na borznih trgih) v 90-ih letih; primerjava Italija – EU - ZDA

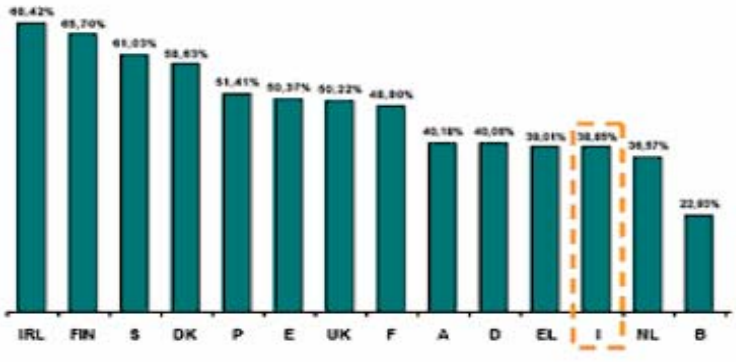


Vir: Linee guida del Governo per lo sviluppo della Societa dell'Informazione nella legislatura (2002: 16).

Graf 3: % delavcev, opismenjenih z IKT

Vir: Linee guida del Governo per lo sviluppo della Societa dell'Informazione nella legislatura (2002: 17).

Graf 4: Razpoložljivost oz. dostopnost vladnih on-line služb



Vir: Linee guida del Governo per lo sviluppo della Societa dell'Informazione nella legislatura (2002: 18).

Prikazane **zaostanke poskuša italijanska vlada zmanjšati s tremi osnovnimi smernicami**:

a) transformacijo javne uprave s pomočjo novih IKT,

b) realizacijo ukrepov na državnem nivoju, povezanih z inovacijami in izvedbo informacijske družbe, s čimer bi se povečala konkurenčnost, in

c) z mednarodnim sodelovanjem, v katerem je Italija v okviru G8 odgovorna za program e-Government for developement; digitalizacijo javnih uprav v deželah v razvoju, kateremu nudi podporo tudi OZN; pa tudi v okviru EU sodeluje v pripravi načrta e-Evrope 2005, ki zadeva izdelavo omrežnih povezav (bilateralnih) s partnerskimi državami (Ibid.).

3.2.2.2. Preobrazba javne uprave; e-vlada

Te smernice se nanašajo na informatizacijo javne uprave na treh ravneh, in sicer na:

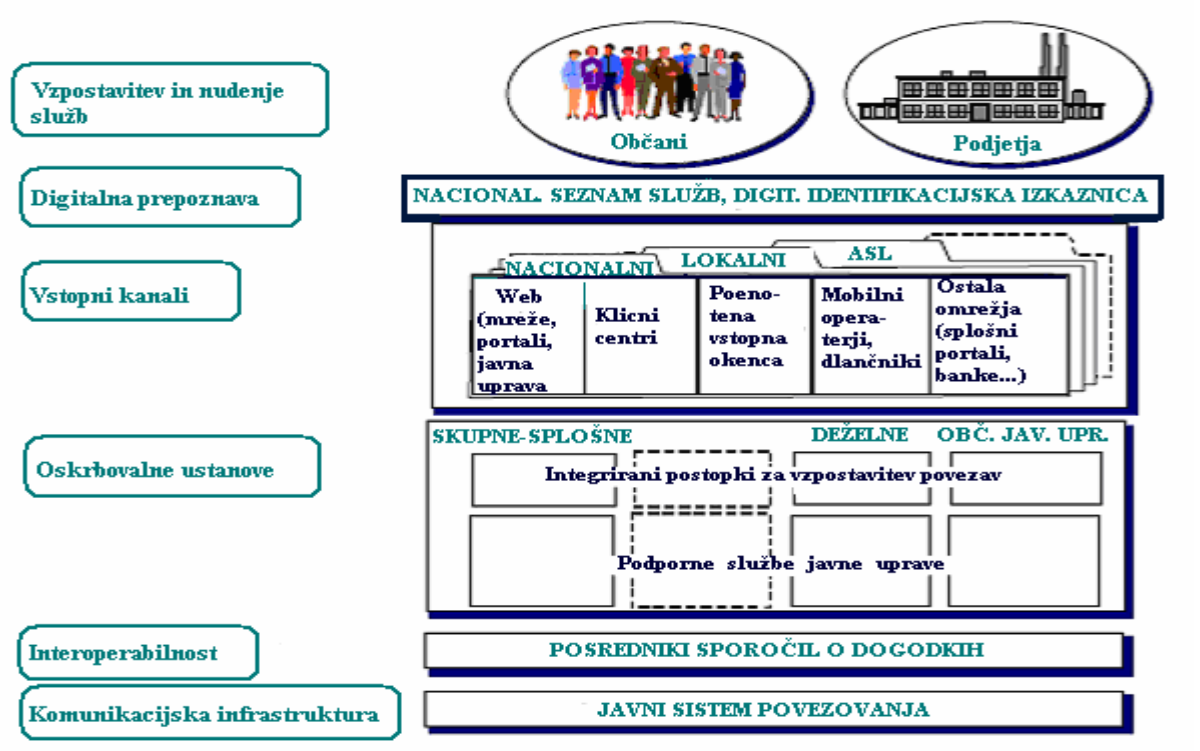
a) centralno javno upravo,

b) lokalno javno upravo,

c) ukrepe za preobrazbo obstoječih infrastruktur.

Za realizacijo in pomoč pri izvajanju smernic je bila v ta namen ustanovljena Nacionalna agencija za tehnološke inovacije.

Shema 1: Model e-vlade javne uprave v Italiji



Vir: Linee guida del Governo per lo sviluppo della Societa dell'Informazione nella legislatura (2002: 28)

Predstavljeni model e-vlade javne uprave sestavlja **šest osnovnih (ključnih) elementov:**

a) vzpostavitev in nudenje služb;

skupek služb, ki morajo biti na razpolago občanom in podjetjem (strankam uporabnikom),

b) digitalne prepoznave;

postopki prepoznave uporabnikov in varnih elektronskih podpisov preko elektronske osebne izkaznice, nacionalne izkaznice služb in elektronskega podpisa,

c) vstopni kanali;

skupek novih inovativnih in raznovrstnih kanalov, skozi katere lahko uporabniki vstopajo v ponujene omrežne storitve: internet, klicni centri, mobilna telefonija, omrežja tretjih oseb…,

č) lokalne skupnosti, regije (dežele), organizacije, upravljavci (računalniški administratorji),

d) interoperabilnost in sodelovanje;

vmesniški standardi med različnimi administrativnimi službami, ki omogočajo učinkovite in pregledne notranje in zunanje povezave,

e) komunikacijska infrastruktura;

ki bi povezala in združila vse administrativne službe.

Poleg teh komponent naj bi tehnologije, ki so na razpolago, omogočile večjo učinkovitost znotraj javne uprave in vrednotenje človeških virov, njihovo učinkovitost in »know-how«.

Za vzpostavitev tega modela javne uprave pa bo potrebno izpolniti naslednje **zakonodajne cilje**:

1. vse službe in njihove storitve morajo biti na razpolago občanom in podjetjem tudi on-line,
2. treba je vzpostaviti notranje učinkovito javno upravo,
3. ponovno je potrebno ovrednotiti človeške vire,
4. omogočiti transparentnost in dostopnost vseh postopkov v uporabi,
5. kvaliteto v izvajanju.

Poleg tega so javne uprave dolžne upoštevati tudi posebne zahteve, izhajajoče iz specifične narave njihovega dela, ki pokrivajo posamezna ministrstva.

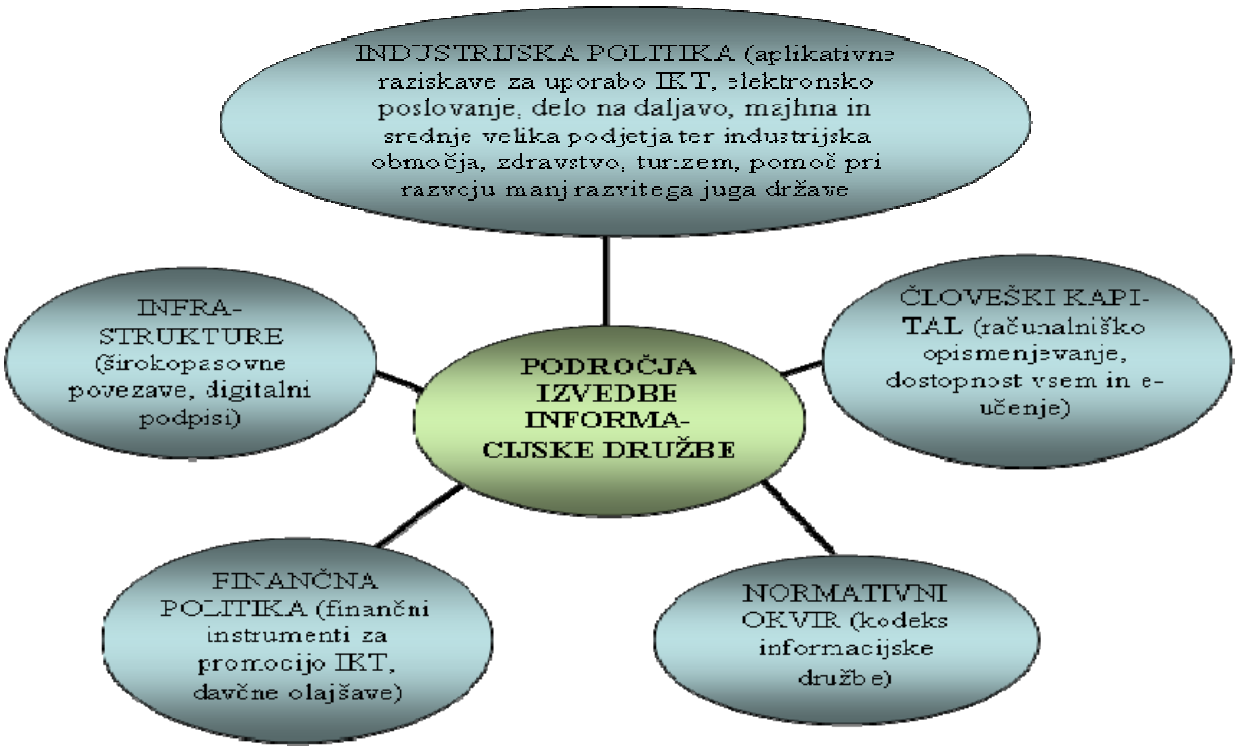
IKT postaja tisti strateški vir, ki bo na novo določil odnos med lokalnimi avtonomijami in jih uskladil na nacionalnem nivoju ter tako dosegel federalistični institucionalni ustroj. Glede na to in upoštevajoč dejstvo, da se IKT in njena zaščita uporablja tako v zasebnem, kot tudi v javnem sektorju, predvsem internet, sta **Ministrstvo za komunikacije** ter **oddelek za inovacije in tehnologijo izdelala strategijo za zaščito IKT, ki temelji na petih predpostavkah**:

- uvajanju te direktive, ki definira osnovne varnostne zahteve,
- ustanovitvi nacionalnega tehničnega komiteja za zaščito IKT, ki bo koordiniral aktivnosti do vzpostavitve sistema,
- vzpostavitvi organizacijskega modela za zaščito IKT kot osnovi za določanje pristojnosti in odgovornosti, sposobni razvijati smernice, priporočila in vse standarde ter verifikacijske procedure,
- vpeljavi nacionalnega načrta za zaščito IKT, s katerim se določa aktivnosti, odgovornosti, potrebne metodologije in čas oz. termine za izvedbo,
- evalvaciji varnosti oz. zaščite IKT v javnih upravah v roku 5-ih let, vsi postopki in standardizacija morajo biti izvedeni v predvidenem času.

Kar zadeva obdelavo osebnih podatkov, mora biti le-ta usklajena z že omenjenim zakonom 675/96, ki v 15. členu določa potrebo po stalnem nadzoru in izvajanju zaščite skladno z razvojem novih tehnologij in s tem povezanih vdorov v informacijske sisteme. Le tako se lahko zagotovi ustrezno raven zaščite in informacijsko varnost (Ibid.).

3.2.2.3. Ukrepi na državnem nivoju

Shema 2: Področja izvedbe informacijske družbe



Povzeto in prirejeno po: Linee guida del Governo per lo sviluppo della Societa dell'Informazione nella legislatura (2002)

Te ukrepe opredeljuje 5 večjih sklopov področij izvajanja informacijske družbe, ki so prikazani v shemi 2, uresničeni pa bodo v sodelovanju z zato odgovornimi posameznimi upravnimi organi s točno določenimi finančnimi potrebami in z usmerjanjem Ministrskega komiteja za informacijsko družbo, minister za inovacije in tehnologijo pa bo koordinator vseh dejavnosti. Uresničevanje in izvedbo se bo merilo na podlagi 10-ih indikatorjev, s katerimi se bo lahko primerjal napredek v primerjavi z ostalimi državami, članicami EU, cilj pa je v nekaj letih pripeljati Italijo v skupino 7-ih najbolj razvitih na osnovi teh indikatorjev:

Tabela 1: Indikatorji IKT napredka v Italiji

Indikator	Mesto, ki ga je Italija zavzemala v EU l. 2001
% prebivalstva, ki uporablja internet	13
% družin (gospodinjstev), ki uporabljajo internet	11
% razširjenosti širokopasovnih povezav	12
Število os. računalnikov z internetno povezavo na 100 študentov	13
% učiteljev, ki uporabljajo internet v didaktične namene	10
% računalniško opismenjenih delavcev	9
% delavcev, ki se poslužujejo dela na daljavo	13
% denarja v obtoku preko e-poslovanja	9
% komunalnih infrastruktur, dostopnih preko interneta	10
% kulturnih dobrin, dostopnih preko interneta	--

Vir: Linee guida del Governo per lo sviluppo della Societa dell'Informazione nella legislatura (2002: 72)

3.2.2.4. Mednarodno sodelovanje: e-vlada za razvoj

Cilj je dokončanje že uvedenih projektov s prvimi petimi državami (Albanija, Gruzija, Mozambik, Nigerija in Tunizija), ki sodelujejo v izvedbi programa, širjenje tega programa tudi na druge zainteresirane države v razvoju, vzpostavitev takšne izvedbene strukture, ki bo omogočila prilagajanje različnih modelov, nudila organizacijsko in administrativno podporo, sodelovanje z ostalimi projektnimi partnerji in stalno možnost nadzora.

V sklopu EU je Italija sodelovala v pripravi programa e-Evropa 2003-2005 in kot predsedujoča je v drugi polovici leta 2003 pripravila konferenco na temo e-vlada, poleg tega

pa Italija nenehno povečuje svojo vlogo v različnih multilateralnih telesih, ki obravnavajo tematiko informacijske družbe (tudi v sklopu **OZN**, kjer se obravnava **tematika digitalizacije**, **G8**, kjer je v teku **izvajanje programa »Dot Force«**, na različnih omizjih in delovnih srečanjih v sklopu **OECD**, kjer je sodelovala pri pripravi **konferenc o informacijski družbi**, ki sta potekali v Ženevi, 2003 in Tunisu, 2005).
Za naslednji cilj pa si je MIT (Ministrstvo za inovacije in tehnologijo) zadalo vzpostaviti mrežo bilateralnih odnosov z glavnimi italijanskimi partnerji tako znotraj EU, kot tudi z državami južne Amerike, pa vse do Azijskih držav, s tem Italija bi vzpostavila odnose z glavnimi mednarodnimi raziskovalnimi telesi na področju napredne informacijske in komunikacijske tehnologije (Ibid.).

Če torej na kratko povzamem ta obsežen dokument, bi lahko dejal, da zelo natančno opredeljuje načine, postopke in sama dejanja za dosego nacionalnega načrta prehoda v informacijsko družbo, s katerim bi se ob uporabi novih IKT v javnem in zasebnem sektorju omogočila nacionalna konkurenčnost nasploh in vpeljal načrt za IKT zaščito in zasebnost, ki temelji na naslednjih osnovnih dejanjih:

- vpeljavi zaščitno-varnostne direktive za področje IKT (da se določi osnovni minimum varnosti, ki jo morajo doseči vsa vladna ministrstva);
- ustanovitvi nacionalno tehničnega komiteja za IKT zaščito (ki bo koordiniral vse aktivnosti);
- vzpostavitvi organizacijskega modela za IKT zaščito (v katerem bodo upoštevane smernice, priporočila, standardi in certifikacijski postopki);
- predstavitvi in uvedbi nacionalnega načrta za IKT zaščito (za določitev aktivnosti, odgovornosti za izvajanje po posameznih področjih in skrajnih rokov za uvedbo potrebnih standardov in metod oz. postopkov za preverjanje varnosti in zaščite na vladnem področju);
- končnem preverjanju zaščite IKT na področju javne uprave v roku petih let.

Italijanska vlada pospešeno izvaja reformo javne uprave, s katero želi čim bolj približati sodobne oz. moderne storitve svojim državljanom. Potrebni koraki so bili podrobno opredeljeni že v juniju 2000 v »akcijskem načrtu za e-vlado«, v katerem je opredeljen model za e-vlado, ki mora temeljiti na sodobni infrastrukturi, ki bo omogočala učinkovite in varne pogoje za številne osnovne izvedbene funkcije. Da bi dosegli ta cilj, je MIT razvil naslednje

strateške referenčne točke ali kot sem jih že prej imenoval in predstavil; ključne elemente za e-vlado:

- zagotavljanje različnih služb,
- digitalno prepoznavo,
- vstopne kanale,
- agencije, ki bodo preskrbovale oz. servisirale te službe,
- interoperabilnost in sodelovanje,
- komunikacijsko infrastrukturo.

3.2.3. Pomembnejši novejši italijanski dokumenti s področja CIIP

Še posebej v zadnjem triletju Italija normativno intenzivno ureja to področje s priporočili in celo časovnimi določitvami za njihovo realizacijo v praksi.

3.2.3.1. Zaščita kritične informacijske infrastrukture – primer Italije

Že omenjena delovna skupina za zaščito kritične informacijske infrastrukture je v oktobru leta 2003 izdala dokument z naslovom: »**Protezione delle Infrastrutture Critiche Informatizzate – La realta Italiana**« ali Zaščita kritične informacijske infrastrukture – primer Italije.

Ta dokument je podrobno predstavljen v intervjuju z Luiso Franchina, generalno direktorico Višjega inštituta za komunikacije in informacijske tehnologije - ISCOM pri Ministrstvu za komunikacije (http://www.isacaroma.it/html/newsletter/?q=node/33). V njem so izpostavljena vsa prizadevanja za ureditev tega področja, opisani so elementi italijanske infrastrukture ter njihova medsebojna soodvisnost in predlagana nadaljnja CIIP strategija. Delovna skupina še posebej predlaga, naj se polna odgovornost za implementacijo te politike dodeli posameznim lastnikom in operaterjem kritične infrastrukture, medtem ko bi bila vlada odgovorna za definiranje splošnih smernic, ki bi zmanjšale soodvisnosti in verižne razpade sistemov. Poleg navedenega pa v dokumentu predlagajo tudi:

- ustanovitev nacionalne interesne skupine za kritično infrastrukturo (GdIN – Gruppo di Interese Nazionale), ki bi nadzorovala zahteve različnih lastnikov in operaterjev,
- določitev nacionalne raziskovalne in razvojne agende na področju zaščite kritične infrastrukture,
- realizacijo virtualnega centra za simulacije in analizo soodvisnosti (SAI – Centro Virtuale di Simulazione e Analisi delle Interdipendenze).

3.2.3.2. Predlogi, ki zadevajo strategijo za zaščito IKT v javni upravi

Novonastali **Nacionalni tehnični komite za IKT zaščito** je tako že v marcu 2004 izdal dokument z naslovom: »**Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione**« - Predlogi, ki zadevajo strategijo za zaščito IKT v javni upravi, v katerem so izdelani organizacijski modeli, ki jih bo morala javna uprava doseči za zagotovitev zaščite in varnosti v svojih IKT sistemih in tudi v sami upravi.

V dokumentu so razdelane ter podrobno dodeljene naloge in odgovornosti posameznih dejavnikov (ministrstev, institucij, organov, ustanov…) za zagotovitev osnovnih funkcij pri zagotavljanju zaščite oz. varnosti. Nekatere imajo naravo centralizirane oblike vodenja in je zanje tudi predvidena ustanovitev potrebnih organizmov, skozi katere se bo zagotovila preskrba s službami, potrebnimi za zagotovitev varnosti v javnih upravah, medtem ko se bodo druge naloge izvajale znotraj posameznih javnih uprav.

Centralizirana oblika je po tem modelu s strani **Ministrstva za komunikacije** in **Ministrstva za inovacije in tehnologijo** z dekretom **24/7/2002 dodeljena** prav **Nacionalnemu tehničnemu komiteju za IKT zaščito**, ki ima nalogo koordinatorja in nadzornika pri zagotavljanju IKT zaščite v javnih upravah, tudi v skladu z mednarodnimi standardi. Pripravlja krizni nacionalni načrt za IKT v javnih upravah in letno preverja stanje napredka ter predlaga nadaljnje ukrepe po potrebi, razvija pa tudi organizacijski model za IKT zaščito, katerega raven razvoja in samo aplikacijo tudi preverja. Ker pa sam komite ne more zagotavljati in izvajati operativnih služb za potrebe javnih administracij, predlaga ustanovitev takšnega organa, ki bo sposoben zagotoviti zahtevano operativnost in bo razpolagal z zato potrebnimi sredstvi. Temu organu so dodelili ime **Centro Nazionale per la Sicurezza Informatica (CNSI) – Nacionalni center za informacijsko varnost**, ki bo imel določeno organizacijsko avtonomijo in pristojnosti, podobne agencijam ali višjim komisariatom, kar pomeni, da mora biti popolnoma avtonomen in neodvisen od informacijsko-zaščitnih proizvodov ali temu namenjenih služb, imeti mora posredne ali neposredne pristojnosti in zmožnosti za oceno informacij, pridobljenih iz drugih virov, poleg tega pa mora biti sposoben kadarkoli in v čim krajšem možnem času nuditi potrebne kvalitetne povratne informacije (Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione, 2004:18).

Kako je organiziran in kako deluje, pa bom podrobneje predstavil v naslednjem poglavju, ko bo govora o dejavnikih, ki tvorijo, razvijajo in izvajajo CIIP v Italiji. V nadaljevanju bom tudi

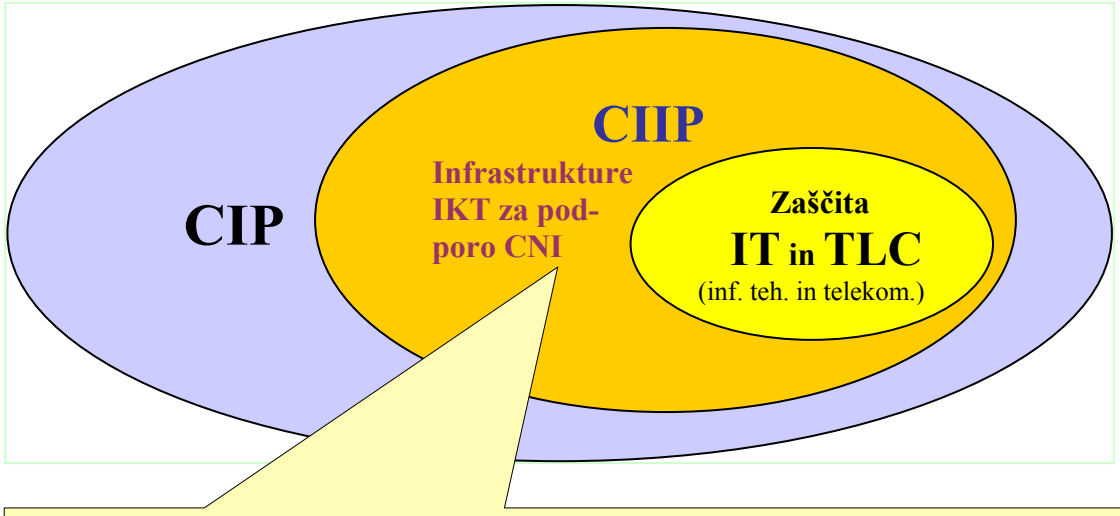
podrobneje opisal delovanje Nacionalnega tehničnega komiteja za IKT zaščito ter ostale pomembne nosilce izvajanja CIIP.

Prej pa je potrebno predstaviti vsaj še tri novejše dokumente zadnjih dveh let, ki se navezujejo na politiko CIIP v Italiji.

3.2.3.3. Varnost omrežij v kritičnih infrastrukturah

Eden takih je vsekakor publikacija, ki jo je leta 2005 izdal **ISCOM – Instituto Superiore delle Communicazioni e delle Tecnologie dell Informazione;** Višji inštitut za komunikacije in informacijske tehnologije, ki deluje v okviru Ministrstva za komunikacije, z naslovom: **La sicurezza delle reti nelle infrastrutture critiche** (Varnost omrežij v kritičnih infrastrukturah).

Shema 3: V pogledu strategij obrambe nacionalnih kritičnih infrastruktur (CIP – Critical Infrastructure Protection) predstavlja CIIP osnovni element, katere pomembnost se povečuje



S terminom **zaščita kritične informacijske infrastrukture** (CIIP – Critical Information Infrastructure Protection) se označujejo vsi tisti postopki in dejanja, ki imajo namen oz. nalogo povečati nivo varnosti (zaščite), zanesljivosti in pravilne izvedbe v vseh kritičnih infrastrukturah, ki delno ali povsem uporabljajo kakršnokoli informacijsko infrastrukturo za njihov nadzor, upravljanje ali obvladovanje.

Vir: La Sicurezza delle Reti nelle Infrastrutture Critiche, 2005:24

V drugem poglavju te publikacije je opisana zaščita nacionalne kritične informacijske infrastrukture s strokovno-tehničnega vidika, od prepoznavanja nevarnosti, oblik groženj, medsebojnih soodvisnosti … do metodologij za reševanje in nemoteno delovanje le-teh.

Namen dokumenta je predstaviti aktivnosti delovne skupine na Ministrstvu za komunikacije, predvsem pa analizirati sledeče aspekte:

- kvaliteto služb in varnost telekomunikacijskih omrežij, upoštevajoč tako nacionalne kot internacionalne standarde in normative,
- problematiko, vzpodbujeno s prisotnostjo medsebojne odvisnosti med CNI (kritičnimi nacionalnimi infrastrukturami) in telekomunikacijskimi infrastrukturami,
- določitev poglavitnih groženj, ki se pojavljajo v telekomunikacijskih infrastrukturah, ki jih uporabljajo CNI,
- določitev osnovnih oz. minimalnih parametrov za vzpostavitev zaščite in opredelitev le-teh na način, ki bo omogočal zadovoljivo zaščito telekomunikacijskih infrastruktur v službi CNI,
- določitev nekaterih minimalnih tehničnih parametrov za kvaliteto služb, ki bodo primerni za zagotavljanje minimalne kritičnosti,
- določitev nekaterih tehničnih parametrov z elementi transparentnosti in zakonskimi termini, ki jih je priporočljivo sprejeti v trgovskih pogodbenih odnosih s ponudniki telekomunikacijskih storitev,
- opis potencialnih vlog, ki jih lahko izvedejo razne institucije pri prepoznavanju in izvajanju skupnih strategij zaščite,
- nekatere predloge za ugotavljanje stopnje kritičnosti in ustrezne organiziranosti znotraj posameznih nacionalnih kritičnih infrastruktur (La sicurezza delle reti nelle infrastrutture critiche, 2005: 25).

V tem dokumentu je ISCOM zasnoval organe za overjanje varnosti in zaščite znotraj sistemov in informacijskih komercialnih proizvodov (programov…), ki omogočajo zagotavljanje stalne zaščite IKT v skladu s splošnimi standardi - »Common Criteria« in ITSEC (Information Technology Security Evaluation Criteria – Kriteriji za varnost informacijske tehnologije) v EU.

V pripravi so tudi posebni programi za ocenjevanje in overjanje kritičnih sistemov, prav tako pa se ISCOM obvezuje, da bo razširjal overjanje in kulturo zaščite IKT na vseh področjih (v javni upravi, podjetjih, kritičnih infrastrukturah, pri občanih …).

3.2.3.4. Varnost omrežij od analize tveganj do strategij zaščite

Drugi tak dokument, ki ga je istega leta (2005) prav tako izdal **ISCOM**, je **La sicurezza delle reti dall` analisi del riscchio alle strategie di protezzione** (Varnost omrežij od analize tveganj do strategij zaščite).

Dokument predstavlja družbeno strukturo omrežij, opisuje aktualno družbo s konotacijo odvisnosti od informacij, s tem povezan nastanek interneta in najpomembnejše pogoje za dosego varnosti in zasebnosti.

V nadaljevanju opredeljuje infrastrukturo omrežij in s tem povezane probleme varnosti s tehničnega vidika in predstavi tudi model enotnega omrežja za javno upravo. Ob tem navaja zakonodajo v svetu in jo primerja z domačo (italijansko). Nadaljuje z analizo ogroženosti, ki je podkrepljena z metodičnim pristopom ugotavljanja kritičnih področij, tako ekonomskih kot etičnih, in temelji na modernem načinu zagotavljanja zaščite glede na izkušnje ter stalno preverjanje ravni ogroženosti in kritičnosti. Samo tako so lahko protiukrepi pravočasni in s tem uspešni.

V zadnjem delu je predstavljeno izvajanje zaščite omrežij v javni upravi in zasebnem sektorju.

Dokument je namenjen predvsem poslovni javnosti in strokovnim delavcem v podjetjih, ki pri svojem delu uporabljajo IKT in se hkrati srečujejo s problemi varnosti in zaščite znotraj omrežij IKT. Skozi zavedanje o tem in poznavanje lastnih struktur ter njihovih značilnosti se lahko optimizira investicije v zaščito z namenom, da se doseže maksimalen učinek (povzeto po: La sicurezza delle reti dall` analisi del riscchio alle strategie di protezzione, 2005).

3.2.3.5. Varnost in prihodnost infrastruktur za električno energijo

Tretji dokument pa je **Sicurezza e Futuro delle Infrastrutture Elettriche** (Varnost in prihodnost infrastruktur za električno energijo)**,** ki ga je leta 2005 izdal **CLUSIT** (Italijansko združenje za informacijsko varnost) in katerega avtor je Augusto Leggio, eden od soustanoviteljev CLUSIT-a.

V dokumentu je podrobno predstavljena električna infrastruktura (sistem za proizvodnjo, prenos in distribucijo električne energije) in njena kritičnost, saj le-ta pomeni enega največjih problemov z varnostnega vidika – njeno pravilno delovanje in oskrba namreč predstavljata osnovo za delovanje (upravljanje) vseh ostalih kritičnih infrastruktur ne le v Italiji, temveč tudi v Evropi in svetu sploh. Italija je velik uvoznik energije, tako električne, kot tudi ostalih energetskih virov (naftnih derivatov, naravnega plina…) in je od uvoza teh virov zelo

odvisna. To se odraža tudi na politiki cen energetskih virov, saj je v tem pogledu Italija ena najdražjih držav v Evropi, če že ne v svetu.[9]

Ko je govora o električni energiji, lahko pri distribuciji le-te prihaja do velikih anomalij, saj zaradi trenutne povečane porabe prihaja do preobremenitev distribucijskih sistemov, njihovih izpadov ali celo do totalnega »black-out-a«, električnega mrka, ki se je v Italiji že zgodil 28. septembra 2003. Ker so ostale kritične infrastrukture v veliki **soodvisnosti** (**interdependency**) od električne, je tako prišlo do popolnega razpada celotnega sistema in Italija je bila v nekaterih delih države popolnoma odrezana od sveta celih 19 ur (v S delu države je bilo normalno stanje vzpostavljeno po približno 5-ih urah, v osrednjem delu po 12-ih urah, na J pa še kasneje).

Ti dogodki so opozorili na izredno pomembnost električne infrastrukture, na soodvisnost z ostalimi kritičnimi infrastrukturami in nenazadnje na potrebo po **zanesljivosti** (**dependability**) v delovanju teh sistemov, saj so se pojavljali elementi kaskadnega razpada (Cascade Failure) in domino efekta v vseh omenjenih sistemih.

Ko govorimo o terminu zanesljivosti, je potrebno poudariti, da je sestavljen iz več dejavnikov:

- razpoložljivosti (pripravljenosti za oskrbo z različnimi službami),
- jamstva (kontinuitete v oskrbi s službami),
- fizične varnosti (nikakršnih škodljivih posledic za ljudi in okolje),
- zaupnosti (tajnosti),
- celovitosti (nikakršne spremembe ali popačenja podatkov) in
- zmožnosti stalnega vzdrževanja (opravljanja potrebnih popravkov in sprememb brez prekinitev v izvajanju), (Leggio, 2005: 25).

Zato je potrebno vse napore za zagotovitev zanesljivosti s strani vlade, industrije, javnega sektorja in ekonomije usmeriti v: varnost omrežij in informacij, nedvoumnost informacij, zaščito kritičnih infrastruktur, brezhibno vodenje podjetij (»corporate governance«), pravočasno obravnavanje ogroženosti informacij in nadzor soodvisnosti znotraj infrastruktur z nadaljnjimi grožnjami (naravnimi nesrečami, terorističnimi napadi, zločinskimi dejanji…), (Ibid.).

---

[9] Te vire Italija nabavlja na prostem trgu in torej poskuša do njih priti po najugodnejših nabavnih pogojih (cenah), kar pa za infrastrukturo lahko pomeni velike težave. Ena takšnih je tudi načrtovana postavitev plinskega terminala v Tržaškem zalivu in v Žavljah pri Trstu, ki dobiva mednarodne razsežnosti s čezmejnim vplivom na okolje in prostor.

Vse aktivnosti za odpravo izrednih razmer in vzpostavitev nadaljnjega izvajanja vseh služb morajo torej biti vnaprej pripravljene in predvidene, vsak sodelujoči subjekt pa mora biti profesionalno podkovan in maksimalno izkoriščen. Vsi odgovori na grožnje morajo biti koordinirani in vpeti v institucionalno strukturo s ciljem, da:

- zaščitijo človeška življenja,
- zaščitijo okolje,
- zavarujejo lastnino,
- omilijo škodo in trpljenje,
- preprečijo širjenje nezgod in izpad služb,
- olajšajo izvedbo preiskav,
- ohranjajo izvajanje pomembnih infrastrukturnih služb,
- čim prej vzpostavijo normalno stanje,
- pospešujejo aktivnosti za pozitivno (psihološko) reakcijo in rekonstrukcijo oseb,
- ocenjujejo učinkovitost izvedenih dejanj z namenom izboljšanja le-teh v prihodnje,
- korektno obveščajo javnost.

Da se ti cilji in aktivnosti lahko dosežejo, pa je praksa pokazala, kako morajo potekati:

- načrti za krizno reševanje morajo biti fleksibilni, ker lahko prihaja ob nesrečah do nepredvidenih dogodkov,
- prednost pri pripravi načrtov je potrebno dati aktivnostim za vzpostavitev normalnega delovanja in ne iskanju vzrokov za nastanek nesreč,
- za to, da je odprava izrednih razmer uspešna, mora biti vpeta v organizacijo oz. službo, ki to odpravo izvaja, ne sme se ji podrediti ali jo prevladati,
- aktivnosti teh organizacij ali služb morajo biti neokrnjene,
- različne organizacije ali oblasti morajo delovati koordinirano,
- zaradi različnih pojavnih oblik samih nesreč ali nezgod ne obstaja univerzalen model za reševanje, zato je potrebno za vsak tak dogodek definirati specifičen model reševanja,
- način reševanja je v marsičem odvisen od ocen lokalnih služb za krizno reševanje, ki so tudi prve na kraju dogodka,
- normativno so te ocene dane od služb, ki izvajajo javni red in mir (policija, gasilci, finančna straža, gozdna uprava, orožniki – »carabinieri«, sem bi lahko poleg navedenih prišteli tudi obalno stražo),
- na kraju dogodka je potrebno vzpostaviti koordinacijsko točko za različne službe, vpletene v odpravo nezgod, z namenom, da se vzpostavi kontinuiteta služb,

- kjer je potrebno, naj subjekt, ki vodi kontrolno točko, vzpostavi čim hitrejšo povezavo s prizadetim območjem in prične z aktivnostmi za odpravo nezgod ter nemoteno izvajanje služb (Leggio, 2005: 36).

Model nacionalnega načrta za krizno reševanje v primeru razpada kritičnih infrastruktur je bil oblikovan z naslednjimi cilji:

- omogočiti vsem subjektom (ki sodelujejo v reševanju kriznih dogodkov), da določijo najprimernejše načine reševanja **usklajeno** z ostalimi sodelujočimi subjekti,
- da se usklajenost doseže, se morajo vsi sodelujoči subjekti **zavedati** svoje **vloge** v reševalnih akcijah,
- **razmejiti** je potrebno različne **nivoje** poveljevanja, nadzora in usklajevanja ter njihovo interakcijo,
- **predvideti** je potrebno določeno **stopnjo fleksibilnosti** v povezavi z lokalnimi okoliščinami.

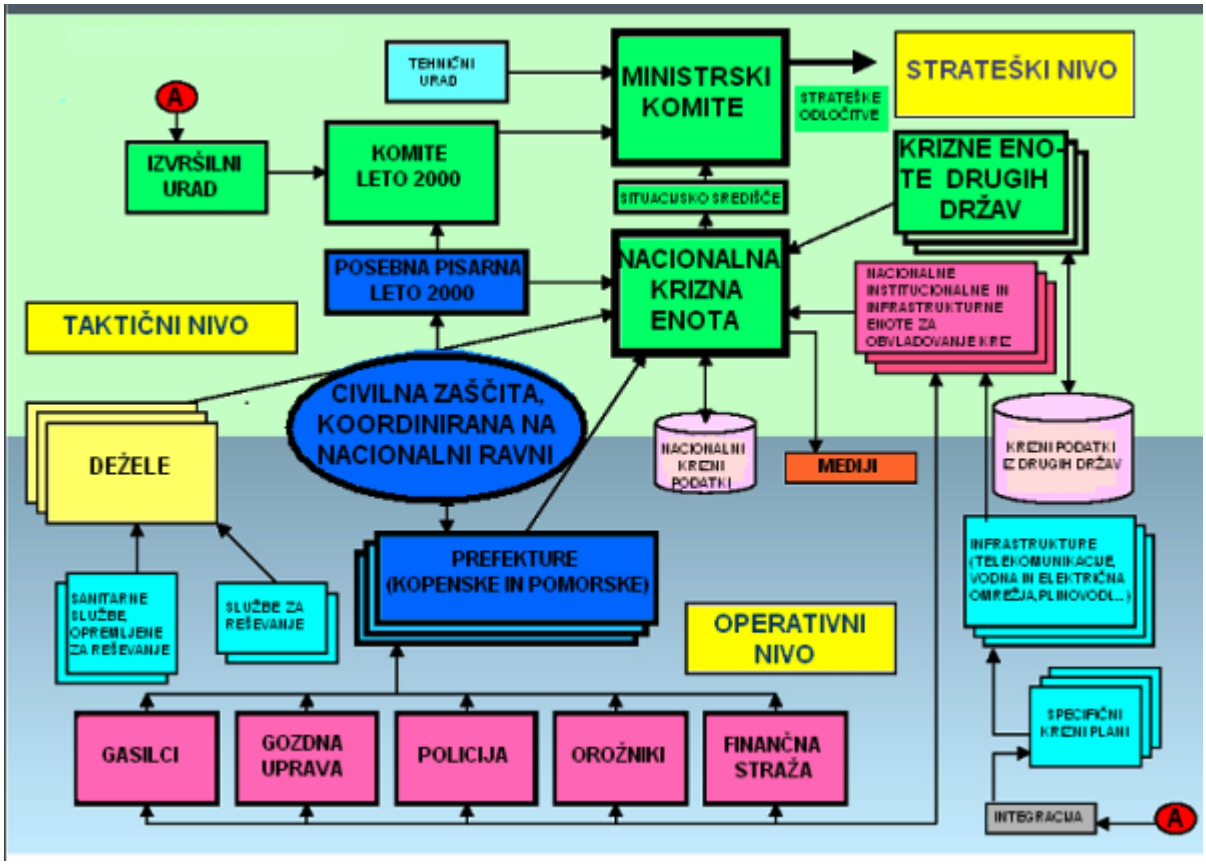
Omenjeni model je strukturiran na treh nivojih poveljevanja, nadzora in usklajevanja:

- **Operativni nivo**:
  - policija
  - orožniki
  - gasilci
  - finančna straža
  - gozdna uprava
  - luške uprave
  - reševalne službe
  - sanitarne službe
  - lokalne kritične infrastrukture (za energijo, telekomunikacije…)
- **Taktični nivo**:
  - pomorske uprave (ki prevzamejo poveljevanje, nadzor in usklajevanje)
  - civilna zaščita
  - sekretariat sveta vlade (in ministrstev)
  - taktični nivo subjektov, ki že delujejo v operativnem nivoju
  - sanitarne službe, opremljene za reševanje
  - infrastrukture na lokalni, regijski in deželni ravni
  - lokalni, regijski in deželni mediji
  - nacionalne krizne enote (ki se povezujejo z kriznimi enotami drugih držav)

- **Strateški nivo**:
  - ministrski svet
  - tehnični sekretariat ministrskega sveta
  - ministri
  - državna, deželna in lokalna oz. mestna vodstva
  - dežele
  - upravni odbor ministrov z operativnimi nalogami, ki poroča predsedniku vlade oz. predsedniku državnega zbora
  - osrednje kritične infrastrukture (državne razsežnosti)

Potreba po aktiviranju vseh teh nivojev pa je **odvisna od razsežnosti** kriznih dogodkov ali nezgod.

Shema 4: Vrednostne relacije italijanskega nacionalnega načrta v kriznih razmerah



Vir: Leggio, 2005: 40

Prav ta model je bil izveden v primeru pojava »milenijskega hrošča« (milenium bug – Y2K). Kot najpomembnejši dejavnik v reševanju krize se je izkazala ravno obširna uporaba telekomunikacij in IKT nasploh, saj so bile pravilne odločitve in ukrepanje odvisni od pravočasnega poznavanja in obdelave različnih informacij, ki so prihajale s terena, tako se je lahko preprečila tudi morebitna eskalacija, pa tudi zastavljeni cilji ne bi bili doseženi brez sodelovanja upravljavcev vseh ključnih infrastruktur, ki so presegli običajne prepreke in težave, tako značilne za tržno okolje pri izmenjavi informacij (Ibid.).

3.3. Definiranje temeljnih dejavnikov, ki tvorijo, razvijajo in izvajajo CIIP

V Italiji ne obstaja centralna enota, ki bi se ukvarjala le s CIP ali CIIP, ampak se s tem ukvarjajo ministrstva in telesa, ki so zadolžena za različne kritične sektorje in z njimi povezano zaščito in varnost, pa tudi nekateri raziskovalni inštituti, tako v državni kot tudi zasebni lasti.

Poleg **Delovne skupine za zaščito kritične informacijske infrastrukture**, ki je bila ustanovljena na **Ministrstvu za inovacije in tehnologijo** leta 2003 znotraj ministrskega sveta, in katere naloga je med drugim tudi koordinacija dejavnosti, povezanih s problemi CIIP na nacionalnem nivoju, se s tem področjem ukvarjajo še: **Ministrstvo za komunikacije**, znotraj katerega deluje že v prejšnjem poglavju omenjeni **ISCOM** (Instituto Superiore delle Communicazioni e delle Tecnologie dell Informazione; Višji inštitut za komunikacije in informacijske tehnologije), **Ministrstvo za notranje zadeve** (Policija za pošto in komunikacije) in **Ministrstvo za obrambo** (povzeto in prirejeno po: Abelle – Wigert in Dunn, 2006: 144).

K tem dejavnikom lahko prištejemo še **Nacionalni center za informatiko v javni upravi** (Centro Nazionale per l`Informatica nella Pubblica Amministrazione – **CNIPA**) in (po mojem mnenju, saj ga CIIP Handbook 2004 ne omenja) **Italijansko združenje za informacijsko varnost** (Associazione Italiana per la Sicurezza Informatica – **CLUSIT**). Prvi je usmerjen v IKT v javni upravi (na institucionalni ravni), drugo pa v CIIP v poslovnem (podjetniškem) sektorju. Sem spadata še **Stalna delovna skupina za omrežno varnost in komunikacijsko zaščito** (Gruppo di lavoro permanente per la sicurezza delle reti e delle Informazioni)**,** ter **Nacionalni tehnični komite za IKT zaščito v javni upravi**.

3.3.1. Minister za inovacije in tehnologijo - MIT

(Ministro per l`Innovazione e le Tecnologie **)**

S strani ministrskega predsednika mu je bilo poverjeno delovanje na področju tehnoloških inovacij, razvoja informacijske družbe in s tem povezanih uporabnih inovacij, koristnih tako za vladne službe kot tudi za občane in poslovne družbe.
Še posebej je MIT zadolžen za: omrežne strukture, tehnologijo in službe, razvoj ter uporabo informacijskih in komunikacijskih tehnologij, pospeševanje elektronskega opismenjevanja ter povezovanje z mednarodnimi in institucijami EU, ki delujejo na omenjenih področjih. Zadolžen je tudi za vodenje Ministrskega komiteja za informacijsko družbo in Ministrskega komiteja iniciativ za skupno satelitsko navigacijo (povezovanje).
MIT-u nudi podporo **DIT** (Dipartimento per l`Innovazione e le Tecnologie – Oddelek za inovacije in tehnologijo), ki koordinira politike različnih ministrstev za razvoj informacijske družbe in promovira novosti javnih služb med poslovnim svetom in državljani (Abelle - Wigert in Dunn, 2006: 145).

3.3.2. Delovna skupina za zaščito kritične informacijske infrastrukture

Na ministrstvu za inovacije in tehnologijo je bila ustanovljena v marcu 2003. V to delovno skupino so vključena vsa ministrstva, ki upravljajo kritične infrastrukture, skupaj z lastniki in operaterji teh infrastruktur, pa tudi nekateri raziskovalni inštituti. Cilj te delovne skupine je pomagati italijanski vladi v boljšem razumevanju problemov, povezanih s CIIP, posebej naključnih ali namernih hib oz. napak, po drugi strani pa pripraviti osnove za identifikacijo organizacijskih zahtev in pobud za povečanje čvrstosti (zanesljivosti) kritičnih infrastruktur (Dunn in Wigert, 2004: 113).

3.3.3. Ministrstvo za komunikacije

Dodeljen mu je nadzor poštnih in telekomunikacijskih služb, opravlja vlogo regulatorja in koordinatorja teh služb. Prav tako je vključeno v definiranje komunikacijskih in internetnih varnostnih politik.
Osnovne naloge tega ministrstva:

- nadzor poštnih, finančnih in telekomunikacijskih služb,
- je v vlogi regulatorja, koordinatorja, nadzornika in upravljavca na podlagi zakonodaje,

- zastopa vlado doma in v tujini,
- preverja in daje soglasja k raziskovalnim načrtom, tako domačim kot mednarodnim, usmerjenim predvsem v razvojne, ekonomske, tehnične in zakonodajne sfere na področju IKT,
- nastopa v vlogi nadzornika IKT tehnologij, preučuje in preverja varnost omrežij, postavlja tehnične normative in usklajuje standardizacijo z evropsko zakonodajo na področju IKT ter definira kvalitativne standarde (http://www.comunicazioni.it/en/index.php?Mn1=5).

3.3.4. Višji inštitut za komunikacije in informacijske tehnologije - ISCOM

(Instituto Superiore delle Communicazioni e delle Tecnologie dell Informazione)

Njegova glavna aktivnost je usmerjena v delovanje IKT podjetij, vladnih agencij in zasebnih uporabnikov. Še posebej je osredotočen na področja zakonodaje, eksperimentalnih aktivnosti, temeljnih in uporabnih raziskav, specialistične vzgoje in izobraževanja v telekomunikacijskih sferah. ISCOM vodi tudi Nacionalno informacijsko-zaščitno certifikatno telo (**OSCI** – Organismo di Certificazione della Sicurezza Informatica), ki se posveča predvsem varnostnim certifikatom sistemov in proizvodov na IKT področju v okviru evropskih ITSEC kriterijev in s tem povezanimi ITSEM metodologijami (Information Technology Security Evaluation Manual – priročnikom, namenjenim za vrednotenje varnosti informacijske tehnologije), ter v skladu z mednarodnim ISO/IEC IS 15408 (Common Criteria) standardom.

Z naslavljanjem varnostnih in zaščitnih vprašanj je ISCOM aktiven tudi v ustvarjanju in izmenjavi mnenj javno-zasebnega foruma (tele-) komunikacijskih omrežij. V letu 2004 je ustanovil posebno delovno skupino, ki se ukvarja z različnimi vidiki varnosti v komunikacijskih omrežjih in s potrebnimi zaščitnimi ukrepi za zagotovitev le-teh na vseh nivojih v službah kritičnih infrastruktur.
Rezultat teh aktivnosti pa sta bili tudi publikaciji, ki sta izšli v letu 2005 z naslovoma »La sicurezza delle reti nelle infrastrutture critiche« in »La sicurezza delle reti dall` analisi del riscchio alle strategie di protezzione«, ki sem ju že predstavil v prejšnjem poglavju in ki obširno opisujeta problematiko CIIP na globalni ravni z aplikativnimi rešitvami in modeli na italijanskem nivoju (http://www.iscom.gov.it/contenuti.asp?ID=65).

3.3.5. Nacionalni tehnični komite za IKT zaščito v javni upravi

(Comitato Tecnico Nazionale per la Sicurezza Informatica e delle Telecomuncazioni nella Pubblica Amministrazione)

Kot sem že v zgodovinskem orisu razvoja CIIP v Italiji povedal, sta ta komite leta 2002 ustanovili Ministrstvo za inovacije in tehnologijo ter Ministrstvo za komunikacije na podlagi direktive o IKT zaščiti za javno upravo, ki uveljavlja priporočila EU za minimalne varnostne standarde na področju IKT v javnih upravah znotraj skupnosti. Nacionalni tehnični komite torej v tem pogledu opravlja vlogo operativne roke nove IKT varnostne politike (http://www.innovazione.gov.it/ita/mit_informa/comunicati/2002_10_11.shtml).

Uveljavljati skuša zadovoljivo raven varnostne politike v informacijskih sistemih in elektronskih komunikacijah v skladu z mednarodnimi standardi in tako doseči oz. zagotoviti neoporečnost in zanesljivost informacij. Predlaga strateške predloge za računalniško in telekomunikacijsko zaščito v javni upravi, še posebej pa razvija »Nacionalni krizni načrt za zaščito informacijske in komunikacijske tehnologije v javni upravi«. Letno preverja raven napredka in predlaga potrebne rešitve za »Nacionalni organizacijski model IKT zaščite za javno upravo«, njegov nivo učinkovitosti in uporabe. Oblikuje tudi predloge za prilagajanje certifikacijskih in varnostnih ocen pa tudi certifikacijske kriterije in smernice za varnostno certifikacijo IKT v javni upravi na osnovi nacionalnih, mednarodnih in sektorskih norm ter priporočil.

Nenazadnje komite izdeluje smernice za skladen razvoj znotraj ministrstva za javno upravo v okviru izobraževanja o IKT varnosti in zaščiti za zaposlene v javni upravi. Eden od predlogov je bil tudi ustanovitev »Computer Emergency Response Team« (CERT-a) za centralno javno upravo (prej CERT-PA, zdaj Gov-CERT.it, ki je prevzel vlogo koordinatorja ostalih CERT-ov v drugih delih javne uprave). Ta organ ima vzpostavljen sistem zgodnjega opozarjanja, ki deluje neprekinjeno (Abelle - Wigert in Dunn, 2006: 147).

Komite je za izvedbo svojih predlogov in lažje uvajanje ustanovil že v prejšnjem poglavju omenjeni **Nacionalni center za informacijsko varnost** (Centro Nazionale per la Sicurezza Informatica - **CNSI**), ki naj bi bil deloval predvsem na reševanju naslednjih predpostavk:

- *Veliko organizacij*, podjetij… ali njihovih vodstvenih delavcev, ki se odločijo za uvajanje novih IKT tehnologij, kasneje *naleti na problem varnosti*. Zato *večina problem zaščite* teh sistemov enostavno *prezre* in tako postanejo ti sistemi lahki cilji za informacijske napade, poleg tega pa so zaščitne tehnologije zelo kompleksne in težje razumljive običajnim uporabnikom, pa tudi težje jih je pravilno upravljati brez

primerne strokovne usposobljenosti, kar pomeni, da je potrebno vzpodbuditi takšne aktivnosti, ki bodo povečale informacijsko varnost, in ustvariti programe (metode, smernice, napotke …) za pravilno in varno uporabo novih tehnologij.

- Potrebno se je zavedati, da *se okoliščine* (v obliki inovativnih in mutirajočih napadov) tam, kjer že obstajajo učinkoviti protiukrepi za zaščito, neprestano *spreminjajo*, pri iskanju primernih rešitev se je zato potrebno posvetovati s strokovnjaki na različnih področjih in dati na razpolago za to namenjene raziskovalne laboratorije.
- *Rešitev problemov,* povezanih z neučinkovito zaščito, lahko *zahteva sodelovanje* več entitet, ne le tistih znotraj nacionalnih okvirov, temveč tudi tistih zunaj, zato je potrebno vzpostaviti odnose z različnimi organizacijami v različnih državah. Te akcije pa se lahko izvršijo samo s primernimi organizmi, torej takšnimi, ki so že bili priznani tako na nacionalnem kot tudi *internacionalnem nivoju* in ki takšne preiskave že opravljajo.

CNSI mora torej pripraviti učinkovite načrte zavedanja (ozaveščanja), pridobiti mora različne vire in pristojnosti, da se bo uspešno spopadel z informacijskimi napadi, predvsem pa mora biti umeščen v internacionalni kontekst (Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione, 2004: 19).

Osnovni cilji CNSI-ja morajo postati:

- povečanje nivoja zaščite informacijskih sistemov internetnih uporabnikov v Italiji, še posebej uporabnikov v javni upravi;
- priprava primernih ukrepov za soočenje z morebitnimi informacijskimi napadi v sistemih javne uprave;
- priprava primernih ukrepov za vzpostavitev pravilnega delovanja ogroženih sistemov v čim krajšem možnem času.

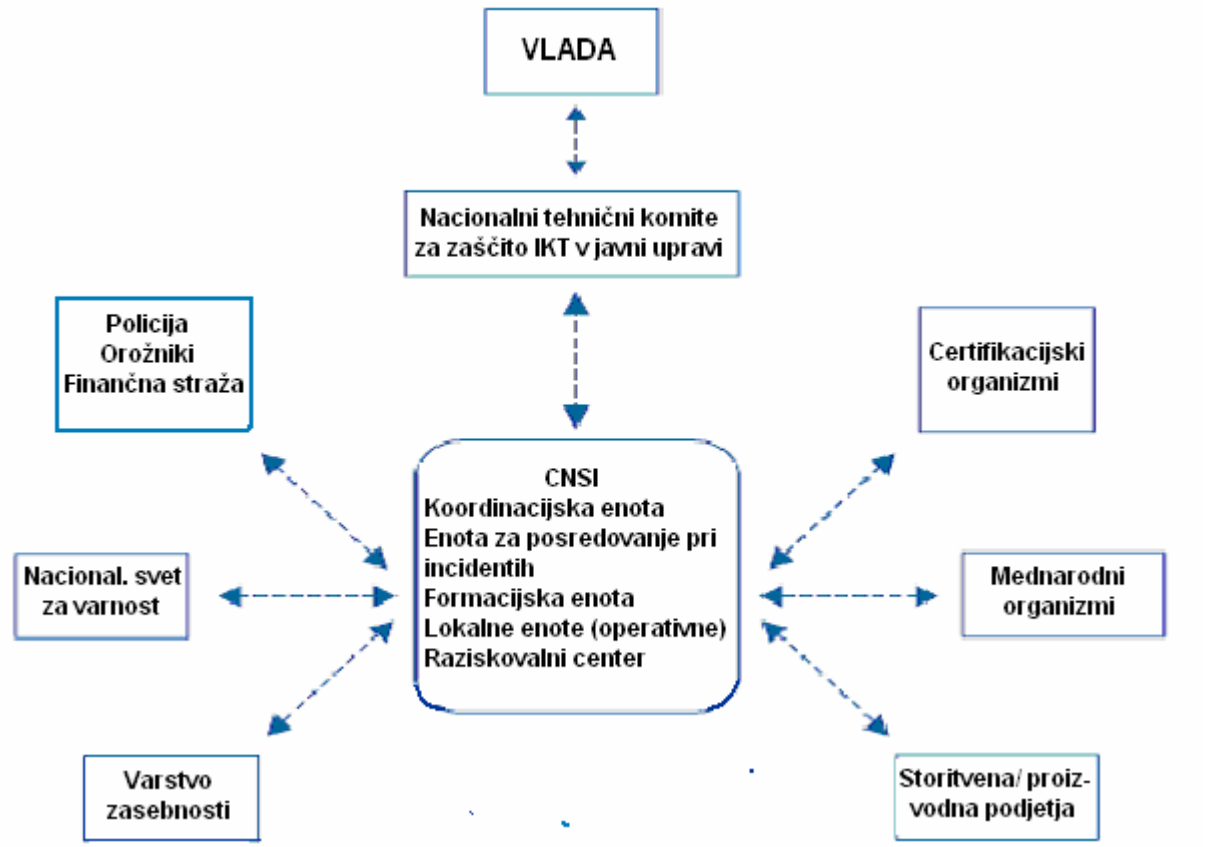
Za uresničitev teh ciljev pa bo potrebno izvesti kar nekaj dejavnosti, ki jih lahko razdelimo v tri skupine glede na njihov namen ali učinek: zaščita, spoznanje oz. določitev in odgovor.

1. *Zaščita:*
    - spodbuditi programe, ki povečujejo zavedanje problema informacijske varnosti med uporabniki interneta,
    - proučevati, vrednotiti in spodbujati načine pravilne uporabe (»best practice«) na področju informacijske varnosti,
    - pridobivati in razdeljevati primerne protiukrepe in ažurne podatke o vdorih,
    - spodbuditi izobraževanje uslužbencev javne uprave,

- spodbuditi upoštevanje varnostnih standardov.

2. *Spoznanje oz. določitev*:
   - spremljati in nadzorovati aktivnosti, ki se odvijajo znotraj omrežij; v tem pogledu je zelo pomemben stalni (in aktivni) monitoring,
   - zbirati in obdelovati sporočila in opozorila končnih uporabnikov.
3. *Odgovor*:
   - nuditi podporo oz. pomoč žrtvam informacijskih napadov in vdorov,
   - povezati se z več raziskovalnimi centri (Ibid).

Shema 5: Interakcijska shema delovanja CNSI



Vir: Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione, 2004: 21

Struktura CNSI predvideva *pet osnovnih enot*, ki so organizirane tako, da omogočajo kar najprimernejšo obliko in posredovanje potrebnih informacij v sistemih javne uprave in bi delovale na nacionalni ravni, čeprav teritorialno razpršene, pa bi bile vodene in povezane v enotno telo in to bi lahko imelo potrebne stike tudi z oblastmi in drugimi institucijami, ki se

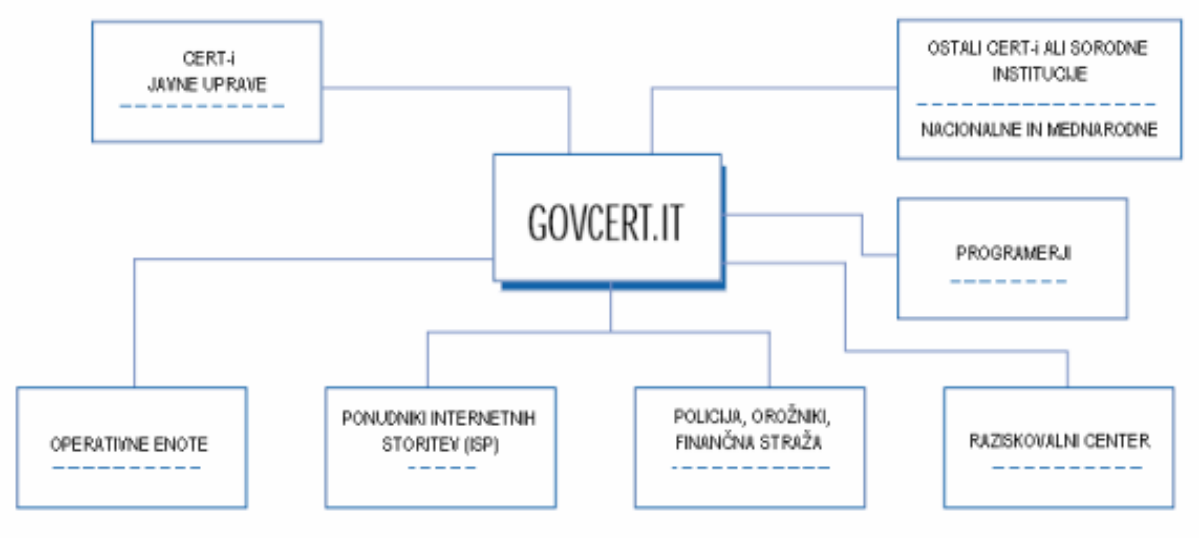
ukvarjajo s tozadevnimi varnostnimi problemi na nacionalni ravni (od vojske, policije, nacionalnega sveta za varnost, do sodišč in zakonodajno pravnih služb…), kot tudi na mednarodnem nivoju.

Strukturo CNSI sestavlja pet enot:

1. *Koordinacijska enota*, ki je zadolžena za aktiviranje in vodenje vseh dejavnosti znotraj centra, še posebej takrat, ko se zahtevajo hitri odzivi in zaščitni ukrepi v javnih upravah, skrbeti pa mora tudi za stalno vzdrževanje stikov s podobnimi organizmi tega sektorja na nacionalni in mednarodni ravni, še posebej je tu mišljena vzpostavitev stikov z evropsko agencijo za informacijsko varnost (ENISA), ameriško agencijo za informacijsko varnost CWIN (Cyber Warning & Information Network), angleškim NISCC (National Infrastructure Security Coordination Centre), švedsko SEMA (Swedish Emergency Management Agency), nemškim BSI (Bundesamt fur Sicherheit in der Informationstechnick) in francoskim »Secretrariat General de la Defense Nazionale«.
2. *Enota za posredovanje pri incidentih (informacijskih vdorih ali napadih)*, ki se neposredno ukvarja z informacijskimi napadi; predvsem gre tukaj za izmenjavo informacij in izkušenj o informacijski ranljivosti pri samih napadih (»Information Sharing«), sposobnost pravočasnega obveščanja o prisotnosti novih oblik nevarnosti in ranljivosti informacijskih infrastruktur (»Early Warning«), posredovanje tam, kjer oddelki javne uprave nimajo lastnih struktur za obvladovanje tega problema, širjenje informacij v prid zaščiti pred informacijskimi incidenti in zbiranje ter obdelavo podatkov o informacijskih incidentih. Za izvedbo teh nalog se enota poslužuje posebne službe (»Computer Emergenciy Response Team« – CERT), imenovane GOVCERT.IT, katere delovanje je prepleteno skozi ves CNSI in posledično tudi vso javno upravo (prav tako vse vladne službe).

   Ta služba (GOVCERT.IT) je osnovna instanca za obvladovanje in odpravljanje težav, povezanih s tehnikami oz. oblikami informacijskih vdorov, ranljivostjo oz. kritičnostjo informacijskih sistemov, zavajajočimi internetnimi povezavami in programskimi dodatki oz. dopolnitvami (»patch-i«) in s tem povezanimi ostalimi tveganji in grožnjami.

Shema 6: Struktura relacij enote za obvladovanje informacijskih napadov (GOVCERT.IT)



Vir: Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione, 2004: 25

Zato je sestavljena iz visoko strokovno usposobljenega osebja, katerega operativno delovanje je umeščeno v CNIPA (Centro Nazionale per l`Informatica nella Pubblica Amministrazione), kjer obstajajo tudi tehnične zmožnosti za opravljanje temu namenjenega delovanja. Nekatere javne uprave že imajo svoje delujoče tovrstne službe (kot npr. Ministrstvo za obrambo – CERT.DIFESA.IT), druge pa še bodo naloge s tega področja poverile GOVCERT.IT-u, pomembno pa je, da se ustvari trdna vez med temi službami v obliki sodelovanja in izmenjave informacij.

3. *Formacijska enota* ima nalogo oblikovati in pripraviti delovanje javne uprave, še posebej njenih uslužbencev, v pogledu IKT zaščite.
4. *Lokalne (operativne) enote* v javnih upravah morajo poskrbeti za zadovoljivo raven varnosti in zaščite v svojih informacijskih sistemih, kar pomeni, da mora biti vsak administrator (upravljavec tega sistema) dobro tehnično podkovan in imeti pripravljen načrt neprekinjenega delovanja (»Business Continuity«). Za dosego tega je nujno vzpostaviti stalno izmenjavo informacij s centrom in te informacije stalno dopolnjevati (jih ažurirati).
5. *Raziskovalni center* opravlja vlogo vira novosti in rešitev na področju IKT in CIIP tako za koordinacijsko enoto kot tudi za enoto za posredovanje pri incidentih. Ni nujno organ CNSI-ja, ampak to lahko postane na podlagi odločitve in potrebe koordinacijske enote po sodelovanju in strokovni pomoči. Pomembno pa je tudi, da ta

raziskovalni center (ali njegovo osebje) ni član kakšne organizacije, ki deluje v komercialne namene.

(Vir: Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione, 2004)

3.3.6. Nacionalni center za informatiko v javni upravi - CNIPA

(Centro Nazionale per l`Informatica nella Pubblica Amministrazione)

Nekdaj »Predstavništvo za informatiko v javni upravi« (l'Autorita per l'informatica nella pubblica amministrazione – **AIPA**), ustanovljeno leta 1993, je bilo preimenovano in preoblikovano v **CNIPA** v letu 2003. Spada pod Ministrstvo za inovacije in tehnologijo, v organizacijskem smislu je to kolegijski organ, sestavljen iz predsednika in štirih članov, ki so priznani strokovnjaki, imenuje pa jih predsednik ministrskega sveta.

Glavna naloga tega centra je nadzor in pomoč pri upravljanju in obvladovanju centralne in lokalnih javnih uprav, še posebej tistih delov, ki delujejo na področju sistemov informacijskih tehnologij. Poleg tega pa je CNIPA zadolžena za uvajanje modernih informacijskih tehnologij v javnih upravah, vzpostavljanje standardov in metod na področju varnosti in zaščite in pripravo priporočil ter tehničnih predpisov za varno uporabo IKT v javnih upravah. Prispeva tudi k oblikovanju vladne politike in svetovanju pri zakonodajnih projektih na področju informatike. Gradi in razvija večje državne omrežne infrastrukture in tako omogoča javnim uradom medsebojne povezave ter odnose le-teh z občani in podjetji, obenem pa skrbi za zaposlovanje in izobraževanje uslužbencev na informacijskem področju v javnih upravah.

V tem pogledu je CNIPA zaključila oblikovanje in izdelavo »Enotnega omrežja za javno upravo« (La Rete Unitaria per la Pubblica Amministrazione - RUPA) in že prehaja na uvajanje novejšega in tehnološko (pa tudi varnostno) bolj izpopolnjenega tako imenovanega javnega sistema povezovanja (Sistema Publico di Connettivita – SPC[10]). Še enkrat pa je potrebno omeniti, da CNIPA vodi tudi delovanje GOVCERT.IT-a, tako po organizacijski kot po izvršni plati (http://www.cnipa.gov.it).

[10] SPC je v projektih CNIPA definiran kot skupek organizacijskih struktur, tehnoloških infrastruktur in tehničnih pravil, namenjenih za razdelitev, integracijo in pretočnost informacijskega imetja javne uprave, ki je potrebna za zagotovitev interoperabilnosti in aplikativnega združevanja informacijskih sistemov ter pretoka informacij, z zagotavljanjem varnosti in zasebnosti prejetih in oddanih informacij (http://www.cnipa.gov.it/site/it-IT/In_primo_piano/Sistema_Pubblico_di_Connettivit%c3%a0_(SPC)/).

3.3.7. Stalna delovna skupina za omrežno varnost in komunikacijsko zaščito

(Gruppo di Lavoro Permanente per la Sicurezza delle Reti e delle Informazioni)

Ustanovljena je bila leta 1998 in je sestavljena iz predstavnikov Ministrstva za komunikacije, Ministrstva za notranje zadeve in Ministrstva za pravosodje, ukvarja pa se z opredeljevanjem oblik kriminalnih dejanj, zakonodajo in sankcijami, pa tudi z ekonomskimi vidiki komunikacijskih poslov, povezanih z internetom, kot je na primer čas trajanja shranjevanja podatkov o opravljenih povezavah.

V okviru te skupine deluje »podskupina internet«, ki preučuje preiskovalne in sodne zmožnosti ter oblike v okviru interneta, pripravlja pa tudi seznam podatkov, ki jih bodo morali ISP (Internet Service Providers – ponudniki internetnih storitev) dostaviti policiji, če bodo sodišča to zahtevala., podoben seznam pa že obstaja za ponudnike stacionarne telefonije. Pred časom je bil ustanovljen tudi koordinacijski center, ki z ostalimi vladnimi institucijami usklajuje boj proti kriminalu, storjenem preko interneta (Abelle - Wigert in Dunn, 2006: 149).

3.3.8. Policija za pošto in komunikacije

(Polizia Postale e delle Comunicazioni)

Ministrstvo za notranje zadeve je že leta 1992 izdalo direktivo, s katero je državni policiji dodelilo specifične odgovornosti in posebne naloge na področju informacijske tehnologije, ki se pravzaprav izvajajo v okviru posebne enote policije, imenovane »Polizia Postale« oz. Policija za pošto in komunikacije. To je fleksibilna enota z osebjem, ki šteje približno 2000 visoko strokovno usposobljenih uslužbencev, razporejenih v 19 regijskih oddelkov in 76 teritorialnih sekcij, vodi pa jo g. Domenico Vulpiani.

Poštna policija ocenjuje in pregleduje zakonske predpise na področju komunikacij, preučuje nove tehnike preiskovalnih strategij za boj proti kriminalu na področju IKT ter usklajuje operacije in preiskave tudi za druge službe. Prav tako sodeluje z drugimi državnimi institucijami, še posebej z Ministrstvom za komunikacije ter zasebnimi operaterji mobilnih in stacionarnih telekomunikacijskih omrežij. Aktivno deluje tudi kot italijanska kontaktna točka v okviru skupine G8 in je dosegljiva 24 ur na dan, kar ji v organizacijskem pogledu omogoča takojšen, strokoven in učinkovit odgovor v primeru groženj (v obliki napadov na IKT) tako znotraj države kot zunaj nje.

Poleg navedenega ima Policija za pošto in komunikacije na razpolago tudi krizne centre na državni in regionalni ravni, s katerimi si pomaga v primeru računalniških (IKT) oblik

napadov na kritično infrastrukturo ter vodi preventivne nadzorne aktivnosti na tehničnem in operacijskem nivoju. Ti centri postajajo osrednja točka za oceno groženj in podajanje protiukrepov za obvladovanje kriznih situacij.
(Povzeto in prirejeno po: Abelle - Wigert in Dunn, 2006: 150)
Policija za pošto in komunikacije operativno pokriva še naslednja področja:

- »hacking« (represivno delovanje v primeru vdorov v informacijske sisteme),
- prevratniško delovanje (nadzor in analizo dokumentov, ki se nanašajo na politični ekstremizem),
- e–Commerce (represijo goljufivih prestopkov, storjenih z uporabo telekomunikacijskih sredstev),
- telefonijo (prestopke, storjene preko telefonskih komunikacij),
- poštne prestopke,
- zaščito avtorskih pravic – informacijsko piratstvo (kršenje avtorskih pravic v obliki nedovoljenega kopiranja in kloniranja pametnih TV kartic),
- on-line pedofilijo.

Nedavno je bila znotraj Policije za pošto in komunikacije ustanovljena posebna enota za analizo informacijskih zločinov (l'Unità d'Analisi del Crimine Informatico – **U.A.C.I.**), ki v sodelovanju s pomembnimi italijanskimi univerzitetnimi inštituti preučuje in analizira fenomene, povezane z računalniškimi zločini. To sodelovanje pa poteka tudi čezmejno z že prej omenjeno skupino G8, pa tudi z EU, Svetom Evrope, OECD, Interpolom in Evropolom.
Leta 2004, točneje od 23. do 26. marca, so v Rimu gostili tudi prvo mednarodno konferenco o informacijskih zločinih, na kateri je sodelovalo 35 držav. Na tej konferenci so med drugim izvajali tudi simulacije različnih oblik informacijskih napadov in terorističnih atentatov z namenom, da se ugotovijo in v praksi dosežejo najprimernejše aktivnosti in strategije za boj proti tovrstnim »cyber« zločinom. Na konferenci se je izpostavila tudi potreba po stalni izmenjavi informacij, usklajenosti normativov in izboljšanju kvalitete postopkov ter oskrba primerne tehnično-operativne priprave za izvedbo teh postopkov (http://www.poliziastato.it/pds/informatica/attivita.html).

3.3.9. Italijansko združenje za informacijsko varnost – CLUSIT

(Associazione Italiana per la Sicurezza Informatica**)**

Leta 2000 ustanovljena organizacija je nastala s ciljem združiti vse strokovnjake, podjetja, organizacije in institucije, katerim je skupno prizadevanje za promoviranje in širjenje znanja

ter zavedanja o računalniški in omrežni varnosti v globalnem smislu, še posebej v Italiji in Evropi. Skupaj z CLUSIF (Francija), CLUSIB (Belgija), CLUSIS (Švica) in CLUSSIL (Luksemburg) predstavljajo evropsko gonilno silo na tem področju.

V to organizacijo je danes vključenih že več kot 400 predstavnikov organizacij in podjetij z najrazličnejših področij: javne uprave, finančnih in bančnih krogov, ponudnikov in izvajalcev raznih služb, velikih korporacij… CLUSIT v svoje okrilje sprejema tako dobavitelje kot tudi uporabnike varnostno-zaščitne opreme, zavedajoč se dejstva, da je sinergija med ponudbo in povpraševanjem ključni element v pospeševanju inovativnih pobud na področju zaščite IKT.

Glavne aktivnosti, ki jih CLUSIT izvaja, so:

- *Promocija in podpora*; organizacija in udeležba na vseh tistih področjih in dogodkih, ki širijo varnostno kulturo glede IKT. CLUSIT je postal znanstveno-raziskovalni partner najpomembnejšega in največjega dogodka na področju predstavitev IKT v Italiji, vsakoletnega sejma (SMAU), v okviru katerega ima glavno povezovalno vlogo med predstavniki in razstavljavci informacijske zaščite, pa tudi kot pobudnik razvoja potreb in zahtev za zagotovitev varnosti in zaščite IKT pri samih uporabnikih (občanih, javnih upravah oz. vladnih agencijah). V letih 2003 in 2004 je bil CLUSIT povabljen na več kot 80 tovrstnih dogodkov v Italiji.
- *Izmenjava*; takšne dogodke CLUSIT organizira z namenom lažje izmenjave izkušenj med ponudniki in uporabniki IKT ter s tem povezanimi možnostmi prikaza novih rešitev za uporabnike in pojavi možnih šibkih točk za ponudnike.
- *Širjenje in razglašanje*; pripravlja in širi dokumente, javna obvestila, varnostna opozorila, smernice in izobraževalne seminarje, pa tudi poročila in ocene različnih varnostno-zaščitnih metodologij in rešitev (ocene ogroženosti, projektnega upravljanja z varnostno konotacijo, vrednotenja kriterijev za varnostno okolje informacijskih tehnologij), statistična poročila, krizne scenarije in orodja za prepoznavanje ogroženosti pri končnih uporabnikih.
- *Izobraževanje*; na razpolago daje obširen izbor izobraževalnih seminarjev s področja zaščite informacijskih tehnologij, v sodelovanju z Oddelkom za informatiko in komunikacije na Univerzi v Milanu izvaja tudi program dodiplomskega študija za »računalniško-varnostne« operaterje, sodeluje pa tudi v izobraževanju in pridobivanju certifikatov EUCIP IT administratorjev.
- *Uvajanje novih projektov*; predvsem takih, ki povečujejo zavedanje in izobrazbo uporabnikov informacijskih tehnologij o njihovi varnosti in zaščiti, ter takih projektov, ki omogočajo lažjo izmenjavo informacij med uporabniki samimi. Nenazadnje je

CLUSIT tudi eden glavnih pobudnikov ustanovitve agencije **ENISA** (European Network Information Security Agency - Evropske agencije za varnost informacijskih omrežij) v EU (Brochure CLUSIT, 2005).

Glavni cilji vseh teh dejavnosti so:

- širjenje informacijske varnostne kulture med podjetji, javnimi upravami in občani,
- priprava zakonov, norm in pravil, ki vključujejo informacijsko varnost, tako na državnem nivoju kot tudi v evropskem merilu,
- priprava (izobrazba) profesionalnih uslužbencev, ki delujejo na področju zaščite IKT (izdaja certifikatov o usposobljenosti za EUCIP v Italiji),
- izdelava metodologij in tehnologij, ki pripomorejo k izboljšanju ravni varnosti v najrazličnejših okoliščinah (Ibid).

V sliki, ki je v prilogi, je le del najpomembnejših družbenikov, predvsem bomo tu našli organizacije in predstavništva tistih podjetij in korporacij, ki delujejo na italijanskem ozemlju, pa tudi nekaterih že prej omenjenih vladnih institucij, organizacij, delovnih teles in raziskovalnih inštitutov.

3.4. Primerjava s ključnimi smernicami EU in OECD

V prejšnjem poglavju sem predstavil dejavnike CIIP-a v Italiji in skozi to predstavitev lahko opazimo veliko vzporednic, ki jih lahko povežemo s smernicami OECD-ja in EU, predvsem na zakonodajnem, organizacijskem, pa tudi izvršnem področju, saj je bila Italija kot članica obeh mednarodnih integracij aktivno soudeležena pri nastajanju le-teh.

Pa vendar se pojavijo nekatere razlike že v definiranju kritičnih infrastrukturnih sektorjev, ki jih EU natančno opredeljuje, medtem ko jih Italija ne, ampak jih le navaja kot sektorje, ki potrebujejo večjo pozornost v varnostnem smislu, OECD pa kritičnih sektorjev sploh ne opredeljuje, temveč je tu pomembna zaščita vseh informacijskih sistemov in IKT ter omrežij na sploh.

Tabela 2: Primerjava kritičnih sektorjev v EU in Italiji

Kritični sektorji, ki jih opredeljuje EU	**Kritični sektorji, ki jim Italija posveča večjo pozornost**
energetske naprave in omrežja	energija
komunikacijska in informacijska tehnologija	(tele-) komunikacije
finance	bančništvo in finance

zdravstvo	javno zdravstvo
hrana	civilna obramba
voda	vode
prevoz	transportni sistemi na kopnem, vodah in v zraku
proizvodnja, skladiščenje in prevoz nevarnih snovi	plinska omrežja (in naftovodi)
vlada	e-vlada
	javna uprava

Vira: Sporočilo Komisije Svetu Evrope in Evropskemu parlamentu KOM/2004/702, ter Dunn in Wigert, 2004: 114

Sklepam, da ta razlika izhaja iz dejstva, da si je Italija zadala kot glavni cilj razvoja postati ena vodilnih držav v digitalizaciji in informatizaciji družbe, kar bom utemeljil v naslednjem poglavju, ne smemo pa pozabiti, da je bilo opredeljevanje kritičnih sektorjev oz. infrastruktur do sedaj prepuščeno posameznim državam, in še eno dejstvo se tukaj izpostavlja, to pa je nenehni splošni napredek ter posledično razvoj IKT in stalne spremembe znotraj infrastruktur (tudi kritičnih).

Italija je ena prvih evropskih držav, v kateri je že leta 1993 na podlagi smernic OECD iz leta 1992 stopil v veljavo zakon, ki opredeljuje in sankcionira računalniški kriminal (napade in vdore v IKT sisteme, vnašanje računalniških virusov, nedovoljeno pridobivanje zaupnih podatkov, uporabo teh podatkov v kriminalne namene…), **legge 547 (zakon 547)**, EU pa je vsebinsko podobno odločbo sprejela v letu 1997 in jo nadgrajevala s posameznimi vsebinami vse do leta 2004 v obliki sporočila o varovanju kritične infrastrukture v boju proti terorizmu. Iz povedanega lahko povzamem, da Italija na zakonodajnem področju sledi tako smernicam OECD, podanim leta 1992 ter revidiranim v letu 2002, kot tudi zakonom, izdanim v EU, ki pa so oznako CIIP dobili v letu 2004. Iz tega sledi, da je Italija na zakonodajnem področju ena naprednejših evropskih držav, saj je svoje zakone, dekrete in direktive na področju CIIP začela uvajati precej zgodaj, torej še pred 11. septembrom 2001, pred terorističnim napadom Al-Kaide na ZDA, ko je bil problem CIIP še posebej izpostavljen in se je pravzaprav ta termin šele začel razvijati, uveljavljati in izvajati. Zgoraj omenjeni italijanski zakon pa je le del vseh tistih zakonodajnih ukrepov s področja CIP in CIIP, ki jih je Italija sprejela in ki jih še pripravlja in uvaja. Sklepam lahko, da imajo zgledno urejeno področje sodne in izvršne oblasti, saj sem že v prejšnjem poglavju opisal zelo dobro sodelovanje med policijo (predvsem je tu mišljena Policija za pošto in komunikacije) v fazi preiskovalnih postopkov in

sodstvom v vodenju teh postopkov v fazi sprejemanja informacij o kršitvah in podajanju le-teh v nadaljnjo obdelavo policiji s ciljem, da se pridobijo trdni dokazi za izrekanje zakonsko utemeljenih tožb in sankcij.

Tudi na področju zgodnjega odkrivanja (tu so mišljena dejanja kot npr. »hacking«, razpošiljanje virusov in računalniških črvov, razni napadi in vdori na vsakovrstne informacijske sisteme s ciljem poškodovanja, nepooblaščenega spreminjanja ali uničenja teh sistemov…) in varovanja IKT sistemov Italija sledi smernicam, ki so bile podane že v dokumentih OECD, v praktičnem smislu pa aktivno sodeluje z ostalimi tako evropskimi kot tudi svetovnimi institucijami in organizacijami. Njeni CERT-i (pa naj si bo to CERT.IT, GOVCERT.IT, CERT.DIFESA.IT in ostali) so v stalnem kontaktu s podobnimi organizacijami in službami v EU in svetu (tako z FIRST-om[11], kot tudi s CERT-i[12] in CSIRT-i[13] ter tovrstnimi skupinami, ki se ukvarjajo s preprečevanjem kršitev in groženj na računalniškem področju) in aktivno sodelujejo v izmenjavi informacij in pripravi rešitev za omenjene težave. Že v prejšnjem poglavju je povedano, da je Italija sodelovala v pripravi in ustanovitvi Evropske agencije za varnost informacijskih omrežij - ENISA. [14]

V pogledu cenejšega in hitrejšega dostopa do interneta in njegovih »uslug«, ki je med drugim težnja in smernica tako OECD kot tudi EU, je Italija v lanskem letu (2005) dogradila sistem RUPA in že izdeluje še hitrejši, cenejši in dostopnejši sistem povezovanja, SPC – javni sistem povezovanja (Sistema Publico di Connettivita), ki naj bi stopil v delovanje v letu 2007 in od katerega si italijanska vlada in predvsem javna uprava obetata večjo varnost in zaščito IKT sistemov za vse tiste uporabnike, ki bodo vstopali v omenjene omrežne povezave. Ta sistem naj bi tudi poenotil sistem varnosti znotraj vseh vladnih in drugih služb ter ga vključil kot enega osnovnih elementov v informacijske sisteme in omrežja. Za dosego tega cilja pa se usposabljajo in izobražujejo vsi uslužbenci v javnih službah, ki na kakršen koli način sodelujejo v uporabi IKT in posredovanju ter sprejemanju informacij. Tako tudi Italija sledi

---

[11] FIRST je okrajšava za Forum of Incident Response and Security Teams, torej forum enot za varnost in odziv na nezgode (povezane z IKT), ki združuje takšne enote po obeh Amerikah, Aziji, Oceaniji in Evropi, članstvo šteje že več kot 170 tovrstnih organizacijskih enot, ki prihajajo iz vladnih, podjetniških in izobraževalnih ustanov (http://first.org/).

[12] CERT je okrajšava za Computer Emergency Response Team, oznaka je registrirana na ameriškem patentnem uradu in tovrstne organizacije, ki želijo uporabiti to kratico v svojem imenu, morajo za dovoljenje zaprositi na CERT Coordination Center (http://www.cert.org/) .

[13] CSIRT je okrajšava za Computer Security Incident Response Team, po svojem namenu in delovanju je to pravzaprav sinonim za CERT, to ime in okrajšavo pa so v zadnjem času začele uporabljati predvsem evropske države (http://www.ecsirt.net/service/coc.html).

[14] ENISA je okrajšava za European Network Information Security Agency, agencijo, ki je bila ustanovljena v letu 2004, deluje v okviru in za potrebe EU in držav članic, združuje pa CERT-e in CSIRT-e ter podobne agencije znotraj EU, sodeluje pa tudi s tovrstnimi agencijami po svetu (http://www.enisa.eu.int/).

težnjam o izobraževanju in širjenju znanja ter zavedanja o ogroženosti in zaščiti informacijskih sistemov, participacija v tem pa bo omogočena velikemu krogu ljudi tako v gospodarski, poslovni, kot tudi izobraževalni sferi. Za izvedbo projekta SPC bo Italija v naslednjih petih letih (obdobje 2005 – 2010) namenila € 1.200.000.000, vse aktivnosti pa bo vodila CNIPA, ki bo del teh sredstev usmerila v izvedbo in uvajanje projekta v prvih dveh letih (http://www.cnipa.gov.it/site/itIT/In_primo_piano/Sistema_Pubblico_di_Connettivit%c3%a0_(SPC)/).

3.5. Trendi nadaljnjega razvoja CIIP v Italiji

Največji napori, ki jih italijanska vlada in njene institucije izvajajo, so usmerjeni v reorganizacijo javne uprave, za katero je veljalo, da je bila močno zbirokratizirana in počasna, pa tudi njeni stroški so enormni. Z uvajanjem novih tehnologij, predvsem IKT, ki naj bi poenotile, pocenile in kar je najvažnejše – povečale učinkovitost in odzivnost v javni upravi kot eni od pomembnejših nacionalnih kritičnih infrastruktur, poskuša italijanska vlada ta problem rešiti na naslednjih (strateških) področjih, povzetih po strateških smernicah, namenjenih upravam za izvedbo triletnega načrta (Linee strategiche volte ad indirizzare le amministrazioni nella predisposizione del piano triennale per l'informatica 2006-2008, 2005):

- razvoju e-vlade,
- zakonodajnem oz. normativnem področju: na tem področju so bili do sedaj doseženi že določeni rezultati, ki predstavljajo normativni okvir za prihodnje trende, in sicer; *zakonodajni dekret*, *s katerim se ustanavlja in urejuje SPC*, ki povezuje vse centralne in lokalne javne uprave ter predstavlja evolucijo omrežja RUPA, obenem pa se s tem omogoča napredek, integracijo in obtočnost informacijskega imetja celotne javne uprave v skladu s kvalitativnimi in varnostnimi standardi; *dekret predsednika republike*, *ki ureja uporabo certificirane elektronske pošte* ne samo v odnosih z javnimi upravami, ampak tudi med samimi občani, in obenem daje pravno podlago za prenos upravno-pravnih dokumentov preko IKT sistemov; *zakonodajni dekret*, *ki uvaja kodeks digitalne javne uprave*, nov pravni inštrument, namenjen realizaciji homogenega normativnega okvirja za aplikacijo novih tehnologij v javni upravi, ki omogoča nove pravice »digitalnim občanom«, istočasno pa omogoča preseganje zastarelih in ustaljenih anahronističnih obvez in povečuje učinkovitost.

Strateške smernice (ki jih je pripravila CNIPA) za obdobje 2006 – 2008 temeljijo na treh smernicah direktive ministra za inovacije in tehnologijo iz januarja 2005:

- na doseganju zakonodajnih ciljev v letu 2005 in začetku leta 2006,
- na prehodu na novo fazo programa v istem obdobju z zaključkom le-te v naslednjem triletju,
- na racionalizaciji in doseganju ekonomičnega delovanja javnih uprav s pomočjo novih IKT, s čimer bi se izognili prikrivanju ali podvajanju upravno-pravnih postopkov v javnih upravah na račun davkoplačevalskega denarja (predvsem v protokolarno informacijskih službah in pri vodenju oz. izdaji dokumentacije) in utrdili infrastrukture (tudi kritične), ki bi bile zmožne neprekinjeno delovati tudi v kriznih razmerah in nesrečah, ter ustvarili možnost deljene uporabe infrastruktur in didaktičnih materialov za e-izobraževanje.

Tako CNIPA v sodelovanju z javno upravo pripravlja izhodišča in izvaja dela na štirih obširnih področjih, ki jih opredeljuje kot:

1. *Infrastrukture in osnovne službe:*

- **Internacionalna mreža** (La Rete Internazionale delle Pubbliche Amministrazioni – RIPA), ki bo omogočila povezovanje upravnih služb preko IP[15], interneta, služb za varnost in VoIP[16] v svetovnem merilu, na podlagi katerih bo možno varno in zanesljivo povezovanje italijanskih uradov v tujini, na ta način pa se bo izboljšala tudi informacijska oskrba v mednarodnem merilu.
- **SPC** (Sistema Pubblico di Connettivita) oz. javni sistem povezovanja, ki sem ga že predstavil v prejšnjem poglavju, omenim lahko še, da bo ta sistem deloval na principu širokopasovnih povezav, ki jih bo kot ponudnik internetnih storitev nudila in izvajala na natečaju izbrana družba PAthNET.
- **Aplikativna kooperacija**, kar pomeni, da morajo vse javne uprave pri načrtovanju in izvedbi služb upoštevati tehnične in organizacijske rešitve, ki so združljive in poenotene, oziroma se bodo sposobne avtonomno uresničevati, neodvisno od fizične ali organizacijske umestitve.

---

[15] IP je okrajšava za Internet Protocol. **IP-naslov** je število, ki natančno določa računalnik v omrežju Internet. Kratica IP označuje *Internet Protoco*l). Število je 32-bitno, običajno je zapisano s štirimi osembitnimi vrednostmi v desetiški obliki npr. 193.95.198.35. (http://sl.wikipedia.org/wiki/IP).

[16] VoIP je okrajšava za Voice over Internet Protocol ali glasovno povezovanje preko interneta – internetno telefonijo (http://sl.wikipedia.org/wiki/VoIP).

- **Službe z razširjeno interoperabilnostjo**, ki bodo neposredno zmanjšale stroške javnih uprav z uvajanjem novih IKT na področjih upravljanja infrastruktur, sporočilnosti, vodenju raznih aplikacij v izvedbi internetnih strani s pomočjo ASP[17] programskega in strojnega okolja.

- **Voice over IP**, tehnologija, ki lahko postane eden pomembnejših dejavnikov v težnji po zmanjševanju stroškov v javnih upravah, saj poleg širokopasovnih povezav in prežetosti IP omogoča integracijo delovnih mest, infrastruktur in novih telekomunikacijskih aplikacij. Vse komunikacijske infrastrukture znotraj sistemov SPC in RIPA so prilagojene tem načinom delovanja in obenem omogočajo kvaliteten prenos tovrstnih signalov, torej tudi glasu in ostalih multimedijskih vsebin.

- **Brezžični sistemi** so prevzeli pomembno vlogo v telekomunikacijskih sistemih, še posebej mobilnih. Tako lahko mobilna telefonija, ki je tudi najbolj uporabljen vir komunikacije s strani italijanskih državljanov, postane najhitrejši in tudi najbolj enostaven način za vzpostavitev stika z občani in nudenje takojšnjih uslug, kot so npr. prepoznava in overjanje, sporočanje (sms, mms…), mobilni plačilni sistem, usluge lokalnega značaja…

Z novimi tehnologijami, kot sta Wi-Fi[18] in WIMAX[19], lahko ekonomično širijo omrežje lokalnih javnih uprav, saj ti tehnologiji omogočata prenos najrazličnejših multimedijskih vsebin tudi brez izgradnje dragega stacionarnega kabelskega omrežja, torej tudi na težje dostopnih mestih.

- **Strukture in sistemi za zaščito pred informacijskimi nesrečami** predstavljajo prioritetno predpostavko in potrebo v uresničevanju triletnega načrta agencije CNIPA za obdobje 2006 – 2008. Zaščita informacijskih sistemov pred škodljivimi dogodki ali okvarami in stalna razpoložljivost služb in uslug, ki jih nudijo javne uprave občanom in drugim družbenim

---

[17] ASP je okrajšava za Active Server Pages, tehniko prenosa podatkov, ki omogoča razširjen http protokol in vsebinsko bogatejšo komunikacijo med računalniki na internetu s tako imenovanim ActiveX zapisom (http://www.webopedia.com/TERM/A/Active_Server_Pages.html), v tem primeru pomeni ta kratica tudi Application Service Provider (pomensko zelo podobno), oz. so to programska podjetja ali ustanove, ki omogočajo programske rešitve in usluge večjemu številu uporabnikov z neke centralne podatkovne baze (http://www.webopedia.com/TERM/A/Application_Service_Provider.html).

[18] Wi-Fi je okrajšava in sinonim za brezžično lokalno omrežje (v zadnjem času se za to uporablja ime WLAN), ki temelji na standardu IEEE 802.11, in je bil v začetku namenjen za mobilne naprave, kot so notesniki, dlančniki …, v zadnjem času pa se vse bolj uporablja pri internetnem dostopu, računalniških igricah in tudi povezovanju med uporabno elektroniko, kot sta npr. televizor in DVD predvajalnik (http://en.wikipedia.org/wiki/Wifi).

[19] WIMAX je okrajšava za **W**orldwide **I**nteroperability for **M**icrowave **Acc**ess in temelji na standardu IEEE 802.16., pomeni pa neke vrste mestno omrežno tehnologijo, ki je sposobna med seboj združiti različne Wi-Fi točke in jih povezati z internetom ter s tem nuditi brezžično alternativo širokopasovnim kabelskim povezovalnim sistemom do končne vstopne točke, vse to na razdalji do 50 km (vidno polje) (http://en.wikipedia.org/wiki/WIMAX).

subjektom, pomeni edino možno alternativo pred nezaželenimi izpadi v delovanju IKT sistemov znotraj javnih uprav, kar med drugim pomeni tudi povečan stroškovni faktor. Zato se rešitve in predlogi za to področje iščejo s skupnimi interesi in močmi več uprav, med drugim tudi tako, da se določene infrastrukture, viri in organizacijski postopki združujejo za istočasno in skupno delovanje več uprav, kar posledično tudi zmanjšuje stroške in – pomembno – omogoča lažji nadzor in zaščito. CNIPA je zato podala pobudo za ustanovitev enega samega oz. »Enotnega centra vseh zaščitnih inštitutov za backup« (Centro Unico di Backup degli Istituti Previdenziali), ki je že v fazi operativne uresničitve.

- **Informacijska varnost** mora biti vpeta v vse pore organiziranja, vodenja in upravljanja IKT infrastruktur v vsaki javni upravi, tako znotraj nje kot tudi v odnosih z občani ali podjetji. Ta težnja pa je pomembna tudi pri uvedbi programa e-vlade (e-Government). CNIPA je zato v letu 2004 ustanovila organizem (GovCERT.it), ki bo v bodoče nudil oporno točko in bo neke vrste zaščitni in podporni center za vse javne uprave v primerih informacijskih nezgod. Med drugim bo ta organizem pripravil tudi podatkovno bazo, ki bo predstavljala poznavanje stanja varnosti in zaščite IKT sistemov v javnih upravah.

2. *Službe, namenjene občanom in podjetjem:*

- **Portali, uporabniške analize in kvaliteta služb** postajajo pomemben kriterij za uporabnost nudenih služb občanom in podjetjem ter obenem izhodiščna točka za razvijanje novih služb oz. ponujenih uslug s strani moderne javne uprave. Zato se javne uprave pospešeno pripravljajo in razvijajo portale, ki predstavljajo virtualna vstopna vrata in neke vrste dobrodošlico v svet javnih uprav, precej bolj prijaznih, vsebinsko polnejših in uporabnejših od tradicionalnih spletnih portalov. Doseganje določene stopnje v razvoju takšnih portalov postaja tudi potreba pri prenosu določenih služb in uslug preko telematskih kanalov.
- **Nacionalni portal občanov**, portal »Italia.gov.it«[20], ki je aktiven že od leta 2002, nudi določene informacije in povezave (teh je vključenih že preko 10.000) na kvaliteten in prikladen način, predstavlja tudi skupno dostopno točko za občane k javnim upravam in njihovim »on-line« službam, pokriva pa tudi različna področja vsakdanjega življenja (od različnih potreb, npr. problematike zaposlovanja ali vzgoje in izobraževanja, do specifičnih skupin uporabnikov, kot so starejši občani, mladina, študenti, izseljenci…). Razvoj tega in podobnih portalov gre v smeri še hitrejšega in učinkovitejšega povezovanja javnih uprav v nudenju najrazličnejših informacij občanom pri reševanju in odpravljanju raznih težav (na

[20] http://www.italia.gov.it/servlet/ContentServer?channel=HTTP&pagename=e-Italia/HomeHttp

vprašanje določenega občana bodo lahko različne javne uprave pripravile skupen odgovor in pomagale pri učinkovitem in hitrem reševanju določenega problema, npr. kako se vpisati na univerzo, kaj vse je potrebno pripraviti za potovanje v tujino…).

- **Službe, namenjene podjetjem**, bodo z razširitvijo in dokončanjem nacionalnega seznama služb (Carta Nazionale dei Servizi – CNS) omogočile večjo uporabnost in zanesljivost uporabnikov s podjetniškega področja v odnosih z javnimi upravami. Tako bo mogoče preko »on-line« služb javnih uprav pripravljati dokumentacijo za potrebe podjetij in njihovega poslovanja na bolj učinkovit in podjetjem prijazen način. S tem se bodo tudi skrajšale birokratske poti.
- **Dostopnost** služb in uslug javnih uprav se bo izboljšala z uvedbo novih metodologij in proizvodov na področju overjanja in varnosti, CNIPA bo v tem pogledu v prihodnje opravila še veliko dela na področju svetovanja, formiranja, informiranja in nadzora v pripravi programov služb in uslug javnih uprav. Z izvedbo programa »interoperabilnosti digitalnega podpisa« in že prej omenjenega CNS bo to lažje uresničiti.
- **Seznam javnih uprav** je informacijska struktura, ki vsebuje podatke o organizacijah in organizacijskih področjih, njihovih internetnih naslovih in certificiranih poštnih predalih vseh italijanskih javnih uprav. CNIPA mu nudi infrastrukturo in potreben tehnološki razvoj z nenehnim dopolnjevanjem dotičnih vsebin ter na ta način omogoča povečevanje in izboljševanje kanalov za telekomunikacijsko povezovanje med samimi javnimi upravami ter tudi z občani in podjetji. Podatki, ki jih ta seznam vsebuje, pomenijo tudi osnovni pogoj za dosego modernizacije in transparentnosti javne uprave.

3. *Notranja učinkovitost:*

- **Informacijski protokol in vodenje dokumentacije** sta od 1. januarja 2004 obvezujoča sestavina javnih uprav, vsaj kar zadeva osnovni del oz. avtomatizacijo protokolnega registra, ki ga CNIPA uvaja in nudi v ASP tehnologiji, za katero se je pokazalo, da omogoča večjo ekonomičnost, varnost in učinkovitost ter fleksibilnost, usklajenost in uporabnost za organizacijske potrebe javnih uprav. Obenem se uvaja tudi optično arhiviranje dokumentacije (tudi to s pomočjo ASP tehnologije) in ostali pripomočki za svetovanje in podporo. Istočasno se ugotavlja, kakšna je kritičnost uvedenih rešitev ter načini in postopki odpravljanja le-te. Opravljala se bo stalna revizija teh postopkov z namenom, da se čim bolj zmanjša ranljivost informacijskih sistemov, tako v javnih upravah kot tudi med ostalimi uporabniki.
- **Uvajanje in razpošiljanje certificirane elektronske pošte ter uporaba elektronskega podpisa** sta naslednja dva elementa modernizacije italijanskih javnih uprav ter izboljšanja

varnosti in zaščite v ostalih kritičnih informacijskih infrastrukturah. Vse vpletene institucije zato pripravljajo poimenski seznam svojih certificiranih poštnih predalov z namenom, da se poenostavi, poenoti in pospeši komunikacija tako z občani in podjetji kot tudi na področju mednarodnih odnosov. Obenem pomeni to tudi večjo zaščito in zasebnost tako za izvajalce kot za uporabnike.

- **Shranjevanje dokumentov v elektronski obliki** je proces, ki bo pomenil večjo fleksibilnost v obdelavi in velike stroškovne ter prostorske prihranke.[21] Tudi normativni okvir določa prehod javnih uprav iz papirnate v digitalno obliko, kar bo obenem pomenilo še lažje zakonodajno opredeljevanje pri informacijskem arhiviranju dokumentov.

- **Informatizirano (elektronsko) pooblastilo in informatiziran (elektronski) plačilni sistem** omogočata plačilni promet javnim upravam od leta 2000. Takrat je v skladu s sporazumom med Banca d'Italia (italijansko narodno banko), Ragioneria Generale dello Stato (državnim računovodstvom), Corte dei Conti (računskim sodiščem) in AIPA (sedaj CNIPA) ob uporabi sistema RUPA pričel z delovanjem sistem SIPA (Sistema Informatizzato dei Pagamenti della Pubblica Amministrazione – informatizirani plačilni sistem javne uprave), ki so ga do sedaj pričele uporabljati že skoraj vse javne uprave. CNIPA ob tem javnim upravam pomaga pri uvajanju novih postopkov in tehnologij.

- **Nadzor in upravljanje** sta v obliki normativnih ukrepov in sprememb na tem področju doživela precejšen napredek in tako izboljšala učinkovitost in varnost v javnih upravah. V prihodnje se pričakuje razvoj informacijskih sistemov, ki bodo sposobni v realnem času omogočati nadzor in dajati kontrolnim centrom dosledne in popolne informacije, obenem pa morajo biti takšni sistemi čim bolj uporabniško poenostavljeni in fleksibilni.

- Uporaba zunanjih virov (open source), kot so novi informacijski programi (»software«) in ostali informacijski pripomočki, izbira ponudnikov in oskrbnikov teh programov, bo temeljila na skupnih in enotnih kriterijih, standardih, metodologijah in sinergijah, tako uporabniških kot varnostnih, ti kriteriji pa se bodo izgrajevali (in bili v stalnem procesu revizije) v okviru CNIPA in drugih tovrstnih organizmov (npr. CLUSIT-a, ISCOM-a…) in s sodelovanjem vseh javnih uprav ter tudi za njihove specifične potrebe. Ta projekt je že pričel z delovanjem v okviru Centra za usposabljanje javnih uprav za »open source« (Centro di competenza

[21] Ne smemo pozabiti, da lahko odprava papirja oz. papirnate dokumentacije pomeni po eni strani hitrejše in s tem učinkovitejše ter bolj varno pregledovanje dokumentov, po drugi strani pa bo vsa ta enormna količina papirja lahko odstopila prostor primernejšim in bolj racionalnim oblikam zapisa, tudi ob upoštevanju ekološkega vidika.

sull'open source nella PA) v okviru CNIPA, katerega odobritev je že sprejel Ministrski svet za informacijsko družbo.

4. *Človeški potencial:*

- **Razvoj pristojnosti** (»izgradnja« uslužbencev) bo potekal preko programa »e-learning« (e-izobraževanje) v obliki različnih uporabniško-didaktičnih pripomočkov, izdelanih v skladu s standardi, ki omogočajo prirejanje in uporabo v različnih javnih upravah, upoštevaje vse formacijske aspekte in tipologijo javnih uprav.
- **Sistemi in načini e-učenja (e-learning)** bodo uporabljali takšno tehnološko platformo, ki bo omogočala uporabo že omenjene ASP tehnike prenosa, kar pomeni kvalitetnejše in vsebinsko bogatejše izobraževalne programe, usmerjene v ozaveščanje o varnostno-zaščitnih ukrepih in postopkih v informacijskih sistemih javnih uprav.

(Povzeto po: Linee strategiche volte ad indirizzare le amministrazioni nella predisposizione del piano triennale per l'informatica 2006 - 2008, 2005)

Vsi našteti ukrepi bodo posredno pripomogli k sprejemu in uvedbi varnostnih meril, ki bodo zagotovila diskretnost in neokrnjenost podatkov, omogočila pa bodo tudi kontinuiteto in razpoložljivost vseh služb v javnih upravah.

4. ZAKLJUČEK

Celotna naloga je osredotočena na zaščito kritične informacijske infrastrukture, in sicer s treh vidikov: teoretičnega, normativnega (v povezavi z mednarodnimi integracijami) in empiričnega na primeru Republike Italije.

Kadarkoli govorimo o razvoju informacijsko-komunikacijske tehnologije, je potrebno istočasno upoštevati tudi njeno varnost oz. zaščito, tako na nivoju posameznega uporabnika kot na nivoju celotne družbe in celo na globalnem (svetovnem) nivoju, saj so skoraj vsa področja sodobne družbe (mnogo avtorjev jo poimenuje kar informacijska) dobesedno prepletena z informacijsko-komunikacijsko tehnologijo in od nje eksistencialno odvisna, posledice, ko njeno delovanje odpove, pa so lahko katastrofalne.

Poleg tega je pomembno tudi, da to področje ne pozna državnih meja in podobnih fizičnih preprek, vse se lahko dogaja (v strogo tehničnem smislu) po »navadnim« človeškim očem nevidnih in težko razumljivih poteh, vsi pa lahko še kako občutimo posledice. Zato je ***prvi pogoj za uspešno zaščito kritične informacijske infrastrukture njena vpetost v normativne okvire na vseh področjih in nivojih***, tako lokalnih, državnih kot tudi mednarodnih, saj se le tako lahko sistematično pristopi k učinkoviti zaščiti oziroma hitri in uspešni sanaciji že nastale škode in s tem tudi omejitvi ali možnemu širjenju oziroma eskalaciji te škode.

Prav s potrebo po normativni ureditvi zaščite kritične informacijske infrastrukture je povezana moja *prva hipoteza*, da *gre razvoj CIIP v Italiji v smeri približevanja zakonodaji EU in smernicam OECD glede varnosti informacijskih sistemov in omrežij (nazadnje spremenjenih in dopolnjenih l. 2002)*, utemeljil pa sem jo v posebnem poglavju, ki govori o primerjavi s ključnimi smernicami teh dveh mednarodnih integracij, zato povzemam le najpomembnejše poudarke. Čeprav se imensko določeni italijanski kritični sektorji ne skladajo povsem s sektorji, ki jih imenuje Evropska unija, pa so pomensko in pojmovno v popolnem skladju s smernicami, ki jih v svojih dokumentih le-ta podaja in jih posredno omenja tudi OECD.

Izkazalo se je tudi, da se na področju sprejemanja zakonodaje in določanju normativnega okvira področja in delovanja CIIP Italija ne le približuje tem smernicam, ampak v njih celo prednjači, saj je bilo ugotovljeno, da je Italija kot članica obeh mednarodnih integracij sodelovala že v pripravi teh smernic in zakonodajno-normativne ureditve ter prispevala pomemben delež, tako preko svojih vladnih institucij kot tudi preko svojih znanstvenih inštitutov, organizacij in posameznikov, ki so vključeni ali celo vodijo nekatera pomembna telesa in institucije na tem področju v evropskem in svetovnem merilu.

Od leta 2002 poteka v Italiji pospešena modernizacija (takrat je MIT izdal prve smernice, ki urejajo področje CIIP) na organizacijskem, normativnem in tehnološkem področju. Tako je ta država dopolnila (že prej sprejete) zakone in jih tudi uskladila z zakoni Evropske unije in normativnimi smernicami OECD, izdanimi v zadnjem obdobju (predvsem je tu pomemben večkrat omenjeni zakon 547, ki je podvržen – v pozitivnem smislu – stalnemu prilagajanju novim okoliščinam in oblikam zlorabe informacijsko-komunikacijske tehnologije, omenim pa lahko še zakon 675, ki govori o zaščiti osebnih podatkov in je bil dopolnjen nazadnje leta 2003, pa tudi zakon 438 (prej zakonski dekret 374/2001), sprejet z namenom izboljšanja delovanja zakonodajnih oblasti pri pregonu vseh oblik terorističnih dejavnosti).

Na organizacijskem področju je vajeti napredka v svoje roke prevzela CNIPA, ki predstavlja gonilno silo oblikovanja in razvoja javnih uprav kot enega pomembnejših kritičnih sektorjev, potrebnih prestrukturiranja. V izvajanju teh aktivnosti pa se naslanja na direktive in smernice ter okvirne predloge MIT-a.

Tudi v infrastrukturnem pogledu je Italija zelo napredna, zato še enkrat omenjam sistem RUPA, ki se v tem času že počasi poslavlja, zamenjal ga bo novejši SPC - javni sistem povezovanja, ki temelji na modernih oblikah multimedijskega komuniciranja in bo med drugim omogočil tudi boljšo zaščito kritične infrastrukture.

Vse to govori v prid *drugi hipotezi*, v kateri sem predvidel, da *poteka razvoj CIIP v Italiji v obdobju zadnjih nekaj let zelo pospešeno (spreminjanje zakonodaje, povečana vlaganja v infrastrukturo, oblikovanje novih varnostnih mehanizmov…).*

Čeprav delujejo v Italiji na tem področju mednarodno priznani strokovnjaki, (Andrea Pirotti – direktor ENISA, Luisa Franchina – direktorica ISCOM-a, Danilo Bruschi – raziskovalec na univerzi v Milanu, GianLuca Petrillo - predsednik nacionalnega tehničnega komiteja za informacijsko varnost, Augusto Leggio - ustanovni član CLUSIT-a…), in inštituti (oddelek za informatiko in komunikacije univerze v Milanu, ISCOM…) pa tudi svetovno priznana podjetja (Marconi, Olivetti…), prenos tega zavedanja in znanj v širšo italijansko družbo poteka prepočasi glede na visoko razvitost teoretične in normativne pokritosti tega področja. Iz izkušenj predvidevam, da **veliko oviro** pri hitrejšem prenosu omenjenih znanj in zavedanja ter izobraževanju kadrov in uporabnikov informacijsko-komunikacijske tehnologije (to pa je danes že vsak človek) **predstavlja jezik**, saj so bila vsa pomembna besedila, računalniška orodja in programi še pred kratkim le v angleškem jeziku, kar je (bil) za Italijane velik problem, saj je (bilo) učenje tujih jezikov v šolskem sistemu zapostavljeno (kot primer naj navedem italijansko literaturo, v kateri se še vedno pojavlja veliko neprevedenih angleških izrazov). Povedano (poleg primerjalnih raziskav, ki jih opravil Eurostat – tabela na str. 33)

potrjuje tudi *tretjo hipotezo*, da *mora Italija glede na postavljene cilje posvečati več pozornosti izobraževanju in usposabljanju kadrov na tem področju, saj le-ti predstavljajo najšibkejšo točko v razvoju CIIP*.

V zadnjem času je opazen velik napredek na tem področju v smislu novih izobraževalnih programov, ki jih je začela izvajati CNIPA za vse javne uslužbence, veliko dela pa v tej smeri opravlja tudi CLUSIT, ki je kot nevladna organizacija usmerjena v izobraževanje v podjetjih in drugih nevladnih ustanovah.

Na koncu želim poudariti, da je zaščita kritične informacijske infrastrukture zelo pomembno področje, ki se dotika prav vseh nas, ne glede na poklic, izobrazbo, starost (tudi otrok, saj so že najmlajši uporabniki mobilnih telefonov in računalnikov), zato je potrebno vključiti ozaveščanje o tem problemu že v vzgojo in izobraževanje v osnovni šoli, sicer bo znanje uporabe IKT vedno prehitevalo znanje o njeni varnosti in zaščiti.
Mnogo izkušenj lahko na primeru Italije implementiramo tudi v Sloveniji, saj se po mojem mnenju naša država s tem področjem ukvarja preveč fragmentarno in na nekaterih področjih celo prednjači pred Italijo (predvsem v znanju uporabe IKT glede na celotno populacijo), nekatera področja pa zanemarja; vsekakor zaostajamo vsaj glede normativne ureditve področja zaščite kritične informacijske infrastrukture. Šele ob vstopu v Evropsko unijo smo začeli povzemati njene smernice in normative in jim (počasi) prilagajamo našo zakonodajo.

Kazalo slik, shem, grafov in tabel

5. LITERATURA

Knjige, članki in raziskovalna dela

1. Abelle – Wigert, Isabelle in Miriam Dunn (2006) *International CIIP Handbook 2006, vol. 1, An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies.* Zurich: Center for Security Studies, ETH Zurich, http://www..isn.ethz.ch/crn/_docs/ciip_handbook_06_vol.1.pdf, 17. 04. 2006.
2. Avižienis, Algirdas, Jean-Claude Laprie in Brian Randell (2000) *Fundamental Concepts of Dependability.* Los Angeles: UCLA, Toulouse: LAAS – CNRS, Newcastle: University of Newcastle, http://www.cert.org/research/isw/isw2000/papers/56.pdf, 18. 05. 2006.
3. *Brochure CLUSIT* (2005). CLUSIT, http://www.clusit.it/BrochureClusit.pdf, 04. 06. 2006.
4. Bučar, Bojko, Zlatko Šabič, Milan Brglez (2002) *Navodila za pisanje - seminarske naloge in diplomskega dela*, II. izdaja. Ljubljana: Fakulteta za družbene vede (Knjižna zbirka Profesija).
5. Dunn, Miriam (2004*) Information Age Securuty: A Qualitative Analysis of Critical Information Infrastructure Protection (CIIP) Policies and the Role of the State as Provider of Security in the Information Age*, *PhD Thesis.* Zurich:, Center for Security Studies, ETH Zurich, http://www.isn.ethz.ch/crn/_docs/info_age_intro_draft.pdf, 07.06. 2005.
6. Dunn, Miriam in Isabelle Wigert (2004) *Critical Information Infrastructure Protection: International CIIP Handbook 2004 – An Inventory and Analysis of Protection Policies in Fourteen Countries.* Zurich: ETH, Swiss Federal Institute of Technology Zurich, http://www.isn.ethz.ch/crn/_docs/CIIP_Handbook_2004_web.pdf, 26. 04. 2005.
7. Dunn, Miriam in Victor Mauer (2006) *International CIIP Handbook 2006, vol. 2, Analyzing Issues, Challenges, and Prospects.* Zurich: Center for Security Studies, ETH Zurich, http://www.isn.ethz.ch/crn/_docs/CIIP_HB_06_Vol.21.pdf, 17. 04. 2006.
8. Grizold, Anton (1999) *Obrambni sistem Republike Slovenije*. Ljubljana: Visoka policijsko-varnostna šola.
9. *Intervista a Luisa Franchina Direttore Generale dell'Istituto Superiore delle Comunicazioni e della Tecnologia dell'Informazione* (2004). Isacaroma Newsletter, http://www.isacaroma.it/html/newsletter/?q=node/33, 20. 07. 2005.
10. Jelušič, Ljubica (1997) *Legitimnost sodobnega vojaštva*. Ljubljana: Fakulteta za družbene vede (Knjižna zbirka Teorija in praksa).

11. *La Siccurezza delle Reti dall` Analisi del Rischio alla Strategie di Protezione* (2005). Roma: ISCOM, http://www.iscom.gov.it/down/Sicurezza_delle_reti.pdf, 28. 05. 2005.
12. *La Sicurezza delle Reti nelle Infrastrutture Critiche* (2005). Roma: ISCOM, http://www.comunicazioni.it/it/Files/4/18/INFRASTRUTTURE%20CRITICHE.pdf, 24. 08. 2005**.**
13. Leggio, Augusto (2005) *Sicurezza e Futuro delle Infrastrutture Elettriche*. Milano: CLUSIT, Comitato Tecnico Scientifico, http://www.clusit.it/download/Q03_abs_web.pdf, 13. 05. 2005 in http://www.clusit.it/download/Q03_web.zip, 13. 05. 2005.
14. Malešič, Marjan (2002) *Legitimnost varnostne politike* (V: Marjan Malešič (ur.) *Nacionalna in mednarodna varnost)*. Ljubljana: Fakulteta za družbene vede (Knjižna zbirka Politični procesi in inštitucije).
15. *NISCC Quarterly*, 02/04. London, http://www.niscc.gov.uk/niscc/docs/re-20040630-00429.pdf, 09. 05. 2005.
16. Oman, Bojan (2005) *Terorizem kot globalni in regijski problem, diplomsko delo.* Ljubljana: Fakulteta za družbene vede.
17. Stantič, Klavdijo (2004) *Propaganda v vojni, diplomsko delo.* Ljubljana: Fakulteta za družbene vede.
18. Svete, Uroš (2005) *Varnostne implikacije uporabe informacijsko-komunikacijske tehnologije, Doktorska disertacija*. Ljubljana: Fakulteta za družbene vede.
19. Svete, Uroš (2005) *Varnost v informacijski družbi.* Ljubljana: Fakulteta za družbene vede (Knjižna zbirka Varnostne študije).
20. *The CIP Report*, *May 2004*, Volume 2/11, http://cipp.gmu.edu/archive/cip_report_2.11, 27. 05. 2005.
21. Turnšek, Tit (2000) *Digitalno bojišče, Ameriška vojska preizkuša informacijsko tehnologijo, ki bo omogočila vojskovanje na daljavo.* Mladina, 36/2000.

Dokumenti

22. *Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189)* (2003). Council of Europe, http://conventions.coe.int/Treaty/en/Summaries/Html/189.htm, 24. 07. 2005.
23. *Convention on Cybercrime (ETS No. 185)* (2001). Council of Europe, http://conventions.coe.int/Treaty/en/Summaries/Html/185.htm, 24. 07. 2005.

24. *Council Resolution on a European approach towards a culture of network and information security* (2003). Official Journal C 048, 28/02/2003 P. 0001 – 0002, http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32003G0228(01):EN:HTML, 22. 07. 2005.
25. *Decision No 276/1999/EC of the European Parliament and the Council adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks* (1999). Official Journal L 033, 06/02/1999 P. 0001 – 0011, http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31999DO276:EN:HTML, 22. 07. 2005.
26. *Decision No 1151/2003/EC of the European Parlament and of the Council amending Decision No 276/1999/EC adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks* (2003). Official Journal L 162, 01/07/2003 P. 0001 – 0004, http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32003D1151:EN:HTML, 22. 5. 2005.
27. *Direktiva 2002/58/ES Evropskega parlamenta in Sveta o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah)* (2002). Official Journal L 201, 31/07/2002 P. 0037 – 0047, http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:SL:HTML, 22. 07. 2005.
28. *Linee guida del Governo per lo sviluppo della Società dell'Informazione nella legislatura* (2002). Roma: Ministro per l'innovazione e le tecnologie, http://www.innovazione.gov.it/ita/documenti/socinfo11_06_02.pdf, 10. 05. 2005.
29. *Linee strategiche volte ad indirizzare le amministrazioni nella predisposizione del piano triennale per l'informatica 2006-2008* (2005). CNIPA, http://www.cnipa.gov.it/site/_files/Linee%20strategiche%202006_2008%20v.1.pdf, 10. 05. 2005.
30. *Odločba št. 1336/97/ES Evropskega parlamenta in Sveta o vrsti smernic za vseevropska telekomunikacijska omrežja* (1997). Official Journal L 183, 11/07/1997 P. 0012 – 0020, http://europa.eu.int/eur-lex/LexUriServ/LexUriServ.do?uri=CELEX:31997D1336:SL:HTML, 22. 07. 2005.
31. *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (2002). OECD Publications, 81829,

http://www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf, 25. 05. 2005.

32. *Okvirni sklep Sveta 2005/222/PNZ o napadih na informacijske sisteme* (2005). Official Journal L. 069, 16/03/2005 P. 0067 – 0071, http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:SL:HTML, 22. 07. 2005.
33. *Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione* (2004). Roma: Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni, http://www.innovazione.gov.it/ita/normativa/allegati/proposte_sicurezza_marzo04.pdf, 26. 04. 2005.
34. *Resolution of the Council and the Representatives of the Governments of the Member States, on illegal and harmful content on the Internet 97/C 70/01* (1997). Official Journal C 070, 06/03/1997 P. 0001 – 0002, http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:41997X0306:EN:HTML, 22. 07. 2005.
35. *Sporočilo Komisije Svetu Evrope in Evropskemu parlamentu – Varovanje kritične infrastrukture v boju proti terorizmu /KOM/2004/0702 končno/* (2004). Bruselj: Komisija evropskih skupnosti, http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0702:SL:HTML, 22. 07. 2005.
36. *Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov* (2001). Official Journal L. 008, 12/01/2001 P. 0001 – 0022, http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32001R0045:SL:HTML, 22. 07. 2005.
37. *Uredba (ES) št.460/2004 Evropskega parlamenta in Sveta o ustanovitvi Evropske agencije za varnost omrežij in informacij (2004).* Official Journal L. 077, 13/03/2004 P. 0001 – 0011, http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:SL:HTML, 22. 07. 2005.

Ostali internetni viri

38. *Active Server Pages: A Word Definition From the Webopedia Computer Dictionary,* http://www.webopedia.com/TERM/A/Active_Server_Pages.html, 15. 06. 2006.

39. *Aplication Service Provider: A Word Definition From the Webopedia Computer Dictionary,* http://www.webopedia.com/TERM/A/Application_Service_Provider.html, 15. 06. 2006.
40. *Associazione Italiana per la Sicurezza Informatica,* Milano: CLUSIT, http://www.clusit.it/soci.htm, 04. 06. 2006.
41. *Attivita ed organizzazione* (2005). Polizia Postale e delle Comunicazioni, http://www.poliziastato.it/pds/informatica/attivita.html, 01. 06. 2005.
42. *eCSIRT.net Code of Conduct* (2006). The European Computer Security Incident Response Team Network, http://www.ecsirt.net/service/coc.html, 15. 06. 2006.
43. *ENISA – defending the future*, http://www.enisa.eu.int/ , 15. 06. 2006.
44. *EU Forum on Cybercrime,* http://cybercrime-forum.jrc.it/default, 25. 07. 2005.
45. *Europa – Kratka predstavitev EU,* http://europa.eu.int/abc/index_sl.htm, 25. 07. 2005.
46. *FIRST – Improving security together*, http://first.org/, 15. 06. 2006.
47. *IP-naslov, Wikipedija, prosta enciklopedija,* http://sl.wikipedia.org/wiki/IP, 15. 06. 2006.
48. *Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione,* http://www.iscom.gov.it/contenuti.asp?ID=65, 20. 04. 2006.
49. *Italia.gov.it: Il Portale Nazionale del Cittadino,* http://www.italia.gov.it/servlet/ContentServer?channel=HTTP&pagename=e-Italia/HomeHttp, 12. 05. 2006.
50. *Italija – Wikipedija, prosta enciklopedija,* http://sl.wikipedia.org/wiki/Italija, 17. 7. 2005.
51. *Kaj je SI-CERT?.* Arnes, http://www.arnes.si/si-cert/opis.html, 20. 05. 2005.
52. *MIT – Comunicato dell 11 ottobre 2002* (2002). Roma: Comunicato a cura dell'Ufficio Stampa del Ministro per l'Innovazione e le Tecnologie, http://www.innovazione.gov.it/ita/mit_informa/comunicati/2002_10_11.shtml, 10. 05. 2005.
53. *Presentata l'attivita del Govcert nel 2005: Sicurezza informatica nella PA* (2006). Roma: CNIPA, http://www.cnipa.gov.it, 01. 06. 2006.
54. *RIS: Raba Interneta v Sloveniji,* http://www.ris.org/ , 12. 05. 2006.
55. *SCADPlus: Information Society,* http://europa.eu.int/scadplus/leg/en/s21012.htm#SECURITY, 20. 07. 2005.
56. *SI-CERT – Slovenian Computer Emergency Responce Team.* Arnes, http://www.arnes.si/si-cert/, 20. 05. 2005.

57. *Sistema Publico di Connettivita (SPC)* (2005). Roma: CNIPA, http://www.cnipa.gov.it/site/it-IT/In_primo_piano/Sistema_Pubblico_di_Connettivit%c3%a0_(SPC)/, 19. 05. 2005.
58. *Svet Evrope* (2003), http://www.coe.int/si/portal/default.asp?L=SI, 23. 07. 2005.
59. *Terminološka baza izrazov Evropske unije,* http://www.gov.si/evroterm/, 12. 05. 2006.
60. *The e-Europe Action Lines* (2001). ETSI, http://www.e-europestandards.org/action_lines.htm#2002, 25. 07. 2005
61. *The Ministry of Communications: General Duties,* http://www.comunicazioni.it/en/index.php?Mn1=5, 23. 05. 2006.
62. *VoIP, Wikipedija, prosta enciklopedija,* http://sl.wikipedia.org/wiki/VoIP, 15. 06. 2006.
63. *Welcome to CERT!*, http://www.cert.org/ , 16. 06. 2006.
64. *Wi-Fi, Wikipedia, the free encyclopedia,* http://en.wikipedia.org/wiki/Wifi, 15. 06. 2006.
65. *WiMAX*, *Wikipedia, the free encyclopedia,* http://en.wikipedia.org/wiki/WIMAX, 15. 06.2006.
66. *Zasebnost in nadzor,* http://www.ljudmila.org/matej/zasebnost/zasebnost99/1.htm, 13. 05. 2006.

Priloge

Priloga 1: CLUSIT – Logotipi vključenih podjetij in organizacij

Vir: http://www.clusit.it/soci.htm

Priloga 2: Logotipi nekaterih dejavnikov, ki tvorijo, razvijajo in izvajajo CIIP v Italiji

- Minister za inovacije in tehnologijo (http://www.mininnovazione.gov.it/)

- Ministrstvo za komunikacije (http://www.comunicazioni.it/en/index.php?Mn1=5)

- Oddelek za inovacije in tehnologijo (http://www.innovazione.gov.it/)

- Policija za pošto in komunikacije (Polizia Postale e delle Comunicazioni)

- Višji inštitut za komunikacije in informacijske tehnologije (http://www.iscom.gov.it/)

- Italijansko združenje za informacijsko varnost (http://www.clusit.it/)

- Nacionalni center za informatiko v javni upravi (http://www.cnipa.gov.it)

- Nacionalni tehnični komite za IKT zaščito v javni upravi (V: http://www.innovazione.gov.it/ita/mit_informa/comunicati/2002_10_11.shtml)