UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Marko Kojc

Informacijska varnost v Republiki Sloveniji

Diplomsko delo

Ljubljana, 2010

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Marko Kojc

Mentor: redni prof. dr. Marjan Malešič
Somentor: docent dr. Uroš Svete

Informacijska varnost v Republiki Sloveniji

Diplomsko delo

Ljubljana, 2010

ZAHVALA

Iskrena hvala moji družini za vso materialno in moralno podporo skozi vsa študijska leta. Kolegom in kolegicam ter vsem bližnjim za vso izkazano razumevanje. Predvsem pa tisti, ki mi je v vseh pogledih najbolj stala ob strani.
Mentorju in somentorju, dr. Marjanu Malešiču in dr. Urošu Svetetu, za strokovne nasvete in usmeritve pri nastajanju mojega diplomskega dela.

INFORMACIJSKA VARNOST V REPUBLIKI SLOVENIJI

Tehnološki in tehnični razvoj ter pojav mnogih uporabnih informacijskih in komunikacijskih tehnologij je omogočil današnji družbi velik razvoj in napredek, s čimer je le-ta postala omrežena. Omrežja, informacijsko komunikacijska tehnologija (IKT) in predvsem internet imajo mnoge uporabne lastnosti tako za državo kot tudi za gospodarstvo in posameznike. IKT se pojavlja v vlogi nosilca družbene moči in kot točka velike ranljivosti sodobnih družb. V diplomski nalogi obravnavam teoretske in praktične pristope k obravnavanju informacijske varnosti. Sistematično predstavljam naddržavni nivo – EU, državni nivo in nivo gospodarskega družbenega podsistema. Zaradi specifik IKT in sodobnih asimetričnih groženj je država pri zagotavljanju varnosti na svojem ozemlju primorana v sodelovanje z EU in s pomembnimi družbenimi podsistemi. Diplomsko delo s pomočjo teorije in praktičnih primerov pojasnjuje interes treh obravnavanih nivojev po zagotovitvi informacijske varnosti.

KLJUČNE BESEDE: varnost, informacijska varnost, interes, koncept omrežne in informacijske varnosti, varnostna politika.

INFORMATION SECURITY IN SLOVENIA

Technological and technical developments and the emergence of many useful information and communication technologies have led to great development and progress of the today's society which has become a networked society. Networks, ICT and especially the internet have many useful properties for the country, the economy and individuals. ICT appears in the role of an institution of social power and as a point of great vulnerability of modern societies. The diploma discusses the theoretical and practical approaches to dealing with information security. The transnational level - the EU, the national level and the level of economic social subsystem will be systematically presented. Due to the specifics of ICT and modern asymmetric threats, the country is forced to cooperate with the EU and with important societal subsystems to ensure security on its territory. By using theory and practical examples, the diploma explains the present interest in three levels to ensure information security.

KEY WORDS: security, information security, interest, network and information security, security policy.

KAZALO

KAZALO TABEL IN SLIK

SEZNAM KRATIC

ARNES Akademska raziskovalna mreža Slovenije

BLOG ang. weB LOG – spletni dnevnik

CERT ang. Computer Emergency Response Team, odzivna skupina za računalniške nevarnosti

CPU ang. Central Processing Unit – glavna procesna enota, procesor

CYBERSPACE internet; kibernetski prostor

CYBERWAR spopad v virtualni sferi

DOS Denial of Service, zatajitev delovanja, zavrnitev storitve

DSL ang. Digital Subscriber Line, digitalni naročniški vod

ENISA Evropske agencije za varnost omrežij in informacij

EU European Union, Evropska unija

GSM Global System Mobile

ID informacijska družba

IKT informacijsko komunikacijske tehnologije

INFOSEC Information Security, informacijska varnost

IP ŠTEVILKA Internet Protocol

ISP Internet Service Provider, ponudnik internetne povezave

IT angl. Information technology, informacijska tehnologija

MALWARE zlonamerni programi

NATO North Atlantic Treaty Organization, Organizacija severnoatlantskega sporazuma

P2P Peer to Peer, uporabnik do uporabnika

SIGEN-CA Slovenian General Certification Authority, izdajatelj digitalnih potrdil za fizične osebe in poslovne subjekte

SIGOV-CA Slovenian Governmental Certification Authority, izdajatelj digitalnih potrdil za državne organe

TCP/IP Transmission Control Protocol/Internet Protocol

TS Telekom Slovenije

VPN Virtual Private Network, navidezno zasebno omrežje

WAN Wide Area Network

WWW World Wide Web

1 UVOD

Državna varnost, mir in lastnina so univerzalne skrbi,
le metode za njihovo obravnavo se skozi čas razlikujejo.
(Svete 2005, 51)

Razvoju informacijsko komunikacijske tehnologije, v prvi vrsti najbolj prepoznavnih računalnikov, lahko sledimo v zelo elementarni obliki že davno v antiki, kjer je preprost mehanizem za osnovne matematične funkcije, imenovan Abakus, predstavljal njihov začetek. Informacijska tehnologija je rasla skupaj z družbo in se razvijala v vedno novih razvojnih ciklih. Teoretiki so si enotni, da je ravno pospešen razvoj informacijsko komunikacijske tehnologije omogočil razvoj današnje sodobne družbe, države in gospodarstva.

Današnja družba je vse bolj prepletena ter odvisna od uporabe in zanesljivega delovanja raznih omrežij, zato v tem kontekstu lahko govorimo tudi o t.i. omreženi družbi. Povečana uporaba in posledična odvisnost delovanja družbenih podsistemov od informacijsko komunikacijske tehnologije (IKT) pa predstavljata novo relevantno varnostno vprašanje za državo ter njene podsisteme, predvsem pa za gospodarstvo. Globalizacija je poleg nekaterih prednosti prinesla tudi številne nevarnosti in tveganja tako za državo kot za globalno delujoče gospodarstvo. Po razpadu blokovske delitve sveta in koncu hladne vojne so se varnostne razmere v svetu spremenile in zavezništva so se bila prisiljena prilagoditi na nove oblike ogrožanj. V težnji po miru in gospodarskem sodelovanju se je začelo tudi povezovanje Evrope v skupno naddržavno asociacijo z nekaterimi skupnimi politikami in mehanizmi. Spremenjeno varnostno okolje, pojav terorizma in transnacionalnih oblik ogrožanja nacionalne varnosti ter odvisnost sodobnih družb od informacij predstavljajo nov varnostni izziv informacijski varnosti in zaščiti kritične informacijske infrastrukture.

Omenjene razmere so vplivale tudi na Republiko Slovenijo, ki je svojo mlado državnost priključila evropskim tokovom, gospodarstvo pa postavila v tržno ekonomsko okolje. Ko govorimo o interesu po oblikovanju učinkovite informacijsko varnostne politike, ne moremo

mimo dejstva, da se le-ta sooblikuje skozi interese Evropske unije, države same in gospodarstva. Slednje je zaradi narave tehnologije pomemben partner državi pri iskanju učinkovitih varnostnih politik, pri čemer pa je postavljeno pred dejstvo, da deluje na prostem trgu konkurenčnega boja. Delovanje gospodarske družbe na zahtevnem polju informacijske varnosti najbolje pojasni teoretski koncept informacijske in omrežne varnosti. Ta govori o notranji varnosti same organizacije ter o zunanji varnosti, pri čemer gre predvsem za varnost informacijskega toka med ponudniki in povpraševalci, ki se smatra za storitev, za katero potrošniki nenazadnje plačujejo.

Če je gospodarstvo postavljeno pred svojevrstno varnostno dilemo med notranjo varnostjo same organizacije ter varnostjo potrošnikov in storitve na drugi strani, je država tukaj v nekoliko drugačnem položaju. V luči novih varnostnih groženj in novih strategij, nastalih po terorističnih napadih 11. septembra 2001, se je odprlo bistveno vprašanje med svobodo in varnostjo, med omejevanjem ene dobrine na račun druge. Posebej aktualno je v tem smislu vprašanje svobode na internetu in omejevanje dostopa do interneta. Nekatere države si namreč pridržujejo povečano mero omejevanja svobode in dostopa do interneta ter tako pod krinko varnosti ali ideologije blokirajo določene vsebine na svetovnem spletu. Države so s tem ustvarile zavedanje o svoji kritični infrastrukturi, med katero je informacijska bistvenega pomena, ter začele z razmišljanjem o zavarovanju le-te. Informacijska varnost se na državnem nivoju zagotavlja s tehničnimi, fizičnimi in organizacijskimi sredstvi, podobna načelna organiziranost pa velja tudi za raven Evropske unije. Gospodarstvo kot tako je pri zagotavljanju informacijske varnosti postavljeno še pred dejstvo človeškega faktorja kot potencialne notranje varnostne grožnje, česar se loteva z represijo na eni in preventivo na drugi strani. Ko je govora o preventivi, gre pri tem predvsem za širjenje varnostne kulture in za izobraževanje ter ostale oblike motiviranja zaposlenih.

Ob novih grožnjah in povečani rabi IKT je država temu področju začela namenjati več pozornosti. Varnostni mehanizmi, organiziranje in politika so v svoje delovanje vključili tudi pojem informacijske varnosti in njegove zagotovitve. Opravljene so bile številne raziskave na temo groženj, ki jih prinašajo spremenjene varnostne razmere, na podlagi katerih se varnostni sistem kot celota prilagaja. Tako Evropska unija kot tudi država in njeno gospodarstvo se zavedajo groženj informacijski varnosti, saj imajo vsi svoje skupne in posebne interese za zagotavljanje učinkovite informacijsko varnostne politike.

2 METODOLOŠKO – HIPOTETIČNI OKVIR

2.1 Opredelitev ciljev proučevanja/analize

Namen tega diplomskega dela je predstaviti in proučiti razumevanje informacijske varnosti v Republiki Sloveniji. Zaradi članstva Slovenije v Evropski uniji in nekaterih skupnih politik je pričakovati, da se informacijska varnost države sooblikuje skozi članstvo v naddržavni asociaciji. Kompleksnost pojma varnosti in specifika področja informacijske in komunikacijske tehnologije pa postavlja državo v položaj, kjer je primorana sodelovati z zasebnim, gospodarskim sektorjem. Velika telekomunikacijska podjetja so v času omrežene družbe pomemben partner države pri oblikovanju učinkovite informacijsko varnostne politike, pri tem pa svoje delovanje nenehno prilagajajo zakonitostim prostega trga. Država je tako vpeta med zahteve Evropske unije in interesi gospodarstva po optimalizaciji dobička, pri čemer mora za svoje državljane zagotavljati najvišjo možno mero zaščite in obrambe pred nevarnostmi informacijske dobe. Ob pomoči definicij ključnih pojmov bom predstavil razumevanje informacijske varnosti na treh nivojih; na nivoju EU, na nivoju države in v gospodarski sferi. Predstavil bom proces oblikovanja informacijsko varnostih politik, prepletanje in medsebojno vplivanje treh ravni, predvsem pa izvor interesa po oblikovanju učinkovitih varnostnih politik.

2.2 Raziskovalna vprašanja

Statistični kazalniki govorijo o povečani rabi informacijsko komunikacijske tehnologije v javni kakor tudi zasebni sferi. Družba in njeni podsistemi postajajo vse bolj odvisni od IKT, kar za državo postavlja resno in relevantno varnostno vprašanje. Teorija varnosti govori, da informacijsko varnost Republike Slovenije determinirajo politično ekonomske povezave z naddržavno asociacijo EU ter njenim politično kulturnim ozadjem (Svete 2005, 256). Gonilna sila razvoja informacijsko komunikacijske tehnologije je gospodarstvo, ki na prostem trgu ponudbe in povpraševanja zasleduje svoje interese, nesporno pa je tudi sooblikovalec informacijsko varnostne politike. Na podlagi opisanega se mi postavljajo naslednja relevantna raziskovalna vprašanja:

»Kakšni so interesi Evropske unije, države Slovenije in njenega gospodarstva za zagotavljanje informacijske varnosti?«

»Kateri so pozitivni in negativni učinki zagotavljanja informacijske varnosti na ravni Evropske unije, države Slovenije in njenega gospodarstva?«

»Katere so glavne ovire pri zagotavljanju informacijske varnosti na ravni Evropske unije, države Slovenije in njenega gospodarstva?«

2.3 Ključne metode dela

Pri oblikovanju diplomske naloge sem uporabil več različnih metod dela, da bi raziskal problematiko, ki je z njo povezana. Varnost je že v svojem izvornem bistvu zelo kompleksen pojem, pri katerem se prepletata tako družboslovni kot tehnološko tehnični vidik obravnave. Slednje dejstvo sili proučevalca varnostne problematike v dokaj visoko mero interdisciplinarnosti. Zaradi budnega spremljanja vsakodnevnih novic in dogajanj na področju informacijske varnosti pred samim pisanjem diplomskega dela sem temeljito razmišljal o obravnavani problematiki.

Sistematična študija materije se je začenjala z *metodo zbiranja virov;* zbral in predelal sem razpoložljivo in relevantno literaturo, ki je vključevala znanstvene monografije, strokovne članke, uradne dokumente. Vire sem izbiral premišljeno in selektivno, saj sem z njihovo pomočjo zasledoval točno določeno raziskovalno vprašanje. Za izhodišče sem uporabil strokovne članke in knjige mojega mentorja. Da bi se izognil podvajanju diplomskih tematik in za orientacijo sem skrbno pregledal snov, ki je bila že napisana v diplomskih delih. Pri pisanju teoretskega okvirja ter pri opredelitvi ključnih pojmov in koncepta informacijske varnosti sem uporabil *metodo analize vsebine primarnih in sekundarnih virov*. Pri opisu stanja in ureditve na področju informacijske varnosti sem uporabil predvsem *opisno metodo*, da bi opisal vse dejavnike, ki odločilno determinirajo proučevano področje. Opisno metodo sem uporabil tudi v nadaljevanju, ko sem predstavil obravnavanje, razumevanje in organiziranje informacijske varnosti na treh različnih hierarhičnih nivojih – na ravni EU in Republike Slovenije ter v sferi gospodarstva, delujočega na prostem trgu.

Ta diplomska naloga raziskuje vplive na področje informacijske varnosti z obramboslovnega vidika, v luči varnostne razprave ter predvsem skozi koncept omrežne in informacijske varnosti. Vsekakor pa je za celovito razumevanje področja informacijske varnosti potrebno vključiti tudi določeno mero tehničnega razumevanja proučevanega področja. Seveda pa je tako kompleksen pojem, kot je varnost, potrebno obravnavati z interdisciplinarnim pristopom. Za potrebe dodatnega pojasnjevanja informacijske varnosti na različnih nivojih sem uporabil *metodo intervjuja* s kompetentnima osebama. Informacije iz prakse, pridobljene z intervjujem, dajejo diplomskemu delu še dodatno kvaliteto. Na podlagi *primerjalnega raziskovanja* bom poskušal podati zaključke in med seboj primerjati tri nivoje razumevanja informacijske varnosti ter tako celovito pojasniti potek oblikovanja informacijske varnosti v Republiki Sloveniji. S pomočjo predstavljenih metod dela bom ob koncu poskušal celovito odgovoriti na zastavljeno raziskovalno vprašanje.

2.4 Struktura analize

Uvodni del diplomskega dela sem namenil opisovanju družbenih razmer in konteksta, v katerega je postavljena tematika informacijske varnosti. Prikazati sem želel relevantnost in kompleksnost pojma varnosti ter upravičenost in smiselnost pozneje postavljenega raziskovalnega vprašanja. S pomočjo nekaterih kvantitativnih kazalcev rabe informacijsko komunikacijskih tehnologij in omrežij v vseh družbenih podsistemih, tako javnih kot zasebnih, pa še dodatno utemeljujem koncept omrežne in informacijske varnosti.

Metodološko hipotetični okvir služi kot temeljno izhodišče nadaljnjega pisanja, saj v njem opisujem in utemeljujem cilje proučevanja, temeljna teoretska izhodišča, konceptualno zasnovo ter na podlagi znanih uvodnih dejstev postavljena raziskovalna vprašanja. V nadaljevanju po načelih in pravilih družboslovnega pisanja in raziskovanja navajam ter pojasnjujem rabo ključnih metod dela, ki bodo uporabljene na poti pojasnjevanja raziskovalnega vprašanja in iskanja ustreznih odgovorov.

Pomemben del diplomske naloge bo natančnejša, na podlagi relevantnih virov izvedena, definicija in opredelitev temeljnih pojmov in ključnih teoretskih konceptov. Ker bo diplomsko delo v določenem poglavju obravnavalo razumevanje informacijske varnosti na ravni gospodarske družbe in se tako ne bo spuščalo na raven posameznika, bom kot relevantni

teoretski koncept v tem delu podrobneje predstavil koncept omrežne in informacijske varnosti. Skladno z raziskovalnim vprašanjem bom definiral ključne pojme, kot so varnost, informacijska varnost, varnostna politika, informacijski sistem, kritična informacijska infrastruktura ter interes.

Osrednji del diplomskega dela bo namenjen predstavitvi razumevanja informacijske varnosti na treh različnih nivojih, za katere menim, da sooblikujejo varnostno politiko tega področja. Najprej bom predstavil razumevanje informacijske varnosti na ravni Evropske Unije in orisal ključno zakonodajo, usmeritvene dokumente, organe in institucije, ki v največji meri obravnavajo to področje. Na ravni Republike Slovenije bom prav tako predstavil ključne organe, zakone in dokumente, ki so vključeni v proces oblikovanja informacijske varnosti, ter na ta način poskušal predstaviti pristop k informacijski varnosti na ravni države. Nivo nižje od države so gospodarske družbe, ki imajo v luči koncepta omrežne in informacijske varnosti dvojen interes za visoko stopnjo informacijske varnosti. Prvi je t.i. model notranje varnosti gospodarskih družb in posledično varstvo zaupnih poslovnih podatkov pred konkurenco, druga komponenta je pa t.i. informacijska zagotovitev, ki zagotavlja nemoten pretok informacij od ponudnika do končnega uporabnika, kar nenazadnje gospodarskim družbam prinaša dobiček. Na primeru telekomunikacijskega podjetja bom tako predstavil razumevanje informacijske varnosti še na tem nivoju. Za potrebe dodatnega pojasnjevanja bom v opise poleg pisnih virov vključil tudi podatke, pridobljene z metodo intervjuja kompetentnih oseb posamezne ravni.

Zaključek je namenjen podajanju odgovorov na raziskovalna vprašanja ter povzemanju ključnih ugotovitev. Zaradi kompleksnosti in interdisciplinarnosti obravnavane tematike je bistvenega pomena, da raziskovalna vprašanja postavim precizno. Tako bom »rdečo nit« s pomočjo smiselnega metodološkega pristopa pripeljal do samega zaključka, kjer bodo podani natančnejši odgovori, ki jih raziskovalna vprašanja zahtevajo.

2.5 Opredelitev pojmov in konceptov

2.5.1 Varnost

Varnost je kompleksen pojem, zagotavljanje varnosti pa pomembna dejavnost vsake države, družbe in vseh njenih podsistemov. O razumevanju varnosti lahko govorimo z več vidikov: z vidika posameznika, družbe, države, mednarodne skupnosti in celo sveta kot celote. Za razumevanje tematike diplomskega dela je bistven teoretski premik v obravnavanju varnosti: varnost se ne obravnava več zgolj kot izključna kategorija mednarodnih odnosov in nacionalne države, temveč se nivo obravnave spušča na raven posameznika, družbenih skupin in podsistemov (Grayson 2003). Varnost se tako obravnava kot kompleksen pojem, ki se ne omejuje zgolj na tradicionalne vojaške in zunanje grožnje nacionalni državi. Obravnava je kompleksna tako v smislu virov ogrožanja referenčnih objektov, na katere se varnost nanaša, kot mehanizmov za njeno zagotavljanje (Malešič 2004).

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. Zaznamujejo ga velika soodvisnost držav, o kateri priča vključenost držav v mednarodne asociacije, in uporaba ter odvisnost od različnih mrež, ki jih omogoča sodobna tehnologija. Slednje pospešuje in povečuje erozijo nacionalne države, svoj prispevek pa nosijo tudi viri ogrožanja, ki učinkujejo čezmejno in se ne zmenijo za koncept suverenosti nacionalnih držav (Malešič 2002, 138).

Pojmovanje varnosti se spreminja vzporedno s spremenjenimi (novimi) viri ogrožanja. Odvisnost družbe, države in njenih podsistemov od splošno razširjene uporabe informacijsko komunikacijske tehnologije poraja nova varnostno relevantna vprašanja. Slednja vidijo razširjeno rabo IKT tako kot vir moči kakor tudi kot vir ranljivosti in s tem povezanimi varnostnimi izzivi, tveganji in grožnjami (Svete 2005, 17).

Novejši teoretski pogledi na varnost v ospredje postavljajo predvsem človeka in njegovo varnost, na tem mestu govorimo o »človekovi varnosti«. Varnost države in varnost med državami sta nujna, vendar nezadostna pogoja za zagotovitev človekove varnosti. Osrednji elementi za zagotovitev človekove varnosti se kažejo v demokratičnosti, vladavini prava in

spoštovanju človekovih pravic. Cilj človekove varnosti je varovati nujno potrebno jedro vseh človeških življenj pred kritičnimi, razširjenimi grožnjami brez hkratnega negativnega vplivanja na dolgoročno človekovo izpolnitev (Vogrin 2008, 32–33).

2.5.2 Varnostna politika

Nacionalno varnost lahko razumemo kot varnost državnega ozemlja (vključno z zračnim prostorom in ozemeljskimi vodami), varnost življenja ljudi in njihove lastnine, ohranitev in vzdrževanje nacionalne suverenosti ter uresničevanje temeljnih funkcij družbe (socialne, gospodarske, družbenopolitične, kulturne, ekološke idr.). Na tej točki teoretske definicije je za potrebe diplomskega dela potrebno izpostaviti gospodarsko funkcijo družbe, ki bo v poglavju informacijske varnosti na ravni gospodarske družbe podrobneje obravnavana. Razumevanje in zagotavljanje varnosti je institucionalizirano v nacionalno-varnostnem sistemu. Nacionalno-varnostni sistem sestavljata varnostna politika in varnostna struktura (Grizold 1999, 25):

Varnostna politika: varnostno politiko v širšem smislu opredelimo kot dejavnost države za pripravo pred ogrožanjem iz okolja. Cilj varnostne politike je zasnova mehanizmov in sredstev, s katerimi se zagotavljata notranja in zunanja varnost družbe. Vključuje zunanjo, obrambno, gospodarsko, socialno, ekološko, zdravstveno, energetsko, izobraževalno in kulturno politiko.

Varnostna struktura: varnostna struktura je namenjena zagotavljanju varnosti na ravni celotne družbe in je sestavljena iz dveh prvin: obrambne in notranjo-varnostne. Naloge obrambne prvine so predvsem spopadanje z vojaškim ogrožanjem družbe in skrb za nemoteno delovanje različnih podsistemov v vojni.

Na podlagi varnostne teorije lahko sklepamo, da je informacijska varnost relevantno varnostno vprašanje za sodobno državo. Slednja teži k temu, da v primeru vojne ali izrednih razmer zagotovi kar najbolj nemoteno delovanje različnih družbenih podsistemov, med katerimi sta gospodarstvo in z njim povezana kritična infrastruktura zagotovo velikega pomena. V luči kompleksnega obravnavanja pojma varnosti ter procesa oblikovanja varnostnih politik bomo v strukturo diplomske naloge povsem relevantno vključili

gospodarstvo ter na podlagi primera prikazali oblikovanje varnostne politike in varnostne strukture še na tem družbenem podsistemu.

2.5.3 Informacijski sistem

Informacijski sistem je termin, ki je mogoče pojasniti, opisati in definirati na različne bolj ali manj široke načine. Za potrebe diplomskega dela bom uporabil nekaj najbolj značilnih premis. Informacijski sistem v polnem pomenu besede opredeljujejo kot celotno infrastrukturo, osebje in komponente, ki so namenjene zbiranju, obdelovanju, hranjenju, oddajanju, prikazovanju, širjenju in dispoziciji informacij (Simšič 2007, 10–11). Nekatere bistvene lastnosti, ki dokaj dobro opišejo informacijski sistem, so: kompleksni, interaktivni, emergentni, kot posebno lastnost pa imajo disfunkcijsko delovanje, ki ga povzroči t.i. hrošč. Na njihovo kompleksnost kažejo vedno bolj zmogljivi in napredni računalniški ter programski sistemi, ki jih poganjajo. Interaktivnost je mišljena v smislu zmogljivosti sistemov, da med seboj povezujejo in izmenjujejo potrebne podatke in informacije. Potencirana oblika slednjega je svetovni splet ali internet, ki je v svojem bistvu velika mreža med seboj povezanih računalnikov. Da je informacijski sistem emergenten, pomeni, da ne deluje tako, kakor so si to zamislili proizvajalci in primarni uporabniki. Poleg predvidenih oblik neškodljive rabe se lahko pojavijo načini uporabe in zlorabe tovrstne lastnosti v varnostno škodljive namene. Posebna anomalija, neponovljivo in nelogično delovanje sistema je pojav, ki ga povzroči t.i. hrošč. Za razumevanje pojma je potrebno pogledati v začetno obdobje razvoja računalnikov, ki so ga zaznamovali kot soba veliki preprosti računalniki in na katerih so dejansko nastajale nelogične napake zaradi živih hroščev, ki so se ujeli med vezji (Schneier 2000, 6).

2.5.4 Informacijska varnost

Državni slovar informacijske sistemske varnosti informacijsko varnost sistemov opredeljuje kot zaščito informacijskih sistemov pred nepooblaščenimi dostopi ali modifikacijami informacij, najsi bo v shranjeni obliki, v procesu ali prenosu, ter zaščito pred zatajitvijo delovanja (DOS) pooblaščenim uporabnikom in zagotovitvijo delovanja nepooblaščenim uporabnikom, vključno z vsemi ukrepi za odkrivanje, dokumentiranje in zavračanje tovrstnih groženj (Hayden 2003, 33). IBM-ov računalniški slovar informacijsko varnost opredeljuje kot

koncepte, tehnike, tehnične in administrativne ukrepe, ki se jih uporablja za zaščito informacij pred namernimi ali nenamernimi nepooblaščenimi pridobitvami, povzročanjem škode, razkritjem informacij, spremembo informacij, manipuliranje z njimi ali izgubo in uporabo informacij (McDaniel 1994, 94).

Glavnina opredelitev informacijske varnosti se osredotoča na specifično uporabo in specifičen medij (primer: zaščititi elektronske podatke pred nepooblaščeno uporabo). V bistvu pa je to nekoliko napačna predstava ali nesporazum, da se informacijsko varnost enači z računalniško varnostjo, ker ta predstavlja ožji pojem. Tovrstne definicije glede prenosa informacij (komunikacijski vidik) in uporabniškega vidika informacijsko komunikacijske tehnologije opredeljuje ter obravnava koncept omrežne in informacijske varnosti, ki ga bom v nadaljevanju natančneje predstavil. Koncept informacijske varnosti pa je širši in kot cilj ogroženosti vključuje celotno IKT, vključno z zbiranjem in obdelavo podatkov, in delovanje strojne opreme nasploh (Svete 2005, 107).

Podjetja se v današnjem poslovnem okolju soočajo z zahtevnim izzivom ohranjanja konkurenčnosti. S ciljem racionalizacije stroškov in približevanja kupcu prilagajajo obstoječo informacijsko infrastrukturo, s čimer odpirajo vrata svojega sistema. V tej točki se pojavi vprašanje informacijske varnosti, ki zajema zaščito podatkov in fizičnih komponent sistema pred namerno ali nenamerno zlorabo. Najpogosteje izvirajo iz raznih prevar in kraj storitev, intelektualne lastnine, privatnih podatkov ter vsakdanjega vandalizma (Gordon in drugi, 2004). Pri obravnavi informacijske varnosti v gospodarstvu bom problematiko nekoliko ožje predstavil v luči omrežne in informacijske varnosti, ki govori tudi o neprekinjenem toku informacij med ponudniki in povpraševalci.

2.5.5 Kritična informacijska infrastruktura

Informacijsko komunikacijska tehnologija je tehnologija, namenjena zbiranju, obdelavi in prenosu podatkov. Na njo se gleda kot na osrednji medij, vsiljen dejavnik proizvodnje in gonilno silo organizacijskih sprememb. Vedno bolj je poudarjena komponenta prenosa podatkov (Svete 2005, 16). S tem se daje poudarek predvsem na komunikacijski vidik tega tehnološko tehničnega sistema, kar pa poraja nov pojem, ki ga je potrebno definirati: kritično infrastrukturo lahko opredelimo kot mrežo neodvisnih, večinoma zasebnih, antropogenih

sistemov in procesov, ki delujejo skupno in sinergično, da bi ustvarili in usmerjali stalen tok pomembnih dobrin in storitev (Dunn 2004, 24).

Novejši teoretski pogledi na pojem kritične infrastrukture izhajajo iz razširjene rabe IKT na vseh nivojih družbenega funkcioniranja in iz pojava sodobnih groženj, predvsem asimetričnega globalnega terorizma. Danes je spekter kritične infrastrukture izjemno širok, nekateri avtorji so celo mnenja, da je težko določiti sektorje, ki niso kritični. Za kontekst diplomskega dela pa je potrebno široko področje nekoliko natančneje definirati. Kritična infrastruktura je temelj zmogljivosti, tehnični sistemi in organizacije, ki zagotavljajo zmogljivosti. Omenjeno omogoča zagotavljanje velikega spektra družbenih aktivnosti, dobrin in storitev. Infrastrukture so po svoji naravi večnamenske in lahko predstavljajo globalna sredstva za nedoločljive cilje (Prezelj 2010, 9). Nemogoče je celovito obravnavati in zaščititi vso kritično infrastrukturo, zato se je potrebno osredotočiti na nekaj konkretnega in obvladljivega. Tukaj se pojavi kategorija kritičnih procesov, kjer se jih ločuje po več nivojih kritičnosti. Kritični procesi se glede na nivo delijo na:

- poslovno kritične procese, to so kritični procesi za podjetja, kamor sodijo tisti procesi, katerih motnje bi lahko ogrozile obstoj podjetja,
- kritične procese za sektor in
- kritične procese za družbo (Prezelj 2010, 12).

Do prepletanja in brisanja mej med nivoji kritičnih procesov lahko pride, ko obravnavamo večje podjetje, ki ima za državo in družbo tudi strateški pomen. Na izbranem konkretnem primeru domačega telekomunikacijskega podjetja bo slednje vsekakor primer, saj s svojim delovanjem omogoča delovanje mnogim družbenim podsistemom in kritični procesi v podjetju bi lahko hitro postali kritični tudi za sektor in družbo. Z navedenim še dodatno utemeljujem relevantnost postavljenega raziskovalnega okvirja, kjer se predpostavlja, da je za informacijsko varnost potrebno sodelovanje tako javnega kot zasebnega sektorja.

2.5.6 Interes

Kategorija interesa je v politologijo prišla postopno in zasedla eno osrednjih mest pri razlagi politoloških procesov. V politični znanosti je pojem interesa zasedel osrednje mesto, pri

čemer se najpogosteje omenja pojem javnega in zasebnega interesa. Interes ima pomembno interpretativno vlogo pri določanju politike kot čim bolj racionalne, predvidljive in objektivne. Različne politične filozofije so oblikovale svoje koncepte interesov, tako da tako pojmovani interesi utelešajo jedro teh političnih filozofij. Liberalizem veže pojem interesa na posameznika in zasebno lastnino, socializem na kolektiv, praviloma razred, pluralizem na skupino, anarhizem na posameznika, vendar brez lastnine, korporativizem na organsko razumljen kolektiv, konservativizem na "naravno" postavljene strukture, kot so družina, verske skupnosti, vojska ipd. (Lukšič 2002, 509). Prepoznavanje in razumevanje ter posledično realiziranje interesa je postavljeno v metodološko izhodišče pričujočega diplomskega dela. Skozi predstavitev varnostnih politik in varnostnega organiziranja na različnih obravnavanih nivojih bom prikazal interese, ki vodijo družbe, države in gospodarstvo v zagotavljanje visoke stopnje informacijske varnosti.

Nacionalni interesi vsake države so v osnovi nacionalni varnostni interesi. Osnovni (vitalni) interes Republike Slovenije in vsake druge sodobne države je, da zagotovi svojim državljanom in institucijam čim višjo stopnjo varnosti oziroma čim nižjo stopnjo ogrožanja nacionalne varnosti. Država ne sme biti pripravljena sklepati kompromisov glede tega interesa. Sam koncept nacionalnega varnostnega interesa se spreminja vzporedno s spreminjanjem ogrožanja varnosti. S širjenjem pojmovanja (ogrožanja) varnosti se je razširil tudi koncept nacionalnega varnostnega interesa. Večdimenzionalnost in kompleksnost, ki sta značilni za sodobno ogrožanje varnosti, postaneta tudi lastnosti nacionalnega varnostnega interesa, kateri je sestavljen iz množice varnostnih interesov, ki ustrezajo dimenzijam in pojavom ogrožanja varnosti (Prezelj 2002, 635). Predstavljene globalne razmere vplivajo tudi na gospodarstvo, ki deluje po svojih tržnih zakonitostih v svobodni konkurenci, kjer obstajajo posebni razlogi za izražanje varnostnih interesov. Grožnje varnosti so v sodobnem globaliziranem in demokratiziranem svetu vse bolj transnacionalne, kar pomeni, da se skoraj nezadržno širijo prek meja, imajo pretežno nevojaški značaj, širijo pa jih predvsem nedržavni subjekti (kriminalne in teroristične skupine). Transnacionalno širjenje ogrožanja varnosti je mnogokrat posledica že eskalirane grožnje na nacionalni ravni (npr. oboroženi konflikt, konflikt med teroristično skupino in državo, razcvet kriminala itn.) ali pa vzrok nadaljnjega stopnjevanja drugih groženj varnosti (npr. povišanje stopnje kriminala v ciljni ali tranzitni državi kor rezultat visoke stopnje ilegalnih migracij). Ta fenomen imenujemo transnacionalno kompleksno ogrožanje varnosti (Prezelj 2002, 635). Transnacionalno pa je tudi delovanje sodobnega, na informacijsko komunikacijski tehnologiji temelječega gospodarstva, ki je na tej

točki še toliko bolj izpostavljeno novim oblikam ogrožanja varnosti, tudi informacijske. Govorimo lahko tudi o zasebnem in javnem interesu. Tako ima gospodarstvo nedvomno svoj varnostni interes v zaščiti delovanja in poslovanja. Izvršuje ga delno z lastnimi varnostnimi politikami, delno pa v okviru varnostnih interesov držav in naddržavnih asociacij, saj je v interesu države, da zagotovi varnost tudi svojemu gospodarstvu.

3 POJEM IN ZGODOVINA INFORMACIJSKE VARNOSTI

Preden se posvetimo nadaljnji vsebini diplomskega dela, je potrebno pojem informacijske varnosti še nekoliko dodatno pojasniti. V ta namen se bomo dotaknili zgodovine in navedli poskus zgodovinske evolucije samega pojma. S pomočjo opisa pojma na podlagi strokovne literature, dosegljivega na spletni enciklopediji, ter z nazorno slikovno shematsko ponazoritvijo pojma bomo ustvarili dovolj široko teoretsko opredelitev.

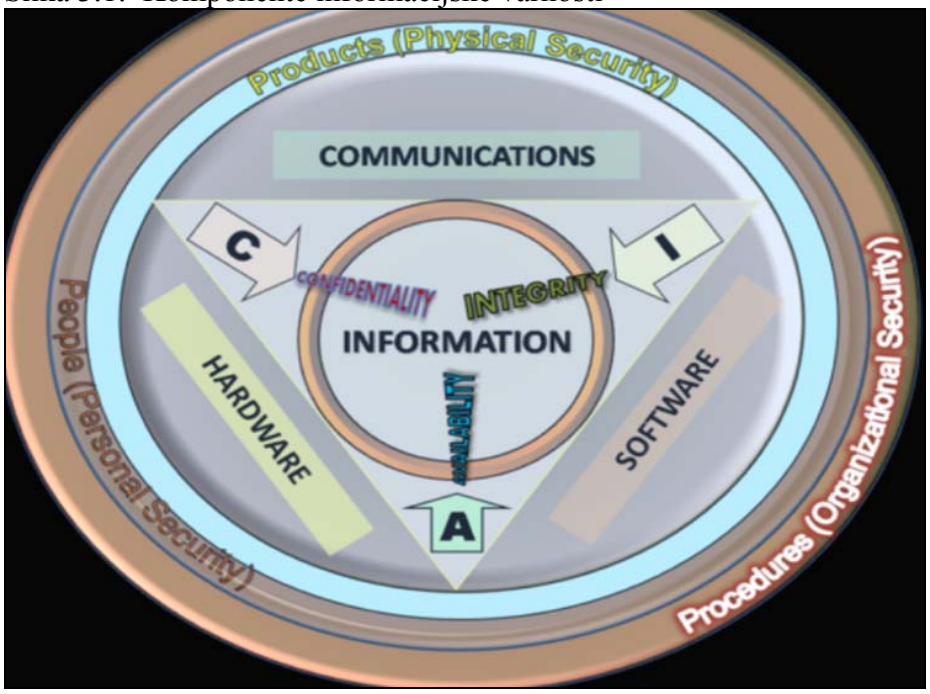
Komponente informacijske varnosti so v teoriji tri. Vrednost informacije tako izvira iz treh glavnih lastnosti ali kvalitativnih parametrov, ti pa so zaupnost, neokrnjenost in razpoložljivost (ang. confidentiality, integrity and availability – CIA). Kot že omenjeno, je informacijski sistem sestavljen iz treh glavnih delov (glej sliko 3.1): strojne opreme, programske opreme in standardov informacijsko varnostne industrije, ki se uporablja kot mehanizem zaščite in preprečitve na treh ravneh – fizičnem, osebnostnem in organizacijskem. Bistveno je, da so ljudje prek administratorjev, uporabnikov in operaterjev informirani o tem, kako uporabljati produkte, da se zagotovi informacijska varnost znotraj organizacije. Omenjeno teorijo bomo v nadaljevanju tudi podrobneje izpostavili, ko bo govora o informacijski varnosti države in gospodarstva (Information security 2010).

Informacijska varnost pomeni varstvo podatkov in informacijskih sistemov pred nezakonitim dostopom, uporabo, razkritjem, ločitvijo, spremembo ali uničenjem. Izrazi informacijska varnost, varovanje računalniških sistemov in varstvo informacij se pogosto uporabljajo kot sinonimi. Kljub temu, da so ta področja v medsebojnem odnosu in si delijo skupne cilje varstva zaupnosti, neokrnjenosti in razpoložljivosti informacij, obstajajo med njimi komaj opazne razlike. Informacijska varnost je lahko razumljena kot zaupnost, neokrnjenost in razpoložljivost podatkov ne glede na njihovo obliko, elektronsko, tiskano ali drugo. Vlada, vojska, finančne institucije, bolnišnice in privatna podjetja kopičijo velike količine zaupnih informacij o njihovih zaposlenih, strankah, proizvodih, raziskavah in finančnem položaju.

Večina teh informacij je zbrana, obdelana in shranjena na računalnikih in prenesena skozi mreže na druge računalnike. Zaupni podatki o poslovnih strankah ali financah nove proizvodne linije bi lahko padli v roke konkurenta, posledično pa v izgubo posla. Varovanje zaupnih podatkov je tako poslovna kot v mnogih primerih tudi etična in pravna zahteva. Informacijska varnost ima za posameznika pomemben vpliv na zasebnost, to pa ljudje v različnih kulturah vidijo različno. Na raven posameznika se pričujoče diplomsko delo podrobneje ne bo spuščalo. V luči pravkar opisanega se v gospodarskih družbah razvija poseben koncept t.i. »varnostne kulture«, zaželeno obnašanje svojih zaposlenih, ki ga v različnih dokumentih opredelijo organizacije, delujoče na prostem trgu konkurence (Preradović 2010).

Področje informacijske varnosti se je in se v zadnjih letih močno razvija. V smislu poklicne kariere obstajajo številne poti, kako se vključiti v to sfero, ki ponuja mnogo področij specializacije, vključno z revizijo informacijskih sistemov, načrtovanja neprekinjenega poslovanja in digitalne sodne znanosti (Wikipedia 2010a).

Slika 3.1: Komponente informacijske varnosti



Vir: Wikipedia (2010).

Slika prikazuje kompleksnost in prepletenost pojma informacijske varnosti ter pojasnjuje širok kontekst v varnostni razpravi. V širšem smislu govorimo tukaj o osebni in organizacijski varnosti ter varnosti storitev, na vse to pa vplivata skupek strojne in programske opreme ter

varnost pretoka informacij, torek komunikacijski vidik. Varnost informacije odlikujejo tri bistvene značilnosti: zaupnost, neokrnjenost in razpoložljivost.

3.1 Zgodovina

Poskus zgodovinskega opisa razvoja pojma informacijske varnosti je potrebno začeti že takrat, ko so glavni državniki in poveljniki vojske od prvega dne pisanja vedeli, da je potrebno nujno vzpostaviti mehanizme varstva zaupnosti dopisovanja. Zaradi želje po varnosti komuniciranja so uporabljali pečatni vosek in druge priprave iz voska, da bi zaznamovali verodostojnost dokumenta, preprečili vmešavanje in zagotovili zaupnost dopisovanja. Tako že na tem zgodnjem primeru vidimo, da se je na nek način že zasledovala triada CIA – confidentiality, integrity and availability. Julij Cesar je zaslovel z iznajdbo cesarske cifre leta 50 pred našim štetjem, da bi preprečil, da bi kdo prebral njegovo tajno sporočilo, če bi padlo v napačne roke. Druga svetovna vojna je prinesla mnogo prednosti na področju informacijske varnosti in zaznamovala njen začetek strokovnega področja. Primer fizičnega varovanja informacij z barikadami in oboroženimi stražami, ki so kontrolirali dostop do informacijskih centrov, se je v danih razmerah izkazal za dokaj učinkovitega. Prispevali so tudi k formalni klasifikaciji baze podatkov na osnovi občutljivosti informacij in kdo lahko dostopa do njih. Konec 20. stoletja in v zgodnjih letih 21. stoletja je prišlo do hitrega napredka v telekomunikacijah, računalniški strojni in programski opremi ter algoritmu za šifriranje podatkov. Obdelava elektronskih podatkov je postala dostopna majhnim podjetjem in domači uporabi zaradi majhne, bolj zmogljive in cenovno ugodnejše računalniške opreme. Računalniki so postali medsebojno povezani preko mreže, splošno imenovane internet ali splet. Hitro rast in široko uporabo obdelave elektronskih podatkov in poslov, ki potekajo na internetu, spremlja tudi mednarodni terorizem, za kar so potrebne boljše metode varovanja računalnikov in informacij. To dejstvo so pri načrtovanju varnostnih politik in varnostnih struktur upoštevali tudi na državnem in evropskem nivoju (Wikipedia 2010b).

4 KONCEPT OMREŽNE IN INFORMACIJSKE VARNOSTI

Številni empirični indikatorji, kot so število uporabnikov interneta, rast informacijskega sektorja sodobnih družb, razvoj novih družbenih infrastruktur na osnovi uporabe IKT ter sprememba starih, kažejo na pomen, ki ga ima IKT v sodobnih družbah. Informacijsko komunikacijsko tehnologijo se uporablja tako v gospodarstvu kot v državni sferi, tako da sta

ekonomska organizacija in večji del družbe precej odvisna od IKT, kar poraja relevantno vprašanje njene zaščite. Izhajajoč iz analize razvoja sodobne varnostne paradigme postajajo zaradi vse večjega pomena IKT v sodobnih družbah omrežja sama referenčni objekt, na katerega se varnost nanaša. V tem primeru govorimo torej o omrežni, oz. v širšem smislu o informacijski varnosti. Tovrstna omrežja presegajo geografske in birokratske omejitve ter zahtevajo mednarodno sodelovanje držav, korporacij in posameznikov (Svete 2005: 106). Omrežna varnost namreč predstavlja eno novejših varnostnih perspektiv in izvira iz naraščajočega pomena omrežnih informacijskih tehnologij v vseh vidikih postindustrijske ekonomije, vključujoč mednarodno proizvodnjo in globalne finance. Nove informacijske tehnologije so neločljivo povezane z bistvenimi spremembami v naravi ekonomske organizacije kakor tudi z drugih vidikov družbe. Ker je torej vse večji del družbe odvisen od omrežne infrastrukture, se je pojavila nova oblika varnostne predstave, ki je usmerjena v zavarovanje omrežja samega pred razpadom sistema, izgubo, krajo ali uničenjem podatkov ter prekinitvijo informacijskih tokov (Svete v Kovač in drugi 2008, 44).

Omrežna varnost ima dve dimenziji:
- notranja varnost
- zunanja varnost

a) Notranja varnost

Notranja varnost se nanaša na zaščito neokrnjenosti podatkov in interni pretok informacij do posameznih korporacij oz. delov sistema. Ker so korporacije in druge družbene organizacije spremenile obliko organiziranosti iz hierarhične na fiksnih lokacijah v horizontalno na geografsko dislociranih območjih, je hiter in zanesljiv informacijski pretok postal bistvenega pomena za njihovo delovanje. Primer takšnega podjetja je v Sloveniji Telekom Slovenije, saj ima svoje poslovne enote geografsko dislocirane po celotni državi. Čeprav so številne korporacije oblikovale svoje lastne zasebne mreže (intranet), pa se pojavlja vse večji pritisk po povezovanju teh mrež. V varnostni namen so korporacije razvile številna orodja, med katerimi so najpomembnejši požarni zidovi, protivirusni programi, alarmni sistemi v realnem času ter različne oblike kodiranja in identificiranja s pametnimi karticami ter biometričnimi postopki, kot so: skeniranje prstnih odtisov, roženice, obraza, rok ali glasu (Svete v Kovač in drugi 2008: 45). Pogosta oblika varnih oblik povezovanja geografsko ločenih poslovnih enot so VPN (Virtual Privat Network) povezave. Prvi primer omrežne varnosti se torej nanaša na

zanesljivo delovanje informacijske infrastrukture. Gre za notranjo omrežno varnost organizacije, ki tovrstno tehnologijo in infrastrukturo uporablja.

b) Zunanja varnost

Druga dimenzija se nanaša na varovanje informacijskega toka med informacijskimi proizvajalci (ponudniki) in potrošniki (uporabniki). Danes je namreč vse več tako komercialnih kot javnih storitev, ki jih lahko uporabljamo v elektronski obliki, po drugi strani pa so določene klasične storitve dobile tudi svojo elektronsko obliko (npr. elektronsko bančništvo, zavarovalništvo, e-javna uprava in e-volitve). Konvergenca komercialnega pritiska in novih tehnologij je tako povzročila pravi vihar na internetu, zlasti pa so velika pričakovanja usmerjena v komercializacijo spleta. Seveda mora temu napredku slediti tudi varovanje toka med ponudniki storitev in uporabniki, kajti le na ta način je možno zagotoviti dovolj visoko stopnjo zanesljivosti. To dimenzijo omrežne varnosti lahko zato opredelimo kot omrežno varnost, usmerjeno v zunanje okolje omrežene organizacije (Kovač in drugi 2008). Zunanje okolje, torej uporabniki, v luči te teorije potrebujejo in nenazadnje tudi plačujejo uravnotežen in stabilen razvoj ter ravno takšno delovanje informacijskega toka, ki ga kot storitev prejemajo od ponudnika. Vsakršna prekinitev na tem toku (prekinitev na delovanju storitve omrežne organizacije) povzroči odziv s strani uporabnikov. Slednje gospodarska družba, kot je Telekom Slovenije, takoj opazi na takojšnjem povečanju obremenitve uporabniškega klicnega centra za prijavo napak na storitvah (Preradović 2010).

Upoštevajoč, da informacijska omrežja (še posebej internet) presegajo ozemeljske in birokratske omejitve ter zahtevajo mednarodno sodelovanje tako držav kot posameznikov in korporacij, ki narekujejo tehnološki razvoj, pa moramo kot pomembno okolje omrežij upoštevati tudi državne jurisdikcije. Grožnje omrežni varnosti vključujejo širok spekter aktivnosti, vključujoč programske napake, ki lahko vodijo do sesutja sistema, računalniške prevare in kraje, posameznike znotraj sistema, ki namerno onemogočajo delovanje sistemov, nedelovanje podpore fizične infrastrukture, aktivnosti hekerjev, industrijsko in drugo tako zasebno kot državno vohunjenje ter nenazadnje zlonamerni programi, kot so virusi, trojanski konji, črvi ipd. (Svete 2005, 105–108).

Omrežna varnost torej izpostavlja komunikacijski (prenos podatkov) in uporabniški vidik IKT kot referenčni objekt, na katerega se varnost nanaša, koncept informacijske varnosti pa za cilj

ogrožanja postavi v ospredje celotno IKT, vključujoč tudi njene zmogljivosti zbiranja in obdelave podatkov ter delovanja strojne opreme nasploh. Ogrožanje delovanja IKT je mogoče razdeliti v štiri skupine.

Tabela 4.1: Oblike ogrožanja informacijske varnosti

Višja sila	**Pomanjkljivosti strojne in programske opreme**	**Človeški dejavnik (nenamernost)**	**Človeški dejavnik (namernost)**
• Potres • Nevihte • Poplave • Strele • Požar • Visoka temperatura • Visoka vlažnost • Onesnaženost • Radarsko sevanje • Akustično sevanje • Elektromagnetsko sevanje v obe smeri • Nestabilnost napajanja z električno energijo • Izredne razmere • Vojno stanje	• Izpad sistema • Tehnične napake na osrednji enoti – strežniku • Tehnične napake na odjemalcih • Logične napake v strežnih programih • Logične napake v aplikativnih programih	• Slaba organizacija • Nedisciplina • Nemarnost • Nestrokovnost • Monotonost • Utrujenost	• Kraje • Prevare • Poneverbe • Falsificiranje • Izsiljevanje • Grožnje • Kršenje zasebnosti • Sabotaže • Sporočanje zaupnih podatkov • Vohunjenje • Pornografija • Propaganda • Vandalizem (crackerji) • Terorizem • Umori • Heking • Izdelava ter distribucija virusov • Piratstvo na področju programske opreme • Napadi DoS

Vir: Svete (2007, 108).

5 INFORMACIJSKA VARNOST V EVROPSKI UNIJI

Evropska unija je s širjenjem članstva, poglabljanjem sodelovanja med članicami in s sprejetjem nekaterih skupnih politik ter ustanovitvijo skupnih ustanov postala referenčni objekt pri obravnavi informacijske varnosti. Pomembnost sektorja IKT za evropsko gospodarstvo, gospodarstvo članic in za evropsko družbo v celoti je nedvomno velika. IKT predstavlja pomemben del inovacij in je zaslužen za skoraj 40 % rasti proizvodnje. Poleg tega je ta izjemno inovativen sektor zaslužen za več kot četrtino celotnih evropskih prizadevanj v zvezi z raziskavami in razvojem ter igra ključno vlogo pri ustvarjanju gospodarske rasti in delovnih mest v celotnem gospodarstvu. Vedno več Evropejcev živi v resnično informatizirani družbi, kjer se je uporaba IKT naglo povečala kot bistvena funkcija človeškega družbenega in gospodarskega vzajemnega delovanja.

Kršitev omrežne in informacijske varnosti ima lahko takšen vpliv, da presega gospodarske dimenzije. Obstaja splošna zaskrbljenost, da bodo varnostni problemi vodili k odvrnitvi uporabnikov in manjši uporabi IKT, saj so razpoložljivost, zanesljivost in varnost predpogoj za zagotavljanje kakovostnih storitev. Poleg tega zaradi večje povezljivosti med omrežji tudi druge ključne infrastrukture (kot so promet, energija itn.) postajajo vedno bolj odvisne od neoporečnosti njihovih zadevnih informacijskih sistemov. Zaradi vsesplošne razširjenosti IKT in informacijskih sistemov predstavlja varnost omrežij in informacij relevantno varnostno vprašanje za EU (COM 2006: 5-6, 251). Evropska unija tako daje priporočila k razumevanju informacijske varnosti na različnih nivojih. Javna uprava mora obravnavati varnost svojih sistemov ne samo zaradi zaščite informacij javnega sektorja, ampak tudi zato, da bi služila kot zgled dobre prakse za druge udeležence. Gospodarstvo in gospodarske družbe morajo obravnavati varnost bolj kot pridobitev in element konkurenčne prednosti in ne kot negativni strošek. Pomembno je, da programi seznanjanja, namenjeni osvetlitvi primerov ogrožanja varnosti, ne spodkopavajo zaupanja potrošnikov in uporabnikov z osredotočanjem na samo negativne vidike varnosti. Zato bi morala biti informacijska varnost, kadar je to mogoče, predstavljena kot prednost in priložnost in ne kot obveznost in strošek. Treba jo je obravnavati kot pridobitev pri gradnji splošnega zaupanja in zaupanja potrošnikov, kot konkurenčno prednost za podjetja, ki delajo z informacijskimi sistemi, in kot vprašanje kvalitete storitve ponudnikov storitev v javnem in zasebnem sektorju (COM 2006, 5-6, 251).

Omenjene načelne opredelitve glede informacijske varnosti Evropske unije je mogoče pogledati tudi v luči raziskovalnega vprašanja, saj se v njih kaže določen interes EU po nemoteni in varni gospodarski dejavnosti ter o varni in zanesljivi birokratski dejavnosti Evropske unije kot takšne. EU prepoznava grožnje informacijski varnosti in temu primerno tudi prilagaja ter na nek način gradi varnostno strukturo na evropski ravni. V nadaljevanju bom predstavil in povzel bistvene naloge ter pristojnosti organov in organizacij, ki s svojimi mehanizmi sooblikujejo in sodelujejo pri kreiranju informacijsko varnostne politike na ravni Evropske unije. Mehanizmi zagotavljanja informacijske varnosti in varovanja kritične informacijske infrastrukture so lahko fizični, tehnološko-tehnični in organizacijski. Evropska unija kot naddržavna asociacija se v svojih institucijah sektorsko loteva tega pomembnega varnostnega vprašanja. Tako se s področjem informacijske varnosti ukvarjajo Evropska komisija, Evropski parlament in posebne agencije.

5.1 Evropska komisija

Evropska komisija je za delovanje evropske integracije najpomembnejša ustanova in gonilna sila pri gradnji Evrope. Ima vlogo pobudnice, je edina, ki lahko pripravlja predloge zakonodajnih aktov, o katerih nato odločata Evropski parlament in Svet Evropske unije. Ima tudi izvršilno funkcijo – skrbi za izvajanje zakonodaje in v okviru tega sprejema podzakonske akte Unije, njene pristojnosti pa segajo tudi na oblikovanje skupnih politik in nadzorovanje evropskega proračuna. Še ena pomembna naloga Evropske komisije je zagotavljanje uresničevanja ustanovitvenih pogodb; kot varuh pogodb lahko pred evropskim sodiščem toži vse druge skupne ustanove ali državo članico oziroma njeno pravno osebo (pred sodiščem prve stopnje). Evropska komisija predstavlja EU navzven, saj se v imenu EU oziroma držav članic pogaja o širitvi Unije, trgovinskih in tarifnih sporazumih ipd., končne dogovore pa potrjuje Svet EU. Sestavlja jo 27 članov (predsednik in 26 komisarjev), ki jih predlagajo države članice in potrdi Evropski parlament. Komisarji ne zastopajo interesov matičnih držav, ampak morajo v prvi vrsti skrbeti za splošne koristi in razvoj Unije. Komisija je za svoje delo odgovorna Evropskemu parlamentu, ki ji lahko z dvotretjinsko večino izglasuje nezaupnico, to pa lahko privede do odstopa celotne komisije (Evropska komisija 2010).

Vidimo, da ima Evropska komisija po svoji funkciji z zakonodajno pobudo in predstavljanjem Evropske unije navzven pomembno vlogo pri oblikovanju politik, tudi varnostnih. Zaradi

dejstva, da je informacijska varnost globalni pojav in globalna skrb, ima Komisija pomembno mesto pri zunanjem zastopanju Unije. Komisija tako s svojimi resorji pokriva celotno delovanje EU, pri tem pa je skrb za informacijsko varnost bolj ali manj porazdeljena med različne resorje. Omenil bom nekatere najpomembnejše in za diplomsko delo relevantne resorje.

5.1.1 Komisar za informacijsko družbo in medije

Resor za informacijsko družbo in medije je pomemben faktor ustvarjanja in soustvarjanja politike širjenja ter implementacije informacijsko komunikacijske tehnologije. Nenehno spremlja stanje kazalcev informacijske družbe, vodi pa tudi politiko širjenja in dostopnosti IKT, saj jo smatra kot komponento, ki prispeva k kvaliteti evropskega državljanstva. Nenehno podpira razvoj, vlaganja in inovacije v IKT ter na njej temelječih servisih za državljane. Navzven zastopa Evropsko komisijo, ko gre za vprašanja, povezana z IKT in mediji, ter tako sodeluje v mednarodnih tokovih. V luči gospodarske perspektive pa resor podpira digitalno prihodnost EU, saj v njej vidi mnoge gospodarske priložnosti, predvsem pa ustvarjanje novih delovnih mest in povečevanju t.i. evropske zavesti (Enisa 2009, 245).

5.1.2 Komisar za raziskave in razvoj

Primarna naloga tega resorja je skrb za politiko raziskovanja in implementacije raziskovalnih dosežkov v gospodarstvu. Resor je do nedavnega vodil slovenski komisar Janez Potočnik. Zavzema se za raziskave v celoti in na vseh področij, od energetike pa vse do informacijske tehnologije, ter skrbi in koordinira skupne raziskovalne programe in projekte z državami članicami (Enisa 2009, 248–250). V kontekstu informacijske varnosti je to pomemben resor, saj je po smernicah Evropske unije IKT tisti dodaten faktor, ki omogoča razvoj in nastajanje novih delovnih mest, s čimer pa že prehajamo bolj na polje osebne, socialne in človekove varnosti. Iskanje varnostnih rešitev v omrežjih in v osebni uporabi IKT pa je stalna raziskovalno razvojna dejavnost novih tehnologij.

5.1.3 Opozorilno informacijsko omrežje

Da bi olajšali izmenjavo informacij o skupnih grožnjah in ranljivostih v EU, je Evropska komisija uvedla opozorilno informacijsko omrežje za kritično infrastrukturo (CIWIN). To omrežje EU je namenjeno pomoči državam članicam, institucijam EU ter lastnikom, operaterjem, da delijo informacije o grožnjah, ranljivostih in primernih ukrepih ter strategijah za zmanjšanje tveganja in o zaščiti kritične infrastrukture. Natančna definicija vozlov tega omrežja še ostaja odprto vprašanje in bo najverjetneje vključevalo avtoritete na različnih nivojih. Evropska komisija je predlagala naslednje tri možnosti za razvoj CIWIN v Green Paperu – CIWIN bi lahko oblikovala forum, ki bi bil namenjen izključno za izmenjavo idej o CIP in dobrih praksah kot podpora lastnikom in operaterjem CI. Druga možnost bi lahko bil hiter CIWIN-ov sistem opozarjanja (orig. Rapid Alert System – RAS), ki bi povezoval države članice. Kot tretje pa bi CIWIN lahko bil večnivojski komunikacijski alarmni sistem z dvema določenima funkcijama: sistem hitrega obveščanja, ki bi povezoval države članice z Evropsko komisijo, ter forum za izmenjavo idej in najboljših praks o varovanju kritične infrastrukture. Ne glede na to, katero možnost se bo izbralo, bo CIWIN dopolnjeval obstoječa omrežja, ne bo pa jih podvajal (Dunn in drugi 2008, 47).

5.2 Evropski parlament

Evropski parlament izvolijo državljani Evropske unije vsakih pet let (zadnje volitve v Evropski parlament so potekale leta 2009) na neposrednih in splošnih volitvah. Poslancev je danes 736 in delujejo v sedmih poslanskih skupinah, največji pa sta skupina Evropske ljudske stranke in skupina socialistov. Vsaka država ima določeno število poslancev (Nemčija 99, Luksemburg 6). Poslanci niso predstavniki države, v kateri so bili izvoljeni, ampak zastopajo svoje volivce in njihove interese ter politične interese evropskih političnih strank. Te so večnacionalne in delujejo v skladu s programom, sprejetim na evropski ravni. Evropski parlament zaseda dvanajstkrat letno v Strasbourgu, preostala zasedanja potekajo v Bruslju, seje odborov (17 stalnih odborov) pa so vedno v Bruslju. Plenarna zasedanja vodi predsednik Evropskega parlamenta, ki ga poslanci izvolijo z navadno večino. Evropski parlament je z dopolnili k ustanovitveni pogodbi v minulih desetletjih pridobival čedalje več pristojnosti, saj je z določili Maastrichtske in Amsterdamske pogodbe prerasel iz povsem svetovalne skupščine v pravi zakonodajni parlament, ki ima danes podobna pooblastila kot nacionalni

parlamenti. Ustaljeni zakonodajni postopek je soodločanje (uveden z Maastrichtsko pogodbo), ki postavlja Evropski parlament in Svet Evropske unije na isto raven, saj je besedilo potrjeno, ko ga potrdita oba, poslancem pa omogoča blokiranje sprejema evropske zakonodaje. Soodločanje je danes ena od najpomembnejših moči Evropskega parlamenta in se nanaša na sprejemanje zakonodaje na področjih svobodnega gibanja delavcev, ustvarjanje notranjega trga, raziskave in tehnološki razvoj, okolje, zaščito potrošnikov, izobraževanje, kulturo in zdravstvo. Evropski parlament ima odločilno vlogo tudi pri razporejanju sredstev v višini 7,5 milijard evrov, namenjenih raziskavam in razvoju. Trenutno se te namenjajo novim načinom zaščite nizko ležečih območij pred poplavami, novim raziskavam in razvoju na področju zdravja, varne prehrane, prometa, tehnologije, energije in okolja (Evropski parlamenti 2010). Zakonodajna moč in moč razdeljevanja sredstev dajeta Evropskemu parlamentu ključno vlogo pri ustvarjanju politik EU. Evropski parlament organizacijsko in resorno deluje s pomočjo odborov, zato bom v nadaljevanju omeni tiste, ki kakorkoli odločilno vplivajo na nastanek informacijsko varnostne politike.

5.2.1 Odbor za industrijo raziskave in energijo

Odbor se primarno ukvarja z načrtovanjem industrijskega in energetskega sektorja, sodeluje pa tudi pri oblikovanju razvojnih in varnostnih politik na področju energetike, informacijske tehnologije in evropskih omrežij. Pomembno ga je omeniti v luči informacijske varnosti, saj na nek način upravlja s področjem kritične informacijske infrastrukture (Enisa 2009, 250). Slednja ureditev priča o tem, da obstaja na ravni EU zavest o kritični infrastrukturi, med katero po teoriji poleg energetike, prometa in ostalega spada tudi informacijsko komunikacijska tehnologija.

5.2.2 Odbor za kulturo in izobraževanje

Odbor je potrebno omeniti v luči širšega koncepta informacijske varnosti, predvsem posameznika. Odbor je v svojih nalogah pristojen za oblikovanje izobraževalne politike tudi na področju avdiovizualnih komunikacij, informacijske in medijske politike ter ostalih zadev iz naslova informacijske družbe (Enisa 2009, 251). S tem na nek način pristopa k informacijski varnosti s preventivnega vidika, izobraževanja in osveščanja ljudi, podobni

koncept k pristopu informacijske varnosti pa bomo v nadaljevanju zasledili pri obravnavi gospodarske sfere in s soočanjem s človeškim faktorjem tveganja informacijske varnosti.

5.3 Evropska agencija za omrežno in informacijsko varnost (ENISA)

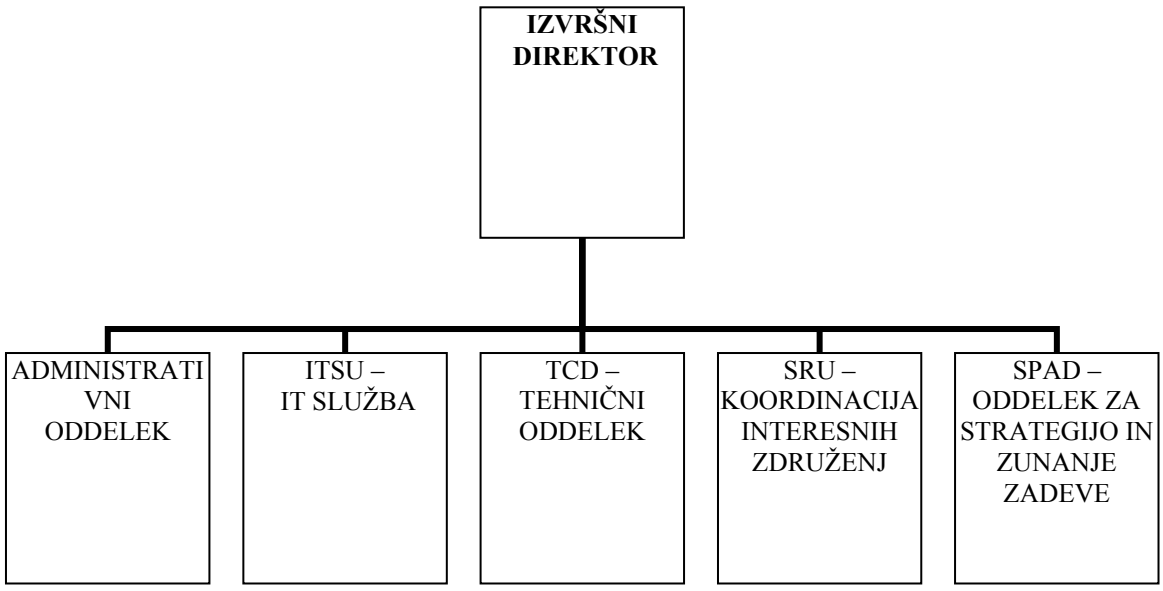
ENISA je bila ustanovljena marca leta 2004. Ko se je junija 2003 EU odločila za ustanovitev ENISE kot legalne entitete, je izboljšala pobude za evropsko koordinacijo informacijske varnosti. Cilj ENISE je zagotavljanje visoke stopnje omrežne in informacijske varnosti znotraj skupnosti. Tako pripomore k razvoju omrežne in informacijske varnosti v dobro državljanov, potrošnikov, podjetij in organizacij javnega sektorja EU, njena dejavnost pa prispeva tudi k nemotenem delovanju notranjega trga. Agencija pomaga Komisiji, državam članicam in posledično poslovni skupnosti, da vzdržujejo omrežno in informacijsko varnost, vključno s sedanjo in prihodnjo zakonodajo na tem področju. ENISA torej služi kot center ekspertnega znanja tako za države članice kot za institucije EU, ko iščejo nasvete, povezane z OIV. ENISINI delovni programi so razvili »seznam pomembnih oseb« z njihovimi kontaktnimi informacijami za področje omrežne in informacijske varnosti v državah članicah. Prav tako je izdala »Inventory of CERT Activities in Europe« in periodično izdaja novice s tega področja. Organizira delavnice za razširitev dobrih praks v državah članicah in med drugim tudi definira prilagodljive informacijske pakete, ki vključujejo dobre prakse za specifične konkretne skupine (na primer za SME in domače uporabnike). ENISA je ustvarila omrežno povezavo sodelavcev, ki vsak dan z državami članicami izmenjujejo informacije in sodelujejo (Informacijska družba 2010). ENISIN zadnji delovni program iz leta 2008 nosi naslov »Build on Synergies – Achieve Impact«, izdan novembra 2007. Osredotoča se na povečanje vpliva agencije pri omrežni in informacijski varnosti v sodelovanju z relevantnimi udeleženci. Delovni program je bil razvit kot nov pristop k določanju prioritet in bolj poglobljenemu sodelovanju z vsemi udeleženci, predstavi pa tudi tri nove ključne elemente pri definiciji t.i. »večletnih tematskih programov« (MTP – orig. Multiannual Thematic Programmes).

Trenutni MTP pokriva naslednje teme (Dunn in drugi 2008, 473):

- izboljšanje odpornosti v evropskih e-komunikacijskih omrežjih,
- razvijanje in ohranitev modelov sodelovanja in
- identifikacija novih tveganj, da bi gradili na zaupanju in samozavesti.

MTP ponuja tudi pregled ENISINIH aktivnosti, vključujoč seznanjanje in promocijo dobrih praks in nadgradnjo sodelovanja. ENISA se zaveda pomembnosti svoje vloge in podpira strategijo Evropske komisije. Z željo po maksimiranju vpliva svojih aktivnosti agencija stremi k spodbujanju obstoječih sinergij in pobud na državnem in evropskem nivoju ter bo tudi naprej sledila bolj osredotočenemu vplivno-orientiranemu pristopu (Dunn in drugi 2008, 473). Agencija tako nudi strokovno podporo Evropski komisiji in državam članicam in deluje kot vezni člen dobre prakse med EU in članicami. Je pomemben element pri konkretnem oblikovanju informacijske varnosti. Svojega predstavnika v ENISI ima tudi Slovenija, to je Gorazd Božič, vodja SI –Certa v Republiki Sloveniji, s katerim je bil za potrebe diplomskega dela opravljen tudi intervju. Božič vidi vlogo ENISE predvsem v naslednji perspektivi: kakor se razvija omrežje in z njim povezane storitve za državljane, do katerih le-ti dostopajo preko spleta, tako se spreminja tudi paleta groženj. Torej vsaka nova spletna storitev odpira prostor novi grožnji informacijski varnosti. Te moramo zato obravnavati glede na trenutno situacijo. Varnostne politike tako nekako sledijo novim pojavnim oblikam ogrožanja, še zdaleč pa niso celovite, saj jih nekatera področja celo sploh nimajo. Pomembno je, da se te politike oblikujejo na nivoju države in EU tako, da bodo predvidele splošne mehanizme za reševanje problemov, ko bo do teh prišlo. Leta 2004 ustanovljena evropska agencija ENISA bo tu zagotovo lahko pomagala z nekaterimi priporočili (Božič 2010).

Slika 5.1: Organiziranost Evropske agencije za omrežno in informacijsko varnost



Vir: prirejeno po ENISA (2010).

5.4 Raziskave na področju informacijske varnosti v EU

Informacijska varnost in varovanje kritične infrastrukture v luči novih groženj sta vsekakor pojma, ki sta relativno mlada in zato še dokaj neraziskana. Evropska unija na tej točki ponuja in vzpodbuja vrsto raziskav tega področja in kot že predhodno omenjeno ima v ta namen ustanovljeno parlamentarno telo in Evropskega komisarja. V nadaljevanju bom omenil dve vidnejši in pomembnejši raziskavi, ki ju je vsekakor mogoče umestiti v kontekst diplomskega dela.

Evropski varnostni raziskovalni program (ESRP – European Security Research Programme) ima za cilj evropskega raziskovanja varnosti, da se vzpostavi bolj varno okolje za državljane in poveča industrijska konkurenčnost. S sodelovanjem in uravnavanjem učinkov na evropski ravni lahko EU v konstantno spreminjajočem se svetu bolje razume grožnje ter se na njih hitreje odziva (Evropska komisija 2010).

Za projekte na področju raziskovanja varnosti so identificirali naslednje prioritetne misije:

• optimizacija varnosti in zaščite omrežnih sistemov,
• zaščita kritične infrastrukture proti terorizmu (tudi bio-terorizmu in dogodkom, povezanih z biološkimi, kemičnimi in drugimi snovmi),
• izboljšanje kriznega managementa (evakuacija, iskalne in reševalne operacije, kontrola in odprava škode),
• doseganje interoperabilnosti ter integracije informacijskih in komunikacijskih sistemov, izboljšanje znanja o dani situaciji (na primer, v kriznem managementu, antiterorističnih aktivnostih, mejni kontroli. Komisija EU je julija 2005 ustanovila tudi Svetovalni odbor za evropsko varnostno raziskovanje (ESRAB). ESRAB deluje v sklopu Komisije in je posvetovalni organ za vprašanja, povezana z vsebino in implementacijo evropskega varnostnega raziskovalnega programa. Izvaja svoje delo s polnim zavedanjem konteksta evropske politike, posebej v raziskovanju in razvoju aktivnosti na državnem nivoju ter podpori evropskih pobud raziskovalni politiki (Evropska komisija 2010). ESRAB je izdal končno poročilo septembra 2006 in nehal delovati decembra 2006. V tem poročilu priporoča ustanovitev Evropskega foruma za raziskovanje varnosti in inovacij (ESRIF – European Security Research and Innovation Forum), ki bi omogočal dialog in skupen pogled na evropske varnostne potrebe. Ustanovitev tega foruma so razglasili na drugi evropski

konferenci o raziskovanju varnosti marca 2007, forum pa je postal javni in zasebni dialog v raziskovanju varnosti že v septembru istega leta. Glavni cilj ESRIF je razvoj združene srednje in dolgoročne varnosti ter z njo povezanih tem, ki bi povezale ugotovitve raziskovanja varnosti z varnostno politiko in njeno implementacijo.

Na podlagi raziskovanja in zavedanja, da ima tako javno kot privatno partnerstvo pomembno vlogo pri zaščiti kritične infrastrukture, so cilji ESRIF-a naslednji:

• združitev relevantnih udeležencev, da bi olajšali razpravo o skupnih varnostnih vprašanjih,
• identifikacija predlogov za oblikovanje strateškega varnostnega raziskovanja in inovacij, vključujoč državne in evropske udeležence, da bi postavili skupen in jasen pogled na potrebe in prioritete evropskega raziskovanja varnosti,
• izražanje idej, pogledov in najboljših praks, da bi čim bolje izkoristili obstoječe možnosti in povečali uporabo tehnologije tudi v domenah, povezanih z varnostjo.

Najbolj pa se ESRIF posveča zaščiti kritičnih informacij. Konec leta 2009 naj bi predstavil Skupno raziskovalno agendo, s tem pa zaključil svoje delovanje (Dunn in drugi 2008, 474–477). Omenjenih zaključkov pa v okviru iskanja in analize virov nisem zasledil.

Na tej točki se mi zdi pomembno povzeti in poudariti zavedanje in predpostavko raziskave, da je za varovanje kritične informacijske infrastrukture in posledično zagotavljanje informacijske varnosti odgovoren tako javni kakor zasebni sektor. To na nek način pojasnjuje v začetku omenjeno in predpostavljeno dejstvo, da je zasebni gospodarski sektor velik lastnik in uporabnik informacijsko komunikacijske tehnologije ter kritične infrastrukture.

Koordinacija raziskovanja kritične informacijske infrastrukture (CIIRCO), je prav tako pomembna in relevantna raziskovalna smer na ravni Evropske unije. EU je sestavila opravilno skupino, da bi raziskala ukrepe, ki so bili sprejeti v 25 državah članicah, z namenom borbe proti (kibernetskim) grožnjam kritični infrastrukturi. Kot del projekta CIIRCO (Critical Information Infrastructure Research Coordination), razglašenega aprila leta 2005, namerava opravilna skupina sestaviti raziskovalne skupine in programe, ki se osredotočajo na informacijsko tehnološko varnost v kritičnih infrastrukturah, kot so telekomunikacijska omrežja in električno omrežje. Obseg sodelovanja je širši kot v EU, saj obstaja težnja po

vključitvi ZDA, Kanade, Avstralije in Rusije. Projekt CIIRCO je bil koordinacijska akcija, soustanovljena z IST FP6.

Glavni cilji CIIRCO projekta so:

• vzpodbujanje koordiniranega pristopa po vsej EU za raziskovanje in razvoj CIIP,
• ustanovitev evropskega raziskovalnega področja o kritični infrastrukturi (ERA – orig. European Research
Area) kot del večjega strateškega cilja IST FP6, torej integriranja in povečanja ERA v smislu zanesljivosti in varnosti,
• osredotočanje na aktivnosti in akcije v vseh 25 državah članicah in državah kandidatkah za vstop. Na spletni strani CIIRCO med drugim najdemo tudi evropske novice in prihajajoče dogodke na tem področju (Infosek News 2005).

Pomembnost in relevantnost te raziskovalne pobude je v tem, da nakazuje težnjo EU po poznavanju pristopov držav članic na področju informacijske varnosti in zaščiti kritične informacijske infrastrukture. Kaže pa tudi na ustrezno razumevanje informacijske varnosti kot globalnega vprašanja, saj sodobna omrežja presegajo geografske in nacionalno jurisdikcijske meje, temu primerno pa sledijo tudi grožnje. EU se na to odziva s proučevanjem problematike tudi s širšim globalnim sodelovanjem.

6 INFORMACIJSKA VARNOST V REPUBLIKI SLOVENIJI

Razmerje med informacijsko komunikacijsko tehnologijo in med državo, predvsem v luči varnostnega vprašanja, smo nekoliko že osvetljevali, kljub temu pa je na tem mestu potrebno osvetliti še nekoliko dodatnih aspektov, da bi lahko tematiko v celoti doumeli. Pogled v zgodovino države nam pokaže, da se je informacijsko komunikacijska tehnologija v državni sferi pojavila že relativno zgodaj. Predvsem se je pojavljala kot tehnološka podpora državno upravnim procesom državne uprave (policijske kartoteke, podatki varnostno obveščevalnih služb itn.). O razmahu IKT v državni upravi lahko govorimo v 90. letih prejšnjega stoletja, k čemur sta bistveno prispevala poenostavljena oblika operacijskih sistemov (Windows) in pisarniškega orodja Microsofta (Office). Pred to poenostavitvijo računalniškega okolja je bila uporaba tovrstne tehnologije pretežno v domeni strokovnjakov za področje informatike. Razumemo pa lahko, da se je togi birokratski aparat države, nevajen velikih posegov v

ustaljen delovni proces, novim tehnologijam dokaj močno upiral. O t.i. e-državi pa lahko začnemo govoriti tedaj, ko birokratski aparat sprejme IKT v svojih delovnih procesih ter jo začne dojemati in uporabljati v smislu poenostavitve svoje dejavnosti (Svete 2008, 49–50).

IKT tako v mnogih pogledih vpliva na pomembno razmerje država – državljan, saj močno poenostavi servisno funkcijo države, ki naj bi jo le-ta nudila državljanu. Sodobna e-država je prisotna že v mnogih sferah in družbenih podsistemih. Kot primer lahko navedemo elemente e-države v šolstvu z raznimi oblikami spletnih referatov, spletnih redovalnic, spletnega učenja in študija na daljavo. Poti za uporabo IKT pa država išče tudi v svojih zunanjepolitičnih dejavnostih. Očitna je tudi širitev države v sfero kibernetskega prostora na področju varnosti. Tukaj lahko omenimo uporabo IKT v raznih oblikah kibernetskega vojskovanja in vohunjenja med državami v namene zunanje varnosti in nacionalnih interesov. V kontekstu razmerja med svobodo in varnostjo, ki je še posebej stopilo v ospredje po terorističnem aktu nad ZDA 11. septembra 2001, pa lahko omenimo stalna prizadevanja po nadzoru dejavnosti svojih državljanov na spletu. S tem poskušajo države omejevati svobodo in demokracijo na spletu z namenom odkrivanja in preprečevanja raznih kaznivih dejanj (Svete 2008, 53). V Sloveniji je bil v tovrstno debato vključen nov zakon o igrah na srečo, ki postavlja omejitve glede spletnega igralništva v tujini in odpira vprašanje o demokratičnosti interneta (Božič 2010).

Svoboda je temeljna predpostavka sodobni državi in o tej dimenziji državnosti je bilo in še bo v prihodnosti veliko govora. Ko govorimo o demokratičnosti, je potrebno v tem kontekstu analizirati tudi spletni prostor in koliko demokracije le-ta dopušča (Svete 2008, 59). O internetu kot eni osrednjih pridobitev informacijske dobe avtorji govorijo kot o tehnologiji, ki osvobaja, ogroža in daje možnost neštetim oblikam nadzora. Nedvomno pa dopušča številne nove poti vplivanja na vladajoče strukture, česar se je poslužila predvsem civilna družba in tako ponovno aktualizirala idejo o neposredni demokraciji, ki vodi v elektronsko demokracijo. Razvija se tudi model participativne demokracije, v kateri po definiciji obstoječe politične predstavniške institucije ostanejo, IKT pa odpre in omogoči mnoge kanale soudeležbe državljanov pri vladanju (Svete 2008, 60).

V Sloveniji poznamo kot dokaj nov in relativno prodoren element omenjene participativne demokracije spletni portal *predlagaj.vladi.si*, ki je v domeni Urada vlade Republike Slovenije za komuniciranje. Spletno orodje deluje na podlagi soudeležbe državljanov pri konstruktivnem oblikovanju vladnih ukrepov. Spletno orodje *predlagam.vladi.si* ureja Urad

vlade za komuniciranje . Ob tem gre poudariti, da večino vsebinskega dela opravijo državni uradniki in funkcionarji po ministrstvih in vladnih službah, ki na predloge pripravljajo ustrezne odgovore in presojajo smiselnost njihove izvedbe.

Moderatorji spletnega orodja pa skrbijo za naslednja področja:

- objavljajo nove predloge:
    - skrbijo za skladnost predlogov s pravili in njihovo primernost; ob morebitni neskladnosti moderator sporoči predlagatelju, zakaj je njegov predlog neprimeren in mu pomaga oblikovati ustreznejšega,
    - kategorizirajo predloge in vpišejo ključne besede,
    - obvestijo pristojni organ, da se na *predlagam.vladi.si* začenja razprava o predlogu, ki spada v njegov resor, in ga prosijo, da se dejavno vključi vanjo,
- skrbijo, da so vsi objavljeni komentarji v skladu s pravili *predlagam.vladi.si*:
    - neprimerne komentarje skrijejo in na njihovem mestu objavijo razlog, zakaj so jih skrili,
- predloge, ki so pri glasovanju dobili zadostno podporo, pošljejo pristojnemu organu,
- objavljajo odzive pristojnih organov,
- vodijo statistiko dejavnosti ter pripravljajo mesečna poročila o njih (Urad vlade za komuniciranje 2010).

Na podlagi navedenega praktičnega primera v Republiki Sloveniji vidimo, da se je relevantnost navedenih teoretskih razmislekov o vlogi IKT in implikacijah, ki jih ima njena razširjena raba za moderno državo, potrdila. Vsekakor pa relevantnost in dejstvo uporabe IKT v državni sferi pred državo postavlja nov varnosti izziv. Zakaj je temu tako in na kakšne načine se država loteva informacijske varnosti, pa bom podrobneje predstavil v nadaljevanju.

6.1 Varnostni pomen IKT za sodobno državo

Razširjena uporaba IKT ima v luči varnostne razprave številne implikacije in predvsem zloraba tovrstne tehnologije lahko povzroči dejanja, s katerimi je prizadet varnostni interes posameznika, družbenih skupin ali države. Najkonkretnejše vprašanje je zaščita kritične informacijske infrastrukture, saj lahko poškodovanje ali onesposabljanje le-te privede do večje krize. Informacijska moč je na tej točki izpostavljena kot pomemben steber družbene moči. IKT je povzročila drugačno predstavo o prostoru in času ter v luči razumevanja

sodobnega varnostnega fenomena prispevala k premiku od državocentričnega pristopa (Svete 2008, 109–110).

IKT ima za družbo in državo tudi funkcijo vzajemnega nadzorovanja in decentralizacije. Avtorji so mnenja, da naj bi s pomočjo razširjene uporabe IKT bili bolj prizadeti interesi države kakor posameznika, primer te domneve je vojaško posredovanje v Iraku. V primeru spornega in nasilnega ravnanja z iraškimi zaporniki so slike in posnetki, narejeni s pomočjo digitalnih fotoaparatov in mobilne tehnologije, kmalu obkrožili svet s pomočjo interneta. Grozljive podobe mučenja so zamajale legitimnost vojaškega posredovanja v Iraku, vladajoči ameriški administraciji pa povzročile padec podpore doma (Svete 2008, 111). Slednji primer jasno kaže, da je sodobna IKT doprinesla tako k decentralizaciji kakor k vzajemnemu nadzoru na relaciji državljan – država. Naftna kriza v 70. letih prejšnjega stoletja je pokazala, da nacionalne države ne ogrožajo zgolj vojaške grožnje na nacionalni ravni, temveč se pojavlja vse več kritičnih sistemov družbene infrastrukture, ki so postali legitimna tarča asimetričnega ogrožanja varnosti. Asimetrija se najbolj kaže na primeru terorizma, ko si le-ta za svoje cilje izbira najšibkejše dele družbenih sistemov in z napadi na njih povzroči veliko gospodarsko škodo, mnogo civilnih žrtev in veliko medijsko pozornost (Svete 2008, 113).

V informacijskih družbah prihaja do pojava t.i. privatizacije varnosti, pri čemer je bistveno, da se tako tarča kot akterji varnosti vse bolj prenašajo v nedržavne sfere, kot so podjetja in posamezniki. Skladno s tem je očitno, da morajo slednji za svojo varnost vse bolj skrbeti sami. Vojaška organizacija tako vse bolj izgublja na svoji moči, raste pa pomen obveščevalnih in varnostnih služb, saj se lahko le-te na preventivni ravni veliko bolje soočijo s preprečevanjem asimetričnih napadov (Svete 2008, 112).

6.2 Mehanizmi informacijske varnosti v Republiki Sloveniji

Glavni nosilec razvoja IKT in glavni subjekt, ki razpolaga z večino kritične informacijske infrastrukture, je gospodarstvo, kljub temu pa je vprašanje informacijske varnosti tolikšnega pomena, da se ga na različne načine loteva tudi država. Raznolikost in obširnost pojma kritične infrastrukture pa pomeni, da skrb za kritično infrastrukturo spada v domeno različnih državnih in nedržavnih institucij.

K varovanju kritične informacijske infrastrukture in zagotavljanju informacijske varnosti lahko pristopimo z več vidikov (Dunn 2004, 21):

- tehnični: zagotavlja se na tehnični ravni s poudarkom na omrežni varnosti. V tem pogledu se z grožnjami soočimo s tehničnimi sredstvi, kot so požarne pregrade, protivirusna programska oprema, avtentikacijski mehanizmi in ustanovitev CERT in CSIRT skupin. Požarne pregrade oziroma »firewalls« si lahko razlagamo kot varnostnika na vratih, kjer ta prepušča le koristen podatkovni promet. Funkcija požarne pregrade je zavračanje in sprejemanje določenega podatkovnega prometa, naloge CERT in CSIRT pa preventivno delovanje.

- na ravni podjetja: informacijsko varnost se tukaj razume predvsem kot zagotavljanje stalnega delovanja. To pomeni stalen dostop do informacijske infrastrukture in stalno delovanje poslovnih procesov, da bi se doseglo zadovoljivo poslovno delovanje. Sredstva za dosego teh ciljev poleg organizacijskih in človeških dejavnikov vključujejo tudi tiste, ki so bili našteti pri tehničnem vidiku. Podrobneje bom o pomenu informacijske varnosti v gospodarstvu spregovoril v naslednjem poglavju.

- vidik organov pregona: organi pregona vidijo varovanje kritične informacijske infrastrukture predvsem v preganjanju kibernetskega kriminala, kar pokrije zelo širok razpon kaznivih dejanj. Vključuje kršitve avtorskih pravic, računalniške prevare, otroško pornografijo in kršitve mrežne varnosti. Proti takšni obliki kriminala se bori na klasičen način, še posebej s sprejemanjem nove zakonodaje in spodbujanjem mednarodnega sodelovanja.

- nacionalno-varnostni: celotna družba je videna kot ogrožena, deluje se na več ravneh (tehnični, zakonodajni, organizacijski ali mednarodni). Akterji vključujejo državne uslužbence različnih organov ter predstavnike zasebnega sektorja in javnosti. Glede na spremenjeno varnostno okolje po 11. septembru 2001 se predlaga vzpostavitev državnih organov, ki se ukvarjajo s problematiko informacijske varnosti, kot so to naredili v več državah (Kanada, Nova Zelandija, Nemčija, Velika Britanija in ZDA) (Dunn 2005, 21). To so tudi vse države, ki so ustanovile specializirane organe bodisi za varovanje kritične infrastrukture bodisi za informacijsko varovanje. Druge države

> urejajo to področje tako, da naloge zagotavljanja varnosti vključijo v sklop delovnih nalog že obstoječih ministrstev. Razlog, ki govori v prid vzpostavitvi centralnega organa, je tudi, da je kritična infrastruktura razdeljena med zelo različne akterje, podjetja iz različnih sektorjev in državne institucije. Komunikacija med temi akterji bi bila olajšana, hkrati pa bi ta državna institucija delovala kot povezovalni element (Simčič 200, 21).

Podoben pristop k informacijski varnosti na državni ravni je ubrala tudi Slovenija. V »informacijsko varnostnem sistemu« tako poznamo elemente preventivnega delovanja in zgodnjega opozarjanja. Pristojnosti na državni ravni so razpršene po nekaterih že obstoječih organih in resorjih.

6.3 SI-CERT v Sloveniji

SI-CERT (Slovenian Computer Emergency Response Team) je center za posredovanje pri internetnih incidentih, koordinira obveščanje in reševanje varnostnih problemov v računalniških omrežjih v Sloveniji. SI-CERT obravnava varnostne incidente ali obvestila o zlorabah, okužbah in vdorih v računalniške sisteme. Predstavlja kontaktno točko, ki opravlja posredniško in svetovalno vlogo, v primeru suma informacijske nevarnosti se ga o tem obvešča. SI-CERT deluje v okviru Arnesa (Akademske in raziskovalne mreže Slovenije), vendar pa (kot nakazuje samo ime) sprejema prijave varnostnih incidentov za vsa računalniška omrežja v Sloveniji. Prvi CERT je bil ustanovljen leta 1988 v ZDA kot odgovor na prvi večji internetni incident – širjenje prvega črva, pozneje imenovanega kar "The Internet Worm". CERT je bil ustanovljen s strani ARPA (sedaj DARPA, Defense Advanced Research Projects Agency, US Department of Defense), nato pa je prešel v upravljanje univerze. S širitvijo interneta po svetu so se začele podobne organizacije in servisi postopoma pojavljati tudi izven ZDA, prvotni CERT pa se je preimenoval v CERT Coordination Center (SI Cert 2010).

Vodja SI-CERTA v Sloveniji je v intervjuju izpostavil pomembno koordinacijsko in tudi mednarodno vlogo ustanove pri zagotavljanju informacijske varnosti. Arnesov varnostni center SI-CERT že 15 let sprejema prijave in pomaga pri koordinaciji ter razreševanju varnostnih incidentov za vsa slovenska omrežja. Pomemben je kot znana kontaktna točka, ki

je povezana z drugimi centri v tujini in vsemi relevantnimi ustanovami doma (Božič 2010). Informacijska varnost je lahko tudi komercialna dejavnost. V Sloveniji obstajajo podjetja, ki se komercialno ukvarjajo s tem. SI-CERT načrtuje v bodoče večji poudarek na preventivni dejavnosti, predvsem preko bolj pogostih obvestil o varnostnih luknjah, navodilih za zaščito in vzpostavitvi baze znanja s področja omrežne varnosti, ki bo dostopna javnosti (Božič 2010). Osrednje mesto SI-CERTU na področju informacijske varnosti mu priznava tudi evropska agencija ENISA.

SI-CERT na svojih spletnih straneh posebej izpostavlja najbolj pogoste oblike *ogrožanja* varnosti na spletu. Pri tem tudi ta organ izhaja iz že omenjene teoretske predpostavke, da nam uporaba omrežja sicer olajša komunikacijo in zabriše zemljepisne omejitve, vendar smo ravno zaradi tega na omrežju tudi bolj izpostavljeni različnim grožnjam. Z izkoriščanjem varnostnih lukenj, ranljivosti v programski opremi ali v naših vedenjskih vzorcih lahko tujci pridobijo nadzor nad našo opremo, podatki in denarjem.

Phishing

S tem imenom poimenujemo krajo podatkov, ki storilcu omogočijo dostop do spletnih storitev v našem imenu in v skrajnem primeru tudi krajo našega denarja. V običajnem scenariju nas skuša storilec z elektronskim sporočilom zvabiti na lažno stran banke ali spletne storitve, običajno pod pretvezo, da se moramo zaradi preverjanja podatkov ali dodatnih ugodnosti prijaviti in "preveriti podatke". Če na tej lažni, "phishing" strani vpišemo geslo za dostop, se le-to posreduje storilcu.

Kraja identitete

Opravljanje storitev preko računalnika ali telefona je udobno, a ima tudi svoje slabosti. Stare postopke osebne identifikacije v živo z osebnim dokumentom so zamenjala uporabniška imena, gesla in digitalna potrdila (certifikati). Na ta način lastno identiteto dopolnjujemo z omrežnimi komponentami. Preko vdora v računalnik, okužbe s *trojanskim konjem* ali z lastno nepazljivostjo nam lahko tujci te identifikatorje ukradejo. Dostop do gesel in certifikatov omogoči goljufom, da zavedejo naše sodelavce ali prijatelje, okrnijo naš ugled ali pridobijo dostop do zaupnih informacij ali celo denarja na našem bančnem računu.

Spletne goljufije

Goljufi preko lažnih oglasov za prodajo, ponudb za nakup in s potvorjenimi sporočili poskušajo do uporabnikovega denarja.

Vdor

Vdor v računalniški sistem je najbolj klasična oblika hekerskega napada, ki se v različnih oblikah pojavi že v 60. in 70. letih prejšnjega stoletja. Pomeni nepooblaščen dostop do sistema (ali omrežne opreme), v običajnem poteku pa napadalec pred vdorom izvaja pregledovanje (skeniranje) omrežja. S posebnimi programi lahko namreč preveri, na katerih komunikacijskih vratih (portih) se javljajo priključene naprave.

Okužbe

Med najbolj razširjene varnostne probleme spadajo okužbe z računalniškimi virusi in trojanskimi konji. Najprej so jih uporabljali za dokazovanje nepredvidenih poti do računalnika (in so včasih lahko bili tudi destruktivni), danes pa se je razvoj zlonamerne opreme razvil v pravo industrijo. Podtaknjena zlonamerna koda (angl. *malware*) služi predvsem kraji identitete in podatkov ter omrežnim napadom.

Spam

Spam lahko v osnovi definiramo kot nenaročeno oglaševanje po elektronski pošti (Božič 2010). Na splošno lahko za "spam" sporočilo smatramo vsako sporočilo, ki je poslano večjemu številu naslovnikov z namenom vsiljevanja vsebine, ki se je naslovniki sami ne bi odločili prejemati. V veliki večini primerov gre za oglaševanje plačljivih storitev ali izdelkov. Ponavadi se s "spam" pošto oglašujejo izdelki ali storitve dvomljive kvalitete, velikokrat pa gre za goljufije. Angleška beseda "spam" se originalno nanaša na konzervirano obdelano šunko, ki je ni potrebno hraniti v hladilnikih. Za prvo masovno komercialno "spam" sporočilo velja oglas za odvetniško firmo Canter&Siegel, poslan v USENET konferenčni sistem leta 1994. Zaradi razširjenosti in neustrezne slovenske besede, ki bi povzela primeren kontekst za neželeno oglaševanje po elektronski pošti, prevzemamo kar pojem iz angleščine. (SI CERT 2010).

SI-CERT se pri svojem delu na področju informacijske varnosti upira na določeno zakonodajo. Vidike omrežne in informacijske varnosti obravnavajo različni zakoni. *Kazenski zakonik* opredeljuje kazniva dejanja (kot je recimo vdor v informacijski sistem), *Zakon o*

elektronskih komunikacijah definira dolžnosti in nadzor nad delom operaterjev, medtem ko *Zakon o elektronskem poslovanju na trgu* širše opredeljuje delovanje vseh ponudnikov storitev. *Zakon o elektronskem poslovanju in elektronskem podpisu* opredeljuje, kdaj so elektronsko podpisani dokumenti enakovredni ročno podpisanim pogodbam in vlogam overiteljev (Božič 2010).

6.4 Državni organi

ENISA je kot povezovalna agencija na ravni Evropske unije za področje omrežne in informacijske varnosti v svojih dokumentih povzela in opredelila pomen vseh državnih, gospodarskih in raziskovalnih ustanov, ki so kakorkoli pomembne za področje informacijske varnosti.

Državni organi na področju informacijske varnosti:

- Agencija za pošto in telekomunikacije Republike Slovenije
- Ministrstvo za javno upravo; Direktorat za e-upravo
- Overitelj digitalnih potrdil (SIGEN-CA, SIGOV-CA)
- SI-CERT
- Ministrstvo za visoko šolstvo, znanost in tehnologijo; Direktorat za informacijsko družbo in Inšpektorat RS za elektronske komunikacije, elektronsko podpisovanje in pošto
- Urad vlade RS za varovanje tajnih podatkov
- Informacijski pooblaščenec (Enisa 2009, 185).

Gospodarske organizacije na področju informacijske varnosti:

- Obrtno gospodarska zbornica; Združenje informatikov in telekomunikacij
- Združenje slovenskih ponudnikov interneta – SISPA (Enisa 2009, 185).

Akademske in raziskovalne ustanove na področju informacijske varnosti:

- Fakulteta za elektrotehniko; Laboratorij za telekomunikacije
- Fakulteta za družbene vede – FDV
- ARNES
- Fakulteta za računalništvo in informatiko

- Fakulteta za varnostne vede, Univerza v Mariboru
- Inštitut Jože Štefan, Ljubljana (Enisa 2009, 185).

S tovrstno klasifikacijo organov, organizacij in združenj na področju Republike Slovenije ENISA razkriva in zasleduje že omenjen pristop k področju informacijske varnosti na ravni Evropske unije. Slednja namreč zasleduje tripartitni pristop k temu področju in na eni strani za pomembno partnerico smatra državo, na drugi pa gospodarsko in raziskovalno sfero. Zaradi vseh kvalitativnih in kvantitativnih lastnostih informacijsko komunikacijske tehnologije je tripartitni pristop ali »trojno partnerstvo« na področju zagotavljanja informacijske varnosti najbolj racionalna odločitev in pristop, ki ga lahko varnostni akterji izberejo. V nadaljevanju bom izpostavil in predstavil nekatere izmed ključnih državnih organov, njihovo vlogo in pristojnosti. SI-CERT bom na tem mestu izpustil, saj je zaradi svoje osrednje vloge v sistemu že bil obravnavan.

Po organizacijskih spremembah leta 2004 so se naloge na področju informacijske varnosti porazdelile na Ministrstvo za javno upravo RS in na Ministrstvo za visoko šolstvo, znanost in tehnologijo RS. Znotraj teh ministrstev so nastali direktorati, ki posamezno področje specifično urejajo.

Na Ministrstvu za javno upravo RS je nastal Direktorat za e-upravo in upravne procese. Njegove naloge so (MJU 2010) :

• strateške
- prenova procesov in pospešen razvoj e-uprave s ciljem približevanja storitev državljanom in gospodarstvu,
• implementacijske
- zagotavljanje povezljivosti registrov in integracija podatkovnih virov z informacijsko podporo procesom,
• operativne
- izboljševanje elektronske podpore odnosom med subjekti v javni upravi in izven nje z uporabo sodobne informacijske in komunikacijske tehnologije,
- izvajanje javnih naročil s področja informacijske infrastrukture,

- posvetovalne

- spremljanje svetovnega razvoja informacijske infrastrukture in priprava usmeritev ter standardov s svojega področja dela,
- sodelovanje na področju odprave administrativnih ovir.

• druge naloge, ki niso vezane na področje informatike:
- skrb za izvajanje predpisov, ki urejajo splošni upravni postopek, upravno poslovanje ter dostop do informacij javnega značaja,
- opravljanje upravnega nadzora,
- sodelovanje z nevladnimi organizacijami.

Ministrstvo za visoko šolstvo, znanost in tehnologijo RS pa je ustanovilo Direktorat za informacijsko družbo. Njegove naloge so (MVZT 2010):

• strateške
- skrb za pospešen, usklajen in učinkovit razvoj informacijske družbe, ki temelji na znanju in vseživljenjskem izobraževanju,
• posvetovalne
- direktorat pri svojem delu sodeluje z različnimi organizacijami tudi na področju zakonodaje, varnosti in zasebnosti v elektronskem svetu, izobraževanju,
• operativne
- spremljanje indikatorjev razvoja informacijske družbe,
- izvedba znanstvenih in strokovnih srečanj,
• implementacijske
- spodbujanje razvoja in lokalizacije programske opreme, temelječe na odprti kodi,
- izvedba projektov za zmanjševanje digitalnega razkoraka.

Inšpektorat RS za elektronske komunikacije, elektronsko podpisovanje in pošto
Gre za neodvisno delujoč organ v sestavi Ministrstva za visoko šolstvo, znanost in tehnologijo, ki opravlja neposreden nadzor nad izvrševanjem zakonov in podzakonskih predpisov s področja elektronskih komunikacij in pošte, pri tem pa se njegove pristojnosti na področju elektronskih komunikacij in pošte dopolnjujejo s pristojnostmi, ki jih imajo glede nadzora na obeh področjih pooblaščene osebe Agencije za pošto in elektronske komunikacije

RS (APEK). Inšpektorat opravlja tudi naloge inšpekcijskega nadzora v skladu z zakonom, ki ureja elektronsko poslovanje in elektronski podpis (MVZT 2010).

Urad vlade Republike Slovenije za varovanje tajnih podatkov (UVTP 2010).
Pomembno se mi zdi izpostaviti omenjen urad, saj na nek način ureja področje varovanja ključnega elementa v pojmu informacijske varnosti, informacije. Pri tem se kaže interes države po zaščiti tajnih podatkov in posledično po zaščiti nekaterih nacionalnih interesov države.

UVTP je pristojen za opravljanje sledečih nalog:

- Spremlja stanje na področju določanja in varovanja tajnih podatkov in skrbi za razvoj in izvajanje fizičnih, organizacijskih in tehničnih standardov varovanja tajnih podatkov v državnih organih, organih lokalnih skupnosti, pri nosilcih javnih pooblastil ter v gospodarskih družbah in organizacijah, ki pridobijo ali razpolagajo s tajnimi podatki.

- Skrbi za izvrševanje sprejetih mednarodnih obveznosti in mednarodnih pogodb o varovanju tajnih podatkov ter na tem področju sodeluje z ustreznimi organi tujih držav in mednarodnih organizacij. Skrbi za zagotavljanje varnosti tajnih podatkov v nacionalnih organih in v tujini ter v zvezi s tem opravlja zlasti naslednje naloge:

- izdaja dovoljenja za dostop do tajnih podatkov,
- izdaja varnostna potrdila pravnim osebam,
- izdaja varnostna potrdila za sisteme in naprave za prenos, hranjenje in obdelavo tajnih podatkov,
- potrjuje izpolnjevanje predpisanih pogojev za obravnavanje tajnih podatkov s strani posameznega organa tujim državam in organizacijam,
- predlaga varnostno preverjanje za izdajo dovoljenja za dostop do tajnih podatkov,
- izdaja navodila za ravnanje s tajnimi podatki tuje države oziroma mednarodne organizacije,
- nadzoruje izvajanje fizičnih, organizacijskih in tehničnih ukrepov za varovanje tajnih podatkov tuje države oziroma mednarodne organizacije in skladno z ugotovitvami nadzora izdaja obvezna navodila za odpravo ugotovljenih pomanjkljivosti, ki so jih organi dolžni

nemudoma izvršiti, ter izmenjuje podatke z nacionalnimi varnostnimi organi in mednarodnimi organizacijami.

- Pripravlja predloge predpisov, potrebnih za izvajanje ZTP-ja.

- Daje mnenje o skladnosti splošnih aktov o določanju, varovanju in dostopu do tajnih podatkov ZTP-ja.

- Koordinira delovanje državnih organov, pristojnih za varnostno preverjanje.

- Predlaga ukrepe za izboljšanje varovanja tajnih podatkov.

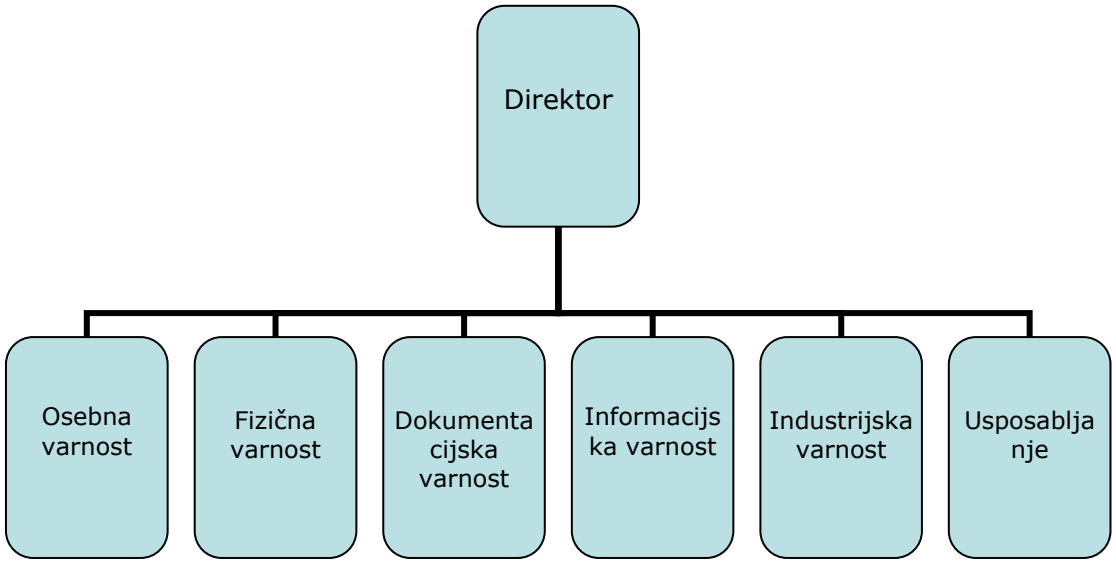
- Vodi evidenco:

- dovoljenj za dostop do tajnih podatkov,
- dovoljenj fizičnim osebam za dostop do tujih tajnih podatkov,
- izdanih varnostnih dovoljenj organizacijam,
- izdanih varnostnih dovoljenj organizacijam za dostop do tujih tajnih podatkov,
- začasnih dostopov do tajnih podatkov.

- Organizira in izvaja usposabljanja s področja varovanja tajnih podatkov.

- Opravlja druge naloge, ki so določene s predpisi, sprejetimi na podlagi ZTP-ja (Zakona o tajnih podatkih).

Slika 6.1: Organizacijska struktura Urada vlade Republike Slovenije za varovanje tajnih podatkov.



Vir: prirejeno po UVTP (2010).

7 INFORMACJSKA VARNOST V GOSPODARSTVU

Gospodarska sfera je v luči informacijske varnosti celotne države velikega pomena. Na podlagi dejstva, da je ravno gospodarska sfera tista, ki je nosilec razvoja in eden večjih uporabnikov informacijsko komunikacijske tehnologije, je jasno, da bo igralo pomembno vlogo pri zaščiti kritične informacijske infrastrukture in informacijske varnosti nasploh. Na gospodarstvo in še podrobneje na gospodarsko družbo je potrebno gledati kot na subjekt informacijske varnosti. To pa lahko navežemo na koncept omrežne in informacijske varnosti, ki na nek način najbolj celovito pojasni razumevanje informacijske varnosti na ravni gospodarske družbe. Takšna družba, delujoča na svobodnem trgu proste konkurence, ima dva interesa; zagotoviti lastno notranjo informacijsko varnost in varnost informacijskega toka, ki povezuje ponudnike ter povpraševalce na trgu storitev. Nekaterim gospodarskim družbam, ki so po svoji naravi delovanja pomembne za delovanje države in državnih podsistemov v kriznih razmerah, zakonodaja iz civilne obrambe nalaga osnovne obveznosti. V tej luči je na primer v Republiki Sloveniji pomemben nacionalni telekomunikacijski operater Telekom

Slovenije, ki mora po obrambnem načrtu zagotoviti 90-dnevno delovanje storitev v kriznih razmerah (Preradović 2010).

Za razumevanje informacijske varnosti v gospodarskih družbah in v gospodarski sferi ter za prepoznavanje in razlago interesa gospodarstva po zagotavljanju informacijske varnosti bom predstavil nekaj teoretskih konceptov. Tematika bo konkretno prikazana na primeru varnostnega organiziranja gospodarske družbe, delujoče na področju informacijsko komunikacijske tehnologije.

7.1 Varovanje informacij

Informacije so poleg kapitala, ljudi, naravnih virov in znanja zelo pomemben vir za poslovanje podjetja in pridobivajo na vedno večji pomembnosti. Zato je potrebna vzpostavitev ustreznih sistemov varovanja informacij na temelju varnostnih standardov, zakonodaje in razpoložljive informacijske tehnologije. Osnovna naloga varovanja informacij je zaščita le-teh pred različnimi nevarnostmi iz okolja kot tudi iz podjetja samega ter zagotavljanje neprekinjenega poslovanja in omejitev poslovne škode na najmanjšo možno raven. Samo varovanje informacij bo učinkovito le takrat, ko se bo sistem varovanja uporabljal na primeren in pravilen način, kar bo prinašalo koristi (zmanjševalo stroške in povečevalo produktivnost) (Štrakl 2003, 19).

Varovanje informacij zajema predvsem zagotavljanje naslednjih treh osnovnih načel (BS/IEC 17799: 2000):

- **Neoporečnost:** varovanje točnosti in popolnosti informacij ter računalniške programske opreme. Podatki, s katerimi se upravlja, morajo biti vredni zaupanja.
- **Zaupnost:** zagotavljanje, da so informacije dostopne samo pooblaščenim osebam. Nanaša se na vse podatke, ki so direktno povezani s programskimi rešitvami, nosilci podatkov, komunikacijskimi in ostalimi procesi.
- **Razpoložljivost:** zagotavljanje, da so informacije in računalniške storitve na voljo pooblaščenim uporabnikom, kadar jih potrebujejo. Poslovni partnerji pričakujejo hiter in zanesljiv dostop do potrebnih podatkov. Je vitalnega pomena za organizacijo. Informacije, ki so potrebne varovanja, se ugotovijo s popisom sredstev, temu pa sledi analiza tveganj. Na podlagi te analize se pripravijo ukrepi za zmanjševanje tveganj in

nadzor njihove uporabe. Vsi ukrepi (načini dela, postopki, organizacijska struktura in funkcije programske opreme) se zapišejo v dokument varnostne politike, ki za vsako posamezno področje ali problem natančno določa, kako ukrepati. Z vsebino varnostne politike morajo biti seznanjeni vsi zaposleni. Zelo pomembno je, da varovanje informacij izhaja iz ciljev organizacije.

7.2 Standardi informacijske varnosti

Vsaka organizacija mora imeti za zaščito pomembnejših poslovnih procesov vpeljan proces, ki omogoča tako poslovanje, da ne bo prekinjeno ob vsakem izpadu informacijskega sistema. Ta jo ščiti pred učinki večjih napak ali katastrof, s tem pa zmanjšuje prekinitev dela na sprejemljivo raven (BS ISO/IEC 17799: 2000).

Upravljanje neprekinjenega poslovanja mora biti sestavni del upravljanja podjetja. Načrtovanje in vzpostavljanje neprekinjenega poslovanja je tesno povezano z vsemi poslovnimi procesi v organizaciji. V praksi velikokrat naletimo na dejstvo, da je načrtovanje teh aktivnosti prepuščeno samo tehničnemu osebju s področja informatike in zato največkrat ne nudi celovitega odgovora organizacije na tveganja, katerim je izpostavljena. To dejstvo nam znova dokaže, da se je varovanja podatkov potrebno lotiti celovito. Organizacija mora objaviti sprejeto politiko in smernice za upravljanje neprekinjenega poslovanja ter poskrbeti za njeno pravilno izvajanje. Podjetja, vladne ustanove in bančne institucije se največkrat odločajo za varovanje informacij zaradi poslovnih in tudi zakonskih zahtev. Informacijska varnost je v močni povezavi z informacijskim pravom. Tu se začnejo odpirati vprašanja s področja dostopa do programske, strojne in sistemske opreme, varstva osebnih podatkov, šifriranja, elektronskega poslovanja in podpisovanja ter intelektualne lastnine (Preradović 2010).

Zakoni, ki v Sloveniji posegajo na področje informacijske varnosti, so (Preradović 2010):

- Zakon o elektronskem poslovanju in elektronskem podpisu
- Zakon o elektronskih komunikacijah
- Zakon o varstvu osebnih podatkov
- Zakon o avtorskih in sorodnih pravicah

- Zakon o pogojnem dostopu do zaščitenih elektronskih storitev
- Zakon o varstvu potrošnikov
- Zakon o tajnih podatkih.

Tudi sam trg zahteva od podjetij, da uredijo svojo varnostno politiko. Podjetja, ki imajo dobro organizirano varnost, so še vedno ogrožena preko poslovanja s podjetji, ki tega nimajo najbolje urejenega. Zavarovalnice v tujini se že ukvarjajo z zavarovanjem pred nevarnostmi elektronskega poslovanja. Vendar pa je potrebno vedeti, da zavarovanja za vrednost podatkov na notranjih pomnilnikih ne bo sklenila nobena zavarovalnica, če ne bo prej dokazano, da je poskrbljeno za dnevno osvežene kopije podatkov in pravilno delovanje informacijskega sistema (Preradović 2010).

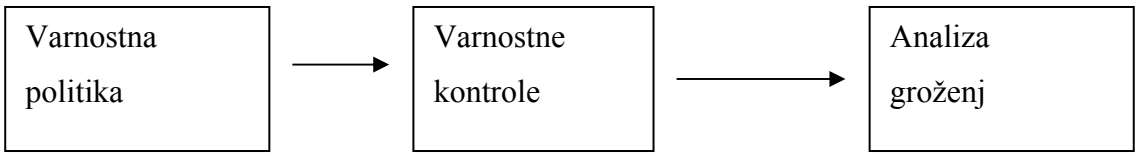
7.3 Varnostna politika

Varnostna politika nudi odgovor na dejavnike, ki ogrožajo informacijsko varnost od zunaj, kot tudi na dejavnike, ki ogrožajo sistem od znotraj. Ob upoštevanju smernic, ki jih navaja varnostni standard BS 7799, pa bomo lahko prepričani v njeno učinkovitost, saj ima standard pokrite vse vidike poslovanja organizacije. Varnostna politika je program varnosti in je v pristojnosti vodstva. V tem programu so definirani cilji, pravila in odgovornosti v zvezi z varnostjo informacijskega področja v podjetju, razni postopki ter pravila. Program obsega pravila o fizičnem in tehničnem varovanju ter pravila, s katerimi je določeno, kakšni bodo načini varovanja. Vsako dejanje, namerno ali nenamerno, ki ne upošteva pravil, določenih v varnostni politiki, se obravnava kot kršenje varnostnih pravil. Dobra varnostna politika ima dovolj informacij o tem, kaj je potrebno postoriti za zaščito informacij, virov in ljudi v podjetju. Sestavljena je iz skupka varnostnih pravil, s katerimi morajo biti seznanjeni vsi zaposleni. Ta pravila opredeljujejo način obnašanja, odgovornosti, naloge in splošna pravila za delo zaposlenih (Štrakl 2003, 20).

Skrbniki informacijskih virov in poslovnih procesov morajo biti pri oblikovanju varnostne politike pozorni na grožnje, ki prežijo iz okolja in iz podjetja samega (Preradović 2010). Prepoznava in vpeljava ustreznih zaščit zahteva sistematično planiranje in podporo vseh zaposlenih v podjetju. V fazi načrtovanja in opredeljevanja varnostne politike je potrebno gledati na velikost podjetja, razpoložljivost finančnih sredstev in stopnjo ogroženosti, saj naj

bi se potem izboljšala razpoložljivost, celovitost ter zaupnost znotraj in zunaj podjetja. V tej fazi se uporabijo rezultati predhodno postavljene ocene tveganj, kjer so se prepoznale vse potencialne grožnje. Popis teh groženj bo osnova za opredelitev varnostne politike. Po opredelitvi se začne izbira varnostnih kontrol in je sestavljena je iz skupka varnostnih pravil, s katerimi morajo biti seznanjeni vsi zaposleni. Ta pravila opredeljujejo način obnašanja, odgovornosti, naloge in splošna pravila za delo zaposlenih.

Slika 7.1: Varnostna politika in njena vloga



Vir: Olovsson (1992, 7).

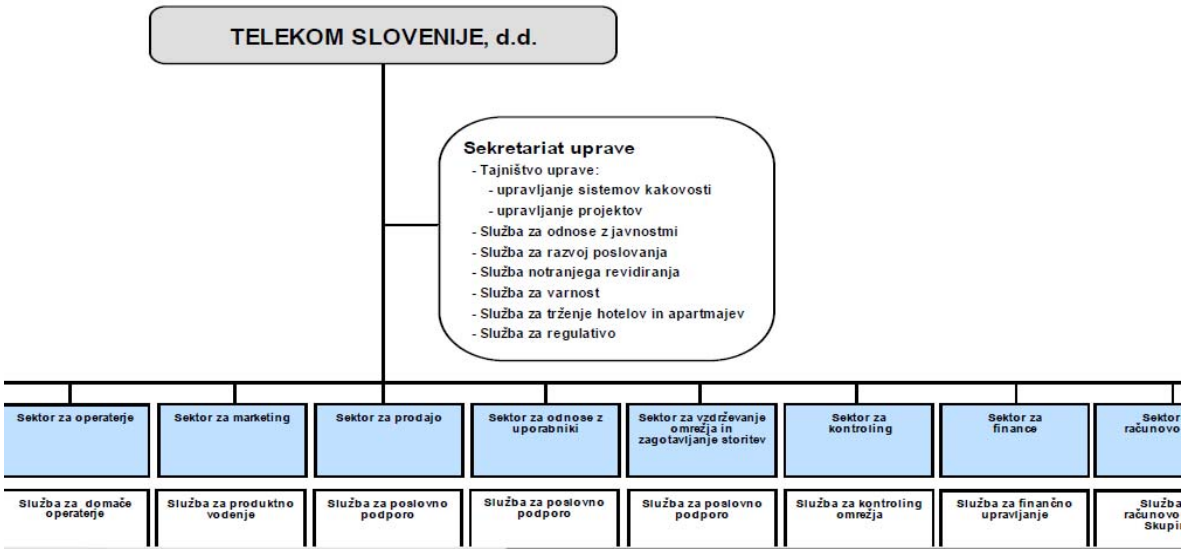
Varnostna politika zajema širok krog varnostnih vprašanj, ki so za vsako podjetje drugačna. Zaradi tega in zaradi specifičnosti poslovanja vsakega podjetja pripravljenega dokumenta varnostne politike ni mogoče kar poenotiti in poenostaviti. Iz tega sledi, da mora vsako podjetje razviti svojo varnostno politiko, v kateri bodo upoštevani vsi dejavniki poslovanja podjetja. Eden od takih pomembnih dejavnikov je značilnost lastnega informacijskega sistema in prav to je potrebno upoštevati, če hočemo razviti optimalno delujočo varnostno politiko. Pri razvoju morajo biti vključeni strokovnjaki z različnih področij delovanja podjetja. Standard BS7799 omenja varnostno politiko le kot eno izmed priporočenih kontrol, ne spušča pa se v podrobna priporočila za pripravo politike (Štrakl 2003, 21). Politika mora biti v pisni obliki in kot taka na voljo vsem zaposlenim, ki so odgovorni za informacijsko varnost. Vodstvo je odgovorno za potrditev dokumenta in za seznanjanje zaposlenih o varnostni politiki. Določi se lastnik dokumenta in ta je zadolžen za njegovo vzdrževanje in preglede.

7.4 Varnostno organiziranje gospodarske družbe

Varnostno organiziranje v sferi gospodarstva in na ravni gospodarske družbe je del poslovnega procesa podjetja, saj se na trgu bolje prodajajo varne storitve, to pa še posebej

velja za sfero informacijsko komunikacijske tehnologije (Preradović 2010). Varnostno organiziranje bomo prikazali na primeru domačega komunikacijskega podjetja Telekoma Slovenije d.d., ki ima zaradi narave svojega delovanja tudi vlogo v civilni obrambi države (Preradovič 2010). Bistveno pri Telekomu Slovenije na obrambnem področju je to, da opravlja nekatere zakonsko določene naloge na področju civilne obrambe, zaščite in reševanja, konkretno pa to pomeni, da mora v kriznih razmerah zagotoviti delovanje telekomunikacij za 90-dnevno obdobje.

Slika 7.2: Izsek organizacijske strukture Telekoma Slovenije d.d.



Vir: prirejeno po Telekom Slovenije (2010).

V primeru Telekoma gre za veliko gospodarsko družbo in nacionalnega operaterja hkrati, v katerem je zaposlenih preko 2000 ljudi, celotna skupina Telekoma pa zaposluje več kot 4000 ljudi (Telekom 2010). Podjetje ima svojo horizontalno in vertikalno organizacijsko strukturo. Kot vidimo na sliki, je organizirano sektorsko, in sicer po vsebinsko smiselnih področjih. Nadalje se organiziranost razčleni v različne službe in posebne delovne skupine znotraj njih. Ko govorimo o področju informacijske varnosti v tej gospodarski družbi, vidimo, da organizacijsko spada v sekretariat uprave, kjer se izvršuje v posebni službi, službi za varnost. S takšno organizacijo je služba za varnost hierarhično stopnjo višje od vseh sektorjev, kar nam daje vedeti, da je interes gospodarske družbe visok in splošno zasledovan na vseh sektorjih delovanja. Služba za varnost ima prav tako svojo notranjo delitev, saj je zadolžena

za celoten spekter varnosti gospodarske družbe – za fizično varovanje ter tehnično in informacijsko varnost (Preradović 2010).

7.4.1 Služba za varnost

Kot omenjeno, ima *služba za varnost* širok spekter pristojnosti, temu primerna pa je tudi njena notranja organiziranost na posamezne oddelke. Nekoliko podrobneje bom predstavil njeno notranjo organiziranost in cilje delovanja, ki jih zasleduje. Na podlagi analize organiziranosti, pristojnosti in nalog služb za varnost in podjetij nasploh bo mogoče do neke mere prepoznati, kje je bistvo interesa podjetja po zagotovitvi obeh komponent omrežne in informacijske varnosti.

Glavni cilji *službe za varnost* so:

- zagotavljanje varnostne politike družbe,
- zagotavljanje varnostne politike informacijskih tehnologij,
- zagotavljanje varovanja premoženja družbe,
- zagotavljanje sistemov za preprečevanje zlorab,
- izvajanje zakonsko določenih nalog s področja varnosti, telekomunikacijskega prometa, civilne obrambe ter zaščite in reševanja (Preradović 2010).

Oddelek za varnost zasleduje predvsem naslednje konkretne naloge:

- uresničevanje varnostne politike družbe,
- priprava in analiza planov s področja dela službe,
- analiza varnostnih rizikov in stanja varnosti družbe ter načrtovanje in izvajanje varnostnih ukrepov,
- planiranje, spremljanje in izvajanje fizičnega ter tehničnega varovanja objektov in premoženja,
- sodelovanje pri gradnji, nadzoru in vzdrževanju sistemov tehničnega varovanja objektov in premoženja,

- organiziranje in zagotavljanje izvajanja zakonsko določenih nalog s področja varnosti, telekomunikacijskega prometa, civilne obrambe ter zaščite in reševanja,
- priprava aktov družbe in navodil s področja varovanja, civilne obrambe, varnosti, nadzora telekomunikacij, informacijske varnosti, tajnih podatkov idr.,
- načrtovanje in izvajanje pogodbenih obveznosti s področja varnosti za druge pravne osebe (Telekom 2010).

Oddelek za varnostni nadzor zasleduje predvsem naslednje naloge:

- nadzor objektov z dostopno kontrolo,
- videonadzor objektov,
- nadzor protipožarne in protivlomne zaščite,
- nadzor drugih sistemov tehničnega varovanja,
- izdelava analiz, poročil in predlogov ukrepov,
- kreiranje, distribucija in analiziranje vstopnih dovolilnic,
- zagotavljanje in vzdrževanje baze podatkov za varnostni nadzor (Telekom 2010).

Oddelek za informacijsko varnost opravlja naslednje naloge:

- celovito upravljanje in nadziranje informacijsko komunikacijske varnosti družbe,
- opredeljevanje politike, smernic, navodil, dobrih praks in nadzornih postopkov za področje informacijsko komunikacijske varnosti,
- zagotavljanje orodij, veščin in znanj za področje informacijsko komunikacijske varnosti,
- zajemanje in analiziranje nadzornih podatkov ter analiziranje potencialnih varnostnih tveganj,
- preiskovanje za določanje, ali so varnostna tveganja prisotna oziroma ali je prišlo do kršitve varnostnih pravil, ter preiskava varnostnih incidentov,
- opredeljevanje vrste in področij varnostnih tveganj ter določanje prioritet (Telekom 2010).

Na podlagi analiziranega varnostnega organiziranja konkretne gospodarske telekomunikacijske družbe lahko vidimo, da varnost, predvsem pa informacijsko varnost, dojemajo v luči koncepta omrežne in informacijske varnosti. Analiza nam pokaže, da se zavedajo obeh dimenzij omrežne in informacijske varnosti. Prednost pa se daje predvsem varni storitvi, saj se varnost razume kot del poslovnega procesa. Kompetentne službe analizirajo družbeno okolje in okolje znotraj podjetja, potencialne zaznane grožnje pa prioritetno obravnavajo (Preradović 2010). Kot izhaja iz teorije, je tudi dejansko eden večjih varnostnih izzivov omrežni in informacijski varnosti gospodarske družbe in tudi sicer še vedno človeški faktor. Tega izziva se tudi na konkretnem primeru lotevajo z varnostnim nadzorom in represijo, zavedajo pa se pomena motiviranja zaposlenih. Poseben poudarek je namenjen izgradnji ustrezne stopnje varnostne kulture, ki bazira na organizacijski kulturi gospodarske družbe (Preradović 2010).

8 ZAKLJUČEK

Povečana raba informacijsko komunikacijske tehnologije in na njej temelječih omrežij je poleg številnih pozitivnih premikov postavila v varnostni razpravi novo relevantno varnostno vprašanje. Država in njeni podsistemi v veliki meri delujejo ob pomoči IKT in raznih omrežij, kar pa nam daje vedeti, da so vse bolj odvisni od učinkovitega in varnega delovanja mrež. Interes po zagotovitvi informacijske varnosti je prisoten na vseh analiziranih ravneh, tako naddržavni in državni kakor tudi v gospodarski sferi. Interes po zagotavljanju ali nezagotavljanju informacijske varnosti na posameznem analiziranem nivoju je različno motiviran. Odgovorni so tukaj v mnogih dilemah med pozitivnimi in negativnimi učinki procesa zagotavljanja informacijske varnosti, soočajo pa se tudi z raznimi ovirami v samem procesu. Informacijsko komunikacijska tehnologija je tako postavljena v dvojno vlogo, postala je vir moči in hkrati vir ranljivosti. Države, zavezništva in gospodarstvo imajo v veliki meri skupne interese po zagotavljanju informacijske varnosti. Interes ima osrednjo vlogo v politološki znanosti in pri razlaganju procesov, ki se v družbi odvijajo, kar pa velja tudi za področje informacijske varnosti.

Nacionalno varnostni sistemi, ki so sestavljeni iz varnostne strukture in varnostne politike, so nove oblike groženj vsekakor zaznali. Nove asimetrične in transnacionalne grožnje, ki pretežno nimajo klasične vojaške oblike ogrožanja nacionalne varnosti, so pojav sodobne dobe, v kateri govorimo o t.i. omreženi družbi. Informacijska varnost v Republiki Sloveniji je

delno sooblikovana s strani Evropske unije ter nekaterih skupnih politik in organizacij s tega področja. V konceptu celovite zagotovitve informacijske varnosti v državi pa ima pomembno besedo tudi gospodarski podsistem kot največji ponudnik in uporabnik informacijsko komunikacijske tehnologije. V luči sodobnih groženj nacionalni varnosti se v politološki razpravi na državnem nivoju pojavlja novo pomembno vprašanje razmerja med varnostjo in svobodo. Demokratičnost sodobne države se odraža tudi v odnosu do interneta in v demokratičnosti interneta v posamezni državi. Demokracija na internetu se pogosto omejuje v interesu varnosti. Gospodarska sfera in gospodarske družbe se v luči informacijske varnosti in interesa po njeni zagotovitvi srečujejo z dilemo med notranjo ter zunanjo omrežno in informacijsko varnostjo organizacije. Obstaja pa tudi dilema med ceno in varnostjo storitve, saj so bolj varne informacijske storitve praviloma dražje in zaradi tega nekonkurenčne na trgu.

Evropska unija ima kot politična in gospodarska naddržavna tvorba izvor interesa na področju informacijske varnosti prav v gospodarstvu. Informacijsko komunikacijska tehnologija je v EU pomemben gospodarski element inovacij, raziskav in razvoja ter posledično na tej osnovi pridobljenih novih delovnih mest. Zaradi morebitne pomanjkljive informacijske varnosti bi se utegnil pojaviti strah pred uporabo IKT, kar bi zavrlo gospodarski razvoj. EU tako preko svojih institucij in strokovnih organizacij s tega področja (ENISA) daje konkretne in načelne usmeritve državam članicam. Interes EU po informacijski varnosti izvira iz težnje po nemotenem delovanju gospodarstva znotraj EU in širše ter iz težnje po nemotenem in varnem delovanju storitev birokratskega aparata EU. Evropska komisija ima močan interes po ustvarjanju novih delovnih mest na bazi IKT, sodobno tehnologijo pa smatra tudi kot pripomoček na poti graditve evropske zavesti. EU ima interes po celoviti obravnavi področja informacijske varnosti in tako poskuša z raziskavami na evropski ravni raziskovati to relativno novo področje. Na ravni EU so prisotni tako pozitivni kakor tudi negativni učinki informacijske varnosti in ovire v procesu njenega zagotavljanja. Bistven pozitiven učinek informacijske varnosti v EU je gotovo višja stopnja zaupanja v elektronske upravne postopke EU, zaupanje v tehnologijo in rast števila delovnih mest v tej gospodarski sferi. Glavne ovire in negativni učinki zagotavljanja informacijske varnosti pa izvirajo predvsem iz dodatnega dela, služb, postopkov učenja in evalvacije, kar posledično zapleta in draži delovni proces birokratskega dela EU.

Interes nacionalne države je, da zagotovi na svojem ozemlju čim višjo stopnjo varnosti in čim manjšo stopnjo ogroženosti. Zagotoviti mora varnost bivanja posameznikov kakor tudi varnost obstoja in delovanja vseh družbenih podsistemov. Sodobne grožnje so transnacionalne, kar sili države, da v interesu varnosti sklepajo zavezništva ter vstopajo v politično-gospodarske tvorbe. V takšnem okolju deluje tudi gospodarstvo, ki pa del nalog za zagotovitev varnega delovanja prevzema kar nase. V Republiki Sloveniji se IKT razume kot podpora pri izvajanju birokratskih procesov. V zadnjem obdobju IKT vse bolj omogoča servisno vlogo sodobne države, kar se kaže v nekaterih elektronskih oblikah birokratskih storitev države. Slednje imajo številne praktične vidike v očeh končnega uporabnika – državljana. Država ima tukaj nedvomno interes po zagotovitvi informacijske varnosti svojih e-storitev, vendar se tukaj odpira vprašanje razmerja med varnostjo in svobodo ter demokratičnostjo interneta. IKT odpira nove poti demokraciji, govori se predvsem o participativni demokraciji, kjer lahko državljani preko IKT vplivajo na obstoječe vladajoče strukture in se tako na nek način soudeležujejo pri vladanju. Z zlorabo IKT se lahko prizadene interese države, tudi varnostne. Interes Republike Slovenije po informacijski varnosti izvira iz težnje po varovanju vseh družbenih podsistemov na svojem teritoriju. K informacijski varnosti se teži tako na ravni državne birokracije kakor tudi mednarodno. Za te namene se s področjem informacijske varnosti ukvarja represivni aparat, iščejo pa se tudi preventivni ukrepi, ki jih v Sloveniji pooseblja SI-CERT. Poglavitne ovire in negativni učinki zagotavljanja informacijske varnosti na ravni države so dokaj podobni tistim, ki jih zasledimo na ravni Evropske unije. Selitev nekaterih upravnih procesov države v virtualno okolje je zahtevalo od države vpeljavo novih služb in transformacijo obstoječega upravnega aparata. Tako se je bil državni birokratski aparat prisiljen prilagoditi na nove delovne procese in na novo učenje, kar je v njihovi percepciji zapletlo rutinski delovni proces. Ovira so gotovo tudi s tem povezani stroški, saj področje IKT zaradi hitrega razvoja zahteva stalna vlaganja v novo tehnologijo in znanja.

Gospodarstvo je nosilec razvoja in velik uporabnik sodobne IKT. V luči teorije omrežne in informacijske varnosti želijo gospodarske družbe zagotoviti tako notranjo kot tudi zunanjo varnost. Gospodarska družba je postavljena v okolje svojega delovanja in temu primerno razvija svojo varnostno kulturo, ki je bolj ali manj skladna s kulturo organizacije same. Takšna družba deluje tudi na prostem trgu, kjer med konkurenti poteka neusmiljen tržni boj. Izvor interesa gospodarske družbe po zagotovitvi informacijske varnosti je v tem, da prepreči varnostne incidente in zavaruje pomembne informacije, ki bi v rokah konkurenta pomenile

tržno prednost. Notranjo varnost gospodarske organizacije ogroža predvsem človeški faktor, česar se podjetja lotevajo z represivnimi in preventivnimi ukrepi. Podjetja svoj interes po informacijski varnosti na podlagi zaznanih groženj kodificirajo v varnostni politiki. Gospodarske družbe, še posebej tiste, delujoče na področju informacijsko komunikacijske in telekomunikacijske tehnologije in storitev, so v veliki meri odvisne od uspešnosti prodaje izdelkov in storitev. Tudi tukaj je del izvora interesa po visoki stopnji informacijske varnosti. Tudi gospodarske družbe, ki uporabljajo IKT ali ponujajo storitve, bazirane na omrežjih ali sodobni IKT tehnologiji, se soočajo z nekaterimi ovirami pri zagotavljanju informacijske varnosti. Pozitivni učinki informacijske varnosti za gospodarsko družbo v glavnem izvirajo iz varovanja vitalnih informacij pred konkurenti na trgu ali potencialnim zunanjim ter notranjim namernim ogrožanjem informacijske varnosti. Glavna ovira in negativni učinek zagotavljanja informacijske varnosti je tudi na ravni gospodarstva podoben tistemu na nivoju države in EU. Višja stopnja informacijske varnosti pomeni določeno omejevanje svobode, ko govorimo o človeškem faktorju. Organizacijsko pa to pomeni uvajanje novih pristojnih služb in novih delovnih procesov ter stalno novo učenje zaposlenih. Vse našteto pa je nujno povezano z višjimi stroški, ki jih pri tem nosi gospodarska družba, to pa draži poslovanje in storitve. Na trgu se bolje prodajajo varne storitve in varne tehnologije in informacijska varnost naj bi bila tako razumljena kot konkurenčna prednost ter ne bi smela biti obravnavana kot negativen strošek.

9 LITERATURA

1. Anžič, Andrej. 1997. *Varnostni sistem Republike Slovenije*. Ljubljana: Uradni list RS.
2. Božič, Gorazd. 2004. *Pogovor z vodjo SI CERT*. Ljubljana. Dostopno prek: http://slotech.com/clanki/04023/ (6. marec 2010).
3. --- 2010. Intervju z avtorjem. Ljubljana, 7. april.
4. Commission of the European Communities. 2005. *Green Paper on an European Programme for Critical Infrastructure Protection (COM(2005) 576).* Brussels. Dostopno prek: http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf (10. april 2010).
5. Dunn, Myriam, Victor Mauer in Andreas Wenger. 2008. *International CIIP Handbook 2008/2009. An inventory of 25 national and 7 international critical information infrastructure protection policies*. Zürich: Center for Security Studies, ETH.
6. Dunn, Myriam in Isabelle Wigert. 2004. *International CIIP Handbook 2004*. Zurich: Swiss federal institute of technology. Dostopno prek: http://e-collection.ethbib. ethz.ch/eserv/eth:31123/eth-31123-02.pdf (15. april 2010).
7. Enisa. 2009. *Who is Who directory on network and information securty*. Version 4.0. edition 2009. Dostopno prek: http://www.enisa.europa.eu/act/sr/files/deliverables/ enisa_who_is_who_2009.pdf/at_download/file (7. april 2010).
8. --- 2010. *Evropska agencija za omrežno in informacijsko varnost*. Dostopno prek: http://www.enisa.europa.eu (11. april 2010).
9. Evropska komisija. 2010. *Stalno predstavništvo Slovenije*. Dostopno prek: http://bruselj.predstavnistvo.si/index.php?id=626 (11. april 2010).
10. Evropski parlament. 2010. *Spletne strani Evropskega parlamenta*. Dostopno prek: http://europa.eu/institutions/inst/parliament/index_sl.htm (11. april 2010).
11. Gordon, A. Lawrence, Loeb P. Martin, Lucyshyn William in Richardson Robert. 2004. *Computer Crime and Security Survey*. San Francisco: Computer Security Institute Publications.
12. Grizold, Anton. 1999. *Obrambni sistem Republike Slovenije*. Ljubljana: Visoka policijsko - varnostna šola.
13. Hayden, Michael. 2003. *National information assurance glossary*, *Committee on national Security Systems*. Dostopno prek: http://www.cnss.gov/Assets/pdf/ cnssi_4009.pdf (15. april 2010).

14. Horjak, Marjeta. 2010. *Vpliv varne informacijske tehnologije na ekonomsko uspešnost podjetja*. Dostopno prek: http://www.mfc-l.si/?s=d&p=horjak2&l=si (20. april 2010).
15. Informacijska družba. 2010. *Informacijska družba*. Dostopno prek: http://www.informacijskadruzba.si/index.php?option=com_content&task=view&id=92&Itemid=108 (11. april 2010).
16. Infosek News. 2005. *EU task force to study IT critical infrastructure.* Dostopno prek: http://www.attrition.org/pipermail/isn/2005-April/001454.html (10. april 2010).
17. Jelušič, Ljubica. 1997. *Legitimnost sodobnega vojaštva*. Ljubljana: Fakulteta za družbene vede (Knjižna zbirka Teorija in praksa).
18. Kovač, Bogomir, Aleksandar Kešeljević, Erik Kopač in Uroš Svete. 2008. *Zaščita varnostnih interesov RS v luči globalizacije*. Ciljni raziskovalni projekt »ZNANJE ZA VARNOST IN MIR 2004 – 2010«. Ljubljana: Univerza v Ljubljani.
19. Lukšič, Igor. 2002. *Interes konceptualizacija pojmov*. Teorija in praksa 39 (4/2002): 509.
20. McDaniel, George. 1994. *IBM Dictionary of computing*. New York: McGraw - Hill, str. 758.
21. MG. 2010. *Ministrstvo za gospodarstvo*. Dostopno prek: http://www.mg.gov.si/si/o_ministrstvu (16. april 2010).
22. MJU. 2010. *Ministrstvo za javno upravo*. Dostopno prek: http://www.mju.gov.si/si/o_ministrstvu (19. april 2010).
23. MVZT. 2010. *Ministrstvo za visoko šolstvo znanost in tehnologijo*. Dostopno prek: http://www.mvzt.gov.si/si/delovna_podrocja (17. april 2010).
24. Olovsson, Tomas. 1992. *A structured approach to computer security*. Chalmers university of technology Gothernburg : Department of computer engineering.
25. Preradović, Željko. 2010. Intervju z avtorjem. Ljubljana, 10. februar.
26. Prezelj, Iztok. 2002. *Konceptualizacija nacionalnih varnostnih interesov*. Teorija in praksa 39 (4/2002): 635.
27. --- 2010. *Kritična infrastruktura v Sloveniji*. Ljubljana: Fakulteta za družbene vede.
28. Schneier, Bruce. 2000. *Secrets and Lies: Security in a networked world*. New York: John Wiley.
29. SI CERT. 2010. *SI CERT Slovenija*. Dostopno prek: http://www.cert.si/o-centru.html (14. april 2010).
30. Simčič, Simon. 2007. *Ogrožanje kritične informacijske infrastrukture v Republiki Sloveniji.* Diplomsko delo. Fakulteta za družbene vede Univerze v Ljubljani.

31. Svete, Uroš in Pintarič Uroš ur. 2008. *E-država: upravno – varnostni vidiki*. Nova Gorica: Fakulteta za uporabne družbene študije.
32. Svete, Uroš. 2005. *Varnost v informacijski družbi.* Ljubljana: Fakulteta za družbene vede (Knjižna zbirka Varnostne študije).
33. Štrakl, Marjan. 2003. *Varnostna politika informacijskega sistema*. Trinajsta delavnica o telekomunikacijah VITEL. Dostopno prek: https://lms.uni-mb.si/vitel/14delavnica/clanki/marjan_strakl.pdf (17. marec 2010).
34. Telekom Slovenije. 2010. *Spletne strani gospodarske družbe Telekom Slovenije d.d.* Dostopno prek: http://www.telekom.si (15. april 2010).
35. Urad vlade za komuniciranje. 2010. *Spletni portal Predlagam vladi.si*. Dostopno prek: http://predlagam.vladi.si/ (12. april 2010).
36. UVTP. 2010. *Urad vlade RS za varovanje tajnih podatkov*. Dostopno prek: http://www.uvtp.gov.si/si/o_vladni_sluzbi/naloge_in_cilji (16. april 2010).
37. Vogrin, Andreja, Prezelj Iztok in Bučar Bojko. 2008. *Človekova varnost v mednarodnih odnosih*. Ljubljana: Fakulteta za družbene vede.
38. Wikipedia. 2010a. *Informacijska varnost*. Dostopno prek: http://sl.wikipedia.org/wiki/Informacijska_varnost#Informacijska_varnost (5. april 2010).
39. ---2010b. *Information security.* Dostopno prek: http://en.wikipedia.org/wiki/Information_security (5. april 2010).