UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Mitja Sovič

Vloga zasebnih podjetij pri zagotavljanju državne informacijske varnosti

Magistrsko delo

Ljubljana, 2016

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Mitja Sovič

Mentor: izr. prof. dr. Uroš Svete

Vloga zasebnih podjetij pri zagotavljanju državne informacijske varnosti

Magistrsko delo

Ljubljana, 2016

S tem magistrskim delom bi se rad zahvalil mentorju, izr. prof. dr. Urošu Svetetu, ki me je tekom študija usmerjal, podpiral in navduševal pri raziskovanju področja informacijsko-komunikacijske tehnologije in informacijske varnosti.

Posebna zahvala gre moji družini, ki mi je omogočila študij in ves čas potrpežljivo stala ob strani do samega zaključka, ter punci Anastaziji, ki me je podpirala ter pomagala pri premagovanju vseh ovir.

Vloga zasebnih podjetij pri zagotavljanju državne informacijske varnosti

Kibernetski prostor in z njim povezana državna informacijska varnost sta abstraktna pojma velikih razsežnosti, s katerima se javni sektor ne more soočiti brez pomoči zasebnega. Oba sektorja imata enoten cilj, to je zagotovitev ustrezne državne informacijske varnosti, vendar imata svoje interese in pričakovanja, ki jih je težko uskladiti. Potreba po sodelovanju je pripeljala do rešitve v obliki javno-zasebnega partnerstva, ki pa še zdaleč ni popolno. Sektorja morata najprej poskrbeti za informacijsko varnost na svojem področju. Gre za področje, kjer država nima dovolj izkušenj in pooblastil, zaradi vedno bolj pogostih incidentov pa se čedalje bolj izraža potreba po regulaciji informacijsko-komunikacijske tehnologije (IKT) in njene uporabe. Državna ključna infrastruktura je večinoma v rokah zasebnega sektorja, ki v določenih primerih deluje popolnoma samovoljno in z nizkimi varnostnimi standardi IKT ogroža celotno državno informacijsko varnost. Naloga države in zasebnega sektorja je, da zagotovita nemoteno delovanje omenjene infrastrukture in preventivno zagotovita ustrezne varnostne ukrepe. V magistrskem delu sem opredelil vloge zasebnega sektorja na področju IKT in informacijske varnosti, mehanizme, ki opredeljujejo določeno stopnjo varnosti IKT, poskus celovitega pristopa k varnosti v okviru javno-zasebnega partnerstva in vlogo države. Zanimalo me je, kaj in na kakšen način lahko storita javni in zasebni sektor, da bosta pripomogla k bolj razviti informacijski varnosti. V empiričnem delu sem se z intervjuji z nekaterimi strokovnjaki dotaknil tudi aktualnega stanja v Sloveniji.

Ključne besede: državna informacijska varnost, informacijsko-komunikacijska tehnologija, kibernetske grožnje, javno-zasebno partnerstvo, zasebni sektor.

Private sector's role in ensuring state information security

Cyberspace and its associated state information security form an abstract concept of large-scale with which the public sector cannot cope without the help of a private. Both sectors have a single objective, namely to ensure an adequate state of information security, but they have their own interests and expectations, which are difficult to reconcile. The need for cooperation has led to a solution in the form of public-private partnership, which is still far from complete. Both sectors must first ensure information security in their area. This is an area where the state does not have enough experience and power, because of increasingly frequent incidents. Those incidents are expressing a need for regulation of information and communication technology (ICT) and its application. National critical infrastructure is largely in the hands of the private sector, which in some cases operates in a completely arbitrary manner and use ICT with low safety standards. Those kinds of actions threaten the entire national security. The tasks of the state and the private sector are to ensure the smooth operation of infrastructure and to ensure appropriate safety precautions. In this thesis, I defined the role of the private sector in the field of ICT and information security mechanisms. I also defined a comprehensive approach to information security in the context of public-private partnerships and the role of the state. I was wondering how can the public and private sector help to develop more safe information environment. In empirical part I interviewed few experts and examined the current situation in Slovenia.

Key words: state information security, information and communication technology, cyber threats, public-private partnership, private sector.

KAZALO

1 UVOD

Živimo v času, ko je uporaba informacijsko-komunikacijske tehnologije (IKT) vsakdanja dejavnost. Pomaga nam pri opravilih, olajša naše napore, povezuje nas z ostalimi in upravlja z danes največjimi dragocenostmi, to je informacijami.

Informacije niso pomembne le za posameznike, ogromen pomen imajo tudi za države in mednarodna zavezništva. Fokus le-teh se je v zadnjih letih preusmeril v razvoj zmogljivosti, ki bodo varovale informacije in zagotavljale ustrezen nivo informacijske varnosti. Za državno varnost je izjemno pomembna ključna infrastruktura, ki omogoča delovanje države. V preteklosti je bila v rokah državnih organizacij, ki so z jasno avtoriteto vplivale na delovanje in nadaljnji razvoj. Nove tehnologije, globalizacija in socialna gibanja so zatresla tla obstoječim strukturam, pod pritiskom privatizacije pa se je lastništvo in upravljanje ključne infrastrukture premaknilo v roke zasebnega sektorja. Faktorji, kot so pomanjkanje izkušenj, hitra menjava lastništva, nepopolne strategije in neustrezno opredeljene dolžnosti, so skupaj z nenehnim razvojem tehnologije kmalu pokazali na pomanjkljivosti izbranih pristopov. Organizacije zasebnega sektorja namreč v večini primerov nimajo jasno opredeljenih vlog, kar jim omogoča bolj ali manj prosto delovanje. Njihova vloga pri informacijski varnosti pa se ne konča pri ključni infrastrukturi. Vsakodnevno uporabljamo IKT, ki se proizvaja v rokah zasebnega sektorja, katerega žene želja po dobičku. S tem se daje prednost nastopu na trgu, torej čim bolj konkurenčni ponudbi, katere pomemben del predstavlja časovna tekmovalnost pri izdaji novih izdelkov in storitev. Na račun hitrosti so nekatera podjetja pripravljena izpustiti fazo intenzivnega testiranja, kar načeloma rešujejo z naknadno objavo popravkov in nadgradenj (v primeru programske opreme). Pomanjkljivosti za zlonamerne akterje kibernetskega okolja predstavljajo priložnost za nezakonito pridobitev informacij, kar posledično povzroči škodo posameznikom/organizacijam, vse skupaj pa vpliva tudi na državo. V samem začetku je bilo primerov zlorab relativno malo, zato tudi ni bilo dovolj političnega interesa, da bi se pravočasno začeli razvijati mehanizmi za varovanje informacij. Sčasoma se je število groženj močno povečalo, tarče pa so postale tudi organizacije, ki skrbijo za ključno infrastrukturo. Politične oblasti so uvidele, da morajo izbrati nove pristope pri soočanju z grožnjami iz tako abstraktne dimenzije. Ker si v veliki meri ne lastijo ključne infrastrukture, ne morejo preprosto pripraviti in legalizirati politike, ki ustreza le javnemu sektorju. V današnjem času imata udejstvovanje družbe in interesi lobijev veliko moč, legitimnost odločitev pa za oblast v tako nepredvidljivem času pomeni ogromno.

Vse kaže, da ima zasebni sektor poseben vpliv na nadaljnji razvoj IKT. Nenehne investicije v IKT ves čas skrbijo za novitete, manjka pa regulacija, ki bi zahtevala zagotavljanje določenih varnostnih standardov. Kibernetske grožnje in napadi se večajo iz leta v leto, zato so se pojavile razne skupnosti, ki opozarjajo na nujnost varne proizvodnje oziroma razvoja IKT. V interesu zasebnega sektorja je dobiček, tega pa ne morejo pridobiti brez baze potrošnikov. Kar ni mogla doseči država brez ustreznih pravnih mehanizmov, sta dosegla pritisk družbe in posledice povečanega števila napadov. Zasebni sektor se je začel udejstvovati znotraj raznih asociacij, saj sodeluje na strokovnih razpravah in pri ozaveščanju javnosti o varni uporabi IKT, razvija in sprejema razne kodekse obnašanja in standarde, hkrati pa je začel sodelovati z javnim sektorjem pri oblikovanju smernic za dosego državne informacijske varnosti.

Tekom let sta oba sektorja kljub različnim interesom (javno dobro in dobiček) uvidela, da sama nista zmožna obravnavati takšnega spektra groženj. Zasebni sektor sicer tudi samostojno razvija nove standarde, ki pa ob pomanjkanju pravne podlage niso zavezujoči za vse akterje. Začela so se javno-zasebna partnerstva, ki so sicer različno organizirana, vendar ciljajo na ustrezen nivo informacijske varnosti, ki bo služil obema sektorjema. Partnerstva se še vedno razvijajo in na primerih dobrih praks iščejo najoptimalnejše načine, ki združujejo interese in cilje obojih. Sektorja sta še vedno preveč različna, vendar z vedno novimi poskusi počasi napredujeta proti skupnemu cilju. K temu veliko pripomorejo mednarodna zavezništva, ključnega pomena za uspeh pa bo zaupanje, ki se bo moralo razviti s pomočjo transparentnega delovanja in skupnih izkušenj.

2 METODOLOŠKI IN HIPOTETIČNI OKVIR

2.1 Predmet in cilji proučevanja

Cilj magistrske naloge je najprej opredelitev vlog zasebnega sektorja pri zagotavljanju državne informacijske varnosti, to so: vloga lastnika/operaterja ključne infrastrukture, vloga ponudnika IKT produktov in storitev, uporabnika IKT in soustvarjalca kibernetskega okolja. S pomočjo študije slovenskega sistema bom opredelil pozitivni in negativni vpliv na informacijsko varnost, predstavil slabosti in prednosti zasebnih podjetij ter opredelil, kakšen odnos imata javni in zasebni sektor na področju zagotavljanja informacijske varnosti (posebej javno-zasebno partnerstvo). Kot primer sem izbral Slovenijo, saj želim izvedeti, kako razvito informacijsko varnost imamo in kakšna je pri nas vloga zasebnega sektorja.

Želim tudi raziskati, zakaj država ne more regulirati dejavnosti zasebnih podjetij, ki so povezana z IKT in sodelujejo pri zagotavljanju informacijske varnosti, kakšna je njena vloga in s kakšnimi pristopi se lahko vpliva na razvoj in uporabo IKT, da bi le-ta ustrezala določenim varnostnim standardom.

2.2 Hipoteza in raziskovalno vprašanje

Raziskovalno vprašanje: Kako lahko država v okviru obstoječe zakonodaje legalno in legitimno regulira dejavnosti zasebnega sektorja pri zagotavljanju informacijske varnosti?

Zasebna podjetja se otepajo vmešavanja državnih struktur tudi zaradi strahu pred možnostjo državnega nadzora in vsiljevanja direktiv, ki bi jim zmanjšale dobiček. Država mora ravnati skladno z zakonodajo in hkrati paziti, da s svojim početjem ne izgubi zaupanja, ki je nujno za optimalno interakcijo, po drugi strani pa mora, če želi zagotoviti ustrezno informacijsko varnost infrastrukture, le-to vzpostaviti v vseh sodelujočih členih (Neal 2008; White House 2009).

Hipoteza: Zasebni sektor je pri zagotavljanju informacijske varnosti popolnoma samostojen; do sprememb lahko pride le v primeru skupne iniciative zasebnih podjetij.

Zgoraj napisano hipotezo sem oblikoval skladno z raziskovalnim vprašanjem, saj na podlagi prebrane literature menim, da je ključ do uspeha sporazum med zasebnimi podjetji, ki so med seboj konkurenčna in s pošiljanjem izdelkov na trg tekmujejo za večji zaslužek. Menim, da med njimi lahko pride do sporazuma, ki bi dal večjo vlogo varnosti njihovih produktov, težava pa se nahaja v pomanjkanju interesa vodilnih podjetij. Tu lahko pride do izraza javno-

zasebno partnerstvo (JZP), ki vključuje večje število članov iz obeh sektorjev, podvrženih skupni debati in iskanju rešitev, ključ do uspeha pa se nahaja v zaupanju akterjev (White House 2009; Zetter 2012).

2.3 Metodologija

Pri pisanju magistrske naloge sem uporabil različne metode raziskovanja, ki so pripomogle k pridobitvi relevantnih informacij. Najprej sem uporabil metodo zbiranja virov. V raznih bazah podatkov sem pregledal, ali je bilo o izbrani temi že kaj napisano, in ugotovil, da ta tema še ni bila obravnavana. Kljub vsemu sem našel nekaj raziskav in člankov, ki opredeljujejo zasebni in javni sektor ter njuno sodelovanje pri varovanju ključne infrastrukture. Ti strokovni viri so služili kot osnova, ki sem jo razdelal za področje informacijske varnosti. Za opis pojmov, aktualnega stanja in nadaljnjega razvoja sem uporabil deskriptivno in sintetično analitično metodo, ki sem jo apliciral na podlagi analize primarnih in sekundarnih virov.

Opravil sem tudi intervjuje s strokovnjaki z zasebnega in javnega sektorja s področja informacijske varnosti, namenjeni pa so razumevanju stališč oseb, ki zagovarjajo pristop svojega sektorja. Dobil sem subjektivne povratne informacije, kako je urejeno JZP na tem področju v Sloveniji in kako ga dojemajo ključni akterji. Odgovore sem analiziral in ugotovitve vključil v primerjalno analizo glede zagotavljanja informacijske varnosti.

3 OPREDELITEV TEMELJNIH POJMOV

3.1 Informacijsko-komunikacijska tehnologija (IKT)

»Informacijsko-komunikacijska tehnologija (IKT) je sposobnost, znanje, spretnost oziroma tehnika, da predvsem z uporabo strojev in naprav, ki omogočajo informacijske dejavnosti (zbiranje, obdelava, prikaz in prenos podatkov), dosežemo želene učinke« (Svete 2005, 16).

3.2 Ključna (kritična) informacijska infrastruktura

»Kritična infrastruktura državnega pomena obsega tiste zmogljivosti, ki so ključnega pomena za državo in bi prekinitev njihovega delovanja ali njihovo uničenje pomembno vplivalo oziroma imelo resne posledice na nacionalno varnost, gospodarstvo, temeljne družbene funkcije, zdravje, varnost in zaščito ter družbeno blaginjo, ocenjene po merilih, ki jih določi Vlada Republike Slovenije« (Vlada Republike Slovenije 2011, 2. čl.).

3.3 Informacijska varnost

Informacijska varnost predstavlja zaščito informacijskih sistemov pred nepooblaščenim dostopom do informacij ali njihovo modifikacijo ne glede na to, ali so shranjene, v obdelavi ali v pošiljanju. Informacijska varnost zagotavlja tudi zaščito pred napadi, ki povzročijo ohromitev storitev pooblaščenim uporabnikom, in onemogoča dostop do informacij za nepooblaščene uporabnike. Za zaščito uporablja metode za zaznavo, dokumentacijo in odvračanje groženj (Vacca 2009, 807).

3.4 Javno-zasebno partnerstvo

> *Javno-zasebno partnerstvo predstavlja razmerje zasebnega vlaganja v javne projekte in/ali javnega sofinanciranja zasebnih projektov, ki so v javnem interesu, ter je sklenjeno med javnim in zasebnim partnerjem v zvezi z izgradnjo, vzdrževanjem in upravljanjem javne infrastrukture ali drugimi projekti, ki so v javnem interesu, in s tem povezanim izvajanjem gospodarskih in drugih javnih služb ali dejavnosti, ki se zagotavljajo na način in pod pogoji, ki veljajo za gospodarske javne službe, oziroma drugih dejavnosti, katerih izvajanje je v javnem interesu, oziroma drugo vlaganje zasebnih ali zasebnih in javnih sredstev v zgraditev objektov in naprav, ki so deloma ali v celoti v javnem interesu, oziroma v dejavnosti, katerih izvajanje je v javnem interesu* (Zakon o javno-zasebnem partnerstvu (ZJZP), 2. čl.).

3.5 Kibernetska varnost

Kibernetska varnost je skupek orodij, politik, varnostnih konceptov, varnostnih varoval, smernic, pristopov upravljanja tveganj, dejavnosti, treningov, najboljših praks, zagotovil in tehnologij, ki se lahko uporabijo za varovanje kibernetskega okolja in sredstev organizacij ter uporabnikov. Sredstva vključujejo povezane računalniške naprave, osebje, infrastrukturo, aplikacije, storitve, telekomunikacijske sisteme in celoto prenesenih in/ali shranjenih informacij v kibernetskem okolju. Splošni varnostni cilji so: razpoložljivost, neokrnjenost in zaupnost (International Telecommunication Union 2008, 2–3).

4 INFORMACIJSKO-KOMUNIKACIJSKA TEHNOLOGIJA IN INFORMACIJSKA VARNOST

Informacijska varnost je zelo širok koncept. Posledice uporabe IKT se zelo razlikujejo in delujejo v veliko različnih ključnih sistemih ter praksah na več nivojih. Izraz informacijska varnost se uporablja za neokrnjenost naše osebne varnosti na spletu, varnost ključne infrastrukture, trgovine, vojaške grožnje in za zaščito intelektualne lastnine. Gre za popolnoma različne spektre, ki jih povezuje uporaba IKT (Carr 2016, 49–50). Hiter razvoj IKT je poenostavil vsakdanja opravila, spremenil družbeno življenje, hkrati pa tudi uvedel nove neznanke za akterje, ki se ukvarjajo z varnostjo. Države različno opredeljujejo in pristopajo k uporabnosti IKT v nacionalnovarnostnih sistemih, saj je le-ta lahko namenjena krepitvi informacijske varnosti, tradicionalnih elementov nacionalnovarnostnih sistemov ali pa vzpostavitvi novih oblik moči (Svete 2005, 12–13).

4.1 Razvoj IKT in vpeljava v nacionalne sisteme

Vpeljava IKT v nacionalne sisteme zajema vse od posameznih naprav do operacijskega nadzora celotnih omrežij, ki jih določena struktura premore. IKT povečuje zmogljivosti nadzora in upravljanja, vendar je podvržena raznim napakam oziroma predstavlja mamljivo tarčo kibernetskih napadov. Z digitalizacijo se je omogočil prenos podatkov, informacij, storitev in postopkov na IKT, to pa so skladno z zahtevami okolja in poenostavljenega delovanja storile tudi organizacijske enote ključne infrastrukture držav. S tem procesom so omenjene infrastrukture postale soodvisne, kar ima poleg prednosti (skupne baze podatkov, hitre komunikacije, delitve informacij itd.) tudi slabosti (vdor v eno lahko služi kot izhodiščna

točka za dostop do ostalih povezanih infrastruktur). Soodvisnost ključnih infrastruktur lahko označimo kot »sistem sistemov«. Infrastrukture so med seboj povezane z velikim številom mehanizmov, kjer izstopa uporaba IKT, ki skrbi za nemoteno izvajanje vsakodnevnih operacij, nujnih za opravljanje funkcij državnega pomena, in služi kot sredstvo sporazumevanja z ostalimi akterji. Soodvisnost ključne infrastrukture lahko razdelimo na štiri večje tipe, in sicer fizično, geografsko, logično in kibernetsko. Za namen magistrske naloge bo najpomembnejša kibernetska dimenzija, ki temelji na informacijski infrastrukturi, prek katere poteka prenos informacij. Vsaka grožnja varnosti mora biti zaradi interakcije med sektorji obravnavana kot grožnja celotni državni infrastrukturi, posledično pa tudi povezanim mednarodnim sistemom (Rinaldi in drugi 2001, 12–15; Rinaldi 2004, 1–2).

4.2 Vpeljava IKT v zasebni in javni sektor

IKT ponuja velike transformacijske priložnosti. Lahko pripomore k večanju produktivnosti, konkurenčnosti, rasti, blaginji, zmanjševanju revščine in spodbuja ekonomijo, ki temelji na znanju. IKT deluje kot sredstvo, s katerim je znanje razvito, shranjeno, nadgrajeno, spremenjeno in deljeno dalje. Omogoča sodelovanje v globalni ekonomiji. Osnovni predpogoj uporabe IKT je razpoložljivost ustrezne opreme in telekomunikacijske infrastrukture, pri učinkovitosti uvajanja IKT v obstoječe strukture javnega in zasebnega sektorja pa ključno vlogo odigrajo stroški IKT, razpoložljivost ustrezno usposobljene delovne sile, zmogljivosti struktur, da izpeljejo projekt, in pristop k uvajanju (strukture lahko pristopijo k uvajanju IKT samostojno ali pa s pomočjo drugih akterjev) (Bučar 2005, 51–54; ICT Regulation Toolkit 2016).

Razni akterji vlagajo v IKT zaradi 2 ključnih ciljev: rasti in konkurenčnosti. Razvoj IKT se zato nenehno nadaljuje in širi po sferah družbe ter gospodarstva, kar lahko vlagatelji s pravim pristopom izkoristijo v svoj prid. IKT je širok pojem, ki zajema družbene, ekonomske, kulturne in tehnološke sfere. V današnjem času, ko podjetja tekmujejo za svojo pozicijo na trgu, je IKT zanje ključnega pomena, saj bi naj vlaganje vanjo povečevalo produktivnost, nižalo transakcijske stroške, pripomoglo k hitrejšim inovacijam, boljši komunikaciji in strukturnim spremembam ter večalo usmerjenost h kupcu. Poleg naštetih sprememb se pri strukturah z intenzivnim vlaganjem v IKT povečujeta še organizacijska in proizvodna prilagodljivost, ki na trgu igrata zelo pomembno vlogo, uspešnost posameznih struktur pa se v končni fazi kaže tudi v pospeševanju gospodarstva. Razne študije so pokazale, da je razvoj IKT pri subjektih, ki imajo ustrezne pogoje za vpeljavo in nadgrajevanje le-te, znatno vplival

na ekonomsko uspešnost, torej rast in produktivnost držav, sektorjev in podjetij (Stare in Bučar 2005, 13–15; Stare in drugi 2005, 135).

Skupne točke raznih raziskav, ki so se nanašale na vpliv IKT na uspešnost poslovanja podjetij, so pokazale, da naložbe izključno v IKT niso dovolj, saj so pri primerih pozitivnega vpliva podjetja opravila dodatne naložbe tudi na nekaterih ostalih področjih, pomembno funkcijo pa so odigrali tudi komplementarni dejavniki. To so:

- strokovna znanja,
- organizacijske spremembe,
- velikost in starost podjetja,
- lastništvo, konkurenca, vodstvo,
- inovativnost,
- čas in
- nacionalne posebnosti (Bučar 2005, 33–36).

Poleg notranjih dejavnikov so izpostavljeni tudi zunanji; to so nacionalne posebnosti, kjer so na podlagi primerjave evropskega in ameriškega okolja prišli do zaključkov, da so aktivnejša vloga ameriške vlade, prednosti ameriškega institucionalnega okolja in prilagodljivost ameriškega trga pozitivno vplivali na širitev IKT in povečevanje prednosti ZDA na področju informatizacije. Trendom ZDA sledi tudi Evropa, vendar se še vedno sooča s posebnostmi posamičnih držav, ki zaradi interesov in nacionalnih karakteristik ne zmore popolnoma poenotiti trga (Bučar 2005, 35–36; Schmitz 2014).

5 ZASEBNI SEKTOR IN INFORMACIJSKA VARNOST

Običajno se kot referenta raznih strategij in politik na področju informacijske varnosti obravnava države, ki pa jih sestavljajo 3 ključne komponente: posamezniki, organizacije in internet. Pri obravnavi interesov države in posameznika večkrat prihaja do razhajanj, saj je do prihoda koncepta »človekove varnosti« veljalo, da to, kar je najboljše za državo, je po definiciji najbolje tudi za državljane. V dokumentih strategij lahko tudi zasledimo opazke, da se interesi teh dveh sfer vedno ne skladajo. To je posebej izrazito pri pomanjkanju spoštovanja do zasebnosti in svoboščin zaradi želje po boljši informacijski varnosti.

Pomembnost interneta v državnih gospodarstvih postavlja v ospredje strategij zasebni sektor (Carr 2016, 50).

Države poudarjajo pomen informacijske varnosti za uspešno gospodarstvo. Obama je leta 2009 izjavil, da bo v 21. stoletju gospodarska blaginja odvisna od kibernetske varnosti, kar se iz leta v leto tudi potrjuje. Trg interneta stvari je leta 2016 ovrednoten na okoli 175 milijard dolarjev, kraja intelektualne lastnine pa zasebnemu sektorju povzroči na milijarde dolarjev škode (Carr 2016, 51; Markets and markets 2016). Za državne interese je zelo pomembno, da poskrbijo za integriteto in tekoče delovanje interneta, od katerega so odvisni skoraj vsi sistemi. ZDA so v svoji prvi državni kibernetski strategiji leta 2010 opredelile internet kot prednost strateškega pomena, katere varovanje je prioriteta državne varnosti, čemur so sledile tudi ostale strategije držav Zahoda. Strategije kibernetske varnosti obravnavajo varnostne koncepte z internetom kot referenčnim objektom, nanašajo pa se na IKT in tiste, ki jo uporabljajo. IKT mora biti zaščitena, saj je ključnega pomena za širšo državno varnost. Do dilem prihaja pri določanju, kdo bi moral biti bolj zaščiten oziroma ali je legitimno posegati v zasebnost in pravice posameznikov, da zaščitiš državo (primer je program PRISM, ko je NSA zbirala osebne podatke za zaščito države) (Carr 2016, 52–53; ICT Regulation Toolkit 2016).

5.1 Opredelitev

Zasebni sektor je del gospodarstva, ki ni nadzorovan s strani države in ga vodijo posamezniki ali podjetja za dobiček. Zajema torej vse profitne dejavnosti, ki niso v lasti države ali vodene z njene strani. Nasproti zasebnemu je javni sektor, s katerim upravlja država, pa tudi prostovoljni sektor, kamor spadajo dobrodelne in nevladne organizacije. Zasebni sektor se opira na štiri ključne elemente, in sicer na:

1. konkurenčne trge z jasnimi in nediskriminatornimi pravili,
2. podjetništvo kot vir inovacij in sprememb,
3. pravice lastnine in
4. urejene delovne pogoje ter trajnostno uporabo okolja (Sida 2004, 4; Privacysense 2016).

Zasebni sektor je fleksibilnejši; nastal je zaradi želje po avtonomiji in neodvisnosti od državnega proračuna, kar pa mu daje tudi večjo moč pri sprejemanju odločitev (Pinter 2005, 18–20).

Na področju IKT imajo podjetja razvrednotena sredstva, saj morajo zaradi močne konkurenčnosti trga in hkrati nenehnega posodabljanja regulacije razvijati nove IKT in storitve. Njihov cilj je razvoj nove IKT na način, ki bi jim optimalno povrnil dobiček za starejšo IKT, ki ji je padla cena. Vodstvo podjetja mora sprejeti težko odločitev, saj se zaveda, da z izdajo nove tehnologije zniža ceno obstoječe. Zaradi prej naštetih dejavnosti se morajo odločiti, ali bodo z novo IKT konkurirali sami sebi ali pa bodo le-to prepustili konkurenci. Nove inovacije podjetja prisilijo k uporabi taktik zavlačevanja, ki pa morajo biti skladna z obstoječimi regulacijami na področju konkurenčnosti. Razni akterji se poslužujejo tudi novejših oblik poslovanja (dostop do produktov/storitev s plačilom pavšala, brezplačen dostop ipd.), ki še bolj pritegnejo kupce, vendar posledično zmanjšujejo promet konkurenci. Prehod iz analognega v digitalno in vpeljava širokopasovne povezave sta podjetjem omogočila možnost nenehnega širjenja informacij o produktih (marketinške dejavnosti) na globalni ravni. Zaradi raznih portalov, spletnih trgovin, spletnih strani ipd. lahko kot prodajalec programske opreme nastopi vsak, ki ima dovolj znanja o programiranju in je pripravil izdelek, ki ustreza minimalnim standardom, določenim na portalu (npr. prodaja aplikacij za pametne telefone ali računalnike). Nakup ali celo brezplačen prenos določene aplikacije lahko opravimo kar preko želene naprave, težava pa lahko nastane, če ima prenesena vsebina ranljivosti ali je kakorkoli namenjena škodovanju stranke (Goodin 2015; European Commision 2016; ICT Regulation Toolkit 2016).

5.2 Vloge zasebnega sektorja pri zagotavljanju informacijske varnosti

Zasebni sektor ima ogromno vlog na področju informacijske varnosti. V prvi vrsti je proizvajalec/razvijalec IKT, kjer mora zagotoviti ustrezno varnost izdelkov in storitev v okolju, ki se nenehno spreminja in zaenkrat še nima razvitega učinkovitega okvira za soočanje z aktualnimi grožnjami. V primeru državne informacijske varnosti poleg varnosti državljanov izstopa tudi ključna infrastruktura, ki je zaradi privatizacije večinoma v rokah zasebnega sektorja. Zasebni sektor tako upravlja s ključno infrastrukturo z uporabo komercialnih izdelkov in storitev, prav tako pa so informacijski sistemi povezani z omrežjem, ki je prav tako v rokah zasebnih ponudnikov internetnih storitev. Po drugi strani zasebni sektor sodeluje pri ozaveščanju o informacijski varnosti, organizacije nudijo različna izobraževanja, standarde in certifikate s področja poznavanja informacijske varnosti, soočanja z grožnjami, varnega programiranja ipd. Nudijo tudi dostop do bazena znanja in dobrih praks, kar je izrednega pomena za strokovnjake na področju informacijske varnosti.

5.2.1 Zasebni sektor lastnik/operater ključne informacijske infrastrukture in ponudnik internetnih storitev

Organizacije s področja informacijske varnosti posvečajo zasebnemu sektorju veliko pozornosti prav zaradi vloge, ki jo igra v državni varnosti, bodisi v gospodarstvu ali aktivnostih znotraj sektorjev, ki so vitalnega pomena za državo. Kljub temu, da je državna varnost tradicionalno v okviru delovanja državnih institucij, se situacija spremeni, ko pride do ključne infrastrukture. Trend Zahoda zadnjih 25 let je bila privatizacija sistemov ključne infrastrukture in uporaba komercialne IKT s strani javnega sektorja, ki je zasebnemu naložila visoka pričakovanja glede zagotavljanja ustrezne informacijske varnosti. V procesu privatizacije se zasebni sektor v samem začetku ni organiziral v oddelke in agencije, ki bi skrbeli za specifična področja (kot je npr. organiziran javni sektor), ter ni razvil in sprejel mehanizmov, ki bi omogočali interakcijo organizacij (Watson 2007, 2–3). Manjkali so vzvodi in regulacije s strani javnega sektorja, ki bi moral zahtevati določeno stopnjo varnosti. Ključna infrastruktura je tako prišla v lastništvo oziroma upravljanje zasebnega sektorja, ki ga vodijo interesi delničarjev in dobičkonosnost. Lastniki in operaterji so previdno izbrali želene sisteme in tehnologijo, s katerimi upravljajo z določenim sektorjem. Mnogi so prešli na učinkovitejše generične programe, sisteme SCADA (Supervisory Control and Data Acquisition Systems), poleg pa so začeli uporabljati izdelke IKT iz komercialne ponudbe (osebni računalniki, operacijski sistemi, aplikacije …). S tem izdelki zadostujejo istim varnostnim standardom kot tisti, namenjeni osebni uporabi, razlika pa je seveda v posledicah morebitnih incidentov. Sistemi SCADA so s centralnim upravljanjem na daljavo povečali produktivnost in interoperabilnost mnogih industrij ter storitev. Kombinacija zasebnega lastništva in ranljivosti SCADA sistemov je ob priklopu na omrežje upravičeno sprožila mnoge pomisleke glede informacijske varnosti (Ericsson 2010, 1501–1504; Lewis 2015, 8; Carr 2016, 53–54).

Ključna infrastruktura je zaradi uporabe IKT postala bolj povezana in soodvisna, uporaba komercialnih izdelkov in storitev IKT z nezadostno varnostjo pa se lahko hitro spremeni v incident državnih ali celo mednarodnih razsežnosti. O pravicah in dolžnostih javnega in zasebnega sektorja je več napisano v poglavju Javno-zasebno partnerstvo na področju informacijske varnosti.

Priklop na internet in soodvisnost ne bi bila mogoča brez ponudnikov internetnih storitev. Ponudniki internetnih storitev (ISPs) so podjetja, ki posameznikom ali organizacijam

zagotavljajo internetne povezave in storitve. ISPs lahko nudijo tudi pakete programske opreme, spletne račune in spletne strani, ki jih lahko gostujejo ali izdelajo. ISPs so med seboj povezani prek dostopnih točk omrežja. Njihove funkcije vključujejo:

- prehodne komunikacije (ISPs kot prenašalci informacij),
- predpomnjenje sistema (pomembno za hitrost in učinkovitost interneta),
- shranjevanje informacij v sistemih ali omrežjih glede na zahtevo uporabnikov,
- orodja za lociranje informacij (iskalniki) (Usman 2013, 71–72).

Vloge ISPs se skladno s karakteristikami kibernetskega prostora nenehno širijo in spreminjajo, rezultat pa se izraža v večji ponudbi storitev. Vsak ponudnik mora zagotoviti določeno stopnjo varnega delovanja. Uporabniki prek interneta sporočajo osebne informacije, naloga ponudnikov pa je, da omogočijo zanesljive storitve in dostop do strani ter storitev, ki jih uporabniki želijo. Zaenkrat še ni zakonodaje, ki bi v podrobnosti opredelila dolžnosti ISPs na področju varnega dostopa do interneta, njihove naloge pa se dotikajo drugih področij zakonodaje (npr. Zakon o varstvu osebnih podatkov). Prednost ISPs je, da posedujejo znanje, napredno tehnologijo in izkušnje o aktualnih kibernetskih grožnjah. V primeru, da ISPs ne zagotavljajo dovolj varnega omrežja, posledice zajamejo na tisoče uporabnikov, med katerimi so tudi organizacije iz javnega sektorja (Usman 2013, 72–73).

5.2.2 Zasebni sektor kot proizvajalec IKT

5.2.2.1 Sektor proizvodnje strojne opreme IKT

Omenjeni sektor sodi pod sektor elektronike, ki je eden izmed največjih in najhitreje rastočih proizvodnih sektorjev. Razlog za hitro rast sektorja IKT je vedno večje udeleževanje držav v razvoju v mednarodnih omrežjih produktivnosti. Sektor proizvodnje strojne opreme zajema širok obseg elektronike, in sicer opremo za računalniško industrijo, kot so osebni računalniki, strežniki, sistemi za skladiščenje in prenosni računalniki. Proizvajalci originalne opreme (OEM) so podjetja, ki razvijejo in proizvedejo produkte, ki nosijo njihovo ime. Med največjimi na področju IKT so IBM, Hewlett Packard, Dell, Sony, Acer ipd. Včasih je strojna oprema veljala za steber varnosti, kar pa se je v zadnjih letih po več incidentih izkazalo za napačno predpostavko. Vgradnja t. i. stranskih vrat (ang. backdoor) je po več škandalih postala razlog za preplah in širjenje nezaupanja (Schipper in De Haan 2005, 5–12; Waksman 2014, 1–2).

Začetki proizvodnje segajo v 70. leta prejšnjega stoletja, ko so v Kaliforniji začeli s proizvajanjem integriranih vezij, mikroprocesorjev in kasneje osebnih računalnikov ter delovnih postaj. Največjo rast pri proizvodnji IKT je opaziti v novih industrializiranih državah, kjer prevladuje Azija. Azijske države (Singapur, Tajvan, Malezija, Tajska, Kitajska, Filipini, Indonezija in Indija) veljajo za nizkocenovne proizvodne enote, ki jim konkurirajo države Latinske Amerike (Mehika) in Vzhodne Evrope (Madžarska, Češka republika, Poljska, Romunija in Estonija). Kljub temu, da je industrija IKT načeloma obravnavana kot čisto delovno okolje, ki potrebuje visoko izobražene delavce, je realnost drugačna. Kot pri ostalih večjih proizvodnih obratih tudi tukaj delo opravljajo neizobraženi delavci, ki opravljajo nadure za nizko plačilo. Podjetja pa ne varčujejo le pri delovni sili, temveč tudi pri izbiri materialov. Znan je primer proizvodnje plošč s tiskanim vezjem, ki jih proizvajajo z uporabo strupenih kemikalij. Če povzamemo z nekaj besedami, sektor IKT sestavljajo večanje konkurenčnega pritiska, kratka življenjska doba produktov, zahtevne proizvodne verige, visok nivo »outsourcinga«, globalizirana omrežja proizvodnje, fleksibilnost, globalni vpliv, nižanje stroškov in selitev proizvodnje v države z nizkocenovno delovno silo (Schipper in De Haan 2005, 14–17; Corporate Computer Services 2016).

OEM nenehno proizvajajo nove produkte, da lahko ohranjajo svoj tržni delež in dobiček. Sama proizvodnja je večinoma preko pogodbe oddana drugim proizvajalcem (outsourcing), saj s tem ohranjajo konkurenčno prednost in zmogljivost hitrejšega prilagajanja tržnim spremembam. Pogodbene stranke zagotavljajo celovito storitev, saj ponujajo skupek oblikovanja, inženiringa, proizvodnje, logistike in po-proizvodnih storitev. S tem se OEM lahko posvetijo temeljnim nalogam, kot so raziskovalne in razvojne dejavnosti, prodaja, marketing ter trženje blagovne znamke; dizajn, proizvodnja in distribucija pa se prenesejo na pogodbene partnerje. Zaradi outsourcinga in ogromnega števila ljudi, ki so imeli dostop do strojne opreme, je težko zagotoviti ustrezen nadzor nad procesi proizvodnje (Schipper in De Haan 2005, 20–22; Waksman 2014, 11–13).

Temeljne značilnosti sektorja:

- Globalizirana proizvodna omrežja (osebni računalnik sestavlja strojna oprema, ki je proizvedena v različnih državah. Le-te med seboj tekmujejo glede višine plač, prednosti in spodbud, ki bi pritegnile investitorje, ni pa nujno, da se ozirajo na zaposlene, okolje, varnostne standarde in samo dobrobit države).

- Modularnost računalniške industrije (računalniki, strežniki in usmerjevalniki so sestavljeni iz standardnih komponent (čipi, pogoni, modemi …), ki so dobavljive na odprtem trgu. Omenjene komponente se tako nahajajo v več različnih računalnikih, saj so le-ti skupek tisočih različnih delcev. Med poceni ponudniki se pojavljajo tudi manjša podjetja, ki za nizko ceno nudijo proizvode slabe kakovosti.).
- Visok nivo outsourcinga (v IKT sektorju okoli 75 % podjetij prenese aktivnosti na zunanjega partnerja ali podizvajalca, katerim tudi prepustijo upravljanje dobavnih delov in delovne sile).
- Visoko konkurenčen sektor (cene IKT nenehno padajo, stopnja dobička proizvodnje pa je nizka, kar podjetja izrabljajo za upravičevanje selitve proizvodnje v države z nizkocenovno delovno silo) (Schipper in De Haan 2005, 20–21).

Globalizirana proizvodnja je posledica številnih novosti poslovanja večjih podjetij. Z nastopom vedno več novih OEM na trgu so se morala tista, ki so v celoti upravljala s proizvodi, prilagoditi novim specializiranim podjetjem, ki proizvajajo le določene komponente IKT (npr. Intel, Microsoft ipd.). Le-ta svoje produkte prodajajo različnim ponudnikom IKT, saj je računalniška industrija zelo modularna. Tako so tudi ostala podjetja začela z vertikalno specializacijo, kar pomeni, da so svojo proizvodnjo razdelila po segmentih in svoje produkte tržijo na visoko specializiranih tržnih segmentih, kjer želijo prevzeti vlogo vodilnega akterja. Prav tako so uvedla vertikalni razpad dobavne verige, kar pomeni, da so se zaradi želje po obvladovanju trga odrekla majhnim dobičkom proizvodnje in le-to prenesle na proizvajalce, s katerimi so podpisali pogodbo. Ti se nahajajo v različnih državah in spadajo pod različne regulatorne okvirje. S poznavanjem pomanjkljivosti regulatornega sistema je multinacionalnim podjetjem omogočen cenovno ugoden in hiter proces proizvodnje strojne opreme brez dodatnih postopkov varnostnega preverjanja. V podjetjih so ugotovili, da so plačani za razumevanje potrošnikovih potreb in distribucijo, zato so manj dobičkonosno proizvodnjo začeli predajati. V drugi polovici 90. let prejšnjega stoletja so OEM začela s prodajo celotnih proizvodnih linij in upravljanja z dobavno verigo pogodbenim proizvajalcem. Njihov cilj je bil doseg večjega tržnega deleža skozi industrijsko konsolidacijo. Pogodbenim proizvajalcem je proizvodnja (in logistika) glavna dejavnost, zato je tudi dobičkonosna. Tudi pri njih igra konsolidacija pomembno vlogo, saj preko nje pričakujejo večjo kupno moč, povečanje ekonomije obsega in manjšo izpostavljenost tržnim nihanjem. OEM morajo povečati fleksibilnost, biti pripravljena odgovoriti hitro se spreminjajočim trgom in tehnologiji s povečanjem ali zmanjšanjem proizvodnje zaradi

nižanja proizvodnih stroškov. Najučinkovitejši odgovor so našla v outsourcingu, ki jim omogoča:

- zmanjšanje proizvodnih stroškov, investicije in fiksne stroške – pogodbeni proizvajalci zagotavljajo OEM fleksibilno proizvodnjo brez potrebnih dodatnih investicij,
- fokusiranje na primarne dejavnosti (raziskave, razvoj, marketing, prodaja),
- dostop do globalnih proizvodnih storitev – preko pogodbenih proizvajalcev proizvajajo produkte na najcenejših lokacijah,
- istočasno proizvodnjo določenih produktov na več lokacijah hkrati, da so le-ti v bližini potrošnikov,
- hitrejši prodor na trg in doseganje proizvodnje velikega obsega,
- izboljšave upravljanja dobavne verige in kupne moči.

Pogodbeni proizvajalci so veliki potrošniki pri nakupu elektronskih komponent in ostalih materialov, tako da lahko zaradi povezave z dobavitelji izkoristijo ekonomijo velikega obsega in se pogajajo za nižje cene. V primerjavi s programsko opremo daje strojna oprema večji poudarek na varnost, saj bi bili stroški reklamacij previsoki, medtem ko pri programski opremi preprosto objavijo popravke in nadgradnje, ki po prodaji rešijo težave brez potrebnega vmešavanja proizvajalca (Schipper in De Haan 2005, 22–31; Waksman 2014, 20–21; Corporate Computer Services 2016).

5.2.2.2 Sektor razvijanja programske opreme IKT

Danes ima programska oprema dvojno vlogo; to sta vloga produkta in vloga sredstva za dostavo produkta. Programska oprema je pretvornik informacij, saj skrbi za njihovo izdelavo, upravljanje, pridobivanje, spreminjanje, prikazovanje ali prenos. Po drugi strani je osnovna komponenta nadzora računalnika (operacijski sistemi), komunikacije informacij (omrežja) in skrbi za izdelavo ter nadzor ostalih programov (orodja in okolja programske opreme). Programska oprema danes skrbi za najpomembnejši sestavni del, in sicer informacije. Skozi čas so se računalniki izjemno spremenili, povečale so se zmogljivosti in tudi možnosti. Za hiter razvoj so bile potrebne spremembe tudi na organizacijski ravni. Na samem začetku so programsko opremo razvijali samostojni programerji, kmalu pa so to vlogo prevzele organizirane skupine specializiranih strokovnjakov (Pressman 2005, 2–5). Nenehen razvoj je omogočil pridobitev in nadgrajevanje zmogljivosti, ki združujejo različne segmente

programske opreme. V zadnjem desetletju je znanje o razvoju programske opreme na voljo vsakemu posamezniku, ki ima željo in dostop do spleta. Razni portali, tečaji in ostale izobraževalne aktivnosti omogočajo hitro pridobivanje znanja, vnaprej pripravljene predloge pa enostavno odskočno desko za izdelavo lastne programske opreme, ki jo lahko nato delijo z ostalimi. Pomanjkanje izkušenj, ranljivost in ostali dejavniki zmanjšujejo varnost in omogočajo lažji dostop grožnjam (Cliff 2014).

Programska oprema predstavlja produkte z edinstvenimi karakteristikami, ki se ne morejo primerjati s produkti fizične narave. V ospredju razvoja sta predstava in logika. Poznamo več delitev programske opreme, splošno pa jo lahko razdelimo na:

- sistemsko programsko opremo,
- poslovno programsko opremo,
- znanstveno in inženirsko programsko opremo,
- vgrajeno programsko opremo,
- programsko opremo osebnih računalnikov,
- spletno programsko opremo,
- programsko opremo, ki skrbi za podatke v realnem času in
- programsko opremo umetne inteligence (Pressman 2005, 8–11).

Kot sem že zapisal, se razvoj programske opreme zelo razlikuje od gradnje strojne. Pri programski opremi je pomembno, da razvijalci, inženirji zelo natančno oblikujejo vizijo, ki jo opredelijo v razvojni strategiji. Le-ta mora vsebovati procese, metode, orodja in faze. Pojavljajo se različne definicije in poimenovanja procesa, npr. razvoj programske opreme, arhitektura programske opreme ipd. Tehnologijo programske opreme pa lahko v širšem pogledu razdelimo na 5 stopenj:

- specifikacija programske opreme (kaj bo zajemala),
- načrtovanje programske opreme (zamisli in načrti),
- programerske tehnike in orodja (na kakšen način),
- verifikacija in validacija programske opreme (varnost, ustreznost …),
- vodenje projektov razvoja programske opreme (vzdrževanje, dokumentacija …) (Kruchten in drugi 2006).

Razvoj programske opreme je socialni učni proces oziroma dialog, ki zbere vso potrebno znanje ter ga umesti v programsko opremo. Proces je interakcija med razvijalci, uporabniki in

orodji (Pressman 2005, 19–21). Za namen informacijske varnosti je v osnovi pomemben varen razvoj programske opreme, ki vsebuje določene varnostne mehanizme. Kmalu so se pojavile težnje po strukturiranemu razvoju programske opreme, s čimer se soočajo razni modeli, ki ocenjujejo razvoj in vzdrževanje življenjskega cikla programske opreme. Ključne karakteristike razvoja programske opreme so obseg, negotovost in interoperabilnost. Potreba po nekakšnem univerzalnem okvirju, ki olajšuje naštete karakteristike programske opreme, je privedla do razvoja standardov, strategij in modelov, ki so postopoma nastajali glede na potrebe in primere dobrih praks. Zelo pomembna je tudi komunikacija med različnimi razvijalci in uporabniki, saj tako izrazijo potrebe in vplivajo na nadaljnji razvoj. Eden izmed prvih modelov, ki je v začetku skrbel za razvoj programske opreme je bil CMM (Capability Maturity Model), danes pa je trg nasičen z raznimi modeli, ki ne zajemajo le programske, temveč tudi celotno organizacijsko kulturo organizacije. Tudi CMM se je sčasoma nadgradil v CMMI (Capability Maturity Model Integration), ki pokriva več spektrov organizacije in njenih procesov. Zasebni sektor ponuja mnogo izdelkov in storitev, ki optimizirajo delovanje organizacij, saj s tem dolgoročno izboljšajo učinkovitost in zmanjšajo stroške, čemur pripomore tudi ustrezen nivo informacijske varnosti (Pressman 2005, 24–25, 58–66; CMMI Institute 2016; Software Engineering Institute 2016).

Danes si ne moremo več predstavljati, da naša IKT ne bi bila povezana s spletom, samoumevne so nam storitve v oblaku, z malo znanja lahko sami urejamo vnaprej pripravljene predloge spletnih strani in aplikacij … Glede na relativno togo komercialno ponudbo programske opreme zasebnega sektorja v preteklosti, kjer so večja podjetja želela v rokah držati vse niti, danes sektor popušča pod težo iniciativ s strani računalniške skupnosti. Le-ta želi možnost sooblikovanja programske opreme in čim večji nadzor nad opremo, ki jo uporabljajo. Cenovno ugodna ali celo brezplačna programska oprema, spremenjena mentaliteta in poznavanje potrošnikov je zasebni sektor prisilila v alternativne metode udejstvovanja. Programska oprema mora zadostovati obstoječim standardom in okvirjem, veliko pa pripomorejo tudi vodilna komercialna podjetja. Le-ta izdajajo različne publikacije, smernice in primere dobrih praks, ki razvijalce usmerjajo k težnji po enotni strukturi in predvsem zahtevam po določeni stopnji varnosti. Kibernetski prostor programski opremi omogoča nenehno nadgrajevanje in raziskovanje novih funkcij. Danes sta posebej aktualna računalništvo v oblaku in odprtokodna programska oprema, ki zaenkrat s svojimi karakteristikami povzročata mnogo težav za strokovnjake, ki se spopadajo z uvedbo enotnih standardov, regulacije in pravnega okvira (Zissis in Lekkas 2010, 583; Open Source Initiative

2016). Le-ti se izražajo v sklopu raznih iniciativ, ki so večinoma prostovoljne, vendar se jih zasebni sektor med drugim udeležuje tudi zaradi komercialne privlačnosti za stranke. Iniciative predstavljajo obliko samoregulacije znotraj zasebnega sektorja, vendar kljub prednostim delovanja niso dovolj učinkovite. Organizacije zasebnega sektorja se prostovoljno odločijo za članstvo v specifični iniciativi, prostovoljen pa je tudi sprejem načel, ki jih širijo. Običajno se organizacija zasebnega sektorja odloči za članstvo zaradi javne podobe, saj imajo vedno bolj ozaveščeni potrošniki višje zahteve po varnosti IKT. Tako imamo na eni strani proizvajalce/razvijalce, ki na trg pošiljajo IKT z določeno stopnjo varnosti in zanesljivosti (IKT ustreza različnim standardom, protokolom ipd.), na drugi strani pa podjetja zasebnega sektorja, ki znotraj iniciativ s predpisanimi postopki poskrbijo za ustrezno informacijsko varnost organizacije, ki kupi te storitve. Po navadi prejmejo potrdilo o ustreznosti in spoštovanju normativ (npr. certifikat), sami procesi vpeljave in ocenjevanja zmogljivosti pa so plačljivi. Rezultat je večje zaupanje partnerjev, ta problematika pa ima velik potencial tudi za javni sektor, da postavi določene zahteve. Zasebna podjetja namreč dobavljajo IKT javnemu sektorju in organizacijam ključne državne infrastrukture, tako da so v določeni meri odgovorna za varnost in zanesljivost teh izdelkov. Ameriški minister za domovinsko varnost je leta 2014 poudaril, da bo v prihodnosti izjemno pomembno zaupanje med javnim in zasebnim sektorjem, ki ga bodo dosegli le s transparentnim delovanjem (Tadjdeh 2014).

5.2.3 Zasebni sektor kot povezovalno, svetovalno in izobraževalno telo

Prihodnost informacijske varnosti je ozaveščena javnost. Zasebni sektor se vključuje v javne debate in iniciative, ki ozaveščajo javnost ter obravnavajo dobre prakse. Organizacije, ki so nosilke iniciativ, se razlikujejo glede organiziranosti. V ZDA prevladujejo vladne organizacije, v EU pa nevladne. Za zasebne organizacije, ki delujejo na področju informacijske varnosti, je značilno, da se znotraj njih oblikuje skupnost strokovnjakov in entuziastov, ki prek forumov, blogov, člankov in srečanj izmenjujejo mnenja ter izkušnje. Nabrano znanje pripomore k temu, da se poznavanje težav in rešitev zanje ves čas dopolnjuje, kar tudi omogoča sledenje novim grožnjam in trendom. Nekatere skupnosti želijo znanje posredovati brezplačno, kar je odlična priložnost, da se z njim seznanijo tudi tisti, ki niso pripravljeni odšteti denarja za članstvo ali vsebino. Bolj poznane organizacije, ki nudijo tečaje, izobraževanja in certifikate s področja informacijske varnosti, so: Cybrary, Information Assurance Support Environment (IASE), InfoSec Institute, SANS Institute, FEMA National Training and Education Division, McAfee, Microsoft itd. (ENISA 2011).

5.2.4 Alternativni pristopi k regulaciji s strani zasebnega sektorja

Države, mednarodne skupnosti in razna združenja iščejo primerne mehanizme zagotavljanja informacijske varnosti. Medtem, ko je »tradicionalna varnost« opredeljena v obstoječih zakonodajah, na področju informacijske varnosti še niso našli primernega mehanizma. Le-ta bi moral opredeliti minimalno informacijsko varnost pri ključnih akterjih, določiti dolžnosti in pravice ter tudi opredeliti sankcije za nespoštovanje. Kot sem zapisal v prejšnjem poglavju, sta javni in zasebni sektor preveč različna, da bi popustila pod pritiskom nasprotnega. Regulacije so tako postale nekakšen krizni odgovor na vzpon kibernetskega kriminala in grožnj, regulatorji pa se soočajo z raznimi težavami. Še vedno je težavna oblika regulacije, soglasje sodelujočih in predvsem priznavanje avtoritete, zato so obstoječe regulacije bolj ali manj svetovalne narave (PWC 2015, 1–2).

Ključna infrastruktura je podvržena raznim regulacijam, ki opredeljujejo zahteve po varnosti, manjkajo pa regulacije, ki bi se specifično posvetile področju uporabe varne IKT, informacijske varnosti organizacij in nujnih ukrepov za višanje le-te. Regulacija IKT mora zajeti mnogo različnih aspektov, od regulacije programske opreme, deljenja informacij, varovanja informacij, poseganja v zasebnost … Gre za zelo širok okvir in prvi korak predstavljajo regulacije na področju deljenja informacij in znanja med javnim in zasebnim sektorjem, organizacijami ter tudi državami članicami v zavezništvih (European Council 2016; White in Halpert 2016).

Na voljo je več tipov regulacije, in sicer: tradicionalna regulacija, alternativne oblike regulacije (samoregulacija, ko-regulacija) in drugi pristopi.

5.2.4.1 Tradicionalna regulacija

Državna oblast se na politiko po navadi odzove z regulacijo, sestavljeno iz pravno obvezujočih pravil, ki jih morajo državljani ali organizacije upoštevati. Splošna opredelitev regulacije je pravilo ali ukaz za upravljavce ali vlado oziroma skupek pravil in standardov, ki opredeljujejo sprejemljivo in pričakovano obnašanje ter hkrati postavljajo omejitve dovoljenemu. Načeloma gre za prisilna pravila s strani avtoritete, ki ima kompetence in moč, da uveljavlja ubogljivost. Regulacija se na področju IKT in delitve informacij ni izkazala za dovolj učinkovito, zato strokovnjaki predlagajo alternativne oblike (Haufler 2001, 8; ENISA 2015, 27). Več o regulaciji je napisano v 7. poglavju: Skupni napori za zagotavljanje državne informacijske varnosti.

5.2.4.2 Alternativne oblike regulacije

a) Ko-regulacija je mehanizem, kjer zakonodajalec zaupa cilje specifične politike, ki so zapisani v zakonodaji ali drugih dokumentih, strankam, ki delujejo na tej sferi (npr. socialnim partnerjem, nevladnim organizacijam ipd.). Tako gre za sodelovanje oblasti in zakonodaje s partnerji, ki skrbijo za operativne zmogljivosti. Primer ko-regulacije je Uredba (EU) št. 1025/2012 Evropskega parlamenta in sveta glede evropske standardizacije, kjer lahko sodelujejo Evropska komisija, standardizacijske organizacije, industrija, podjetja in ostali deležniki družbe (EUR-LEX 2012).

b) Samoregulacija običajno zajema skupino gospodarskih subjektov, kot so podjetja določene industrije ali skupine strokovnjakov, ki prostovoljno razvijajo pravila ali kodekse ravnanja. Ta so namenjena regulaciji oziroma vodenju obnašanja, aktivnosti in standardov članov. Skupina, ki jih razvija, običajno tudi skrbi za vpeljavo in ubogljivost med člani. Obstaja več vrst samoregulacije, najpogostejša je tržno usmerjena. Samoregulacija se lahko izraža v obliki protokolov, kodeksov ipd., največja težava pa je pomanjkanje moči nadzornikov, ki nimajo vladne in pravne podpore. Gre predvsem za prostovoljno upoštevanje. Najvidnejši primer samoregulacije so kodeksi ravnanja, sem pa spadajo tudi programi upravljanja, organizacijski modeli ipd., ki vsebujejo zahteve revizije, računovodstva, nadziranja in poročanja o delovanju. Podjetja so se začela povezovati v razne asociacije, ki se običajno povezujejo tudi z nevladnimi organizacijami in skupaj razvijajo ter implementirajo nove standarde (Haufler 2001, 13–14; ENISA 2015, 28).

5.2.4.3 Ostali pristopi

Sem spadajo predvsem ozaveščanje, informacije in izobrazba glede določene tematike. Informacije hitro dosežejo želene naslovnike, vplivajo na njihovo znanje in percepcijo ter poskrbijo, da se informacije nadalje širijo po raznih notranjih mrežah. Sem spadajo tudi razne iniciative, programi ozaveščanja o nevarnostih kibernetskega okolja, pozivi k prijavi groženj, incidentov itd. (ENISA 2015, 29). Programi se velikokrat izvajajo pod okriljem organizacij, ki aktivno sodelujejo pri razvoju samoregulacije in ko-regulacije.

5.2.5 Primeri alternativnih oblik regulacije zasebnega sektorja

V zadnjih nekaj desetletjih je večina večjih multinacionalnih korporacij skupaj z nekaterimi manjšimi začela z razvijanjem novih kodeksov obnašanja, ki so postavili standarde za opravljanje aktivnosti. Trend zadnjih let je tudi prispevek k družbi, natančneje razni ekološko in socialno obarvani programi, zaradi česar med drugim zasebna podjetja sklepajo partnerstva z neprofitnimi organizacijami. Samoregulacija industrije z mehanizmi za dosego kolektivnega cilja (z ali brez javnega sektorja) predstavlja potencialen vir globalnega upravljanja. Njihov vpliv je lažji tudi zaradi bolj omejene regulacije s strani držav, ki vedno več odgovornosti prelagajo na zasebni sektor. Zasebni sektor ima interes za samoregulacijo in sprejem prostovoljnih standardov tudi zaradi tega, ker veljajo kot legitimni pristop pri boju z mednarodnimi pravili, pritiskom raznih aktivističnih gibanj, večajo konkurenčnost in dobro ime organizacij ter tvorijo ideje za dosego dolgoročne dobičkonosnosti. Tudi državnim oblastem je v interesu, da postanejo ukrepi samoregulacije legitimni, saj z njimi zaščitijo družbo pred škodljivimi aktivnostmi. Pomanjkljivost samoregulacij je v prostovoljnosti ter tudi v pomanjkanju nadzora in odgovornosti. Če zasebni sektor ne izpolnjuje zapisanih obveznosti in dosega javnih ciljev, javni sektor pa je popolnoma brez moči, bi lahko samoregulacijo označili kot nelegitimno in nedemokratično (Haufler 2001, 1–3).

Pri nakupu programske opreme se potrošniki soočajo z mnogimi informacijami glede kakovosti, ustreznosti, interoperabilnosti in varnosti izdelka. Proizvajalci/razvijalci z uporabo priznanih postopkov ali modelov zagotovijo določeno stopnjo varnosti in pridobijo potrebno zaupanje. Enako velja za končne uporabnike, ki želijo v svoji organizaciji implementacijo varnostnih mehanizmov, postopkov in varne IKT. Spodaj je naštetih nekaj najbolj prepoznavnih in najučinkovitejših iniciativ ter asociacij, ki skrbijo za razvoj in življenjski cikel varne programske opreme, razvoj in implementacijo varnostnih mehanizmov v organizacije in širijo znanje o informacijski varnosti.

5.2.5.1 OWASP Comprehensive, Lightweight Application Security Process (CLASP)

Iniciativa, ki nudi strukturiran pristop k integriranju elementov varnostnih procesov v zgodnjih fazah življenjskega cikla programske opreme (SDLC). Sestavljen je iz petih vidikov:

1. vidik konceptov (pojasnjene so interakcije med komponentami procesov CLASP),
2. vidik, ki temelji na vlogah (pojasnjene so vloge, ki so zahtevane s strani varnostnih projektov),

3. vidik ocene aktivnosti (ocena aktivnosti CLASP se poda skladno z vidikom ranljivosti),
4. vidik implementacije aktivnosti (opravijo se aktivnosti, ki so bile naštete v vidiku ocene aktivnosti),
5. vidik ranljivosti (identificirajo se ranljivosti in protiukrepi) (OWASP 2016).

Cilj te iniciative je večanje obsega dostopnosti varne opreme.

5.2.5.2 Microsoft Security Development Lifecycle (SDL)

Gre za proces varnega razvoja programske opreme, ki ga sestavljajo obvezne varnostne aktivnosti, razporejene po fazah tradicionalnega SDLC. Cilj je pomoč razvijalcem, da gradijo varnejšo programsko opremo, in soočanje z zahtevami varnostnih predpisov ter hkrati nižanje stroškov razvoja (ENISA 2011, 25–27; Microsoft 2014).

Model je sestavljen iz sedmih faz:

1. usposabljanje (osnovno varnostno usposabljanje),
2. zahteve (opredelitev in integracija osnovnih varnostnih zahtev, najnižjih še sprejemljivih nivojev varnosti, opredelitev in odprava hroščev ter ocena tveganj varnosti ter zasebnosti),
3. dizajn (določitev zahtev dizajna, analiza potencialnega področja napadov in omejitev dostopa, vzpostavitev strukturiranega pristopa k upravljanju z grožnjami),
4. implementacija (uporaba in objava odobrenih orodij, izogib nevarnim funkcijam in nadomestilo z varnimi alternativami, statična analiza),
5. verifikacija (dinamično testiranje, »fuzz« testiranje in ponovni pregled potencialnega področja napadov),
6. objava/izdaja (priprava načrta odziva na morebitne nove grožnje, končni varnostni pregled, arhiviranje podatkov in certifikacija izdelka),
7. odziv (izpeljava aktivnosti, skladnih z načrtom odziva na morebitne grožnje) (Microsoft 2014).

SDL je skupek dobrih varnostnih praks in se nenehno razvija. Na začetku je bil namenjen le Microsoftovim izdelkom, kjer je 2004 postal obvezna direktiva. Nekaj let kasneje so ga pod Microsoftovo licenco predstavili javnosti, leta 2010 pa je pridobil tudi licenco Creative Commons, ki omogoča fleksibilnejše ravnanje z avtorskimi pravicami postopka in je tako razvijalcem na voljo za kopiranje, distribucijo in prenos. Cilj je vpeljava določenih standardov

v razvoj programske opreme, saj so programi, aplikacije ipd. v medsebojni interakciji in pomanjkljivosti enega vplivajo na varnost vseh ostalih (Seltzer 2010; Microsoft 2014).

Microsoftovo profesionalno omrežje na področju SDL zagotavlja sredstva širitve metodologije do skupnosti razvijanja programske opreme in jim hkrati omogoča sodelovanje ter izmenjavo idej. Omrežje sestavljajo svetovalci, organizacije, ki nudijo usposabljanja, in ponudniki orodij, ki so strokovnjaki na področju metodologije SDL in različnih tehnologij. Svoje storitve nudijo tudi ostalim podjetjem, ki želijo v svoje procese implementirati metodologijo SDL (ENISA 2011, 25–27; Microsoft 2014).

5.2.5.3 Software Assurance Maturity Model (SAMM)

SAMM je odprt okvir, ki pomaga organizacijam, da formulirajo in implementirajo strategijo varnosti programske opreme, primerno za specifična tveganja. Projekt OpenSAMM je aktivnost OWASP in je namenjen:

- evalvaciji obstoječih praks s področja varnosti programske opreme,
- izgradnji uravnoteženega programa, ki preverja in zagotavlja varnost,
- demonstraciji konkretnih izboljšav s področja zagotavljanja varnosti,
- opredelitvi in meritvam aktivnosti, ki so povezane z varnostjo (ENISA 2011, 27; OpenSAMM 2016).

5.2.5.4 The Systems Security Engineering Capability Maturity Model (SSE-CMM)

SSE-CMM je referenčni model, ki je osredotočen na zahteve implementacije varnosti v sistem. Promovira integracijo disciplin varnega inženiringa (sistemov programske in strojne opreme). The International Systems Security Engineering Association (ISSEA) je neprofitna mednarodna organizacija in skrbi za ohranjanje modela SSE-CMM ter povezanega materiala. SSE-CMM je prepoznan kot mednarodni standard ISO/IEC 21827 (ENISA 2011, 28; ISO 2016).

Model sestavlja 11 območij varnosti, ki se osredotočajo na nadzor, grožnje in odkrivanje ter odpravljanje ranljivosti. To so:

1. upravljanje z varnostnimi kontrolami,
2. ocena vpliva,
3. ocena varnostnega tveganja,
4. ocena grožnje,

5. ocena ranljivosti,
6. argument o zagotovilu varnosti (opredelitev in dosega ciljev varnostnih potreb),
7. koordinacija varnosti,
8. nadzor varnostne drže,
9. zagotovilo varnostnega prispevka,
10. opredelitev varnostnih potreb,
11. preverjanje in potrditev varnosti (ENISA 2011, 28).

5.2.5.5 Building Security in Maturity Model (BSIMM)

BSIMM je zbirka aktualnih idej in aktivnosti s strani podjetij, ki razvijajo programsko opremo. Je študija obstoječih iniciativ s področja zagotavljanja varne programske opreme. Misija BSIMM je meriti aktivnosti, ki se izvajajo skladno z obstoječimi iniciativami, da bi na ta način omogočili načrtovanje, izpeljavo in meritev rezultatov lastnih iniciativ tudi ostalim akterjem. Gre za primerjavo izdelka z varnostnimi standardi industrije. Model je nastal skozi proces razumevanja in analiziranja podatkov izkušenj z varnostjo programske opreme devetih podjetij, ki jih je nato potrdil in prilagodil s podatki dodatnih 21 podjetij. Do sedaj so izmerili že več kot 104 podjetja. Uporabljajo deskriptivni model, ki temelji na dejstvih; rezultat je poročilo z opazovanji. BSIMM je razvil Software Security Framework (SSF), ki nudi skupen jezik za opis najpomembnejših elementov okvira varnosti programske opreme znotraj podjetja (ENISA 2011, 29–32; BSIMM 2016).

Model sestavlja 112 aktivnosti, ki so povezane v štiri domene:

1. upravljanje (prakse, ki pomagajo pri organizaciji, upravljanju in meritvah okvira varnosti programske opreme; sem spada tudi razvoj osebja),
2. znanje (zbirka korporativnega znanja, ki se uporablja pri izvajanju varnostnih aktivnosti programske opreme skozi organizacijo),
3. SSDL Touchpoints (dobre prakse, povezane z analizo in zagotovitvijo določenega razvoja, produktov in procesov programske opreme. Vse metodologije varnosti programske opreme vsebujejo te prakse, zajemajo oceno kode in analizo arhitekture.),
4. uvajanje (prakse, ki so stičišče tradicionalne omrežne varnosti in vzdrževanja programske opreme. Konfiguracija, vzdrževanje in ostale dejavnosti programske opreme imajo neposreden vpliva na varnost.) (BSIMM 2016).

5.2.5.6 Iniciativa OWASP (Open Web Application Security Project)

OWASP je nastala leta 2004 kot neprofitna dobrodelna organizacija v ZDA, ki poudarja varnost v aplikacijah. Je mednarodna organizacija, ki nudi brezplačna orodja, dokumente in udeležbo na raznih forumih. Spodbuja udeležbo vseh, ki jih zanima to področje, prav tako pa aktivno sodeluje na globalnem področju varnosti spletnih aplikacij. Razdeljena je na mnogo lokalnih sekcij, med katerimi imajo svojega predstavnika skoraj vse države EU. OWASP omogoča članom, da v okviru organizacije objavijo iniciative, projekte, debate ipd. Skupnost OWASP aktivno sodeluje znotraj teh projektov, saj so člani gonilna sila le-teh. Varnost aplikacij obravnavajo v okviru treh sklopov, to so: ljudje, procesi in tehnologija. Objavljajo dokumente in orodja s treh glavnih področij:

- varovanje pred napakami dizajna in njihovo zaznavanje,
- implementacija ter
- varnost življenjskega cikla.

OWASP prireja letne konference in objavlja tudi dokument z naslovom TOP 10, ki po mnenju mednarodnih strokovnjakov opozarja na deset najbolj ključnih pomanjkljivosti spletnih aplikacij (ENISA 2011, 4–7; OWASP 2016).

5.2.5.7 IEEE Computer Society (CS)

IEEE CS je mednarodna neprofitna akademska organizacija. Sekcija CS je namenjena IKT. Gre za organizacijo z nameni znanstvene, literarne in izobraževalne narave. Glavni projekti so namenjeni objavljanju standardov na področju IKT. Produkti iniciative so razne knjige, konference, publikacije, revije, spletni tečaji, certifikati, standardi in tehnični dnevniki (ENISA 2011, 10–11; IEEE Computer Society 2016).

5.2.5.8 International Society of Automation (ISA)

ISA je mednarodna neprofitna organizacija, ki razvija standarde za industrijo, certificira strokovnjake, zagotavlja usposabljanja in izobraževanja, objavlja knjige in tehnične članke ter vodi konference in predstavitve (ENISA 2011, 14–15; ISA 2016).

5.2.5.9 Software Assurance Forum For Excellence In Code (SAFECODE)

Zasebna iniciativa, ki so jo vzpostavili razvijalci in prodajalci programske opreme. Teži k povečanju zaupanja v izdelke IKT, kar želijo doseči z vpeljavo raznih metod, ki zagotavljajo

varno programsko opremo. SAFECode poudarja, da lahko industrija programske opreme dostavi varnejšo in zanesljivejšo programsko opremo, strojno opremo in storitve. Produkti iniciative so dokumenti z dobrimi praksami, ki vključujejo tudi življenjski cikel programske opreme.

V prihodnosti želi SAFECode še dodatno povečati vpliv na naslednjih področjih:

- identifikacija in deljenje dokazanih dobrih praks,
- promocija širše implementacije teh praks v kibernetski prostor,
- sodelovanje z vladami in s ponudniki ključne infrastrukture, da bi lahko vplivali na sedanje prakse, ki dopuščajo preveč tveganj (ENISA 2011, 15–16; SAFECode 2016).

5.2.5.10 SANS Software Security Institute (SSI)

SANS SSI je mednarodna akademska iniciativa, ki nudi usposabljanja, certifikacijo in arhiv raziskav ter iniciativ skupnosti, ki so namenjena razvijalcem, programerjem in upravljavcem varnosti aplikacij. Cilj je zagotoviti čim višjo stopnjo varnosti programske opreme. SANS SSI zbira in s pomočjo bloga, novičnikov, člankov in dokumentov objavlja aktualne informacije o tehničnih zadevah, ranljivostih in napadih. SSI je raziskovalna in izobraževalna organizacija, ki nudi programe z namenom širitev varnega kodiranja in življenjskega cikla razvoja programske opreme. Objavlja tudi letno poročilo o 25 najbolj nevarnih napakah programiranja (ENISA 2011, 16–18; SANS 2016).

5.2.5.11 Web Application Security Consortium (WASC)

Mednarodna neprofitna organizacija, ki pripravlja dobre prakse spletnih aplikacij. Njen cilj je razvijati, izbrati in zagovarjati standarde za varnost spletnih aplikacij (ENISA 2011, 19–20; Web Application Security Consortium 2016).

5.2.5.12 SANS Institute

SANS je ameriško zasebno podjetje, ki je specializirano na področju informacijske varnosti in kibernetske obrambe. Poleg širokega nabora tečajev imajo tudi knjižnico relevantnih raziskav in člankov ter sistem, znotraj katerega člani beležijo zlonamerne aktivnosti, ki ogrožajo informacijsko varnost. Leta 1999 so osnovali Global Information Assurance Certification (GIAC), skupek certifikatov, ki velja za enega izmed bolj priznanih na tem področju. Deluje mednarodno (SANS 2016).

5.2.5.13 CIS (Center for Internet Security)

CIS je ameriška neprofitna organizacija, ki želi okrepiti informacijsko varnost javnega in zasebnega sektorja. Deluje na področju ZDA. S pomočjo močnih partnerstev z vladnimi in zasebnimi organizacijami želi CIS izboljšati globalno informacijsko varnost. Zbira najboljše prakse, pripravlja rešitve za kibernetske incidente in gradi skupnosti, ki želijo omogočiti zaupanje v kibernetski dimenziji. Znotraj CIS deluje center MS-ISAC (Multi-state Information Sharing & Analysis Center), ki dela na izboljšavah informacijske varnosti državnih, lokalnih in teritorialnih oblasti. Z interakcijo med člani zasebnega in javnega sektorja in Ministrstvom za domovinsko varnost ZDA zagotavlja ključne informacije (Center for Internet Security 2016).

5.2.5.14 InfoSec Institute

InfoSec Institute je inštitut, ustanovljen leta 1998, ki nudi širok spekter tečajev in možnosti certificiranja. Gre za podobno organizacijo, kot je SANS, saj sodelujejo razni strokovnjaki, javnosti pa nudijo dostop do virov, ki sledijo aktualnim trendom na področju informacijske varnosti (InfoSec Institute 2016).

5.2.5.15 McAfee

Zasebno podjetje, ki nudi izdelke in storitve s področja varovanja informacijskih sistemov, deluje pa tudi na področju ozaveščanja ter izobraževanja. Primer tega so tečaji Foundstone (MCAFEE). Tečaji nudijo celovito izobraževanje, ki pomaga pri razvoju varne programske opreme in aplikacij, ocenitev ranljivosti in obrambo pred kibernetskimi grožnjami ter ključne veščine s področja računalniške forenzike, ki omogočajo boljši odziv na incidente (Intel Security 2016).

5.2.5.16 Cybrary

Cybrary je skupnost, ki teži k čim višji informacijski varnosti. Gre za mlado organizacijo, ki je nastala šele leta 2015. Člani želijo doseči, da postane industrija s področja informacijske varnosti dostopnejša za vse, ki imajo željo po znanju na tem področju, ne samo za tiste z denarjem. Cybrary je nekakšen skupek ljudi, podjetij in treningov, ki omogoča brezplačno sodelovanje vseh zainteresiranih s področja izobraževanja o informacijski varnosti. Nudijo brezplačen dostop do učnih elementov in vsebine s strani izkušenih zaposlenih na področju

informacijske varnosti, teoretikov in podjetij, ki pripravljajo novosti s področja informacijske varnosti (Cybrary 2016).

6 JAVNO-ZASEBNO PARTNERSTVO NA PODROČJU INFORMACIJSKE VARNOSTI

6.1 Opredelitev

Informacijska varnost predstavlja enega izmed največjih izzivov informacijske dobe. Vpliva na državno varnost, ekonomijo, človekove pravice in svoboščine ter pravne okvirje. Po dolgoletnem razvijanju raznih mehanizmov in pristopov so države začele razvijati strategije kibernetske varnosti. Mnogo držav ima velik delež ključne infrastrukture v rokah zasebnega sektorja. Dokumenti, ki opredeljujejo obveznosti in pravice akterjev, temeljijo na javno-zasebnem partnerstvu (JZP), varnostnem mehanizmu, skozi katerega zmanjšujejo grožnje. V ZDA in raznih mednarodnih partnerstvih je prav JZP opredeljeno kot temelj strategij kibernetske varnosti. Države se srečujejo s podobnimi kibernetskimi grožnjami, razlikuje pa se nivo pripravljenosti nanje in spekter varnostnih mehanizmov. Medtem, ko nekatere države opozarjajo na grožnje, spet druge ne posvečajo dovolj pozornosti in sredstev v večanje informacijske varnosti. Soodvisnost in povezanost raznih sektorjev ključne infrastrukture na državni ravni se izraža tudi v interakciji z drugimi državami, kar pomeni, da interna grožnja posamični državi lahko kmalu preraste v grožnjo partnerskim državam. Pobudo za obvezni dvig informacijske države so tako prevzele mednarodne vladne organizacije. Na področju informacijske varnosti je JZP večplastno. Vlade imajo različne odnose s ponudniki internetnih storitev (ISPs), korporacijami, zasebnimi varnostnimi podjetji, organi pregona, organizacijami s področja človekovih pravic, državljani itd. JZP na tem področju se pogosto obravnava preveč enoplastno, kjer vse te različne skupnosti obravnavajo kot eno entiteto – zasebni sektor. V JZP na področju informacijske varnosti se kot ključne akterje v zasebnem sektorju omenja lastnike/operaterje ključne infrastrukture, ki je osnova državne varnosti (Commission of the European Communities 2009, 3–11; European Commision 2013b; Carr 2016, 43–45).

Za razvoj JZP je torej potrebno medsebojno sodelovanje, ki pa ne more biti uspešno brez zaupanja in izmenjave tajnih informacij. Za uspešno partnerstvo je potrebno jasno razdelati ključne težave, s katerimi se dandanes sektorja soočata, in sicer:

- skupno načrtovanje,
- spodbujanje novih oblik JZP,

- razčistiti, kdo skrbi za informacijsko varnost zasebnega sektorja,
- balansiranje delitve stroškov med zasebnim in javnim sektorjem,
- razvoj izvedljivega pristopa, ki bi omogočal državi, da lahko z odgovornostjo deli zaupne podatke o informacijski varnosti z zasebnim sektorjem (Farwell 2012, 22–34).

Upad vlaganja denarja v razvoj obrambne industrije se je pojavil že v 80. letih prejšnjega stoletja, ko se je končevalo obdobje hladne vojne, dokončne temelje pa so prinesle direktive Clintonove administracije. Osnovno vodilo je postala relokacija investicij. Denar, ki so ga namenjali raziskavam in razvoju obrambne industrije, so v 90. letih namenili komercialnim tehnologijam s ciljem, da le-te presežejo investicije v vojaško tehnologijo v času hladne vojne. S tem se je oblikovalo JZP na področju raziskav in razvoja komercialnih tehnologij. Clintonova administracija je poudarjala pomembnost zasebnega sektorja na področju IKT. Le-tega so opredelili kot edinega, ki ima sposobnosti in veščine za upravljanje kompleksnih procesov razvoja novih tehnologij in dostavljanje na trg, država pa igra ključno vlogo pri omogočanju teh naporov zasebnega sektorja. Z globalizacijo so se začele razvijati potrebe po mednarodnem regulacijskem okvirju, kar pa so države postopoma in neorganizirano začele prepuščati v roke zasebnega sektorja (Haufler 2001, 12–15; Carr 2016, 47–48).

Z začetkom obširne privatizacije so države spletle različne načine sodelovanja z zasebnim sektorjem. Zasebni sektor sicer poseduje primere dobrih praks in učinkovitost s področja gospodarstva, vseeno pa sam ne more skrbeti za državno informacijsko varnost in državne interese. Že sama besedna zveza JZP poudarja skupne dolžnosti in medsebojno zaupanje. Za informacijsko varnost so izjemno pomembne državne strategije kibernetske varnosti, ki identificirajo potencialne grožnje. Akterji so glede na dejavnosti v kibernetskem okolju razdeljeni v štiri večje skupine, to so:

- konvencionalni kibernetski kriminal (klasične kriminalne dejavnosti, ki se dogajajo s pomočjo IKT),
- politično in vojaško vohunstvo (kraja vojaških oziroma politično relevantnih podatkov in informacij),
- gospodarsko vohunstvo (kraja intelektualne lastnine podjetij) in
- kibernetski konflikt oziroma bojevanje (asimetrično bojevanje v kompleksnem prostoru) (Flynn Goodwin in Nicholas 2013, 7–8).

V kibernetskem okolju jih je dosti težje prepoznati in ujeti, saj znajo zakriti izvor napada. Za uspešno reševanje groženj so tako potrebni skupni napori obeh sektorjev, ključnega pomena pa je hitra izmenjava informacij. Napori se izražajo tudi na nivoju mednarodnih organizacij. Za magistrsko delo je posebej zanimiv dokument EU Sporočilo o zaščiti kritične informacijske infrastrukture (CIIP) iz leta 2009, kjer se je Komisija dotaknila izzivov prihodnosti. Nujna je potreba po novem modelu upravljanja. Države članice bi še zmeraj morale biti zadolžene za pripravo politik na področju ključne informacijske infrastrukture, sama implementacija pa bi se morala izvajati skupaj z zasebnim sektorjem, ki si lasti velik delež prej omenjene infrastrukture. Kot rešitev je Evropska komisija izpostavila JZP na evropski ravni, ki pa še vedno ni uspešno realizirano. Predlog je bil, da bi se razvil okvir upravljanja na evropski ravni, kjer bi s pomočjo agencije ENISA zasebni sektor sodeloval pri pripravi in operativnih dejavnostih strategij javnega sektorja. S takšnim pristopom bi se sektorja lažje usklajevala in pripravila realno izvedljive politike (Commission of the European Communities 2009, 3–11; European Commision 2013a).

Poleg pojmovanja napadalcev sta glede na državne kibernetske strategije držav Zahoda nepopolno urejeni še dve izjemno pomembni sferi, to sta gospodarstvo in zaščita ključne infrastrukture. Ključna infrastruktura je običajno razdeljena na sektorje, ki so v pristojnosti različnih vladnih agencij ali ministrstev, lastništvo oziroma operativne dejavnosti pa v rokah zasebnega sektorja. JZP je glede na okoliščine pričakovano sredstvo za doseganje varnosti. Od države se pričakuje odgovornost za zagotavljanje državne varnosti. Ključna infrastruktura igra zelo pomembno vlogo za državno varnost in posledice večjega kibernetskega napada vsekakor sprožajo skrbi pri državnih oblasteh. Po drugi strani so v upravljanju oziroma lastništvu zasebnega sektorja, kar pomeni, da lahko ustrezno informacijsko varnost sektorja zagotovi le s skupnimi napori. Kot rešitev se je pojavila težnja po JZP, ki bi morala biti skupek samoregulacije industrije, najboljših praks in koordinacije na področju deljenja informacij z vlado. JZP ima razne definicije in opredeljuje različne dogovore, od skupnega zagotavljanja storitev z delnim vladnim nadzorom (npr. zdravstvo) do pogodb z zunanjimi izvajalci na projektih infrastrukture (gradnja zgradb, mostov, gostovanje evropskih športnih prvenstev, Olimpijskih iger ipd.) (Ericsson 2010, 1501–1504; Lewis 2015, 8; Carr 2016, 53–54).

Klasifikacija in identifikacija partnerskih dogovorov sta po navadi opredeljeni znotraj okvirjev avtoritete in odgovornosti. Wettenhall je definiral dve širši kategoriji odnosov znotraj JZP, to sta:

- horizontalni dogovori brez hierarhije, ki so oblikovani s soglasnim sprejemanjem odločitev,
- hierarhično organizirani odnosi, kjer ima ena stranka vlogo nadzornika (Wettenhall 2003, 90).

Kot »pravo JZP« je opredelil prvo kategorijo.

6.2 Prednosti in slabosti javno-zasebnega partnerstva

Do težav pri JZP na področju informacijske varnosti je prišlo že v samem začetku, saj so se politiki izogibali oblikovanju in poostritvi državne zakonodaje na področju informacijske varnosti, na drugi strani pa se je zasebni sektor otepal odgovornosti in obveznosti pri zagotavljanju državne varnosti. Zaradi tega vloge akterjev niso dobro opredeljene, posledično pa ni pripeljalo do učinkovitih rešitev. Tradicionalno velja, da je zagotavljanje državne varnosti osrednja naloga države, področje informacijske varnosti pa je bilo v domeni zaprtih skupnosti članov iz vojaške, akademske in IT sfere. Danes prihaja do dilem držav, ki »morajo« skladno s strategijami prepustiti določen delež odgovornosti organizacijam, ki so tržno usmerjene. Ključno pričakovanje partnerstva je deljenje aktualnih informacij s strani obeh sektorjev, vendar se JZP sooča z mnogimi ovirami. Zasebni sektor težko nemudoma razlikuje med tehnično težavo, manjšim napadom ali napadom večjega obsega. Poročanje ranljivosti lahko škodi komercialnim interesom, posebej v primeru, ko jim zaznava le-te daje konkurenčno prednost. Informacije, ki jih zasebni sektor deli, bi lahko javni sektor delil s konkurenco. Poslovni model organizacij zasebnega sektorja temelji na pridobivanju, držanju in prodaji informacij, ne deljenju. Z dilemami pri deljenju informacij se srečuje tudi javni sektor. Tajni podatki ne smejo biti posredovani do oseb, ki nimajo ustreznih varnostnih pooblastil. Po drugi strani marsikdaj ne smejo ukrepati na podlagi teh informacij, da jih ne bi razkrili. Potrebno je zaupanje, saj javni sektor omogoča (določen) dostop do baz podatkov, ki so tajne, po drugi strani pa se mora zanašati na informacije s strani zasebnega sektorja, ki jih je le-ta pripravljen deliti v okviru partnerstva/projekta. Za sodelovanje pri izmenjavi tajnih informacij morajo organizacije zasebnega sektorja zagotoviti ustrezno informacijsko varnost. Od javnega sektorja se pričakujejo natančne informacije, kar pomeni, da morajo iti skozi razne postopke preverjanja, ki upočasnjujejo prenos časovno pomembnih informacij. V zasebnem sektorju se je izkazalo, da gre za veliko boljše sodelovanje in deljenje informacij med zaposlenimi iz različnih organizacij, če imajo le-ti močan osebni ali profesionalni odnos. Človeški faktor igra veliko vlogo, vendar ga politike s področja informacijske varnosti

zaenkrat še ne upoštevajo dovolj. Dobri, trdni odnosi bodo olajšali potrebne procese. Dosedanja JZP so že nakazala na določene izboljšave v odnosih, cilji pa so naslednji: večje poenotenje ciljev obeh sektorjev, večje zaupanje, skupen pristop k problematiki in razvoj učinkovitih metod, ki zmanjšajo stroške (Čaleta 2011, 49–50; Farwell 2012; ENISA 2014, 6–8; D'Elia 2015, 10; Carr 2016, 58).

Dunn-Cavelty in Brunner sta opredelila implikacije informacijske dobe na mednarodno politiko, in sicer sta izpostavila dva trenda z vplivom na varnost, ki sta nastala kot posledica tehnološkega razvoja in zmanjšujeta pomembnost države. To sta *večanje internacionalizacije* in *večanje privatizacije*. Trenda sta zajeta v opredelitvi JZP na področju informacijske varnosti, močno pa vplivata na dojemanje vlog držav in zasebnega sektorja ter hkrati razmerja med razvojem gospodarstva in državne varnosti. Lahko bi rekli, da je fokus javnega sektorja usmerjen na težave, zasebni sektor pa se prilagaja danim priložnostim (Dunn-Cavelty in Brunner 2007, 8–10; Dillon in ostali 2010, 230–231; Farwell 2012).

Partnerstvo je običajno uspešno, če so ključne odločitve sprejete in opredeljene v načrtu pred samim partnerstvom, zapisani dosegljivi cilji, določene stimulacije za partnerje, če imajo le-ti jasno začrtane odgovornosti in se spremlja napredek. Strategije in razni dokumenti s področja informacijske varnosti za eno izmed ključnih sredstev poudarjajo deljenje informacij. Le-to je osnova za koncepte JZP, vendar ga je potrebno natančno opredeliti. Za učinkovitost je potrebno predstaviti vse izzive, s katerimi se soočata sektorja, njuna pričakovanja, odgovornost in avtoriteto. Zelo pomembno je tudi zaupanje. Države se izogibajo predlogom po hierarhičnih odnosih pri JZP ter poudarjajo skupne napore in interese. Z nejasno opredelitvijo odnosov otežujejo zaznavanje skupnih izzivov in groženj, saj dajejo vtis, da so izzivi in grožnje enaki za oba sektorja, kar pa na podlagi izkušenj iz prakse ne drži. Zasebni sektor obravnava izzive informacijske varnosti kot finančne in domnevne, torej ne kot javno skupno dobro, kar vodi državne oblasti. Stephen Linder je opredelil različne uporabe pojma JZP (glede na težave in cilje, ki povzročijo nastanek JZP); za področje informacijske varnosti lahko uporabimo dva tipa, in sicer partnerstvo kot reforma upravljanja in partnerstvo kot delitev moči (Linder 1999, 42; ENISA 2014, 10; Carr 2016, 54–59).

6.2.1 Partnerstvo kot reforma upravljanja

Partnerstvo kot reforma upravljanja se nanaša na pričakovanje, da bodo vladni upravljavci prevzeli logiko upravljavcev zasebnega sektorja in preusmerili fokus z administrativnih procesov na bolj komercialne in fleksibilne pristope, torej posle, ki privlačijo kapital.

Omenjena perspektiva je grajena na predpostavki, da je trg superioren in stimulira inovacije ter kreativno reševanje težav. Takšen pristop je izrazit predvsem v dokumentih ZDA, ki poudarjajo pomembno vlogo in potrebo po vodenju s strani zasebnega sektorja pri zagotavljanju informacijske varnosti. V zahodnih državah se pojavlja mnenje, da oblast nima ne avtoritete ali zmogljivosti, da bi lahko zagotavljala ustrezno informacijsko varnost. Po Linderju je JZP v tem primeru reforma upravljanja, vendar oblasti zavračajo potrebne spremembe, ki so del definicije. Javni sektor namesto sprememb poudarja dva prepričanja:

1. zasebni sektor mora sprejeti odgovornost in obveznosti za varnost lastnih omrežij,
2. fleksibilnost in inovacije zasebnega sektorja le-tega postavljajo v boljši položaj, da se soočajo z zagotavljanjem informacijske varnosti (Linder 1999, 42–43; Carr 2016, 55).

S strani zasebnega sektorja se pojavlja nova težava. Obe tezi nekako držita, vendar je vpletena tudi državna varnost, saj so nekatera omrežja zasebnega sektorja zelo pomembna zanjo (uporablja jih tudi ključna infrastruktura). Zasebni sektor razvija lastne strategije kibernetske varnosti, ki se ne skladajo z vladnim konceptom, ki kot središče opredeljuje »javno dobro«. Odločitve se oblikujejo znotraj poslovnega modela, ki se razvija glede na dobiček in interese delničarjev. Kot odgovor na opredelitev njegove vloge podaja naslednja dva pomisleka:

- Stroški zagotavljanja informacijske varnosti na nivoju državne varnosti bi bili izredno visoki.
- Družba zahodnih držav (še posebej ameriška) je preveč prepirljiva in industrija bi se upirala sprejetju odgovornosti za izdelke in sisteme (Carr 2016, 55–56).

To, kar je najboljše za družbo na področju informacijske varnosti, ni nujno najboljše tudi za organizacije zasebnega sektorja, ki jih žene dobiček. Lastniki zasebnega sektorja sprejemajo odgovornost za varovanje sistemov, dokler ocenjeni stroški grožnje presegajo stroške varnostnih mehanizmov. Varnostni mehanizmi so večinoma namenjeni napadom manjšega obsega (npr. samostojnim hekerjem), niso pa ustrezni za spopad z napadom na državni ravni. Mnogi še vedno trdijo, da mora za večje napade na državni ravni s strani organiziranega kriminala, teroristov in ostalih državnih groženj poskrbeti državna oblast, bodisi z organi pregona ali državno obrambo. Na področju informacijske varnosti je zelo razdeljen tudi javni sektor, ki ga tvori veliko število akterjev, kot so obveščevalne službe, preiskovalni organi, obrambni sektor, odzivne sile itd. Za nekakšno osnovo sklepanja partnerstev velja, da se zanjo odločita stranki, ki sami ne moreta doseči začrtanih ciljev. Ali obe stranki potrebujeta pomoč za dosego lastnih ciljev ali pa gre za finančni dogovor, ki naredi partnerstvo privlačno za obe.

Obstoječa JZP se srečujejo s težavami, kot so nejasno začrtane vloge in odgovornosti, pomanjkanje zaupanja, različni jezik (tehnološki in birokratski), različni interesi in pričakovanja. Partnerstvo s fokusom na delitvi informacij zaradi informacijske varnosti je tako nekakšna posebnost. Sicer ima finančne priložnosti (plačilo informacij o ranljivostih ipd.) in nekaj skupnih iniciativ, vendar nobena komponenta ne prevladuje (ENISA 2014, 3; D'Elia 2015, 10; Carr 2016, 56–57).

6.2.2 Partnerstvo kot delitev moči

Ostane nam druga Linderjeva perspektiva, to je partnerstvo kot delitev moči, ki temelji na sodelovanju, kjer zaupanje zamenja težaven odnos do regulacije ukazovanja in nadzora. Mora biti tudi nekaj skupne delitve odgovornosti, znanja in tveganja. Obe stranki doprineseta nekaj, kar ima vrednost za drugo, pričakuje pa se tudi pogajanje glede zadev, ki bi jih sicer bilo zelo težko doseči. Ta perspektiva bi ustrezala prej navedenim opredelitvam obstoječega JZP na področju zagotavljanja informacijske varnosti, ki temelji na sporni namesto deljeni odgovornosti. Pričakuje se delitev znanja, krepitev zaupanja in sodelovanja (Linder 1999, 74; Carr 2016, 57–58).

Do podobnih ugotovitev je pri pregledu delovanja evropskega JZP prišla ENISA, ki je po intervjujih s sodelujočimi opredelila naslednje rešitve:

- Vodstvo bi bilo učinkovito, če bi ustrezalo pristopu upravljanja, s katerim so se strinjali udeleženci. Potrebna je tudi vzpostavitev strukture odgovornosti, ki bi spremljala napore udeležencev.
- Financiranje bi moralo biti sorazmerno z napori in vloženim časom udeležencev. Spodbude, kot so lastništvo ciljev projekta, zmanjševanje izpostavitve grožnjam ipd., bi morale biti uporabljene za izboljšanje udeležencevega razmerja med stroški in koristmi.
- Izkupiček iniciativ bi se moral obravnavati na mednarodni ravni, čeprav je nastal zaradi težave na ravni države. Večina težav s področja informacijske varnosti ima vzor ali implikacije na mednarodni ravni.
- Ustrezno je potrebno opredeliti pravila vključitve v JZP.
- Udeležba mora biti omejena glede na učinkovite in proaktivne prispevke h glavnemu cilju. S tem bi se zagotovila skladnost ciljev in rezultatov partnerstva (ENISA 2014, 6).

6.3 Primer dobre prakse v EU

Primerov dobrih praks je ogromno, kar sem izpostavil že v poglavju *Primeri alternativnih oblik regulacije zasebnega sektorja*. Kot sem že omenil, je informacijska varnost tesno povezana z globalizacijo. Določene države še vedno ne želijo vlagati več sredstev, zato so pobudo sprejela zavezništva. Opredelil bom poskuse EU, saj to zavezništvo najbolj neposredno vpliva na Republiko Slovenijo in njen razvoj zmogljivosti. Glavni akter je agencija ENISA, ki deluje kot osrednje telo na področju informacijske varnosti v EU in državah članicah. V nadaljevanju bom omenil tudi poskus EU za JZP – EP3R in povzel ugotovitve ter izkušnje, ki so jih pridobili v nekaj letih delovanja. Le-te so osnovno vodilo nadaljnjega razvoja JZP v EU, kot tudi za Slovenijo.

6.3.1 ENISA

Agencija Evropske unije za varnost omrežij in informacij (ENISA) je organizacija, ki predstavlja bazen znanja o evropski kibernetski varnosti. ENISA asistira EU in državam članicam, da razvijejo ustrezno znanje in mehanizme za odkrivanje, preprečevanje in odzivanje na grožnje informacijski varnosti. Sodeluje pri pripravi pravnih aktov in politik na področju informacijske varnosti, prav tako pa nudi strokovno pomoč in pomoč organizacijam javnega in zasebnega sektorja na ravni držav članic ali EU. Osrednji fokus sicer namenja javnemu sektorju, hkrati pa se aktivno udeležuje izmenjave informacij in znanja z vsemi ostalimi akterji s področja informacijske varnosti (ENISA 2016).

»ENISA ima tudi močno mrežo deležnikov iz javnega in zasebnega sektorja, ki ji pomagajo na naslednjih področjih:

- Strokovno znanje: predvidevanje in podpora Evropi pri soočanju z novimi izzivi na področju varnosti omrežij in informacij ob upoštevanju razvoja digitalnega okolja.
- Politike: pomoč državam članicam in institucijam EU pri razvoju in izvedbi politik, ki so potrebne za izpolnjevanje pravnih in regulativnih zahtev nacionalne informacijske varnosti.
- Zmogljivost: podpora Evropi pri izboljšanju najsodobnejših zmogljivosti na področju varnosti omrežij in informacij.
- Skupnost: izboljšanje sodelovanja med državami članicami in med skupnostmi s področja nacionalne informacijske varnosti« (ENISA 2016).

Njena naloga je tudi organizacija evropskih vaj s področja kibernetske varnosti, pomoč pri pripravi državnih strategij kibernetske varnosti in tesno sodelovanje z drugimi mednarodnimi organizacijami, ki so povezane z informacijsko varnostjo. Redno objavlja publikacije in letna poročila o delu, kjer so zapisane pomembne informacije o aktualnem stanju informacijske varnosti (ENISA 2016).

6.3.2 Evropsko javno-zasebno partnerstvo za odpornost (EP3R)

EP3R je potekalo med letoma 2009 in 2013, to je bil prvi poskus evropskega tovrstnega partnerstva. ENISA je izdala poročilo, v katerem je zapisala pomembne ugotovitve, ki jih je pridobila od članov. Izjavili so, da je JZP dragocena možnost naslovitve različnih tipov kompleksnih problemov, da se JZP lahko prilagaja danim situacijam, vpliva na sprejemanje odločitev (večja moč zasebnemu sektorju), da je učinkovitost pristopa odvisna od stopnje lastništva projekta in da je »bottom-up« pristop nujen za ustrezno soočanje s problematiko, dosego rezultatov in ohranjanje interesa sodelujočih (ENISA 2014, 4–5).

EP3R je na področju JZP uveljavil:

- pristop vodenja, ki temelji na koordinaciji udeležencev,
- shemo financiranja glede na čas in napore udeležencev,
- pričakovane rezultate, ki so strogo povezani z deljenjem informacij, identifikacijo prioritet politik, opredelitvijo varnostnih standardov ključne informacijske infrastrukture in promocijo varnosti ter dobre prakse odpornosti,
- prostovoljno udeležbo, ki temelji na zaupanju, in
- pravila vključitve glede na profil deležnikov (le-ti morajo biti iz ustrezne sfere) (ENISA 2014, 12).

7 SKUPNI NAPORI ZA ZAGOTAVLJANJE DRŽAVNE INFORMACIJSKE VARNOSTI

7.1 Pristop k regulaciji

IKT sektor je relativno nov pojav. V preteklosti je glavno vlogo igral telekomunikacijski sektor, ki je v preteklih letih doživel ogromno sprememb. Dokler je bil v rokah javnega sektorja, so vladni organi s pravno podlago zagotavljali standarde in smernice, ki jim ni bilo mogoče oporekati. Mnogi javni operaterji so bili privatizirani in v sektorju je začela prevladovati liberalizacija, ki je spodbujana z evolucijo novih tehnologij in storitev, večanjem pomembnosti telekomunikacij za pomen državnega gospodarstva in razvoj mednarodnega poslovanja. Potreba po regulaciji se je zaradi hitre razširitve med ljudmi najprej pojavila v okviru elektronskih komunikacij, ki so doživele korenite spremembe. Države zadnja leta pospešeno iščejo rešitve, kako regulirati varnost IKT opreme, iščejo soglasje pri oblikovanju politik, ki bi opredelile vlogo IKT in organizacij, ki jo uporabljajo, ter celovit pristop k informacijski varnosti. Regulatorni okvirji s področja elektronske komunikacije posredno zajemajo uporabo IKT, posvečajo pa se tudi konkurenčnosti in tržnim zakonitostim, kar zanima zasebni sektor. V preteklosti je pripadala regulacija IKT pod agencije, ki so že regulirale pošto, telegrafske storitve in telekomunikacije. Le-te so tudi dale podlago za razvoj novih politik, določile so tehnične standarde, razvile in potrdile opremo, nadzorovale radijski spekter, upravljale s sredstvi, sprejemale odločitve na področju investicij, določale ceno, dodeljevale privilegije in izvajale vpliv nad državnimi komunikacijskimi administracijami. Vse to se je začelo postopoma spreminjati v 80. in 90. letih prejšnjega stoletja, ko se je s pomočjo hitro se razvijajoče tehnologije začela interakcija novih poslovnih priložnosti in večjih institucionalnih sprememb. V tem času je telegraf izgubil na pomembnosti, pošta in telekomunikacije pa sta postala ločeni sferi, ki sta načeloma imeli svoje regulatorje. Konec leta 2009 je 153 držav oziroma administrativnih območij ustanovilo državne regulatorje za IKT in telekomunikacijske sektorje. Funkcije in jurisdikcije omenjenih regulatorjev se skladno s trendi gibljejo proti liberalizaciji, v okviru katere so državni operaterji delno ali v celoti preneseni v zasebni sektor. To je posebej izrazito v telekomunikacijskih sektorjih, prav tako pa tudi v poštnem in informacijskem. S privatizacijo podjetja prenesejo lastnino in odgovornost v že obstoječih organizacijah iz državnega v zasebni sektor, prav tako pa je odprt trg za nove, komercialne ponudnike. Tako je v večini držav prišlo do spremembe v strukturi sektorja, in sicer iz monopolnega v konkurenčnega. IKT je »prisilila« države, da so

posodobile obstoječe regulacijske okvire. To so storile s sprejemom novega pravnega okvira in ustanovitvijo novih regulacijskih teles, ki implementirajo pravni in regulacijski okvir. Do podobne situacije je prišlo v ostalih sektorjih ključne infrastrukture, kjer pa se varnosti IKT ni posvečalo zadostne pozornosti. V novih pravnih okvirjih so določeni regulatorji in njihove pristojnosti (Scott 2002, 6; AKOS 2016; Carr 2016; ICT Regulation Toolkit 2016).

Regulacija sektorja elektronskih komunikacij je bila primarno namenjena konkurenčnosti trga, saj so želeli odpraviti tradicionalni monopol državnih operaterjev. V primeru regulacije konkurenčnega trga IKT opreme (kjer kljub široki ponudbi prevladuje manjše število multinacionalk) bi lahko zadostila marsikaterim vprašanjem, ki trenutno onemogočajo sprejem soglasja. Konkurenčnost trga namreč ne pomeni, da le-ta več ne potrebuje regulacije, temveč ravno nasprotno. Regulacija se poveča, ko država omogoči konkurenčnost, še posebej v začetni fazi, ko želijo zagotoviti učinkovitost. Za to fazo je v sektorju IKT zaradi stopnje razvoja že prepozno, vseeno pa je naloga regulatorjev, da razvijejo regulacijski okvir, ki omogoča reševanje sporov, zlorab konkurenčnosti, varuje potrošnike in teži k državnim ciljem, kot so varnost, univerzalni dostop, konkurenčnost industrije ali ekonomska produktivnost in rast. Naslednja faza bi morala biti določitev institucij/-e, ki bo implementirala odločitve. Največ težav se običajno pojavi pri pripravi osnutkov predlogov in kasneje sprejetju okvira. V primeru tradicionalne državne regulacije bi moral to biti organ javnega sektorja, ki ga opredeljuje pravo. V relativno kratkem obdobju morajo odgovorni razrešiti zadeve, kot so ustrezni standardi, univerzalni dostop in storitve, regulacijski procesi, sredstva reševanja sporov, metodologija tržnih opredelitev, avtorizacija postopkov in principov določanja tarif. Večina teh težav se hkrati nanaša tudi na ostale komponente regulacijskega telesa, tako da se le-to lahko spreminja skladno s tržnim in tehnološkim razvojem. Priporočila sektorja telekomunikacij lahko prenesemo tudi na področje varnosti IKT in državne varnosti. Kot sem že napisal v poglavju Javno-zasebno partnerstvo na področju informacijske varnosti, javni sektor od zasebnega v JZP poleg deljenja informacij pričakuje tudi izpolnjevanje načrtov in priporočil, kar pa se je do sedaj zaradi trenutne regulativne ureditve na področju IKT izkazalo za neučinkovito. V kolikor bi bilo uresničevanje načrtov na želenem nivoju, ne bi bilo potrebe po državni regulaciji. Eden izmed razlogov je tudi ta, da zasebni sektor v primeru zagotavljanja nezadostnih storitev ni toliko odgovoren za informacijsko varnost, kot bi na istem mestu bil javni sektor, od katerega se pričakuje zagotovitev javne blaginje. V okviru večjih institucionalnih sprememb so nastale neodvisne institucije, ki opravljajo vlogo regulatorja v kontekstu novih politik IKT v

specifičnem sektorju. Regulacije se spreminjajo in nadgrajujejo kot odgovor na tržne in tehnološke spremembe. JZP ne omejuje regulacije. Lahko pride do konfliktov interesov, še posebej, če so interesi zasebnega sektorja izven normativnih ciljev. V tem primeru mora država spremljati in regulirati dejavnosti ter tako poskrbeti, da želja po dobičku ne preseže načrtovanih storitev. V primeru informacijske varnosti se od zasebnega sektorja pričakuje, da bo zaradi javnega interesa v varnostne mehanizme vlagal več sredstev, kot jih je pripravljen na podlagi analize stroškov in koristi. Stimulacije trga niso dovolj, da bi lahko spodbujale takšen nivo varnosti, zato sta poleg stimulacij potrebna nadzor in določena stopnja regulacije. Primarna regulacija mora biti sestavljena iz okvira, ki bo uporabljen za regulacijo sektorja. Le-ta mora biti v čim večji meri izdan s strani pravnih instrumentov, da se prepreči razveljavitev s strani državnih organizacij. S tem se zagotovita stabilnost in predvidljivost. Jasno morajo biti definirani ključni elementi okvira, kot so vzpostavitev regulatorja, njegove pravice in dolžnosti, moč izvrševanja ter zmogljivost sankcioniranja. Mnogi strokovnjaki poudarjajo, da zasebni sektor v aktivnostih državnih kibernetskih strategij ne sodeluje bolj poglobljeno, ker oblast ni pripravila dovolj prepričljivega poslovnega primera, ki bi zasebni sektor prepričal v investicije. Dunn-Cavelty in Suter priznavata pomembnost JZP, vendar mora priti do sprememb pri opredelitvi konceptov in organizaciji. Predlagata spremembe v vodenju in politiki varnosti. Le-ta bi morala biti grajena na samoregulaciji in samoorganiziranih omrežjih. S tem bi se vloga državne oblasti spremenila iz nadzora v koordiniranje omrežij in izbiranje sredstev, da bi ta omrežja opravljala naloge varovanja ključne infrastrukture (Dunn-Cavelty in Suter 2009, 180; Carr 2016, 59–61; ICT Regulation Toolkit 2016).

Koristi regulacij so:

- gospodarska rast,
- zagotovitev določene stopnje varnosti,
- večje število investicij,
- nižje cene,
- kakovostnejše storitve,
- prodor na trg in
- hitrejši porast tehnoloških inovacij v sektorju (ICT Regulation Toolkit 2016).

7.1.1 Mednarodni vpliv na regulacije

IKT omogoča globalizacijo ter s tem tudi skupek mednarodnih in čezmejnih regulacijskih izzivov. Vloga mednarodnih zavezništev na področju regulacije nikakor ni zanemarljiva. Zavedajo se, da je težko uskladiti pravice in dolžnosti sektorjev na državni ravni, še težje pa spremeniti obstoječe državne pravne okvirje. Skupne iniciative in zavezujoče pogodbe bistveno pripomorejo k pospešitvi dejavnosti na državni ravni. Predlog direktive Evropskega parlamenta in sveta o ukrepih za zagotavljanje visoke skupne ravni varnosti omrežij in informacij v Uniji je dober primer dokumenta. Cilj je, da EU in države članice s skupnimi močmi dosežejo visoko skupno raven varnosti omrežij in informacij (VOI). Ključ za uspeh je v interakciji sodelujočih akterjev in večanju zmogljivosti, prav tako pa v regulativnih spremembah, ki bodo odpravile zakonodajne pomanjkljivosti. Predlog obravnava dva nova pristopa k VOI, to sta regulativni (zakonodajni predlog k vzpostavitvi skupnega pravnega okvira EU pri zmogljivostih držav članic, mehanizmih evropskega sodelovanja in skupek zahtev za ključne akterje javnega in zasebnega sektorja) in mešani (kombinacija regulativnih zahtev in prostovoljnih iniciativ). Kot učinkovitejši pristop so na samem začetku opredelili regulativni okvir, saj so izkušnje pokazale, da v primeru prostovoljnega spoštovanja regulacij sodeluje le nekaj držav, ki imajo visoko VOI, medtem ko se ostale izogibajo investicijam v VOI. Uveljavitev in spoštovanje določenih minimalnih zahtev VOI morajo sprejeti vse države članice in znotraj njih vsi akterji s tega področja, pri razvoju in vpeljavi pa jim pomaga agencija ENISA. Države morajo sprejeti tudi določene varnostne standarde, ki zagotavljajo specifično raven varnosti IKT. Direktiva določa obveznosti za države članice pri postopkih preprečevanja, obravnavanja in odzivanja na tveganja ter incidente, ki imajo vpliv na omrežja in informacijske sisteme, vzpostavlja mehanizem za sodelovanje med državami članicami in določa varnostne zahteve za sodelujoče akterje javnega in zasebnega sektorja (European Commision 2013b).

Velik korak se je v zadnjih nekaj letih zgodil na področju delitve informacij o kibernetskih grožnjah in incidentih. Delitev informacij je po prepričanju mnogih strokovnjakov osrednji temelj boja proti kibernetskim grožnjam. ZDA in EU sta tej tematiki posvetili največ pozornosti in sprejeli pomembne dokumente, ki zavezujejo organizacije k sodelovanju. EU je že leta 2005 izpostavljala nujnost, da se koordinirajo napori glede zaupanja deležnikov v elektronskih komunikacijah in storitvah, ter leta 2006 sprejela dokument za varno informacijsko družbo. Vlogo svetovalnega in koordinacijskega telesa so predali agenciji ENISA, začele so se iniciative za spremembo obstoječe zakonodaje, pozivi k zagotavljanju

informacijske varnosti, sodelovanje z ZDA, Natom in razvoj kapacitet za izmenjavo informacij. Poleg razvoja zmogljivosti je za države članice ključna komunikacija. Države so uvedle nacionalne točke (CERT), ki so zadolžene za interakcijo in hitro posredovanje informacij. V dokumentu so objavili akcijski načrt za prihodnost, ki bi pripravil varnostne mehanizme (Commission of the European Communities 2009, 3–11; European Commision 2013a; AKOS 2016; Carr 2016, 6; ICT Regulation Toolkit 2016).

7.1.2 Regulatorji

Regulacijska telesa so osrednji mehanizem izvajanja regulacije, vendar njihovo delovanje ne zajema le pravic in dolžnosti. Regulatorji lahko pomagajo pri soočanju z globalno ekonomsko krizo, saj igrajo ključno vlogo pri višanju samozavesti, zmanjševanju tveganja in spodbujajo investicije v IKT sektor. Imajo dve ključni vlogi, in sicer v obliki paketa finančnih spodbud in JZP ter nižanja stroškov poslovanja, implementirajo pa tudi pravila, ki večajo učinkovitost sodelujočih. Za učinkovitost regulatorjev je ključna neodvisnost (v določeni meri). Namen vzpostavitve neodvisnih regulacijskih institucij na primeru telekomunikacij temelji na nediskriminatorni obravnavi vseh akterjev na liberalnem trgu, kar doseže s štirimi zahtevami poslovanja:

1. sodelovanje mora biti omogočeno v konkurenčnem okolju, saj se s tem omogočijo enaki konkurenčni pogoji med neenakovrednimi subjekti na trgu,
2. vsi dobavitelji IKT opreme se morajo obravnavati enako na trgih, kjer prevladuje kupec, ki ima predhodna močna razmerja z določenimi dobavitelji,
3. vsi novi udeleženci in investitorji morajo biti obravnavani enako s strani dominantnega konkurenta, ki bo prevzel vlogo »nadzornika« v poslovanju za nove udeležence;
4. vse stranke morajo imeti pravico, da izrazijo pritožbe in interese, ki morajo biti nato ustrezno naslovljeni (ICT Regulation Toolkit 2016).

Da bi zasebni sektor upošteval regulacije, je torej potrebno vzpostaviti funkcionalno in ugodno okolje (katerega del so tudi regulatorji in regulacije), ki bo privabilo zadostno število trajnostnih investicij, s katerimi bi zadovoljili povpraševanje, povečali zalogo in predstavili nove storitve. Javni sektor mora prilagoditi svoj model poslovanja in ga približati zasebnemu. Neodvisnost veča zaupanje investitorjev in zmanjšuje regulacijsko tveganje, vendar to ne sme biti popolna neodvisnost. Regulatorji ne smejo slediti lastni agendi, vplivu raznih lobijev in političnim interesom, temveč morajo implementirati določeno vladno politiko (pri tem morajo

poskrbeti, da proces regulacije ni spolitiziran) in sprejemati le tiste odločitve, ki so skladne z njihovimi pristojnostmi. Gre za nekakšno de facto neodvisnost. Na neodvisnost namreč še vedno vplivajo 3 dimenzije, to so: status regulatorja (dolžina mandata, možnost obnovitve, formalni odnosi z drugimi organizacijami …), odnos z izvoljenimi politiki (ali je neodvisnost formalna, opredelitev obveznosti) in finančna/organizacijska neodvisnost (kdo financira, ali lahko razvija svoja telesa ipd.). Regulatorji služijo kot nekakšni posredniki med vlado in tistimi, ki jih regulacija zajema (Gilardi in Maggetti 2011, 202–204; ICT Regulation Toolkit 2016).

Regulatorji morajo doseči ravnovesje med neodvisnostjo in odzivanjem na širše cilje politike, ki jo izvajajo. Omenjeno ravnovesje se lahko doseže s sledečimi varovali:

- izbira regulatorja z ločeno avtoriteto, ki ni pod nadzorom ministrstva,
- natančno opredeljeni strokovni kriteriji za imenovanje,
- pri procesu imenovanja morata biti vključena izvršna in zakonodajna veja oblasti,
- imenovanje regulatorjev za določeno obdobje in prepoved njihove odstranitve (razen v primeru točno določenih razlogov),
- člani odborov morajo imeti časovno različne termine opravljanja funkcije, da jih vsako novo vodstvo ne more menjati naenkrat,
- zanesljiv in ustrezen vir financiranja (optimalno brez možnosti političnega vmešavanja),
- ustrezna plača uslužbencev, ki pritegne najsposobnejše strokovnjake in zmanjša možnost korupcije,
- prepoved izvršni veji, da ovrže sprejete odločitve (razen če niso skladne z zakonom) (ICT Regulation Toolkit 2016).

7.2 Pravna regulacija in regulacija programske opreme

Za informacijsko varnost ni dovolj le splošna regulacija, posebej se bo potrebno posvetiti tudi posebnostim kibernetskega okolja, kjer prevladuje programska oprema. Pri soočanju z regulacijo programske opreme imajo strokovnjaki veliko težav z obstoječimi pravnimi okviri, ki niso bili pisani za tako abstraktno področje. Regulacija programske opreme je težje obvladljiva, saj pravna ureditev nima dovolj sredstev, da bi lahko ves čas dohajala spremembe dinamičnega kibernetskega okolja. Na področju kibernetske zakonodaje delujeta dva ključna dejavnika, in sicer tradicionalno pravo ter zmogljivosti in omejitve programske opreme. V

poznih 90. letih prejšnjega stoletja so razni akademiki trdili, da tehnologija igra ključno vlogo pri regulaciji. Lawrence Lessig je objavil, da vsi vemo, kako deluje pravo v realnem življenju (preko pravnih aktov in institucij), v kibernetskem prostoru pa moramo razumeti, kako deluje koda (programska in strojna oprema, ki omogočata kibernetski prostor) in kako regulira kibernetski prostor. William Mitchell je izjavil, da v kibernetskem okolju velja: koda = zakon (code = law) (Grimmelmann 2005, 1721; Wagner 2005, 459).

Skozi študije se je pokazalo, da imata pravna in programska koda regulatorne učinke, da sta povezani ter da je končna regulacija produkt pravne regulacije in regulacij programske opreme. Programske kode lahko s svojimi zmogljivostmi in omejitvami vplivajo na obstoječe regulacije oziroma tvorijo lastne, vendar je pomembno, v kakšnem odnosu so s pravnimi regulacijami. V primeru, da pride do odstopanj med regulacijami, torej da regulirata na različne načine (glede na moč, pomanjkljivosti, stroške in koristi), lahko pride do raznih pravnih zapletov. Stična točka programske opreme in prava je ravnovesje med raznimi regulacijskimi učinki, na katere imajo vpliv pravo, tehnološke okoliščine ter zasebne analize stroškov in koristi. Obstajajo področja IKT, ki zakonsko niso ustrezno (dovolj) urejena in jih zato regulira programska oprema ter obratno. Obe vrsti regulacij se torej dopolnjujeta in tudi vplivata druga na drugo. Novosti v tehnološkem okolju bodo spodbudile določene spremembe pravne ureditve, ki lahko povečajo ali zmanjšajo obseg regulacij. Programska oprema, ki se uporablja v specifičnih sektorjih (npr. letalstvo, medicina), je regulaciji podvržena že od samega začetka, saj sektor ne omogoča uporabe pomanjkljive programske opreme. Gre torej za osnoven odnos med pravom in programsko opremo, pravno in programsko kodo, odvetniki in programerji, da sprejemalcem odločitev zagotovijo izziv in ustrezno nagrado za upoštevanje regulacije (Wagner 2005, 460–463; Bush 2007, 44–48).

Pri sprejemu novih politik je potrebno upoštevati tudi odziv regulacije programske opreme, ki ga je sicer težko predvideti ex-ante. Nove spremembe pravnih politik morajo ustrezno predvideti odziv regulacije programske opreme, ker se zaradi napačnih predpostavk lahko izjalovi celotna politika. Posebnost kibernetskega okolja je dinamičnost (spremembe tehnologije, inovacije ipd.), ki vrši pritisk nad stičiščem pravne in regulacije programske opreme. V kibernetskem okolju ne moremo regulirati dejavnosti le z obstoječimi pravnimi predpisi, temveč je potrebno najti optimalno kombinacijo omenjenih regulacij in nato opraviti ustrezno evalvacijo normativnih učinkov (kakšen je uspeh predpisa) in instrumentalnih učinkov (kako dobro vpliva predpis na stičišče med pravom in programsko opremo). Sprejemalci politik se soočajo z dvema večjima težavama. Prva je pomanjkanje ustreznega

znanja in izkušenj analitikov, ki ne poznajo kibernetskega prostora, kot bi ga morali. Programska oprema uporablja specifičen jezik, orodja in platforme. Četudi zberejo ekipo strokovnjakov, se morajo še vedno soočiti z dnevnimi spremembami IKT, kar pomeni, da morajo, zaradi relativno dolgega časa sprejema želene politike, ustrezno predvideti nadaljnji razvoj in trende, kar je skoraj nemogoče. IKT je v nekaj letih postala milijardni posel in omogoča razvoj trendov, ki jih pravni strokovnjaki ne morejo predvideti (npr. družbeni trendi, kot so vpliv družbenih omrežij, blogi, aplikacije, piratstvo ipd.). Prišteti je potrebno tudi nestalnost programske opreme. Na določenih področjih je sprejeto ravnovesje med regulacijama (npr. avtorske pravice glasbenikov, ki so regulirane s pravom in upravljanjem digitalnim vsebin), ki pa se zaradi razvoja tehnologije pomika k regulaciji programske opreme (Wagner 2005, 474–477; Warrier 2010).

Regulacija programske opreme ima tudi temno plat, in sicer negativno javno podobo v primerjavi s pravno regulacijo. Glavne razlikovalne lastnosti so:

- Programiranje – regulacija programske opreme deluje v relativno stalni, strogi obliki, ko pride do določanja rezultatov. Vse dejavnosti so vodene s strani programiranih algoritmov, ki ne poznajo odstopanj, katerih programer ni predvidel.
- Omejen obseg vložkov – mehanizmi uporabljajo vnaprej določen in običajno omejen obseg vložkov pri implementaciji regulacijskih pravil. Količina, področje in narava teh vložkov so omejeni s strani kreativnosti programerjev, kompleksnosti programske opreme ali okolja, v katerem delujejo.
- Samozadostnost – regulacije programske opreme izvajajo samostojni mehanizmi, ki načeloma ne sodelujejo z ostalimi akterji pri aktivnostih, kot je pri pravni regulaciji (sodišča, arbitraže …).
- Stroški – pri operacijah regulacij programske opreme po začetnih stroških običajno ne prihaja do dodatnih, saj je s finančnega vidika načeloma vseeno, kolikokrat se operacije izvedejo (Wagner 2005, 478–479).

Manjkajo ji t. i. varnostne zaklopke, kot so npr. udeležba tretje stranke, ki bi blažila ekstremne dogovore, nujnost evalvacije stroškov uveljavitve regulacije in primernost regulacije glede na količino uporabe. Našteti faktorji nakazujejo, da pretirana uporaba regulacije programske opreme vodi v regulacijsko okolje, ki je veliko bolj ekstremno in manj stabilno od pravnega. Na različnih področjih se uporabljajo različne kombinacije prava in regulacije programske opreme, vendar se je pokazalo, da je zaradi hitrih sprememb programske opreme za stabilnost

primernejša pravna regulacija. Le-to se lahko doseže prek JZP, priporočeno pa je, da zasebni sektor najprej zagotovi ustrezno regulacijo s standardi (Wagner 2005, 480–508; Bush 2007, 50).

7.3 Standardi

Svetovna ekonomija danes je vedno bolj vezana na informacije, zato je potrebna spretnost pri upravljanju, saj sta od tega odvisna konkurenčnost in uspeh organizacij zasebnega sektorja. V informacijski dobi so ključne informacije, do katerih s pomočjo IKT dostopamo in jih razpečujemo. Vrednost naprav IKT temelji na njeni zmožnosti, da lahko učinkovito komunicira z drugimi napravami. IKT igra osrednjo vlogo pri poslovanju zasebnega sektorja, prav tako pa pri uporabi s strani potrošnikov. Da bi novosti IKT dosegle poln potencial, je potrebno poskrbeti, da so skupaj s svojo podporno infrastrukturo popolnoma interoperabilne. Za to poskrbijo standardi; to so tehnične specifikacije s ciljem podpore razvoja odprtega in konkurenčnega trga v korist ponudnikom in potrošnikom. To pa ni edina prednost standardov. V prejšnjih poglavjih sem standarde že omenil kot možne zavezujoče mehanizme (samo)regulacije. Ključ do optimalnega izkoristka IKT je njena interoperabilnost, natančneje povezljivost komponent. Če določen produkt ali storitev nima visoke interoperabilnosti, je njegovo delovanje omejeno. Enako je pri uporabi programske opreme, saj morajo biti proizvodi različnih proizvajalcev kompatibilni, če želimo doseči skupno uporabo določenih aplikacij (npr. video konferenca). Standardi IKT so s tehnološkega vidika namenjeni zagotavljanju interoperabilnosti, saj bi pomanjkanje le-te pripeljalo do negativnih gospodarskih in socialnih posledic, veliko vlogo pa odigrajo tudi pri zagotavljanju varnosti. Tehnični standardi nimajo pomembne vloge le pri oblikovanju IKT v prihodnosti, temveč vplivajo tudi na delovanje organizacij in odnose med njimi. Standardi, ki opredeljujejo varnostne zahteve, tako vplivajo na celotno infrastrukturo podjetja (NO-REST 2005, 8–9; Microsoft 2009, 2–3).

Prej samostojne telekomunikacije, množični mediji in računalniška industrija so vedno bolj konvergentni in vodijo do ustanovitve t. i. informacijske avtoceste. Konvergenca posameznih tehnologij (stacionarni in mobilni telefoni, sateliti, kabelska TV, prizemna TV in radio ter internet) tvori globalno komunikacijsko omrežje. V njem so različne komponente nadgrajene ob različnem času, na različnih mestih in na različne načine. Rezultat je kompleksno in spreminjajoče se okolje, ki še močneje nakazuje na potrebo po standardizaciji. Standardi bi naj ustvarili univerzalne koristi za družbo, torej posameznike ter zasebni in javni sektor.

Posamezniki oziroma potrošniki bi imeli večjo izbiro in nižje stroške (standardi zagotavljajo večjo konkurenčnost med proizvajalci in izvajalci storitev), hkrati pa standardi ohranjajo odprtost trga. Podjetja zasebnega sektorja bi imela koristi zaradi ekonomije obsega (standardizacija bi omogočila hitrejšo dosego kritične mase in posledično povrnitev stroškov raziskav in razvoja, prav tako pa bi odprla vstop na globalen trg), zaupanja potrošnikov (posledica zaupanja v učinkovitost standardov) in večje prodaje (fleksibilni in interoperabilni produkti so privlačnejši za potrošnike). Standardi imajo velik vpliv na zagotavljanje varnosti IKT. Javni sektor lahko preko standardov zavaruje iniciative obstoječih politik, in sicer zaradi njihove vloge pri razvoju interoperabilnih aplikacij, ki so pomembne za gospodarsko rast. IKT uporabljajo tudi organizacije javnega sektorja (npr. elektronske aplikacije za zdravstvo, davke, eUprava ipd.). Za svoje potrebe so razvile rešitve, ki niso nujno ustrezne za ostale sektorje. Podobno kot pri elektronskem poslovanju zasebnega sektorja bi morale biti prioritete usmerjene v povezljivost, integracijo podatkov, dostop in upravljanje z vsebino. Za uporabo elektronskih storitev je pomembna tudi fizična infrastruktura, čeprav so meje med fizičnim in virtualnim vedno bolj zabrisane (npr. računalništvo v oblaku) (NO-REST 2005, 5–6; Blind in Gauch 2009, 9–10).

Internet je močno pospešil difuzijo notranjih omrežij in okrepil interakcijo med organizacijami. Nove metode udejstvovanja družbe na internetu ves čas pritiskajo na oba sektorja, da poskrbita za ustrezno učinkovitost delovanja in varovanja (npr. spletno bančništvo). V razvoj standardov se vključuje tudi civilna družba, ki uporablja storitve javnega sektorja. Vodilo teh iniciativ je predvsem zaupanje v storitve. Ločimo med de facto (razvoj preko trga) in de jure standardi (potrjeni s strani formalne organizacije). Standardi so pridobili na strateški vrednosti, saj vplivajo na razvoj tehnologije in usmerjajo razvoj trga. Danes so mnogi standardi obravnavani kot samostojni izdelki. Na področju IKT ima močan vpliv sektor proizvodnje/razvoja IKT, saj je glavni nosilec inovacij. Proizvajalci IKT imajo možnost vpliva na standarde, kar jim v primeru patentov in avtorskih pravic omogoča tudi zakonodaja. Proizvajalci pri razvoju IKT uporabljajo mnoge že obstoječe standarde, vendar običajno ne sodelujejo pri razvoju novih, ki bi zajeli obsežnejšo problematiko. Nekatere države že imajo standarde, ki pa niso nujno interoperabilni z mednarodnimi (NO-REST 2005, 24; Hawkins 2009, 32–35).

7.3.1 Pristop k oblikovanju standardov

Za učinkovitejši razvoj standardov bi morali spremeniti pogled na vlogi ponudnikov in uporabnikov, in sicer v obliko triade prodajalcev, ponudnikov in potrošnikov IKT. Prodajalci priskrbijo izdelke in storitve (IKT komponente, sistemi in programska oprema proizvajalcev), ponudniki zagotovijo komponente s strani prodajalcev in jih konfigurirajo za določen namen in okolje ter s tem dodajo vrednost (pogosto morajo opraviti raziskave za ustrezno implementacijo), potrošniki uporabljajo komponente, ki jih priskrbijo ponudniki, vendar načeloma IKT ne dodajajo vrednosti. Med njimi prihaja do nenehne interakcije in povratnih informacij, ta odnos pa bi v standardizacijskem okolju moral biti osnova za nadgradnjo obstoječih in razvoj novih standardov. Standardizacijsko okolje sestavljajo strokovnjaki, administracije, asociacije, konzorciji in standardizacijska telesa. Nasičenost akterjev in soodvisnost okolja je zabrisala meje med formalnimi in neformalnimi standardi, do težav pa je prišlo tudi med akterji (posredniki), ki sodelujejo v različnih partnerstvih in med seboj tekmujejo za podporo ostalih deležnikov. Posredniki imajo lastne poslovne modele in cilje, ki bi jih morali za zagotovitev ustreznih standardov uskladiti (Hawkins 2009, 36–37).

Aplikacijo standardov na področju IKT lahko glede na čas razdelimo v tri kontekstne okvirje:

- neposredna aplikacija (standardi so neposredno vključeni v nove izdelke/storitve s strani proizvajalcev/prodajalcev/ponudnikov),
- posredna aplikacija (dodani standardi izdelku/storitvam s strani ponudnikov zaradi dodane vrednosti),
- aplikacija končnih uporabnikov (do nje pride, ko končni uporabniki uporabijo funkcionalnosti izdelkov ali storitev, omogočene s strani standardov).

Primer te opredelitve je lahko proizvodnja in uporaba mobilnega telefona. Proizvajalec poskrbi za terminal, omrežje in opremo za izmenjavo, ki je ustrezna za standard GSM (neposredna aplikacija). Opremo nadalje razpečujejo ponudniki (operaterji omrežij, ISPs), ki ji dodajo vrednost s konfiguriranjem funkcionalnosti standarda GSM, da le-ta omogoča uporabo komercialnih omrežij (posredna aplikacija). Končni uporabnik lahko priključi opremo na napravo za prostoročno telefoniranje (Hawkins 2009, 37).

Pri oblikovanju standardov razni akterji delujejo posredno ali neposredno, odvisno od njihove motivacije. Tradicionalni pristopi k standardizaciji so se pogosto izkazali za neustrezne, saj so bili prepočasni za tako dinamičen trg (od sprejema do implementacije standardov mine do dve

leti), ki se v tem času lahko usmeri v popolno drugo smer. Pomembno je, da se standardi uvedejo ob pravem času. Deležniki se danes lahko neposredno udeležijo razprav ali pa posredno vplivajo z izbiro (priljubljenostjo) le določenih standardov ali nekaterih njihovih karakteristik. Hawkins je delovanje deležnikov razdelil na tri tipe vpliva na razvoj standardov:

1. prevladujoč vpliv (večji finančni ali tehnični prispevki k razvoju standarda),
2. vpliv prispevkov (splošna podpora iniciativam z vsaj minimalno udeležbo pri razvoju, odobritvi in/ali vpeljavi standarda),
3. zunanji vpliv (izražanje želenih lastnosti standarda, po navadi viden z analizo odločitev in dobrih praks) (Hawkins 2009, 37–38).

Organizacije izbirajo ustrezne standarde na podlagi več faktorjev, npr. poslovnih modelov, strategij, na podlagi IKT, ki jo uporabljajo itd. Standardizacija predstavlja stičišče tehničnih in ne-tehničnih faktorjev (gospodarski, organizacijski in socialni). Standardi niso le produkt tehničnih pomislekov, temveč tudi vpliva sodelovanja deležnikov in izraz ekonomskih interesov s strani večjih akterjev (Jakobs in Kritzner 2009, 82).

Za javni sektor je priporočen premislek o uporabi odprtih standardov, ki se jih zasebni že poslužuje. Uporaba odprtih standardov vključuje:

- zmanjšanje odvisnosti od zunanjih dobaviteljev programske opreme in večji spekter možnosti,
- način boja proti monopolu na trgu programske opreme in preprečitev izkoriščanja monopolnega položaja,
- izboljšavo kakovosti vladnih informacijskih sistemov na področju dostopnosti informacij, transparentnosti aktivnosti in varnosti,
- zmanjševanje stroškov implementacije programske opreme,
- izboljšanje izmenjave podatkov med sektorji (Blind in Gauch 2009, 9–10).

7.3.2 Standardizacijska telesa

Standardi temeljijo na ponudbi in povpraševanju. Povpraševanje tvori trg, ponudbo pa pripravljajo standardizacijska telesa (Jakobs in Kritzner 2009, 82).

Standardizacijska telesa so organizacije javnega ali zasebnega sektorja, ki predlagajo, razvijajo, vzpostavijo, nadzorujejo in/ali koordinirajo standarde. Omenjena telesa med seboj sodelujejo (včasih je potrebno prevzeti določene standarde, jih nadgraditi ipd.) in hkrati

tekmujejo (standardi so komercialni izdelki). Povečano število standardizacijskih teles ima tudi pomanjkljivosti, npr. fragmentacijo trga. Podjetja lahko izbirajo med raznimi telesi in zato posedujejo izdelke z različnimi standardi. Težava je tudi v razčlenjenosti sektorja IKT, ki ga sestavlja več različnih sektorjev industrije s specifičnimi potrebami in zahtevami. Temu primerno se razvijajo standardi, ki zajemajo specifikacije točno določenega sektorja (npr. spletne aplikacije). Standardizacije bi se morali lotiti s celovitim pristopom, ki bi upošteval gospodarske, socialne in tehnične aspekte procesa (NO-REST 2005, 5; Bartleson 2013).

IKT sektor se sooča z vedno več standardi s strani konzorcijev, vendar so ti večinoma v obliki tehničnih specifikacij. Zasebna podjetja z udeležbo v zaprtih konzorcijih lahko izkoristijo za hitrejši dostop do produktov, pa tudi prednost določene mere ne-transparentnosti in v večji meri nadzorujejo informacije, ki so potencialno občutljive narave za potrošnike. Slabost konzorcijev je, da so lahko pristranski, selektivni in ne-transparentni ter s tem ne služijo javnemu interesu. Prav tako pri njihovem delovanju obstaja možnost, da ne gre za popolno konkurenčni trg in s tem ne sledi zakonom o konkurenčnosti. Obstaja več kot 400 večjih konzorcijev na področju IKT, ki standarde uvajajo na različne načine. Težava je tudi pri pomanjkanju udeleževanja majhnih ali srednje velikih podjetij in predstavnikov potrošniških skupin, saj si večinoma ne morejo privoščiti visokih stroškov vstopa. S tem nimajo možnosti vplivanja na odločitve in tudi njihovi produkti niso kompatibilni s produkti članov konzorcija. Obstaja tudi možnost v obliki odprtega procesa, ki kombinira med tradicionalno standardizacijo in novim tržno usmerjenim pristopom. Standardi imajo veliko vlogo za informacijsko varnost, saj zagotovijo določeno raven varnosti izdelkov, težave pa se po navadi pojavijo pri pridobitvi, saj so večinoma v komercialni ponudbi. Javni in zasebni sektor bosta morala s skupnimi napori izbrati večje število standardov, ki bomo postali obvezni za izdelke, ki se uporabljajo v ključni infrastrukturi. S tem se del odgovornosti prenese tudi na nacionalne organe za standardizacijo (Updegrove 2007; ICT Regulation Toolkit 2016).

Narodni urad za standarde in tehnologijo ZDA (NIST) je dober primer organizacije, ki želi izboljšati informacijsko varnost. Leta 2014 je urad po Odredbi 13636 izdelal okvir kibernetske varnosti, ki je skupek dobrih praks, standardov in konceptov. Dokument predlaga razne pristope k večanju varnosti v organizacijah, poudarek pa je na izmenjavi informacij in potrebi po ukrepih, da se zagotovi informacijska varnost. Prednost dokumenta je priprava enotnega leksikona izrazov s področja kibernetske varnosti in s tem lažja komunikacija med potencialnimi partnerji. Dokument ima potencial de facto standarda za regulacijo informacijske varnosti in zasebnosti, danes pa se že pozna njegov vpliv na mehanizmih

zagotavljanja varnosti. NIST se v dokumentu ni posvetil standardom s področja zasebnosti in svoboščin, ker organizacije iz zasebnega sektorja niso sprejele soglasja glede ključnih problematik. Dokumentu manjka še kar nekaj izjemno pomembnih tematik, kot so npr. nujnost vpeljave procesov identifikacije specifičnih potencialnih groženj glede na vrsto organizacije, obveznosti organizacij do zagotavljanja kibernetske varnosti in dolžnost organizacij, da nadgradijo obstoječo ter priskrbijo novo IKT. Okvir je dobro zasnovan, vendar je naletel na težave pri implementaciji, ker predstavlja veliko finančno investicijo. Ena izmed težav je tudi pomanjkanje ustreznega znanja in sredstev za samostojno vpeljavo, zato pri uvedbi znotraj organizacij predlagajo pomoč tretje stranke z znanjem in izkušnjami. Vpeljava v organizacije je prostovoljna, še posebej pa je priporočljiva za organizacije, ki sodelujejo pri ključni infrastrukturi (NIST 2014; PWC 2014).

Standardizacijski organi izdajajo standarde, ki so priznani na nacionalni, evropski ali mednarodni ravni. Glavne standardizacijske organizacije so:

- Mednarodna raven: ISO International Organization for Standardization (Mednarodna organizacija za standardizacijo), IEC International Electrotechnical Commission (Mednarodna elektrotehniška komisija), ITU International Telecommunication Union (Mednarodna zveza za telekomunikacije).
- Evropska raven: CEN European Committee for Standardization (Evropski komite za standardizacijo), CENELEC European Committee for Electrotechnical Standardization (Evropski komite za standardizacijo v elektrotehniki), ETSI European Telecommunication Standards Institute (Evropski inštitut za telekomunikacijske standarde) (Zakon o standardizaciji, 2. čl.).

Izpostavil sem dve izjemno pomembni mednarodni organizaciji za standardizacijo na področju IKT in zagotavljanja informacijske varnosti, to sta ISO in CC.

7.3.2.1 Mednarodna organizacija za standardizacijo ISO (International Organisation for Standardisation)

Nevladna organizacija je eno izmed največjih mednarodnih standardizacijskih teles na splošnem področju. Pripravlja razne mednarodne sporazume, ki so objavljeni v obliki mednarodnih standardov. Oznaka teh standardov je ISO in so prostovoljni za uporabo. ISO le razvija in objavlja standarde, samo certifikacijo pa opravijo certifikacijski organi. Znotraj

tehničnih odborov sodelujejo razni strokovnjaki in predlagajo standarde, ki morajo biti odobreni s strani članov ISO (ENISA 2011, 12; ISO 2016).

Tehnični odbor, ki se ukvarja s standardi s področja IKT, se imenuje JTC 1. Sestavljen je iz treh pododborov, in sicer:

1. JTC 1/SC 7: Standardi na področju programskega inženirstva,
2. JTC 1/SC 22: Programski jeziki, njihova okolja in vmesniki sistemske programske opreme in
3. JTC 1/SC 27: Varnostne tehnike IKT (ENISA 2011, 12; ISO 2016).

Za področje informacijske varnosti skrbi ISO 27001 – Sistemi upravljanja informacijske varnosti (Information security management), poleg tega pa se nenehno pojavljajo novi standardi. Standarda ISO/IEC 27001 in ISO/IEC 27002 danes predstavljata osnovo na področju varovanja informacij pri poslovanju organizacije in minimalni temelj, ki je potreben za ustrezno informacijsko varnost (ENISA 2011, 13; ISO 2016).

Glavni produkti ISO so objavljeni standardi, ki so javno dostopni in plačljivi.

7.3.2.2 CC The Common Criteria for Information Technology Security Evaluation

CC je mednarodni standard, ki skrbi za certificiranje računalniške varnosti. Gre za okvir, ki omogoča uporabnikom računalniških sistemov, da določijo varnostne, funkcionalne in zavarovalne zahteve. Proizvajalci nato objavijo varnostne lastnosti svojih produktov, ki jih nato pregledajo neodvisni testni laboratoriji in podajo oceno. CC zagotovi, da je bil proces specifikacije, implementacije in ocene varnosti računalniškega izdelka opravljen temeljito in skladno z usklajenimi visokimi standardi (ENISA 2011, 7; Common Criteria 2016).

Certifikat izdajo javni državni organi, t. i. Certifikacijska telesa (Certification Body CB). Evalvacija produkta vključuje več faz:

1. zahteve: Dokument Protection Profile (PP) identificira varnostne zahteve,
2. implementacijo: Dokument Security Target (ST) identificira varnostne lastnosti,
3. testiranje: produkt testirajo skladno s Security Target (ENISA 2011, 8; Common Criteria 2016).

Sporazum deluje na vladnem nivoju. Države podpišejo Common Criteria Recognition Agreement (CCRA), ki daje veljavo CC. Trenutno šteje 25 držav članic (Avstralija, Kanada,

Francija, Nemčija, Indija, Italija, Japonska, Malezija, Nizozemska, Nova Zelandija, Norveška, Republika Koreja, Španija, Švedska, Turčija, Velika Britanija, ZDA, Avstrija, Češka republika, Danska, Finska, Grčija, Madžarska, Izrael in Pakistan) (Common Criteria 2016).

Sporazum SOG-IS je sporazum med nekaterimi evropskimi državami članicami EU ali EFTA in priznava skupno prepoznavanje evalvacij certifikatov po standardih CC za vse nivoje evalvacije. Po evalvaciji CC izdelek prejme oceno EAL1-EAL7, ki velja za mednarodni standard. Ocene predstavljajo različne nivoje, na katerih je bil izdelek testiran (SOGIS 2016).

7.4 Študija obstoječega slovenskega sistema

Slovenija je članica raznih mednarodnih zavezništev, ki zaradi nenehnih kibernetskih napadov močno preusmerjajo interes v višanje informacijske varnosti, kar zahtevajo tudi od držav članic. Medtem ko civilna javnost prek raznih organizacij sodeluje pri ozaveščanju, to počne tudi država. Organizacij je vedno več, interes pa je tudi pri zasebnih podjetjih, ki prek izobraževanj in usposabljanja ponujajo svoje izdelke ter storitve. Sodeluje pri projektih zavezništev (EU, Nato itd.) in skladno s priporočili prilagaja svoje politike.

V zadnjih letih je zaradi raznih incidentov in neupoštevanja priporočil vlogo koordinatorja na področju državne informacijske varnosti prevzela Evropska unija. Smernice je začrtala že leta 2010, ko je skladno s projektom Evropa 2020 pripravila tudi Evropsko digitalno agendo (ang. Digital Agenda for Europe – EDA), kjer so opredeljene tudi zahtevane smernice razvoja uporabe IKT, razvoja informacijske varnosti in cilji za dosego enotnega digitalnega trga. EDA državam članicam dopušča, da ustvarijo lastne strateške okvirje za dosego pričakovanih ciljev. Slovenija je na področju digitalne rasti po kazalniku Uspešnost digitalne rasti glede na indeks digitalnega gospodarstva in družbe šele na 19. mestu med 28 državami v EU (meritev za leto 2014). Slovenija je marca 2016 sprejela strategijo Digitalna Slovenija 2020 in poleg tudi strateška dokumenta Načrt razvoja omrežij naslednje generacije do leta 2020 ter Strategijo kibernetske varnosti (Republika Slovenija 2016a, 4–5, 42).

7.4.1 Digitalna Slovenija 2020

V Digitalni Sloveniji 2020 so zapisali vizijo Slovenije, in sicer:

»Vizija Slovenije je, da s pospešenim razvojem digitalne družbe izkoristi razvojne priložnosti IKT in interneta, da postane napredna digitalna družba in referenčno okolje za uvajanje inovativnih pristopov pri uporabi digitalnih tehnologij« (Republika Slovenija 2016a, 12).

Vizija je razdeljena na več ciljev, kjer so med drugim navedeni tudi varen kibernetski prostor, osredotočeno vlaganje v razvoj digitalne družbe, razširitev uporabe IKT v vse segmente družbe in zaupanje v kibernetski prostor ter varovanje človekovih pravic (Republika Slovenija 2016a, 12).

Pomemben je tudi korak k standardizaciji in interoperabilnosti na evropski ravni. V dokumentu se zavedajo, da se pri standardizaciji soočajo interesi obeh sektorjev, za rešitev pa je potreben konsenz. To želi EU doseči s platformo, ki skrbi za povezovanje deležnikov. Dokument se dotakne tudi področja kibernetske varnosti, kjer kot strateški cilj navaja vzpostavitev celovitega sistema zagotavljanja kibernetske varnosti kot pomembnega integralnega dejavnika nacionalne varnosti. Le-ta bo poskrbel za varen kibernetski prostor, hkrati pa preprečeval oziroma odpravljal posledice varnostnih incidentov s področja informacijske varnosti. Več o tem je zapisano tudi v Strategiji kibernetske varnosti (Republika Slovenija 2016a, 20, 35).

7.4.2 Strategija kibernetske varnosti

V Sloveniji so februarja 2016 pripravili Strategijo kibernetske varnosti z namenom vzpostavitve sistema, ki bo skrbel za visok nivo kibernetske varnosti. Dokument je skupek prispevkov raznih ministrstev, agencij in organizacij. V dokumentu je zapisano, da je sistem za zagotavljanje informacijske varnosti draga investicija, ki pa je kljub vsemu neprimerljivo cenejša od posledic morebitnih incidentov. Slovenijo k zagotavljanju ustrezne informacijske varnosti zavezujejo že razni strateški dokumenti na državni in mednarodni ravni, kjer velja, da je obramba/varnost celotnega zavezništva enako močna, kot je obramba/varnost njenega najšibkejšega člena (Republika Slovenija 2016b, 1–3).

Trenutne operativne zmogljivosti so na ravni države porazdeljene med SI-CERT, Sektorjem za informacijsko varnost (Ministrstvo za javno upravo), Ministrstvom za obrambo (področje obrambe in varstva pred naravnimi ter drugimi nesrečami), Policijo in Slovensko obveščevalno-varnostno agencijo (SOVA). Imamo torej kar nekaj različnih organizacij, ki skrbijo za svoje področje, vendar jim primanjkuje kadra, sredstev in organizacije. Za celovito informacijsko varnost države manjka tudi najpomembnejši del, to je povezovalno telo, ki bo usklajevalo aktivnosti in skrbelo za hitro ter nemoteno izmenjavo kritičnih informacij. Zaenkrat sodelovanje med raznimi organizacijami ni formalizirano, ga pa določajo nekateri zakoni (npr. Zakon o elektronskih komunikacijah, ki ob grožnjah v 81. členu določa

izmenjavo informacij med AKOS in SI-CERT). Slovenija sicer sodeluje v okviru raznih mednarodnih vaj v organizaciji Agencije EU za varnost omrežij in informacij (ENISA 2016).

Strategija želi do leta 2020 z vzpostavitvijo celovitega sistema zagotavljanja kibernetske varnosti prispevati k odprtemu, varnemu in varovanemu kibernetskemu prostoru. Le-ta je ključnega pomena za nemoteno delovanje države. Strategija želi razviti uspešen sistem, ki bo skrbel za preprečevanje in odzivanje na varnostne incidente ter na ozaveščanje ciljnih skupin o pomenu kibernetske varnosti (Republika Slovenija 2016b, 5, 10–11).

V Strategiji kibernetske varnosti je navedeno:

> *Slovenija bo do leta 2020 vzpostavila učinkovit sistem zagotavljanja kibernetske varnosti, ki bo preprečeval in tudi odpravljal posledice varnostnih incidentov. Ta cilj obsega osem podciljev:*
>
> 1. *okrepitev in sistemska ureditev nacionalnega sistema zagotavljanja kibernetske varnosti,*
> 2. *varnost državljanov v kibernetskem prostoru,*
> 3. *kibernetska varnost v gospodarstvu,*
> 4. *zagotavljanje delovanja kritične infrastrukture v sektorju informacijsko-komunikacijske podpore,*
> 5. *zagotavljanje kibernetske varnosti na področju javne varnosti in zatiranje kibernetskega kriminala,*
> 6. *razvoj obrambnih kibernetskih zmogljivosti,*
> 7. *zagotavljanje varnega delovanja in razpoložljivosti ključnih informacijsko-komunikacijskih sistemov ob velikih naravnih in drugih nesrečah,*
> 8. *krepitev nacionalne kibernetske varnosti z mednarodnim sodelovanjem* (Republika Slovenija 2016b, 5).

V Strategiji kibernetske varnosti so navedeni razni deležniki, ki igrajo pomembno vlogo pri zagotavljanju informacijske varnosti. Napisano je, da sodelujejo organizacije iz javnega in zasebnega sektorja, med katerimi je potrebno izpostaviti odzivne centre, AKOS, upravljavce telekomunikacijske infrastrukture, ponudnike in operaterje storitev, stanovska in strokovna združenja, akademsko-raziskovalno sfero ter proizvajalce programske opreme. Za državno informacijsko varnost niso pomembni le državni akterji, temveč tudi tuje organizacije, ki

sodelujejo na tem področju. Med mednarodnimi akterji so za Slovenijo pomembne organizacije, ki sodelujejo znotraj EU in Nata (Republika Slovenija 2016b, 8).

Za učinkovito informacijsko varnost je potrebno smotrno izkoristiti obstoječe vire in poskrbeti za ustrezno organizacijo na več nivojih, kar bi uredili z vzpostavitvijo osrednje koordinacije nacionalnega sistema. Le-ta bo predstavljala enotno kontaktno točko mednarodnega sodelovanja in na strateški ravni koordinirala zmogljivosti, ki se bodo uporabljale na nižjih ravneh. Odločitve glede oblike koordiniranosti bo sprejela Vlada Republike Slovenije. Operativno raven bodo prevzeli prej omenjeni akterji, ki posedujejo potrebne zmogljivosti, in sicer SI-CERT (nacionalna raven), MO, Policija (javna varnost), SOVA in nastajajoči SIGOV-CERT (javna uprava).

Za magistrsko delo je zelo pomembna 6. točka, kjer Strategija kibernetske varnosti med drugim opredeli tudi deležnike iz zasebnega sektorja. Fokus je še vedno na upravljavcih ključne infrastrukture, kamor spadajo tudi ponudniki storitev, operaterji ipd. Korak naprej pa želijo narediti tudi na področju ozaveščanja, izobraževanja in raziskav. Pomembno vlogo dajejo akademsko-raziskovalni sferi, ki s svojimi programi ter predmeti osvešča in izobražuje prepotrebni kader, večjo vlogo pa bi naj igrali tudi izsledki raziskovalnih organizacij. Sodelovanje med javnim in zasebnim sektorjem bo ključnega pomena tudi pri nadaljnjem razvoju zmogljivosti (npr. na področju soočanja s kibernetskim kriminalom). Nov sistem bi naj bil odprt tudi za pobude civilne družbe. Ta pristop je že nekaj časa navzoč v nekaterih drugih državah, v Sloveniji pa nekako še ni prišel do potrebne stopnje, da bi vplival na odločitve na nacionalni ravni. V Strategiji kibernetske varnosti se osredotočajo predvsem na pobude za izboljšave in pomoč pri ozaveščanju s strani raznih strokovnih združenj s področja IKT, ki pa niso bolj podrobno opredeljena (Republika Slovenija 2016b, 9–15).

Sodelovanje med javnim in zasebnim sektorjem je predvideno pri ukrepih za dosego ciljev. Za višanje usposobljenosti in pripravljenosti državnih mehanizmov bo potrebna poglobljena interakcija na vseh ravneh. Sedanja IKT oprema se bo postopoma nadgradila s takšno, ki po raznih kriterijih velja za varno, vzpostavil se bo tudi sistem, ki bo kompetentno preverjal IKT opremo. Ustrezno je potrebno poskrbeti tudi za državljane, da se lahko dvigne kultura informacijske varnosti. V načrtu je, da se nadaljuje z obstoječimi ter doda nove programe ozaveščanja in vključitev civilne družbe na področju informacijske varnosti. Zaradi učinkovitosti želijo družbo razdeliti na ločene ciljne skupine (po starostnih skupinah, glede na gospodarske subjekte ipd.). Pomembno je, da se kultura informacijske varnosti vpelje tudi v

izobraževalni sistem, prav tako pa morajo ključni akterji sami poskrbeti za ustrezno usposobljenost svojih zaposlenih (Republika Slovenija 2016b, 11–13).

Kot sem že omenil, ima v državi velik pomen gospodarstvo. Le-to je potrebno ustrezno zaščititi, saj se posledice napada na večji posamični sektor razširijo in imajo implikacije tudi na ostale povezane sisteme. V Strategiji kibernetske varnosti se zavedajo, da so za uspešno informacijsko varnost pomembne investicije v razvoj, raziskave in inovacije. Slovenija ima digitalizirano gospodarsko okolje, ki mora biti ustrezno zaščiteno in imeti varno komunikacijsko okolje. Zato bi naj država sofinancirala projekte in ciljno usmerjene raziskave, ki potencialno prispevajo h kibernetski varnosti. S tem bo država spodbujala povezovanje gospodarstva in akademsko-raziskovalne sfere ter nudila okolje za nadaljnji skupni razvoj na državni in mednarodni ravni. Cilj je, da se pridobijo strokovnjaki, ki bodo s pomočjo JZP sposobni razvijati produkte z dodano vrednostjo. Po drugi strani bodo še naprej nadaljevali z ozaveščanjem podjetij na področju informacijske varnosti ter prednostih in pasteh IKT. Zelo pomemben je tudi zapis, da se bosta spodbujala razvoj in uporaba standardov na tem področju. S tem lahko Slovenija sčasoma razvije ustrezen okvir, ki bo dopuščal uporabo le tiste IKT, ki bo resnično zadostovala želenim standardom (Republika Slovenija 2016b, 14).

Strategija kibernetske varnosti kot največje tveganje za uresničitev ciljev navaja nezadostno zavedanje o pomembnosti informacijske varnosti in posledično nizke splošne varnostne kulture, ki vodi do pomanjkanja politične volje in soglasja za ustrezno ter sistemsko ureditev na nacionalni ravni (Republika Slovenija 2016b, 17).

Uspešno izvajanje strategije pa bo nasprotno pozitivno vplivalo na zagotavljanje nacionalne varnosti in imelo pozitivne multiplikativne učinke, povezane s povečano stopnjo varnosti. Prav tako bo vplivalo na porast zaupanja uporabnikov v internet ter s tem razvoj novih storitev in poslovnih modelov, povezanih z njegovo uporabo, kar se bo izrazilo v digitalni gospodarski rasti in povečanju družbene blaginje.

7.4.3 Pomembni akterji in iniciative

Na strani javnega sektorja sta poleg javnega zavoda Arnes pomembna Agencija za komunikacijska omrežja in storitve Republike Slovenije (AKOS), ki je državni regulator telekomunikacij, elektronskih medijev ter poštnih in železniških storitev, in SI-CERT, ki je

državni osrednji center za prijavo incidentov in nadaljnjo interakcijo z mednarodnimi organizacijami (AKOS 2016, SI-CERT 2016a).

7.4.3.1 SI-CERT

SI-CERT (Slovenian Computer Emergency Response Team) od leta 1995 deluje v okviru zavoda Arnes in je nacionalni odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. Od leta 2010 je vladni center za odzivanje na omrežne incidente. Svetuje in pomaga pri reševanju različnih incidentov, hkrati pa izdaja aktualna obvestila o trenutnih grožnjah, ki so namenjena širši javnosti. SI-CERT je del mednarodne skupine CERT/CC, član FIRST (Forum of Incident Response and Security Teams) in nekaterih drugih organizacij, kar mu omogoča hiter dostop do ključnih informacij. Med drugim je izbran za kontaktno točko za Varnostni organ Generalnega sekretariata Sveta EU in državno fokusno točko za program IMPACT (Mednarodna telekomunikacijska zveza ITU). Center skrbi tudi za usposabljanje pripadnikov Slovenske vojske. Poleg obvestil, opozoril in možnosti prijave incidentov letno pripravlja poročilo o omrežni varnosti v Sloveniji, kjer so zbrani statistični podatki in aktivnosti (SI-CERT 2016a; SI-CERT 2016b).

7.4.3.2 Direktorat za informacijsko družbo

Direktorat za informacijsko družbo koordinira aktivnosti na področju informacijske družbe. Direktorat dela v smeri vključevanja informacijske družbe, kar gre z roko v roki z razvojem informacijske varnosti. Informacijska družba bo s svojim znanjem in potencialom poskrbela za pospešen razvoj družbe kot celote, Direktorat pa skrbi za usklajevanje in dela v smeri pospešitve procesov. Poleg tega pripravlja zakonodajo na področju informacijske družbe in elektronskih komunikacij v Sloveniji, nudi podporo dejavnostim društva Arnes in izvaja naloge nadzornega organa po Uredbi (EU) št. 910/2014 Evropskega parlamenta. Direktorat za informacijsko družbo je prav tako aktiven v nacionalnih in mednarodnih projektih ter na področju nacionalne koordinacije komunitarnih programov (MIZS 2016).

7.4.3.3 Pregled večjih iniciativ in projektov

V Sloveniji se izvajata dva večja projekta, ki skrbita za ozaveščanje javnosti o informacijski varnosti in sta financirana s strani ministrstva, in sicer Varni na internetu in Safe.si. Poleg javnih projektov in akademskih skupnosti (zelo pomemben je javni zavod Arnes) pa o pomembnosti varne uporabe interneta in IKT osveščajo razna podjetja, ki prodajajo izdelke in storitve iz tega področja (npr. Microsoft, Viris ipd.) in hkrati organizirajo srečanja ter

konference, nekatera podjetja se povezujejo v konzorcije (primer Tehnološka mreža ICT), v Sloveniji pa obstajajo tudi računalniške skupnosti, med katerimi po prepoznavnosti najbolj izstopa Kiberpipa (Arnes 2016; Kiberpipa 2016; Tehnološka mreža ICT 2016). Pomembno vlogo igra tudi Inštitut za korporativne varnostne študije (ICS), ki prek vsebin nenehno poziva k višanju razvitosti informacijske varnosti v podjetjih, prav tako pa s predstavitvijo tematike širi znanje in razumevanje ter posledično viša motivacijo deležnikov, da poskrbijo za višjo raven informacijske varnosti. Organizacije in iniciative pripravljajo bolj ali manj neobvezujoča priporočila, ki zasebnega sektorja ne obvezujejo k sprejetju in spoštovanju obveznosti. Ogromno upov se polaga tudi v iniciativo Gospodarske zbornice, ki je še v nastajanju. V njenem okviru bodo sodelovali predstavniki različnih sektorjev s ciljem, da se zagotovi razvita informacijska varnost.

7.4.3.4 Varni na internetu

Projekt je financiran s strani Ministrstva za izobraževanje, znanost in šport, izvaja pa ga SI-CERT pod okriljem javnega zavoda Arnes (Direktorat za informacijsko družbo). Namenjen je celotni slovenski javnosti, posebej pa se osredotoča tudi na mala podjetja. Cilji so: dvig informacijske varnostne kulture, informiranje o raznih grožnjah v kibernetskem okolju, predlaganje rešitev in informiranje o varstvu osebne identitete na družbenih omrežjih. Gre za nacionalni program, ki deluje od leta 2011 (Republika Slovenija 2016b, 5; Varni na internetu 2016).

7.4.3.5 SAFE.si, TOM telefon in Spletno oko

Center za varnejši internet skrbi za tri programe, to so: SAFE.si, TOM telefon in Spletno oko. Center vodi konzorcij, ki ga koordinira Fakulteta za družbene vede Univerze v Ljubljani s partnerji Arnes, Zvezo prijateljev mladine Slovenije in Zavodom MISSS, financiran pa je s strani Evropske komisije (Generalni direktorat Connect) in Ministrstva za izobraževanje, znanost in šport (Republika Slovenija 2016b, 5; Spletno oko 2016).

Projekt SAFE.si je opredeljen kot točka osveščanja o varni rabi interneta in mobilnih naprav za otroke, najstnike, starše in učitelje (SAFE.si). Program TOM telefon je namenjen otrokom in mladim, ki se soočajo z izzivi odraščanja, katerega del je dandanes tudi udejstvovanje na internetu. Temu primerno TOM opozarja na varno uporabo. Spletno oko je spletna prijavna točka, ki od marca 2007 omogoča slovenskim uporabnikom interneta anonimno prijavo kršitev (predvsem nezakonitega gradiva zlorabe otrok in sovražnega govora). Spletno oko

sodeluje z raznimi vladnimi in nevladnimi organizacijami, pri hitri obravnavi prijav pa ji pomagata tudi Vrhovno državno tožilstvo Slovenije in Policija (Republika Slovenija 2016b, 5; SAFE.si; Spletno oko 2016; TOM 2016).

8 ANALIZA INTERVJUJEV IN SKLEP

8.1 Analiza intervjujev s strokovnjaki s področja informacijske varnosti

Za področje slovenske informacijske varnosti nisem našel veliko literature, še posebej ne primerov iz prakse, saj slovenska družba še pred nekaj let tematiki ni posvečala pretirane pozornosti. Zanimal me je vpogled s strani strokovnjakov, ki tako ali drugače že nekaj časa sodelujejo v organizacijah, namenjenih oblikovanju informacijske varnosti. Opravil sem štiri intervjuje, in sicer z mag. Damijanom Marinškom (sekretar na Ministrstvu za javno upravo), mag. Albinom Poljancem (OE Nadzor telekomunikacij v AKOS), izr. prof. dr. Denisom Čaleto (predsednik Sveta Inštituta za korporativne varnostne študije ICS) in Gorazdom Božičem (vodja SI-CERT). Njihovi odgovori predstavljajo njihova stališča in ne nujno stališče organizacije.

Oblikoval sem šest sklopov vprašanj, ki zajemajo pregled trenutnega stanja in pozivajo k iskanju predlogov za krepitev slovenske informacijske varnosti.

V prvem sklopu vprašanj sem se dotaknil aktualnega stanja v Sloveniji. Zanimalo me je, ali je slovenska varnostna kultura ustrezna in ali oba sektorja pravilno pristopata do nje.

1) *Menite, da je slovenska informacijska varnostna kultura ustrezna?*

Intervjuvanci so podali podobne pomisleke, da slovenska varnostna kultura ni ustrezna (Božič 2016; Čaleta 2016; Marinšek 2016; Poljanec 2016).

2) *Ali javni in zasebni sektor pravilno pristopata k pereči tematiki?*

Čaleta je izpostavil pomanjkanje izobraževalnih elementov, ki bi morali biti prisotni že v osnovni šoli, kar se izraža v nizki varnostni kulturi družbe. Le-ta tekom življenja velikokrat ni nikoli več podvržena zahtevam po višji informacijski varnosti. Poljanec je omenil, da zasebni sektor skrbi bolj za lastne interese, javni sektor pa bi moral biti zgled z dobrimi praksami, kar pa na tem področju ni. Božič in Marinšek sta se strinjala, da določeni segmenti javnega sektorja dobro opravljajo svoje delo. Božič je omenil kritično infrastrukturo in izpostavil

banke, Marinšek pa Direktorat za informacijsko družbo, ki nenehno skrbi za ozaveščanje in razvoj slovenske informacijske varnosti. V zasebnem sektorju je posebej izpostavil strokovnjake s tega področja, ostali pa postopoma dojemajo pomembnost problematike (Božič 2016; Čaleta 2016; Marinšek 2016; Poljanec 2016).

Drugi sklop sem namenil JZP in obstoječim slovenskim iniciativam. Zanimalo me je mnenje intervjuvancev o obstoječih iniciativah JZP, delitvi vlog znotraj JZP in ali takšno JZP v Sloveniji že obstaja oziroma je izvedljivo.

3) *Kakšno je vaše mnenje o teh iniciativah?*

Čaleta je poudaril, da so te iniciative kratkoročne in je nemogoče opraviti ustrezne meritve, ki bi pokazale dejanske rezultate. Marinšek je izpostavil JZP kot edino rešitev za uspešnost, saj država ni zmožna zagotoviti primernih finančnih sredstev za strokovnjake. Božič in Poljanec sta bila skeptična, da so lahko iniciative uspešne. Oba sta izpostavila različne interese potencialnih deležnikov (Božič 2016; Čaleta 2016; Marinšek 2016; Poljanec 2016).

4) *Kako bi morale biti razdeljene vloge znotraj partnerstva?*

Božič in Poljanec sta izpostavila pomembnost transparentne opredelitve vlog deležnikov in skupne interese za dosego ciljev. Marinšek je mnenja, da bi država morala imeti pobudo, koordinacijo, nadzor in pregled, operativa pa bi naj bila prepuščena zasebnemu sektorju. Čaleta je poudaril, da mora iti za celovit pristop, saj bi prekinjenost delovanja kritične infrastrukture škodovala obema sektorjema. Pomembno je, da oba sektorja najdeta stične točke in opredelita delitev obveznosti in stroškov. Sodelovanje bi bilo dobičkonosno za oba sektorja (Božič 2016; Čaleta 2016; Marinšek 2016; Poljanec 2016).

5) *Mislite, da je v Sloveniji takšno partnerstvo mogoče in ali poznate kakšen primer dobre prakse?*

Čaleta je kot primer dobre prakse omenil Slovensko združenje korporativne varnosti (ICS), kjer sodelujejo gospodarske organizacije in javne inštitucije (SI-CERT, Urad za varovanje tajnih podatkov, Urad inf. pooblaščenke itd.). Poljanec je omenil, da na področju telekomunikacij takšno partnerstvo že poznamo, primer je npr. gradnja odprtih širokopasovnih omrežij (GOŠO). V njem sodelujejo Evropska komisija, država in zasebni sektor. Božič je mnenja, da bi z ustrezno pripravljenim okvirjem verjetno bilo mogoče,

Marinšek pa je omenil, da obstaja nekaj primerov kratkoročnih partnerstev, vendar zaenkrat ni ustreznega JZP (Božič 2016; Čaleta 2016; Marinšek 2016; Poljanec 2016).

Tretji sklop sem namenil vlogi države v razmerju z zasebnim sektorjem pri zagotavljanju državne informacijske varnosti. Postavil sem dve vprašanji, in sicer glede legitimnosti zapovedovanja ukrepov zasebnemu sektorju in glede regulativne vloge države.

6) *Ali lahko država legitimno zapove organizacijam zasebnega sektorja, da morajo poskrbeti za lastno informacijsko varnost?*

Po mnenju Marinška bi lahko za to poskrbela Uredba o informacijski varnosti, akt vlade, s katerim lahko zapoveduje akterjem, ki so priključeni na njihovo omrežje. Naslednji korak je sprejem ustreznega zakona, operativna podlaga pa je že v 74. členu Zakona o javni upravi, kjer pa se soočajo s težavami pri tolmačenju (Marinšek 2016).

Čaleta je omenil, da je pri liberalni usmeritvi gospodarstva večna dilema, do kod lahko država posega. V Sloveniji imamo mnogo aktov, ki pa se v praksi ne izvajajo. Legitimnost bi se izražala v primeru, da tisto, kar država zapiše, tudi nato v praksi izvaja. Božič meni, da bo morala država zaradi prepletenosti akterjev predpisovati minimalne standarde, pod katerimi bodo morala podjetja delovati, kot je vidno tudi na nivoju EU, kjer bodo morale države članice opredeliti operaterje kritične infrastrukture. Poljanec je omenil, da država pri infrastrukturah javnega interesa že zapoveduje organizacijam zasebnega sektorja, vendar se srečuje s težavami pri finančnih obveznostih. Za večjo legitimnost bi morala država poskrbeti za rešitev pri financiranju projektov (Božič 2016; Čaleta 2016; Poljanec 2016).

7) *Menite, da lahko država opravlja vlogo regulatorja na področju informacijske varnosti? Če da, s kakšnimi mehanizmi?*

Čaleta, Marinšek in Poljanec so se strinjali, da država to nalogo v določeni meri že opravlja, Čaleta in Poljanec sta omenila AKOS, ki je nacionalni regulator na področju elektronskih komunikacij ter z zakoni in podzakonskimi akti že regulira dejavnosti na omenjenem področju. Marinšek je izpostavil posredni vpliv države, ki s predstavitvijo novih trendov vpliva na odziv zasebnega sektorja, prav tako pa je omenil, da bo s sprejetjem ustrezne pravne podlage neposredno vplival na razvoj, kljub temu pa bo določen del aktivnosti ostal v rokah zasebnega sektorja. Božič je rekel, da država lahko opravlja vlogo regulatorja s pomočjo zakonodaje, s pristojnimi inšpekcijskimi organi in na drugi strani s primernimi programi ozaveščanja ter spodbujanja uvajanja dobrih praks. Čaleta je izpostavil težave, s katerimi se

srečujejo manjše države, ko se soočijo z interesi multinacionalk. Regulacija se mora izboljšati s pomočjo ustrezno plačanih strokovnjakov (Božič 2016; Čaleta 2016; Marinšek 2016; Poljanec 2016).

Četrti sklop je namenjen pravni opredelitvi tematike. Pravni okvirji se nenehno soočajo z izzivi v kibernetskem prostoru, zanimalo pa me je, kako imamo to področje urejeno v Sloveniji in kako bi bilo to najlažje urediti.

8) *To področje nekako pokrivajo znotraj mednarodnih zavezništev, kako pa je v Sloveniji? Tudi vaša organizacija je akter, ki opozarja na potrebno ureditev. Kako bi bilo po vašem mnenju to najlažje urediti in ali se tej temi namenja dovolj interesa?*

Božič ne vidi pravne podlage kot edine bistvene ovire. SI-CERT že 20 let uspešno deluje in gradi na prostovoljnem sodelovanju drugih akterjev iz javnega sektorja in gospodarstva. Po njegovem je najboljši pristop z uravnoteženo pravno podlago in skrbjo za operativno sodelovanje. Bistveni problem vidi pri resnem pomanjkanju zavedanja o pomembnosti tega področja na vrhu politike, pri odločevalcih v državi. Čaleta se strinja, da gre za težavo in meni da zamujamo z razvojem na tem področju ter da politika odriva sprejemanje dokumentov, ki prinesejo tudi finančne obveznosti. Marinšek izpostavlja problematiko manjših držav, ki zaradi pomanjkanja virov ne morejo slediti vsem predlogom in zahtevam večjih držav ter zavezništev (npr. na področju certificiranja interneta stvari). Poljanec je pojasnil, da je na področju elektronskih komunikacij pravna podlaga že aktivna; Splošni akt o varnosti omrežij in storitev določa organizacijske ukrepe, ki jih operaterji morajo sprejeti. Prav tako dokument temelji na standardu SIST ISO/IEC 27001, ki operaterje zavezuje k nenehnim analizam in razvoju varnostnih mehanizmov (Božič 2016; Čaleta 2016; Marinšek 2016; Poljanec 2016).

Ena izmed ključnih nalog za razvitejšo informacijsko varnost je ozaveščanje javnosti. To je opredeljeno tudi v Digitalni Sloveniji 2020 in Strategiji kibernetske varnosti. Zanimalo me je, ali slovenska družba kaže interes za ponujene vsebine in kako bi se le-ta lahko zvišal.

9) *Ozaveščanje javnosti je ena izmed vaših aktivnosti, zanima pa me, ali menite, da Slovenci pokažejo dovolj interesa? Ali organizacije izkoristijo znanje in izkušnje, ki jim ga nudite? Kaj bi še lahko naredili na tem področju, da se zviša interes javnosti?*

Intervjuvanci so odgovorili s stališča področja, kjer so aktivni. Čaleta je namenil največ pozornosti podjetjem, ki so ena izmed ciljanih publik ICS. Z integriranim pristopom, ki z ekonomskim jezikom cilja na menedžment in lastnike podjetij, že beležijo uspehe. Pokazalo

se je, da se je med zaposlenimi v podjetjih, ki sodelujejo znotraj ICS, povečalo zavedanje o informacijski varnosti in dvignila varnostna kultura na tem področju. Marinšek je opredelil vlogo Direktorata za informacijsko družbo, ki želi ozaveščati zaposlene javnega sektorja, ARNES-a, ki ozavešča širšo javnost, računa pa tudi na Iniciativo Gospodarske zbornice, ki lahko le doprinese k večjemu uspehu. Poljanec je omenil, da AKOS sodeluje v projektu Safe.si, v okviru katerega so izdali mnogo publikacij, nasvetov in ostalih gradiv. Občasno sodelujejo tudi na osnovnih šolah. Božič ima izkušnje s programom Varninainternetu.si, ki je zelo dobro sprejet. Omenil je, da so ljudje veseli, da država financira takšne aktivnosti, dobivajo dobre odzive in tudi opažajo interes. Poljanec opaža, da je težko meriti učinek pripravljenega gradiva, Božič pa je poudaril, da bo ljudi težko prisiliti k izobraževanju, če sami ne bodo imeli interesa (Božič 2016; Čaleta 2016; Marinšek 2016; Poljanec 2016).

V zadnjem sklopu sem se posvetil Strategiji kibernetske varnosti, ki bi morala biti podlaga nadaljnjega razvoja. Opazil sem, da je dokument spisan precej splošno in da nikjer ni mogoče zaslediti jasno opredeljene vloge zasebnega sektorja, zato sem intervjuvance vprašal, ali menijo, da je preveč poudarka le na vlogi države.

10) *Menite, da je v tej strategiji vloga zasebnih podjetij dovolj opredeljena ali je preveč poudarka na vlogi države in njenih teles?*

Čaleta je omenil, da se konkretizacija ne pričakuje od Strategije kibernetske varnosti, temveč od akcijskega načrta, ki bi se moral sprejeti čim prej. Znotraj tega bo potrebno podrobno opredeliti vire, dejavnosti, prioritete, sredstva, cilje ipd. Za uspešnost bi bilo potrebno dolgoročno spremljati in ocenjevati delovanje in prilagoditi nadaljnje aktivnosti. Država prav tako lahko doprinese k uveljavitvi slovenskih podjetij v mednarodni sferi, zato morajo le-ta vložiti trud na tem področju (Čaleta 2016).

Božič meni, da v Strategiji kibernetske varnosti ni začrtane natančnejše opredelitve podjetij, ker še nismo prišli do konsenza glede vloge zasebnega sektorja. Najprej je bilo potrebno poskrbeti za osnovno delovanje mehanizmov, ki so znotraj javnega sektorja (Božič 2016).

Poljanec je Strategijo kibernetske varnosti opredelil bolj kot izhodišče za naprej, kot podlago za nadaljnje smernice, akte, sporazume ipd. Omenil je, da primanjkuje virov in strokovnjakov, ki bi jih bilo potrebno ustrezno plačati. Prav tako meni, da je celotna zadeva zaenkrat malo zamrla (Poljanec 2016).

Marinšek kot prvi korak k večji vlogi in ozaveščanju zasebnega sektorja predstavlja ustanovitev sekcije Gospodarske zbornice, ki je v nastajanju, hkrati pa meni, da mora svojo vlogo odigrati tudi država, ki mora prepoznati svojo ključno nalogo in ji ustrezno opraviti (Marinšek 2016).

8.2 Sklep

S pomočjo intervjujev sem ugotovil, da intervjuvani strokovnjaki menijo, da v Sloveniji nimamo ustrezne varnostne kulture. Manjka ozaveščanje mladih, kar bi najlažje in morda tudi najučinkoviteje zagotovili z vpeljavo tematike v osnovne in srednje šole. Določeni segmenti javnega in zasebnega sektorja sicer že opravljajo aktivnosti ozaveščanja, vendar je na voljo še veliko prostora za izboljšave, kot tudi potreba po vključevanju večjega dela akterjev.

Nekakšen trend učinkovitega zagotavljanja informacijske varnosti na mednarodni ravni je postalo javno-zasebno partnerstvo. V Sloveniji le-to po mnenju intervjuvancev še ni razvito, saj se sektorja povezujeta le v okviru kratkoročnih projektov. Prav tako se soočata z različnimi interesi, ki bi jih bilo potrebno uskladiti. Zelo pomembno je, da se pri oblikovanju JZP transparentno opredelijo vloge, pričakovanja, cilji in načini za dosego le-teh. Kritično je tudi področje financiranja in prevzema stroškov. Zasebni sektor mora velikokrat sam kriti stroške projektov, za učinkovito JZP pa bo morala država najti rešitev, ki bo deloma razbremenila zasebni sektor. Učinkovito JZP bi bilo dobičkonosno za vse prisotne akterje in v končni fazi bi profitirali tudi državljani. Še vedno se išče soglasje glede razdelitve vlog znotraj JZP; Marinšek je predlagal, da bi poskusili z modelom, ki je prisoten na mnogih drugih področjih, in sicer da država prevzame pobudo, koordinacijo in nadzor, zasebni sektor pa operativo. V Sloveniji zaenkrat še nimamo dolgoročnega JZP na področju celovitega zagotavljanja informacijske varnosti. Poznamo JZP na področju elektronskih komunikacij, sodelovanje v okviru raznih organizacij (npr. ICS), manjka pa nam ustrezno opredeljeno JZP, ki bi se celovito lotilo problematike.

Država že izvaja določene aktivnosti regulacije v panogah, ki imajo v osnovi zelo visoke tehnične zahteve in pričakovanja (bančništvo, letalska industrija ipd.). Mednarodni trendi nakazujejo, da se bo morala država vedno bolj vmešavati v zasebni sektor. To lahko stori s sprejemom zakonov, zaradi legitimnosti pa je pričakovan bolj postopen pristop. Dobre prakse lahko najdemo na primeru operaterjev ključne infrastrukture, kjer države že prepisujejo minimalne standarde. Pomaga si lahko tudi na primeru elektronskih komunikacij, kjer v Sloveniji opravlja vlogo regulatorja AKOS. S svojimi dejavnostmi ozaveščanja sicer posredno

že vpliva na ravnanje zasebnega sektorja, neposredno pa bo to lahko opravila le z razvojem pravne podlage. Pomanjkanje le-te ni glavna težava, manjka predvsem politična volja. Politika ima v rokah dovolj sredstev, da lahko pospeši razvoj ustreznih mehanizmov, kar pa predstavlja stroške, ki niso zaželeni. Ključnim odločevalcem in pravnikom velikokrat manjkajo poznavanje in razumevanje kibernetskega prostora, IKT ter predvsem razsežnosti potencialnih groženj. Akterji v Sloveniji želijo to odpraviti z ozaveščanjem, ki je že v polnem teku. Na voljo je kar nekaj projektov in iniciativ, ki nudijo literaturo in izobraževanja. Lahko bi rekli, da so sredstva za dosego cilja na voljo, ostalo pa je v rokah družbe. Posameznikov namreč ne gre prisiliti, da bi pokazali interes.

Na področju informacijske varnosti sta za Slovenijo pomembna dokumenta Digitalna Slovenija 2020 in Strategija kibernetske varnosti. Le-ta je spisana zelo splošno, za dosego zapisanih ciljev pa bo potrebno pripraviti dodatne ukrepe, ki bodo zagotovili implementacijo. Opaža se, da sta angažiranost in vnema po sprejemu dokumenta rahlo poniknila, kar ni dobro glede na začrtane cilje do leta 2020. Javni sektor se spopada s pomanjkanjem virov in primernega kadra, saj strokovnjaki ne želijo delati za ponujen denar, ko jim zasebni sektor za podobno delo plača veliko več. To je le še ena iztočnica več, da je potrebno konkretneje pristopiti k oblikovanju JZP in dosegi začrtanih ciljev.

V Sloveniji k sreči še nismo bili tarča večjih kibernetskih incidentov, strokovnjaki pa se bojijo razsežnosti posledic, če bi do teh prišlo. V primerjavi z drugimi državami EU se pri ključnih indikatorjih gibljemo med zadnjimi 10 državami, kar ni ravno spodbudno za prihodnost, še vedno pa imamo možnost, da pospešimo razvoj. Družba se mora začeti zavedati pomembnosti informacijske varnosti in poskrbeti, da postane vsakodnevna tema. S tem se bo še dodatno povečal interes politike in morda zagotovil odločnejši pristop k omenjeni temi.

9 ZAKLJUČEK

Za raziskovalno vprašanje me je zanimalo, kako lahko država v okviru obstoječe zakonodaje legalno in legitimno regulira dejavnosti zasebnega sektorja pri zagotavljanju informacijske varnosti.

Ugotovil sem, da država določene segmente že regulira legalno in legitimno, vendar je ostalo še mnogo zelo pomembnih, kjer nima vpliva (npr. proizvodnja/razvoj IKT, razvoj določenih standardov ipd.). Država ima nadzor nad tistimi segmenti, ki so tesno povezani z državnimi institucijami, kritičnimi sektorji, ki zahtevajo zadostovanje raznim tehničnim standardom (npr. bančništvo, letalska industrija ipd.), in tistimi, ki so se razvili iz prej državnih (elektronske komunikacije). Delovanje držav še vedno sloni na ključni infrastrukturi, ki pa je s procesom privatizacije vedno bolj v rokah zasebnih podjetij. Države so tekom privatizacije večinoma spustile vajeti in niso zagotovile dokumentov, ki bi zasebne lastnike/operaterje zavezovali k spoštovanju določenih direktiv. Danes marsikaterega lastnika/operaterja ključne državne infrastrukture pravno nič ne zavezuje, da bi spoštoval navodila države, vsekakor pa so se po nekaj kibernetskih incidentih hitro našli skupni interesi. Oba sektorja sta spoznala, da oviranje delovanja infrastrukture povzroča škodo obema – država ne more zagotoviti varnosti, zasebni sektor izgublja dobiček. Kibernetska dimenzija je zelo abstraktna in informacijska varnost se lahko zagotovi le s sodelovanjem več akterjev. Rešitev se je pojavila v obliki JZP. Zasebni sektor prepoznava problematiko pomanjkanja koordinatorja, finančne podpore, pravne podlage in nadzornega organa, ki bi skrbeli za spoštovanje sprejetih pravil znotraj sektorja. Javni sektor se zaveda, da jim primanjkuje strokovnjakov, da ključna infrastruktura ni v njihovih rokah in da bo vsak samovoljen poskus vsiljevanja pravil naletel na močan odpor s strani industrije. Četudi bi razvil pravno podlago, bi le-ta morala biti dinamična, saj tradicionalno pravo ne more zajeti vseh novosti kibernetske dimenzije, težavo pa predstavljajo tudi tehnično nepodkovani pravniki. Potrebno bi bilo razviti popolnoma novo podlago, ki bi zajemala abstraktna pravila in bi se nenehno posodabljala skladno z napredkom IKT.

JZP so že nekaj časa prisotna v večjih državah, še posebej v ZDA. Izkušnje so pokazale, da še vedno niso našli univerzalnega modela, kako bi moralo biti JZP oblikovano. Zasebni sektor še vedno želi samostojnost, javni sektor pa večji nadzor. Primeri dobrih praks so izpostavili pomembnost jasne opredelitve vlog in ciljev deležnikov v samem začetku partnerstva, prav tako pa pomen zaupanja, ki je ključno za nadaljnji razvoj. Šele ko bodo vse pravice in

dolžnosti jasno opredeljene, ko bosta oba sektorja našla kompromis glede prispevka k partnerstvu in ko se bo razvilo zaupanje, bo JZP postalo učinkovito.

Države sicer imajo pooblastila, da sprejmejo zakone, ki bi omejevali dejavnosti na področju informacijske varnosti, vendar trenutno še niso našle sistema, ki bi celovito zajel celotno problematiko. JZP bo lahko osnova za legitimen razvoj pravne podlage, ki bo zajemala vse segmente IKT. Ko se bodo interesi sektorjev uskladili, bo mogoče razviti sistem regulacije, ki bo koristil celotni družbi.

V hipotezi sem napisal, da je zasebni sektor pri zagotavljanju informacijske varnosti popolnoma samostojen; do sprememb lahko pride le v primeru skupne iniciative zasebnih podjetij.

Če se najprej osredotočim na prvi del stavka, torej da je zasebni sektor pri zagotavljanju informacijske varnosti popolnoma samostojen, ugotavljam, da temu ni popolnoma tako. Zasebni sektor sicer je samostojen pri razvoju novih tehnologij, vendar je vseeno tudi pri tem odvisen od trga in ostalih faktorjev. Podjetja so v rokah raznih deležnikov, ki zahtevajo dobre rezultate in dobičkonosnost. Današnja družba je veliko bolj informirana o komercialni ponudbi IKT, ki je na voljo, prav tako pa ji je na voljo široka izbira produktov, kar jim daje možnost izbire. Razne iniciative in programi ozaveščanja o informacijski varnosti počasi, a vztrajno sledijo začrtanim ciljem in skrbijo, da ideje o varnosti in varovanju osebnih podatkov dosegajo mišljenje potencialnih strank. Če je še pred kakšnim desetletjem bila za podjetja pomembna le časovna konkurenčna prednost, ne pa varnost produkta, se je to tekom zadnjih let korenito spremenilo. S povečanjem kibernetskih napadov in incidentov so se povečali tudi stroški posledic. Težava ni bila le na finančnem področju, proizvajalci so začeli izgubljati tudi na ugledu, ki je dandanes za blagovne znamke zelo pomemben, saj s slabim imenom ne moreš ohraniti strank, kaj šele pridobiti novih. Družba danes želi relativno varno IKT. Končni uporabniki se sicer ne obremenjujejo z vsemi podrobnostmi, se pa temu posvečajo različne strokovne in ljubiteljske skupnosti, ki imajo vpliv na percepcijo končnega uporabnika. Zasebni sektor je tako primoran zadovoljiti delničarje in poskrbeti, da si končni uporabniki želijo uporabljati njihove produkte. Zagotoviti si morajo nekakšno zaupanje, kar pa težko storijo s samovoljnostjo. Zaupanje pridobijo z raznimi certifikati, standardi, prevzemi modelov programiranja ipd., ki so v osnovi namenjeni zagotavljanju določene stopnje varnosti IKT.

V drugem delu stavka sem zapisal, da do sprememb lahko pride le v primeru skupne iniciative zasebnih podjetij. Ta del lahko potrdim, saj se to že dogaja. Zgoraj sem omenil, da lahko podjetja pridobijo zaupanje s pomočjo standardov, certifikatov ipd., ti pa so produkt izmenjave idej znotraj sektorja. Liberalno usmerjen trg ne želi, da država posega v delovanje zasebnega sektorja, zato je razvoj marsikatere norme padel v roke le-tega. Načeloma velja, da organizacije zasebnega sektorja sodelujejo med seboj in znotraj sodelovanja razvijejo norme, kodekse obnašanja ipd., ki jih želijo razširiti tudi do drugih organizacij. Nekateri mehanizmi se razvijejo do te mere, da postanejo nekakšno osnovno merilo minimalne varnosti, ki se zahteva od produktov. Težava je, da te norme večinoma niso zavezujoče in tudi ne obstaja pravna podlaga ter organ, ki bi kaznoval kršitelje. Drugače je s standardi, ki jih morajo določena podjetja dosegati, če želijo sodelovati z drugimi, še posebej z javnim sektorjem. Ko pride do sodelovanja in vključitve v zavarovano omrežje javnega sektorja, morajo akterji spoštovati kriterije in pravila, ki jih določijo v pogodbi. Standardi skrbijo tudi za interoperabilnost IKT, ki je v sedanjem času izjemno pomembna. Tako nobena organizacija zasebnega sektorja ni odvisna le od svojih interesov, temveč se mora prilagajati trendom. Največji vpliv imajo velike multinacionalke, ki imajo že skoraj monopol nad določenimi segmenti trga. Sredstva in kadri jim omogočajo, da je razvoj varnostnih zahtev prilagojen njihovim potrebam, kar pa ni nujno slabo. S tem vseeno skrbijo za nekakšno poenotenje industrije, po drugi strani pa so podvrženi pričakovanjem in pritiskom s strani družbe, kar zajema vse od organizacij do posameznikov. Multinacionalke sodelujejo znotraj raznih obstoječih iniciativ in organizacij, ki skrbijo za ozaveščanje in razvoj varnostnih pričakovanj. Ne glede na razlog za vključitev v iniciative so podjetja pod drobnogledom in vsak spodrsljaj lahko v trenutku povzroči nepopisno škodo. Izkušnje so pokazale, da je bolje biti med vodilnimi zagovorniki in prodajalci varne IKT kot pa tvegati z nepopolno IKT, ki je prva na trgu.

Državna informacijska varnost močno pridobiva na prepoznavnosti, kar kažejo napori večjih držav, ki že nekaj časa intenzivno vlagajo v razvoj kibernetskih zmogljivosti. Manjše države so zaradi pomanjkanja virov in politične volje v zaostanku, to pa se spreminja s sodelovanjem v mednarodnih zavezništvih. Za Slovenijo so zelo pomembna pričakovanja EU, ki je s projektom Evropa 2020 zastavila visoke cilje za zavezništvo in njene države članice. Države, ki so še pred nekaj leti indiferentno spremljale dogajanje in se izgovarjale, da so premalo pomembne za kibernetski napad, morajo danes vsaj v teoriji razvijati ustrezne varnostne

mehanizme. Med temi državami je tudi Slovenija, ki je Strategijo kibernetske varnosti sprejela šele leta 2016.

Dejstvo je, da so za razvitejšo informacijsko varnost potrebni napori vseh udeleženih, od posamičnih organizacij pa je odvisno, koliko so pripravljene vložiti v spoštovanje dogovorov in nadaljnji razvoj mehanizmov, ki služijo zagotavljanju informacijske varnosti.

10 LITERATURA

1. *AKOS (Agencija za komunikacijska omrežja in storitve Republike Slovenije)*. 2016. Dostopno prek: http://www.akos-rs.si/ (20. februar 2016).
2. *Arnes*. 2016. Dostopno prek: http://arnes.splet.arnes.si/ (18. marec 2016).
3. Bartleson, Karen. 2013. *10 Standards Organizations That Affect You (Whether You Know It Or Not)*. Dostopno prek: http://electronicdesign.com/communications/10-standards-organizations-affect-you-whether-you-know-it-or-not (18. marec 2016).
4. Blind, Knut in Stephan Gauch. 2009. The Demand for E-Government Standards. V *Information Communication Technology Standardization for E-Business Sectors: Integrating Supply and Demand Factors*, ur. Kai Jakobs, 9–23. Hershey: IGI Global.
5. Božič, Gorazd. 2016. Intervju z avtorjem. Ljubljana, 25. julij.
6. Bučar, Maja. 2005. Zakaj obravnavati učinke informacijsko komunikacijskih tehnologij? V *Učinki informacijsko komunikacijskih tehnologij*, ur. Metka Stare in Maja Bučar, 23–36. Ljubljana: FDV.
7. Bush, William R. 2007. Software, Regulation and Domain Specificity. *Information and Software Technology* 49 (1): 44–54. Dostopno prek: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.104.3828&rep=rep1&type=pdf (13. april 2016).
8. *BSIMM*. 2016. Dostopno prek: https://www.bsimm.com (18. marec 2016).
9. *Center for Internet Security*. 2016. Dostopno prek: https://www.cisecurity.org/ (18. marec 2016).
10. Cliff, Saran. 2014. *Executive interview: Microsoft targets the non-professional developers*. Dostopno prek: http://www.computerweekly.com/news/2240214693/Executive-interview-Microsoft-targets-the-non-pro-developers (18. marec 2016).
11. *CMMI Institute*. 2016. Dostopno prek: http://cmmiinstitute.com/ (18. marec 2016).
12. Commission of the European Communities. 2009. *Communication on Critical Information Infrastructure protection (CIIP) – Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*.

Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri =COM:2009: 0149:FIN:EN:PDF (18. marec 2016).

13. *Common Criteria*. 2016. Dostopno prek: https://www.commoncriteriaportal.org/ (18. marec 2016).
14. Corporate Computer Services. 2016. *IT Outsourcing: The Reasons, Risks and Rewards*. Dostopno prek: http://www.corpcomputerservices.com/articles/outsourcing-reasons (7. junij 2016).
15. *Cybrary*. 2016. Dostopno prek: https://www.cybrary.it/ (18. marec 2016).
16. Čaleta Denis. 2011. Kibernetska varnost v družbi in delovanje kritične – Analiza stanja na obrambnem področju v Republiki Sloveniji. V *Sodobni vojaški izzivi (Contemporary military challengens)*, ur. Branimir Furlan in ostali, 39–51. Ljubljana: Tiskarna Collegium Graphicum, d. o. o.
17. --- 2016. Intervju z avtorjem. Ljubljana, 29. julij.
18. D'Elia Danilo. 2015. *Public-Private Partnership: The Missing Factor in the Resilience Equation – The French Experience on CIIP*. Dostopno prek: http://www. cyberstrategie.org/sites/default/files/media/danilo_delia_extrakt_-_public-private_ partnernship_the_missing_factor_in_the_resilience_equation_the_french_experience_ on_ciip_.pdf (12. marec 2016).
19. MIZS. 2016. *Direktorat za informacijsko družbo*. Dostopno prek: http://www. mizs.gov.si/si/delovna_podrocja/direktorat_za_informacijsko_druzbo/ (2. julij 2016).
20. Dunn-Cavelty, Myriam in Elgin M. Brunner. 2007. Introduction: information, power, and security – an outline of debates and implications. V *Power and security in the information age: investigating the role of the state in cyberspace*, ur. Myriam Dunn Cavelty, Victor Mauer in Sai Felicia Krishna-Hensel, 1–18. Aldershot: Ashgate Publishing.
21. Dunn-Cavelty, Myriam in Manuel Suter. 2009. Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection* 2 (4): 179–187. Dostopno prek: http://www.sciencedirect.com/science/article/pii/S1874548209000274 (10. maj 2016).
22. ENISA. 2011. *Secure software engineering initiatives – Listing SSE initiatives across Europe and abroad*. Dostopno prek: https://www.enisa.europa.eu/publications/secure-software-engineering-initiatives (20. februar 2016).

23. --- 2014. *EP3R 2010-2013: Four Years of Pan-European Public Private Cooperation*. Dostopno prek: https://www.enisa.europa.eu/publications/ep3r-2009-2013 (7. maj 2016).
24. --- 2015. *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches*. Dostopno prek: https://www.enisa.europa.eu/publications/ cybersecurity-information-sharing (1. marec 2016).
25. --- 2016. Dostopno prek: https://www.enisa.europa.eu/ (18. februar 2016).
26. EUR-LEX. 2012. *Uredba (EU) št. 1025/2012 Evropskega parlamenta in sveta*. Dostopno prek: http://eur-lex.europa.eu/legal-content/SL/TXT/HTML/ ?uri=CELEX: 32012R1025&from=EN (1. marec 2016).
27. European Commision. 2013a. *Policy on Critical Information Infrastructure Protection (CIIP)*. Dostopno prek: https://ec.europa.eu/digital-single-market/en/ news/policy-critical-information-infrastructure-protection-ciip (2. marec 2016).
28. --- 2013b. *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*. Dostopno prek: http://register.consilium.europa.eu/doc/ srv?l=EN&f=ST%206342%202013%20INIT (4. marec 2016).
29. --- 2016. *Why We Need Digital Single Market*. https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/digital_single_ market_factsheet_final_20150504.pdf (2. julij 2016).
30. European Council. 2016. *Improving cyber security across the EU*. Dostopno prek: http://www.consilium.europa.eu/en/policies/cyber-security/ (8. maj 2016).
31. Ericsson, Göran N. 2010. Cyber Security and Power System Communication – Essential Parts of a Smart Grid Infrastructure. *IEEE transactions on Power Delivery* 25 (3): 1501–1507. Dostopno prek: http://www.csit.qub.ac.uk/media/pdf/ Filetoupload,286696,en.pdf (26. februar 2016).
32. Farwell, James P. 2012. Industry's Vital Role in National Cyber Security. *Strategic Studies Quarterly, Winter 2012* 6 (4): 10–41. Dostopno prek: http://www.au.af.mil/au/ ssq/2012/winter/winter12.pdf (2. marec 2014).
33. Flynn Goodwin, Cristin in Paul Nicholas. 2013. *Developing a National Strategy for Cybersecurity: Foundations for Security, Growth and Innovation*. Dostopno prek: http://www.microsoft.com/en-us/search/Results.aspx?q=Developing+a+National (1. marec 2014).

34. Gilardi, Fabrizo in Martino Maggetti. 2011. The independence of regulatory authorities. V *Handbook on the Politics of Regulation*, ur. David Levi-Faur, 201–214. Cheltenham: Edward Elgar Publishing Limited.
35. Gerst, Martina, Eric Iversen in Kai Jakobs. 2009. An Integrated View of E-Business and the Underlying ICT Infrastructure. V *Information Communication Technology Standardization for E-Business Sectors: Integrating Supply and Demand Factors*, ur. Kai Jakobs, 1–8. Hershey: IGI Global.
36. Goodin, Aaron. 2015. *4 Ways to Market Your Business for Free*. Dostopno prek: https://www.entrepreneur.com/article/241607 (22. maj 2016).
37. Grimmelmann, James. 2005. Regulation by Software. *The Yale Law Journal* 114: 1719–1758. Dostopno prek: http://www.yalelawjournal.org/pdf/209_jbwrex6h.pdf (3. junij 2016).
38. Haufler, Virginia. 2001. *A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy*. Washington: Carnegie Endowment for International Peace.
39. Hawkins, Richard. 2009. Business Models and the Dynamics of Supply and Demand for Standards. V *Information Communication Technology Standardization for E-Business Sectors: Integrating Supply and Demand Factors*, ur. Kai Jakobs, 31–50. Hershey: IGI Global.
40. *ICT Regulation Toolkit*. 2016. Dostopno prek: http://www.ictregulationtoolkit.org/ (17. februar 2016).
41. *IEEE Computer Society*. 2016. Dostopno prek: https://www.computer.org/ (13. marec 2016).
42. *InfoSec Institute*. 2016. Dostopno prek: https://www.infosecinstitute.com/ (12. marec 2016).
43. *Intel Security*. 2016. Dostopno prek: http://www.mcafee.com/ (13. marec 2016).
44. International Telecommunication Union. 2008. *Overview of cybersecurity (Recommendation ITU-T X.1205)*. Dostopno prek: https://www.itu.int/rec/T-REC-X.1205-200804-I (18. marec 2016).
45. *ISA*. 2016. Dostopno prek: https://www.isa.org/ (13. marec 2016).
46. *ISO*. 2016. Dostopno prek: http://www.iso.org/ (12. marec 2016).
47. Jakobs, Kai in Jan Kritzner. 2009. How to Select the Best Platform for ICT Standards Development. V *Information Communication Technology Standardization for E-Business Sectors: Integrating Supply and Demand Factors*, ur. Kai Jakobs, 81–95. Hershey: IGI Global.

48. *Kiberpipa*. 2016. Dostopno prek: http://www.kiberpipa.org/ (18. junij 2016).
49. Kruchten, Philippe, Henk Obbink in Judith Stafford. 2006. The Past, Present, and Future of Software Architecture. *IEEE Software March/April*. Dostopno prek: https://profesores.ing.unab.cl/~gbadillo/archivos/cursos/software-arch/Papers/The%20Past,%20Present,%20and%20future%20of%20Sw%20Arch.pdf (8. maj 2016).
50. Lewis, Ted G. 2015. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation (Second edition)*. New Jersey: John Wiley & Sons.
51. Linder, Stephen H. 1999. Coming to Terms With the Public-Private Partnership: A Grammar of Multiple Meanings. *American Behavioral Scientist* September 43: 35–51.
52. Marinšek, Damijan. 2016. Intervju z avtorjem. Ljubljana, 22. julij.
53. Markets and markets. 2016. *Internet of Things (IoT) Market by Software Solution (Real-Time Streaming Analytics, Security, Data Management, Remote Monitoring, & Network Bandwidth Management), Platform, Service, Application Domain, and Region – Global Forecast to 2021*. Dostopno prek: http://www.marketsandmarkets.com/Market-Reports/internet-of-things-market-573.html (12. junij 2016).
54. Microsoft. 2009. *Standards in the ICT Industry*. Dostopno prek: http://download.microsoft.com/download/7/F/9/7F9FEC37-84FF-4020-A243-9BEBE70DC0B9/Standards_in_the_ICT_Industry.pdf (3. junij 2016).
55. *Microsoft*. 2014. Dostopno prek: https://www.microsoft.com (27. februar 2014).
56. Neal, Stacy Reiter. 2008. Business as Usual? Leveraging the Private Sector to Combat Terrorism. *Perspectives on Terrorism* 2 (3): 10–13. Dostopno prek: http://www.terrorismanalysts.com/pt/articles/issues/PTv2i3.pdf (10. marec 2014).
57. NIST. 2014. *Framework for Improving Critical Infrastructure Cybersecurity*. Dostopno prek: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (14. marec 2016).
58. NO-REST. 2005. *Networked Organisations – Research into Standards and Standardisation*. Dostopno prek: http://citeseerx.ist.psu.edu/viewdoc/ download?doi=10.1.1.116.6035&rep=rep1&type=pdf (24. maj 2016).
59. *OpenSAMM*. 2016. Dostopno prek: http://www.opensamm.org/ (12. marec 2016).
60. *Open Source Initiative*. 2016. Dostopno prek: https://opensource.org/ (16. marec 2016).
61. *OWASP*. 2016. Dostopno prek: https://www.owasp.org/ (12. marec 2016).
62. Pinter, Andrej. 2005. *Sodobne teorije javne sfere*. Ljubljana: Fakulteta za družbene vede.

63. Poljanec, Albin. 2016. Intervju z avtorjem. Ljubljana, 27. julij.
64. Pressman, Roger S. 2005. *Software Engineering: A Practitioner's Approach. McGraw-Hill Series in Computer Science (Sixth Edition*). New York: McGraw-Hill.
65. Privacysense. 2016. *Private Sector*. Dostopno prek: http://www.privacysense.net/terms/private-sector/ (3. marec 2016).
66. PWC. 2014. *Why you should adopt the NIST Cybersecurity Framework*. Dostopno prek: https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf (17. junij 2016).
67. --- 2015. *Cyber; Think risk, not IT*. Dostopno prek: http://www.pwc.com/us/en/financial-services/regulatory-services/publications/assets/cyberrisk.pdf (18. maj 2016).
68. Republika Slovenija. 2016a. *Digitalna Slovenija 2020*. Dostopno prek: http://www.mizs.gov.si/si/delovna_podrocja/direktorat_za_informacijsko_druzbo/digitalna_slovenija_2020/ (13. junij 2016).
69. --- 2016b. *Strategija kibernetske varnosti*. Dostopno prek: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/si-ncss (13. junij 2016).
70. Rinaldi, Steven M., James P. Peerenboom in Terrence K. Kelly. 2001. *Critical infrastructure Interdependencies*. Dostopno prek: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.89.2276&rep=rep1&type=pdf (2. marec 2016).
71. Rinaldi, Steven M. 2004. *Modeling and Simulating Critical Infrastructures and Their Interdependencies*. Dostopno prek: http://www.google.si/url?sa=t&rct =j&q=&esrc=s&source=web&cd=1&ved=0CC0QFjAA&url=http%3A%2F%2Fciteseerx.ist.psu.edu%2Fviewdoc%2Fdownload%3Fdoi%3D10.1.1.98.1206%26rep%3Drep1%26type%3Dpdf&ei=K2D1UOapJMWptAam8oDAAQ&usg=AFQjCNGdPwoIO0ODQkB59ZsgaX8y_Y3wIg&bvm=bv.41018144,d.Yms (7. marec 2013).
72. *SAFECode*. 2016. Dostopno prek: http://www.safecode.org/ (13. marec 2016).
73. *SANS*. 2016. Dostopno prek: https://www.sans.org/ (12. marec 2016).
74. Schmitz, Andreas. 2014. *Europe Lagging in the ICT Market*. Dostopno prek: http://news.sap.com/europe-lagging-ict-market/ (6. maj 2016).
75. Schipper, Irene in Esther de Haan. 2005. *CSR issues in the ICT hardware manufacturing sector – SOMO ICT Sector Report*. Amsterdam: Centre for Research on Multinational Corporations (SOMO).

76. Scott, Colin. 2002. Contemporary Governance. *Journal of Law and Society* 29 (1): 56-76. Dostopno prek: http://researchrepository.ucd.ie/bitstream/handle/10197/6737/ PrivateRegOfPublicSector.pdf?sequence=2 (21. marec 2016).
77. Seltzer, Larry. 2010. Microsoft Releases SDL Docs With Creative Commons License. *Security Watch*, 27. april. Dostopno prek: http://securitywatch.pcmag.com/security-software/ 283800-microsoft-releases-sdl-docs-with-creative-commons-license (14. marec 2016).
78. *SI-CERT*. 2016a. Dostopno prek: https://www.cert.si (19. marec 2016).
79. --- 2016b. *Poročilo o omrežni varnosti za leto 2015*. Dostopno prek: https://www.cert.si/letna-porocila-o-omrezni-varnosti/ (20. junij 2016).
80. Sida. 2004. *Private Sector Development*. Dostopno prek: http://www.sida.se/ globalassets/publications/import/pdf/en/private-sector-development.pdf (29. februar 2016).
81. *Software Engineering Institute*. 2016. Dostopno prek: http://www.sei.cmu.edu/ (11. marec 2016).
82. *SOGIS*. 2016. Dostopno prek: http://www.sogis.org/ (6. maj 2016).
83. *Spletno oko*. 2016. Dostopno prek: http://safe.si/spletno-oko (27. junij 2016).
84. Stare, Metka in Maja Bučar. 2005. Zakaj obravnavati učinke informacijsko komunikacijskih tehnologij? V *Učinki informacijsko komunikacijskih tehnologij,* ur. Metka Stare in Maja Bučar, 13–19. Ljubljana: FDV.
85. Stare, Metka, Andreja Jaklič in Patricia Kotnik. 2005. Vpliv vlaganj v informacijsko-komunikacijske tehnologije na učinkovitost podjetij v Sloveniji. V *Učinki informacijsko komunikacijskih tehnologij,* ur. Metka Stare in Maja Bučar, 98–114. Ljubljana: FDV.
86. Dillon, Stuart, Buchanan John in Corner Jim. 2010. Comparing Public and Private Sector Decision Making: Problem Structuring and Information Quality Issues. V *45th Annual Conference*, ur. Andrew Mason in Matthias Ehrgott, 229–237. Dostopno prek: https://secure.orsnz.org.nz/conf45/program/ProceedingsORSNZ10.pdf (3. marec 2014).
87. Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana: FDV.
88. Tadjdeh, Yasmin. 2014. Johnson: DHS Must Build Trust With Private Sector to Counter Cyber-Attacks. *National Defense*. Dostopno prek: http://www.nationaldefensemagazine.org/archive/2014/March/Pages/JohnsonDHSMustBuildTrustWithPrivateSectortoCounterCyber-Attacks.aspx (12. marec 2014).

89. *Tehnološka mreža ICT*. 2016. Dostopno prek: http://www.ict-slovenia.net/index.php (28. junij 2016).
90. *TOM*. 2016. Dostopno prek: http://www.e-tom.si/ (27. junij 2016).
91. Updegrove, Andrew. 2007. *The Essential Guide to Standards*. Dostopno prek: http://www.consortiuminfo.org/essentialguide/whatisansso.php (5. maj 2016).
92. Usman, Shuaibu Hassan. 2013. A review of responsibilities of internet service providers toward their customers' network security. *Journal of Theoretical and Applied Information Technology* 49 (1): 70–78. Dostopno prek: http://www.jatit.org/volumes/ Vol49No1/9Vol49No1.pdf (16. februar 2016).
93. Vacca, John R., ur. 2009. *Computer and Information Security Handbook*. Burlington: Elsevier.
94. *Varni na internetu*. 2016. Dostopno prek: https://www.varninainternetu.si (18. junij 2016).
95. Vlada Republike Slovenije. 2011. *Uredba o evropski kritični infrastrukturi*. Dostopno prek: http://www.uradni-list.si/1/objava.jsp?sop=2011-01-1799 (5. maj 2016).
96. Wagner, R. Polk. 2005. On software regulation. *Southern California Law Review* 78 (2): 457–520. Dostopno prek: http://lawreview.usc.edu/issues/past/ view/download/ ?id=1000373 (3. junij 2016).
97. Waksman, Adam. 2014. *Producing Trustworthy Hardware Using Untrusted Components, Personnel and Resources*. Dostopno prek: http://www.cs. columbia.edu/~waksman/PDFs/thesis.pdf (16. maj 2016).
98. Warrier, B. S. 2010. *Learning the legal aspects of computing*. Dostopno prek: http://www.thehindu.com/features/education/learning-the-legal-aspects-of-computing/article952108.ece (7. junij 2016).
99. Watson, Kenneth C. 2007. *Private-sector preparedness in critical infrastructure protection*. Dostopno prek: http://www.hsgac.senate.gov/ download/71207-testimony-ken-watson (6. marec 2016).
100. *Web Application Security Consortium*. 2016. Dostopno prek: http://www. webappsec.org/ (13. marec 2016).
101. Wettenhall, Roger. 2003. The Rhetoric and Reality of Public-Private Partnerships. *Public Organization Review* 3 (1): 77–107. Dostopno prek: http://link.springer.com/article/10.1023/A:1023000128175 (28. februar 2016).

102. White, Sydney M. in Jim Halpert. 2016. *Cybersecurity Law Alert (US)*. Dostopno prek: https://www.dlapiper.com/en/us/insights/publications/2016/02/cybersecurity-2015s-top-legal-developments/ (2. julij 2016).
103. White House. 2009. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Dostopno prek: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf (9. marec 2014).
104. *Zakon o javno-zasebnem partnerstvu* (ZJZP). Ur. l. RS, 127/06. Dostopno prek: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO4323 (12. maj 2016).
105. *Zakon o standardizaciji* (ZSta-1). Ur. l. RS, 59/1999. Dostopno prek: https://www.uradni-list.si/1/content?id=20030 (9. julij 2016).
106. Zetter, Kim. 2012. *Hoping to Teach a Lesson, Researchers Release Exploits for Critical Infrastructure Software*. Dostopno prek: http://www.wired.com/threatlevel/2012/01/scada-exploits/ (10. marec 2013).
107. Zissis, Dimitrios in Dimitrios Lekkas. 2010. Addressing cloud computing security issues. *Future Generation Computer Systems* 28 (3): 583–592. Dostopno prek: http://www.sciencedirect.com/science/journal/0167739X/28/3 (22. maj 2016).

PRILOGE

PRILOGA A: Intervju z mag. Albinom Poljancem (Ljubljana, 27. 7. 2016)

1. Državna informacijska varnost je odvisna od mnogih dejavnikov, med drugim tudi od varnosti informacijsko-komunikacijske tehnologije akterjev, ki sodelujejo pri aktivnostih kritične infrastrukture, gospodarstvu in drugih sektorjih z vplivom na državo.

   - Menite, da je slovenska informacijska varnostna kultura ustrezna?

Težko bi govorili o informacijski varnostni kulturi, saj ljudje niso primerno poučeni. Gre za nov pojav, ki se bo ukoreninil skozi čas.

- Ali javni in zasebni sektor pravilno pristopata k pereči tematiki?

Zasebni sektor skrbi bolj za lastne interese, javni sektor pa bi moral biti zgled z dobrimi praksami, kar pa v tem primeru ni.

2. Javni in zasebni sektor zelo različno pristopata k informacijski varnosti. Medtem, ko je v interesu javnega sektorja »javno dobro«, za zasebni sektor velja vodilo dobičkonosnosti in interesa delničarjev. Razni dokumenti in iniciative pozivajo k nekakšnemu javno-zasebnemu partnerstvu, ki bi bilo zmožno zagotoviti ustrezno informacijsko varnost.

   - Kakšno je vaše mnenje o teh iniciativah?

Iniciative bodo težko dosežene, saj prevladujejo različni interesi potencialnih deležnikov.

- Kako bi morale biti razdeljene vloge znotraj partnerstva?

Partnerstvo bi moralo prevzeti nek model, kjer bi se vloge ustrezno razdelile, interesi pa bi se morali poenotiti.

- Mislite, da je v Sloveniji takšno partnerstvo mogoče in ali poznate kakšen primer dobre prakse?

Na področju telekomunikacij takšno partnerstvo že poznamo npr. gradnja odprtih širokopasovnih omrežij (GOŠO). V njem sodelujejo Evropska komisija, država in zasebni sektor.

3. Državna varnost je tradicionalno v domeni države, pri informacijski varnosti pa le-ta ne more samostojno opravljati potrebnih aktivnosti. Pomanjkanje interesa organizacij

zasebnega sektorja in neustrezna notranja informacijska varnost imata implikacije na celoten sistem (npr. napad na večje podjetje lahko posledično povzroči škodo celotnemu slovenskemu gospodarstvu).

- Ali lahko država legitimno zapove organizacijam zasebnega sektorja, da morajo poskrbeti za lastno informacijsko varnost?

Država to že dela pri infrastrukturah javnega interesa (npr. banke), kjer z raznimi akti zahteva ustrezno varnost v njihovih omrežjih. Težava je, da država poda pravila, stroške pa mora ponavadi prevzeti zasebni sektor. Za dosego legitimnosti bi država morala poskrbeti za ustrezno rešitev pri financiranju projektov.

- Menite, da lahko država opravlja vlogo regulatorja na področju informacijske varnosti? Če da, s kakšnimi mehanizmi?

AKOS je nacionalni regulator, ki ureja in nadzira trg elektronskih komunikacij, radiofrekvenčni prostor itd. Država na področju varnosti elektronskih komunikacij z zakoni in podzakonski akti, ki pa so zaradi nenehnih sprememb na tem področju bolj smernice in na načelni ravni. Noben akt ne opredeli popolnoma natično, kakšni morajo biti ukrepi, ukrepi se namreč nalagajo na podlagi analiz stanja, analiz tveganja, vplivov na poslovanje itd.. Le-te se redno izvajajo, rezultat pa so lahko ureditvene odločbe, da se dosežejo zastavljeni zakonski cilji. Skratka, zakon ali podzakonski akti določajo cilje in namene. Pot do realizacije teh ciljev pa so specifični ukrepi, ki jih operaterji določijo sami ali AKOS z odločbami.

4. Kibernetski prostor je poln izzivov in posebnosti, s katerimi se tradicionalni pristopi zagotavljanja varnosti ne morejo uspešno kosati. Medtem, ko se razvijajo različni postopki obravnave kršitev, še vedno manjka ustrezna pravna podlaga. To področje nekako pokrivajo znotraj mednarodnih zavezništev, kako pa je v Sloveniji? Tudi vaša organizacija je akter, ki opozarja na potrebno ureditev. Kako bi bilo po vašem mnenju to najlažje urediti in ali se tej temi namenja dovolj interesa?

Na področju elektronskih komunikacij, Splošni akt o varnosti omrežij in storitev ter delovanje v izjemnih stanjih določa organizacijske ukrepe, ki jih morajo sprejeti operaterji za ustrezno zagotavljanje varnosti omrežij in storitev. Splošni akt temelji na standardu SIST ISO/IEC 27001. Standard sledi načelu nenehnih izboljšav (PDCA), kar v praksi pomeni, da operater mora redno izvajati analize varnostnih tveganj, prepoznavati nove grožnje in ranljivosti svojega omrežja in/ali storitev, določati ukrepe za zmanjšanje tveganj itd. Ravno tako,

operater ima obveznost, da poroča o varnostnih incidentih. AKOS te podatke obdeluje, jih anonimizira in jih enkrat na leto pošilja evropski varnostni agenciji (ENISA). ENISA te podatke, ki jih dobi tudi od drugih članicah EU obdela, in če ENISA ugotovi, da gre za tveganja, ki zadevajo večji del prostora EU, predlaga komisiji EU ukrepe, ki naj bi jih implementirale vse članice EU.

Operaterji v skladu z zakonom o elektronskih komunikacijah in omenjenim splošnim aktom morajo izvajati analize varnostnih tveganj, AKOS pa skozi nadzorne postopke izvaja preglede teh analiz, ali so prepoznane vsa tveganja, ali so ukrepi pravilno implementirani itd. Posebej so pomembni procesi pri katerih se obdelujejo osebni podatki v povezavi s prometnimi podatki. Izvaja se torej inšpekcijski nadzor pri operaterjih z namenom ugotavljanja ali delujejo v skladu z zakoni in podzakonskimi akti in izdanimi odločbami.

5. Kibernetski prostor zna biti nevarno mesto za vsakega gosta, še posebej za tiste, ki nimajo nobenega znanja o nevarnostih. Zadnja leta so vidni napori raznih organizacij, da se ozavesti posameznike/organizacije o varni rabi. Ozaveščanje javnosti je ena izmed vaših aktivnosti, zanima pa me, ali menite, da Slovenci pokažejo dovolj interesa? Ali organizacije izkoristijo znanje in izkušnje, ki jim ga nudite? Kaj bi še lahko naredili na tem področju, da se zviša interes javnosti?

AKOS sodeluje v projektu Safe.si, kjer vsak deležnik prispeva informacije s svoje sfere. AKOS posreduje nasvete s pomočjo operaterjev, ki imajo vpogled v aktualno dogajanje v omrežjih. V okviru projekta smo izdali že mnogo publikacij, nasvetov in ostalih gradiv, projekt pa se izvaja tudi na slovenskih šolah. V osnovi je projekt zasnovan za otroke in mladostnike, kljub temu pa se osredotoča tudi na starše in učitelje, da širijo znanje. Žal se ne ve, kakšen učinek ima vso to gradivo in ali javnost spremlja ter upošteva nasvete.

6. Februarja 2016 je Vlada sprejela Strategijo kibernetske varnosti, kjer so začrtane smernice in vloge države. Menite, da je v tej strategiji vloga zasebnih podjetij dovolj opredeljena, ali je preveč poudarka na vlogi države in njenih teles?

Imamo jo, je pa bolj izhodišče za naprej, natančneje podlaga za nadaljnje smernice, akte, sporazume ipd. Celotna pobuda je kot kaže zaenkrat malo zamrla, težava pa je v pomanjkanju ljudi. Manjkajo namreč viri in predvsem kader (strokovnjaki). Težava je v plačilu, saj bi bilo potrebno strokovnjake ustrezno plačati, denarja pa zaenkrat ni.

Opomba: Izjave izražajo intervjuvančeva osebna stališča in poglede, in ne nujno tudi AKOS, v kateri je zaposlen.

PRILOGA B: Intervju z Gorazdom Božičem (Ljubljana, 25. 7. 2016)

1. Državna informacijska varnost je odvisna od mnogih dejavnikov, med drugim tudi od varnosti informacijsko-komunikacijske tehnologije akterjev, ki sodelujejo pri aktivnostih kritične infrastrukture, gospodarstvu in drugih sektorjih z vplivom na državo.

    - Menite, da je slovenska informacijska varnostna kultura ustrezna?

Mislim, da je še dosti možnosti za izboljšanje. Prepogosto se še skrb za informacijsko varnost smatra kot nepotreben strošek, oziroma se nanjo po misli naknadno.

    - Ali javni in zasebni sektor pravilno pristopata k pereči tematiki?

Morda bi lahko rekel celo, da je del javnega sektorja, ki operativno upravlja s kritično infrastrukturo, bolj ozaveščen o potrebnosti zaščite sistemov, kot gospodarstvo v splošnem. Kot pozitivno izjemo tam bi izpostavil banke v Sloveniji, ki so že nekaj časa izpostavljene raznim omrežnim napadom (bolj natančno: njihovi komitenti) in se zavedajo pomembnosti zaščite in ustreznega odzivanja na grožnje.

2. Javni in zasebni sektor zelo različno pristopata k informacijski varnosti. Medtem, ko je v interesu javnega sektorja »javno dobro«, za zasebni sektor velja vodilo dobičkonosnosti in interesa delničarjev. Razni dokumenti in iniciative pozivajo k nekakšnemu javno-zasebnemu partnerstvu, ki bi bilo zmožno zagotoviti ustrezno informacijsko varnost.

    - Kakšno je vaše mnenje o teh iniciativah?

Zmerno skeptičen sem. Vprašanje je, ali je kultura sodelovanja pri nas na dovolj visokem nivoju, da je možen zrel partnerski odnos z uravnoteženjem javnih in zasebnih interesov. Mislim pa, da moramo na tem delati in da je sodelovanje potrebno.

    - Kako bi morale biti razdeljene vloge znotraj partnerstva?

Odvisno od ciljev in namena partnerstva. Bistveno je, da so vloge vseh partnerjev zelo natančno določene že na začetku in da vsi partnerji jasno razumejo svojo vlogo in se z njo strinjajo.

- Mislite, da je v Sloveniji takšno partnerstvo mogoče in ali poznate kakšen primer dobre prakse?

Z ustrezno pripravljenim okvirjem verjetno je.

3. Državna varnost je tradicionalno v domeni države, pri informacijski varnosti pa le-ta ne more samostojno opravljati potrebnih aktivnosti. Pomanjkanje interesa organizacij zasebnega sektorja in neustrezna notranja informacijska varnost imata implikacije na celoten sistem (npr. napad na večje podjetje lahko posledično povzroči škodo celotnemu slovenskemu gospodarstvu).

   - Ali lahko država legitimno zapove organizacijam zasebnega sektorja, da morajo poskrbeti za lastno informacijsko varnost?

Zaradi omenjene prepletenosti akterjev bo morala država predpisovati minimalne standarde, pod katerimi bodo morala podjetja delovati. Ta trend se vidi tudi na nivoju EU, kjer bodo države članice morale opredeliti operaterje bistvenih storitev (ta pojem počasi zamenjuje pojem kritične infrastrukture). Analogije recimo najdemo v požarni varnosti ali varnosti, vezani na transport.

   - Menite, da lahko država opravlja vlogo regulatorja na področju informacijske varnosti? Če da, s kakšnimi mehanizmi?

S pomočjo zakonodaje, s pristojnimi inšpekcijskimi organi in na drugi strani s primernimi programi ozaveščanja in spodbujanja uvajanja dobrih praks.

4. Kibernetski prostor je poln izzivov in posebnosti, s katerimi se tradicionalni pristopi zagotavljanja varnosti ne morejo uspešno kosati. Medtem, ko se razvijajo različni postopki obravnave kršitev, še vedno manjka ustrezna pravna podlaga. To področje nekako pokrivajo znotraj mednarodnih zavezništev, kako pa je v Sloveniji? Tudi vaša organizacija je akter, ki opozarja na potrebno ureditev. Kako bi bilo po vašem mnenju to najlažje urediti in ali se tej temi namenja dovolj interesa?

Sam ne vidim pravne podlage kot edine bistvene ovire. Nenazadnje SI-CERT že 20 let uspešno deluje in gradi na prostovoljnem sodelovanju drugih akterjev iz javnega sektorja in gospodarstva. Najboljši pristop je z uravnoteženo pravno podlago in skrbjo za operativno sodelovanje. Bistveni problem vidim pri resnem pomanjkanju zavedanja o pomembnosti tega področja na vrhu politike, pri odločevalcih v državi.

5. Kibernetski prostor zna biti nevarno mesto za vsakega gosta, še posebej za tiste, ki nimajo nobenega znanja o nevarnostih. Zadnja leta so vidni napori raznih organizacij, da se ozavesti posameznike/organizacije o varni rabi. Ozaveščanje javnosti je ena izmed vaših aktivnosti, zanima pa me, ali menite, da Slovenci pokažejo dovolj interesa? Ali organizacije izkoristijo znanje in izkušnje, ki jim ga nudite? Kaj bi še lahko naredili na tem področju, da se zviša interes javnosti?

Naše izkušnje s programom varninainternetu.si so, da je program ozaveščanja zelo dobro sprejet. Odziv javnosti je dober, interesa vidimo dovolj, tako pri posameznikih, kot tudi v gospodarstvu. Ko nas odkrijejo, so pozitivno presenečeni in veseli, da država tovrstne aktivnosti financira. Z več sredstvi bi bilo možno doseči širšo publiko in razširiti program, a ozaveščanje je tek na dolge proge.

6. Februarja 2016 je Vlada sprejela Strategijo kibernetske varnosti, kjer so začrtane smernice in vloge države. Menite, da je v tej strategiji vloga zasebnih podjetij dovolj opredeljena, ali je preveč poudarka na vlogi države in njenih teles?

Strategija sicer opredeljuje varnost kibernetskega okolja kot pomembno za delovanje gospodarstva, a bolj natančne vloge podjetij tam ne najdemo, po moje zato, ker še nismo prišli do konsenza o tem, kolikšna in kakšna naj bo vloga zasebnega sektorja, res pa je tudi, da smo morali najprej poskrbeti za osnovno delovanje mehanizmov, ki so znotraj javnega sektorja.

PRILOGA C: Intervju z izr. prof. dr. Denisom Čaleto (Ljubljana, 29. 7. 2016)

1) Državna informacijska varnost je odvisna od mnogih dejavnikov, med drugim tudi od varnosti informacijsko-komunikacijske tehnologije akterjev, ki sodelujejo pri aktivnostih kritične infrastrukture, gospodarstvu in drugih sektorjih z vplivom na državo.

- Menite, da je slovenska informacijska varnostna kultura ustrezna?

Je še vedno na relativno nizkem nivoju in to je problem, ko želimo poseči po višji stopnji varnosti. Skrbi nas, ker ni nizka le pri državljanih, temveč tudi v organizacijskih okoljih, kjer bi pričakovali višjo. Predvsem izpostavljamo kritično infrastrukturo, kjer niha pripravljenost od zelo dobre do zelo slabe. Na drugi strani imamo javnost, ki je podvržena kibernetskim

tveganjem (npr. na področju transakcij) – njihovo zaznavanje je odvisno od medijske pokritosti, dogodkov; boljše zaznavanje zaznamo, ko se tematika javno obravnava.

- Ali javni in zasebni sektor pravilno pristopata do pereče tematike?

V Sloveniji je pomanjkanje izobraževalnih elementov, ki bi jih morali vpeljati od osnovne šole dalje. Varnostna kultura je proces, ki ga je težko kar tako vpeljati. Pomanjkanje varnostne kulture mladih se pojavlja tudi pri novih zaposlitvah, ker mladi nimajo dovolj dobrega znanja, še posebej zaskrbljujoče pa je, če pridejo v organizacije z nizko varnostno kulturo, kar pomeni, da tudi tam zaposleni niso izpostavljeni problematiki in potrebnemu izobraževanju.

2) Javni in zasebni sektor zelo različno pristopata do informacijske varnosti. Medtem, ko je v interesu javnega sektorja »javno dobro«, za zasebni sektor velja vodilo dobičkonosnosti in interesa delničarjev. Razni dokumenti in iniciative pozivajo k nekakšnemu javno-zasebnemu partnerstvu, ki bi bilo zmožno zagotoviti ustrezno informacijsko varnost.

- Kakšno je vaše mnenje o teh iniciativah?

Te iniciative so kratkoročne, niso usmerjene v dolgoročno delovanje, kjer bi se lahko ustrezno merila učinkovitost. Zanima nas, ali je proces projekta prinesel rezultate in vzroki za uspeh ali neuspeh iniciative. Na tem področju manjkajo analize, ki bi jih lahko opravili z meritvami daljšega obdobja delovanja.

- Kako bi morale biti razdeljene vloge znotraj partnerstva?

Manjka zavedanje, da je ukrepe možno uspešno izvesti le s celovitim pristopom. ZJP mora biti usmerjeno k zavedanju, da je potrebno sodelovati in skupaj razvijati, šele nato se bodo pokazali rezultati na področju izobraževanja, mehanizmov in nove tehnologije. Pomembna je tudi povezljivost zasebnega in javnega omrežja (virus v zasebnem lahko pomeni prenos virusa v javno omrežje). Pri kritični infrastrukturi je ključna neprekinjenost delovanja. Tudi zasebni sektor se mora zavdati, da neprekinjenost delovanja njihove infrastrukture prinaša dobiček. Država mora videti strateški del, saj bi se nedelovanje kritične infrastrukture izrazilo na širši družbi. Država mora z zasebnimi izvajalci najti stične točke, morala bo nositi del finančnih obveznosti (ne nujno financiranje, lahko tudi kakšen drug pristop, npr. oprostitev davkov). Fokus bi moral biti na neprekinjenosti delovanja, in sodelovanja na področju usposabljanja

ter prenosa dobrih praks. Država ima veliko institucij, ki lahko poskrbijo za to, tako upravljalci ne bi rabili razvijati svojih modelov. Pod pokroviteljstvom države lahko skupaj naredijo nekakšen »think-tank«, kjer bi profitirala oba sektorja.

- Mislite, da je v Sloveniji takšno partnerstvo mogoče in ali poznate kakšen primer dobre prakse?

Slovensko združenje korporativne varnosti je primer, kjer sodelujejo gospodarske organizacije in javne inštitucije (SI-CERT, Urad za varovanje tajnih podatkov, Urad inf. pooblaščenke itd.). Akterji so prepoznali potrebo po sodelovanju za boljše delovanje in dosegli, da tudi upravljalci kritične infrastrukture vidijo globlji pomen odločitev, ne samo »ukazov«. Z razumevanjem problematike vsi akterji bolj vneto pristopijo k informacijski varnosti.

3) Državna varnost je tradicionalno v domeni države, pri informacijski varnosti pa le-ta ne more samostojno opravljati potrebnih aktivnosti. Pomanjkanje interesa organizacij zasebnega sektorja in neustrezna notranja inf. varnost imata implikacije na celoten sistem (npr. napad na večje podjetje posledično povzroči škodo celotnemu slovenskemu gospodarstvu).

- Ali lahko država legitimno zapove organizacijam zasebnega sektorja, da morajo poskrbeti za lastno inf. varnost?

Vedno je dilema, do kje lahko država kot krovna institucija posega, še posebej v poslovnem svetu. Liberalna usmeritev gospodarstva želi čim manj poseganja države. Za pričakovati je manjše poseganje, sicer imamo polno aktov, ki jih v praksi ne izvajamo. Legitimnost bi se izražala v primeru, da tisto kar država zapiše, tudi nato v praksi izvaja.

- Menite, da lahko država opravlja vlogo regulatorja na področju inf. varnosti? Če da, s kakšnimi mehanizmi?

Država ne more bežati pred svojo odgovornostjo, saj ima organizacije, ki so namenjene opravljanju točno določenih aktivnosti (npr. AKOS, Urad za varovanje tajnih podatkov ...). Do problema pride, ko se soočimo z bogatimi multinacionalkami, ki imajo na razpolago ogromno sredstev, strokovnjakov, pravnikov ipd., nad katerimi je težko izvajati regulativno vlogo. Regulacija se mora povečati s strokovnjaki, ki bodo ustrezno plačani, drugače bo

vloga bolj pasivna in bomo nekako le sledili trendom. Korak naprej bi znal mogoče biti tudi v smeri centralizacije (združevanje kadrov).

4) Kibernetski prostor je poln izzivov in posebnosti, s katerimi se tradicionalni pristopi zagotavljanja varnosti ne morejo uspešno kosati. Medtem, ko se razvijajo različni postopki obravnave kršitev, še vedno manjka ustrezna pravna podlaga. To področje nekako pokrivajo znotraj mednarodnih zavezništev, kako pa je v Sloveniji? Tudi vaša organizacija je akter, ki opozarja na potrebno ureditev. Kako bi bilo po vašem mnenju to najlažje urediti in ali se tej temi namenja dovolj interesa?

Zamujamo, ne bi smelo biti nejasnosti, izkrivljenih informacij (sprejem dokumentov pod pritiskom), zamujamo z akcijskim načrtom, opredelitvijo nalog določenih organov … Politika odriva sprejemanje dokumentov, saj le-ti s sabo potegnejo razna vlaganja, živimo pa v času, ko je miselnost v smeri premika sredstev na druga področja.

5) Kibernetski prostor zna biti nevarno mesto za vsakega gosta, še posebej za tiste, ki nimajo nobenega znanja o nevarnostih. Zadnja leta so vidni napori raznih organizacij, da se ozavesti posameznike/organizacije o varni rabi. Ozaveščanje javnosti je ena izmed vaših aktivnosti, zanima pa me, ali menite, da Slovenci pokažejo dovolj interesa? Ali organizacije izkoristijo znanje in izkušnje, ki jim ga nudite? Kaj bi še lahko naredili na tem področju, da se zviša interes javnosti?

V okviru ICS imamo izkušnje, ki kažejo, da je k varnosti potrebno pristopiti integrirano. Tako vsebino informacijske varnosti vključujemo v vse ostale vsebine, s katerimi se ukvarjamo. Ozaveščanje o informacijski varnosti je prisotno je v vsaki zgodbi (konference, projekti). V zadnjih 10 letih se je zavedanje dvignilo, lahko bi sicer bilo hitreje, vendar je trend rasti. Menedžment in lastniki v podjetjih so ključ do visokega dviga ali upada zavedanja inf. varnosti, zato je potrebno pristope prilagoditi njim, da skozi poslovno logiko razumejo pomembnost inf. varnost. Vsebino je potrebno prikazati skozi ekonomski jezik. Izkazalo se je, da kjer je bilo uspešno zavedanje, so bili končni rezultati dobri. Zavedanje o informacijski varnosti se je med zaposlenimi povečalo. Slovensko združenje korporativne varnosti skrbi za širitev idej, krog deležnikov se veča, rezultati pa se kažejo na celoviti ravni Slovenije.

6) Februarja 2016 je Vlada sprejela Strategijo kibernetske varnosti, kjer so začrtane smernice in vloge države. Menite, da je v tej strategiji vloga zasebnih podjetij dovolj opredeljena, ali je preveč poudarka na vlogi države in njenih teles?

Od Strategije ni pričakovati, da bo konkretizirala stvari; to je naloga akcijskega načrta, ki mora biti sprejet čimprej. Le-ta mora opredeliti vire, terminsko opredeliti vse dejavnosti, prioritete področij in ostala področja. Potrebno se bo začeti konkretno pogajati o ciljih, sredstvih in načinih dosege ciljev. Po nekem določenem obdobju bo potrebno oceniti delovanje ter načrt prilagoditi oziroma obnoviti. Napredek je potrebno spremljati dolgoročno, beležiti pluse in minuse ter uspešnost akterjev. Slovenija lahko pomaga slovenskim podjetjem na marsikaterim področju, znanje lahko posreduje v mednarodno okolje. S tem mora spodbuditi napore slovenskih podjetij in institucij na tem področju, saj lahko s pomočjo države prodrejo v mednarodno sfero in tudi tam črpajo informacije in vire (sofinanciranje s strani mednarodnih organizacij) za nadaljnji razvoj.

PRILOGA Č: Intervju z mag. Damijanom Marinškom (Ljubljana, 22. 7. 2016)

1) Državna informacijska varnost je odvisna od mnogih dejavnikov, med drugim tudi od varnosti informacijsko-komunikacijske tehnologije akterjev, ki sodelujejo pri aktivnostih kritične infrastrukture, gospodarstvu in drugih sektorjih z vplivom na državo.

- Menite, da je slovenska informacijska varnostna kultura ustrezna?

Ni ustrezna oziroma je sploh ni.

- Ali javni in zasebni sektor pravilno pristopata do pereče tematike?

Javni sektor, natančneje MJU, da. Direktorat za informacijsko družbo že nekaj let gradi na tem, vendar se sooča z velikim problemom, tj. pomanjkanjem virov. Kljub temu ima kar nekaj rezultatov, kot je npr. že to, da se govori in razmišlja o informacijski varnosti. Sprejeta je bila Strategija o kibernetski varnosti, kjer je še vedno kar nekaj prostora za napredek. Prav tako se pripravlja Uredba o informacijski varnosti, je pa še vedno težavno razumevanje tematike. Kot rešitev so morda primerni programi ozaveščanja.

V zasebnem sektorju do tematike pravilno pristopajo strokovnjaki s tega področja, večina ostalih pa je tudi začela razmišljati o pomembnosti informacijske varnosti, seveda pa bodo vedno prisotne napake. Nekateri sektorji morajo obvezno poročati o dogajanju na tem področju (Direktiva NIS), vendar pa normativno urejanje zaostaja.

2) Javni in zasebni sektor zelo različno pristopata do informacijske varnosti. Medtem, ko je v interesu javnega sektorja »javno dobro«, za zasebni sektor velja vodilo

dobičkonosnosti in interesa delničarjev. Razni dokumenti in iniciative pozivajo k nekakšnemu javno-zasebnemu partnerstvu, ki bi bilo zmožno zagotoviti ustrezno informacijsko varnost.

- Kakšno je vaše mnenje o teh iniciativah?

To je edina pot, saj javni sektor ugotavlja, da ne ponuditi dovolj velikega plačila, da bi strokovnjaki želeli opravljati to delo. Velik korak v to smer je Iniciativa gospodarske zbornice, ki pa je še v povojih. Le-ta namreč združuje tudi državo in univerzo.

- Kako bi morale biti razdeljene vloge znotraj partnerstva?

Država bi morala imeti pobudo, koordinacijo, nadzor in pregled, operativa pa bi bila prepuščena zasebnemu sektorju.

- Mislite, da je v Sloveniji takšno partnerstvo mogoče in ali poznate kakšen primer dobre prakse?

Obstajajo primeri partnerstva z zunanjimi izvajalci iz zasebnega sektorja, vendar gre le za časovno omejene projekte. Zaenkrat ni javno-zasebnega partnerstva.

3) Državna varnost je tradicionalno v domeni države, pri informacijski varnosti pa le-ta ne more samostojno opravljati potrebnih aktivnosti. Pomanjkanje interesa organizacij zasebnega sektorja in neustrezna notranja inf. varnost imata implikacije na celoten sistem (npr. napad na večje podjetje posledično povzroči škodo celotnemu slovenskemu gospodarstvu).

- Ali lahko država legitimno zapove organizacijam zasebnega sektorja, da morajo poskrbeti za lastno inf. varnost?

Za nekaj takšnega bo poskrbela Uredba o informacijski varnosti. Gre za akt vlade, s katerim lahko zapoveduje akterjem, ki si priključeni na njihovo omrežje. Sem ne spadajo le vladne organizacije, temveč tudi razne druge (npr. občine), med katerimi najdemo tudi nekatere iz zasebnega sektorja, ki sodelujejo pri izvajanju vladnih dejavnosti. Tudi ta morajo v tem primeru sprejeti pravila delovanja v omenjenem omrežju.

Ko bo sprejet ustrezen zakon, bo lahko država ustrezno zapovedala. Operativna podlaga je v 74. členu Zakona o javni upravi, vendar se soočamo s težavami pri tolmačenju.

- Menite, da lahko država opravlja vlogo regulatorja na področju inf. varnosti? Če da, s kakšnimi mehanizmi?

Posredno že vpliva s širitvijo idej. Direktorat za inf. družbo je predlagal mnogo rešitev, ki pa jih zasebni sektor zaradi prilagodljivosti prevzame in razvije še preden se javni sektor odzove na pobude. Država bo slej ali prej opravljala nalogo regulatorja. Zaenkrat posredno, ko bo sprejet ustrezen zakon pa tudi neposredno. Seveda bodo določene zadeve ostale v rokah zasebnega sektorja.

4) Kibernetski prostor je poln izzivov in posebnosti, s katerimi se tradicionalni pristopi zagotavljanja varnosti ne morejo uspešno kosati. Medtem, ko se razvijajo različni postopki obravnave kršitev, še vedno manjka ustrezna pravna podlaga. To področje nekako pokrivajo znotraj mednarodnih zavezništev, kako pa je v Sloveniji? Tudi vaša organizacija je akter, ki opozarja na potrebno ureditev. Kako bi bilo po vašem mnenju to najlažje urediti in ali se tej temi namenja dovolj interesa?

Pristop k tematiki je različen glede na države. Kot primer lahko izpostavim Internet stvari (angl. Internet of Things). Evropska unija pripravlja dokumentacijo, da bi ti produkti potrebovali nekakšen certifikat (standardizacijo). Težava je, ker velike države to spodbujajo, manjše države (kjer je seveda tudi Slovenija) pa nimajo dovolj kadra, institucij ipd. za ustrezno ureditev in izdajo certifikatov. Tako bodo manjše države ostale brez certificiranih izdelkov, kar škodi lastnemu trgu. Npr. Gorenje ne bo moglo izdajati certificiranih produktov, če bodo želeli postopke opraviti v tujini, pa je zopet vprašanje glede korektnosti, saj se zna zgoditi, da bo tuja država želela zaščititi lastna podjetja in zato upočasnjevala postopke certificiranja podjetij drugih držav.

5) Kibernetski prostor zna biti nevarno mesto za vsakega gosta, še posebej za tiste, ki nimajo nobenega znanja o nevarnostih. Zadnja leta so vidni napori raznih organizacij, da se ozavesti posameznike/organizacije o varni rabi. Ozaveščanje javnosti je ena izmed vaših aktivnosti, zanima pa me, ali menite, da Slovenci pokažejo dovolj interesa? Ali organizacije izkoristijo znanje in izkušnje, ki jim ga nudite? Kaj bi še lahko naredili na tem področju, da se zviša interes javnosti?

Direktorat za informacijsko družbo pripravlja ozaveščanje za zaposlene v javnem sektorju, SI-CERT (Arnes) za državljane, nič pa ne bo narobe, če zaživi Iniciativa GZ in prevzame določen delež ozaveščanja. Sicer pa bo ljudi težko prisiliti, da se izobrazijo na tem področju, če ne bodo imeli sami interesa.

6) Februarja 2016 je Vlada sprejela Strategijo kibernetske varnosti, kjer so začrtane smernice in vloge države. Menite, da je v tej strategiji vloga zasebnih podjetij dovolj opredeljena, ali je preveč poudarka na vlogi države in njenih teles?

Prvi korak k temu je ustanovitev Sekcije GZ, ki se sicer trenutno sooča s sprejetjem poslovnika. Svojo vlogo pa mora odigrati tudi država, ki mora prepoznati svojo ključno nalogo in jo ustrezno opraviti. Brez tega koraka ne bo rezultatov.