UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Jure Dokl

Kibernetska varnost omrežij

Magistrsko delo

Ljubljana, 2012

UNIVERZA V LJUBLJANI

FAKULTETA ZA DRUŽBENE VEDE

Jure Dokl

Mentor: doc. dr. Uroš Svete

Kibernetska varnost omrežij

Magistrsko delo

Ljubljana, 2012

Scientia potentia est.

Per aspera ad astra.

ZAHVALA

Iskrena zahvala mentorju doc. dr. Urošu Svetetu za strokovno pomoč in usmeritve pri pisanju. Hvala tudi vsem domačim, da ste me spremljali tekom študijske poti.

Posebno zahvalo namenjam moji Karolini za neomajno podporo ter izkazano ljubezen in tople besede vzpodbude, da sem ta projekt lahko uspešno pripeljal do konca.

POVZETEK

Kibernetska varnost omrežij

Vse več ključnih storitev v našem življenju temelji na informacijskih sistemih. Ti predstavljajo temeljni element naše sposobnosti vse od hitrega komuniciranja in oskrbe z osnovnimi dobrinami do najbolj zapletenih in strukturiranih protokolov pri zagotavljanju varnosti. Ti informacijski sistemi za svoje delovanje potrebujejo različna omrežja, varnost teh omrežij je torej ključna za njihovo delovanje. Skupek omrežij in informacijskih sistemov tako lahko združimo pod okrilje ključne informacijske infrastrukture.

V magistrskem delu sem se osredotočal predvsem na kibernetski vidik varnosti teh omrežij in sistemov. Ta segment varnosti ključne informacijske infrastrukture prevzema poglavitno vlogo, saj postopoma vsi ostali sistemi temeljijo na elektronskih procesih in omrežjih. Kibernetske grožnje postajajo kompleksnejše in napadi pogostejši, zato je ključno, da odgovorni posamezniki in institucije prepoznajo ta vidik kot izredno pomemben.

Za boljše in celovito razumevanje problematike v delu tako predstavim nekaj pogostejših kibernetskih groženj in principov delovanja, s katerimi bi lahko bila ogrožena varnost omrežij. Kot najbolj prikrito in kompleksno obliko ogrožanja, ki združuje več tehnik, naj omenim le t. i. napredne trajne grožnje, od ostalih groženj jih ločijo predvsem vztrajnost in obsežna sredstva napadalca. Tovrstni napadi so neposredna grožnja sistemom ključne informacijske infrastrukture in s tem njihovi varnosti. V nadaljevanju izpostavim načrtovane ukrepe na različnih ravneh, s katerimi nameravajo institucije dvigovati raven varnosti omrežij. Brezmejna narava kibernetskih groženj zahteva premagovanje razlik v nacionalnih pristopih na področju kibernetske varnosti in vzdržljivosti ključnih sistemov ter terja okrepljeno vlogo mednarodnih institucij.

V delu sem tako poskušal odgovoriti na osrednje vprašanje mojega raziskovanja: katere so temeljne grožnje kibernetski varnosti omrežij in kateri so ukrepi za povečanje varnosti in preprečevanje oz. omejevanje negativnih posledic kibernetskih napadov. V zaključku sem izluščil bistvene elemente in ukrepe, ki pripomorejo k celovitem izboljšanju kibernetske varnosti omrežij. Ključna pa je ugotovitev, da posamezen ukrep ali celo skupina ukrepov na posameznem segmentu ni in ne bo dovolj za reševanje uganke kibernetske varnosti. Odgovor se skriva v skupni rezultanti vseh ukrepov.

Ključne besede: varnost, kibernetska varnost, kibernetske grožnje, ključna informacijska infrastruktura, zaščita ključne informacijske infrastrukture.

ABSTRACT

Network Cyber Security

Information systems and cyberspace touches nearly every key service in our lives. They constitute a fundamental element of our ability for rapid communication and fulfilment of our basic needs up to the most complex and structured protocols to ensure safety. These information systems need various types of networks for their operation, security of these networks is therefore crucial to the operation of information systems. Furthermore, networks and information systems are the basis of critical information infrastructure.

This master's thesis is focused primarily on cyber security aspects of critical information infrastructure. The importance of cyber security of critical information infrastructure is increasing at a high pace, due to its key position and the transition of all other systems to digital processes and networks. Cyber threats on the other hand are becoming more complex and attacks more frequent, it is therefore vital that decision makers and key institutions recognize this aspect of security as extremely important.

Due to better and more comprehensive understanding of the problem the work examines some common cyber threats and principles of operation, which could compromise the security of networks. The most subtle and complex form are advanced persistent threats, which combine several techniques and differentiate from other threats by intruder’s perseverance and resources. Such attacks are a direct threat to critical information infrastructure systems and thus their safety. Moreover the work explains some planned actions at various levels of the institutions with which they intend to raise the level of network security and resilience. The boundless nature of cyber threats requires overcoming differences in national approaches to cyber security and resilience of critical systems and in addition demands an enhanced role for international institutions.

The following thesis tries to answer the core question of my research that is, *which are fundamental threats to network cyber security and what are the measures to increase safety and prevent or limit the negative consequences of cyber attacks*. To sum things up, I highlighted key elements and actions that contribute to the overall improvement of cyber security of critical information infrastructure. The key finding would be that a particular action or even group of measures in a given segment does not and will not be sufficient to solve the puzzle of cyber security. The answer lies within the total sum of all actions.

Keywords: security, cyber security, cyber threats, critical information infrastructure, critical information infrastructure protection.

KAZALO

KAZALO SHEM

KAZALO TABEL

KAZALO GRAFOV

1 Uvod

Preteklo stoletje sta prvenstveno oblikovali razvoj industrializacije in z njo razplamtela globalizacija. Mnogo odkritij je bilo prav tako kot v preteklih stoletjih gnanih z razvojem tehnologije. Pravi tehnološki preskok in veliko spremembo vsakdanjika pa je omogočil razvoj mikročipa in s tem sodobne informacijske tehnologije. Človeštvo je z digitalno revolucijo napredovalo iz industrijske v informacijsko dobo. V 21. stoletju razvoj sledi trendu zadnjih desetletij, to je nadaljevanju informatizacije oz. digitalne revolucije. Informacijska doba je tu, posamezniki in drugi akterji imajo z njo možnost skorajda brezplačno prenašati informacije kamorkoli in komurkoli, družba je s tem in z razvojem komunikacij postala neverjetno povezana, dostopnost informacij je postala trenutna.

Vse te spremembe nezadržno vplivajo na vire ogrožanja, ki so danes aktualni; nove grožnje niso zamenjale starih, temveč so postale povsem nova dimenzija. V 19. stoletju je človeštvo v bitki za prevlado poskušalo svojo prednost pridobiti na morju, v 20. stoletju je bila odločujoča sfera delovanja v zraku, v 21. stoletju pa se bodo boji odločali tudi v kibernetskem prostoru; s temi besedami Velika Britanija orisuje pomembnost strategije za varnost kibernetskega prostora. Uporaba informacijsko-komunikacijskih tehnologij (Brunner in Suter 2009, 35) je pomembno preobrazila okolje, v katerem delujemo, bliskovit razvoj celotne panoge pa zaradi svojih specifičnosti pušča velik del javnosti v ozadju. Posamezniki, organizacije oz. države s spretnim izkoriščanjem in poznavanjem prednosti novih tehnologij skorajda obvladujejo sedanjost. V tem segmentu informacijske dobe se tako razvija področje, kjer se bodo bojevale nove bitke in dosegale nove zmage. Kibernetsko bojevanje oz. kibernetska vojna je tako realnost našega vsakdanjika. Kot je že znameniti Carl von Clausewitz v svoji knjigi *O vojni* definiral vojno »kot nadaljevanje politike z drugimi sredstvi«, lahko danes to definicijo razširimo še na kibernetsko dimenzijo. Pojmovanje uporabe sile je tako danes preneseno tudi na področje bitov in bajtov oz. v kibernetski prostor[1], pravilna uporaba te sile pa je tako pomembna kot še nikoli, saj

[1] Islovar kibernetski prostor definira kot ljudi, podatke in računalnike, povezane tako, da delujejo drug na drugega (http://www.islovar.org/iskanje_enostavno.asp, 28. april, 2011). Zanimivo pa je, da

se razviti svet čedalje bolj poslužuje uporabe kibernetskega prostora, s tem pa odpira novo dimenzijo obstoječim varnostnim izzivom.

Kibernetska varnost omrežij je tako le segment v celotni problematiki informacijske varnosti, glede na današnjo razpredenost različnih omrežij pa ima osrednjo vlogo pri obrambi in preventivi pred neželenimi vplivi (Schmitt 2005, 7). Napadeno omrežje je lahko element kateregakoli področja, obrambno-varnostnega, telekomunikacijskega, električnega, poslovnega oz. računalniškega, rezultati napada so v vsakem primeru lahko uničujoči. V primeru napadov na omrežja nacionalnega pomena so posledice lahko vidne takoj (ali pa tudi ne) in imajo neposreden vpliv (ali pa tudi ne) na širše množice, v primeru napada na omrežja gospodarskih subjektov pa so učinki lahko subtilnejši oz. se manifestirajo skozi daljše obdobje ali pa povsem na drugem področju, čeprav je vzrok za te posledice lahko kibernetskega izvora. Najmanj obsežne posledice pa imajo kibernetske grožnje na ravni posameznika; čeprav so grožnje majhne po obsegu z vidika človeštva, imajo za posameznika lahko velike posledice.

Vloga varnosti teh omrežij je torej ključnega pomena za njihovega uporabnika, in sicer ne glede na obsežnost in razvejanost omrežja. Že danes so opazne glavne pomanjkljivosti naše družbe v odzivih proti tovrstnim grožnjam, vsaj kot jih vidijo v globalno vodilnem podjetju[2] (McAfee 2009) področja tehnologij informacijske varnosti. Prva ovira je neprepoznavnost tovrstnih groženj s strani odločevalcev, saj v njihovi percepciji še niso dovolj pomembne. Druga ključna ovira je brezmejnost kibernetskih groženj, saj jim geografske razdalje, politične strukture in omejene pravne pristojnosti olajšujejo delovanje. Tretja pomanjkljivost pa je slaba pripravljenost in opremljenost ter *ad-hoc* struktura inštitucij, ki težko sledijo tempu zasebne pobude kibernetskega kriminala.

Teh nekaj idej in konceptov je temeljnih pri razumevanju teme mojega magistrskega dela, saj bom v njem poskušal identificirati glavne grožnje omrežjem in poiskati ključne ukrepe, ki varnost omrežij in s tem nas vseh izboljšujejo. Zavedam se, da

---

Encyclopedia Britannica oriše kibernetski prostor kot regijo, ki bi lahko pomembno vplivala na strukturo našega gospodarstva, razvoj naših skupnosti in varovanje naših pravic. Povzeto po: *Encyclopedia Britannica*, Inc. http://dictionary.reference.com/ browse/cyberspace (29. april, 2011).

[2] McAfee Inc. je trenutno največje svetovno podjetje, ki se ukvarja z informacijsko varnostjo in tehnologijo.

bodo zaradi izredne kompleksnosti problematike in množice vpletenih akterjev ter visokega tempa sprememb na tem področju, predlagani ukrepi samo del inštrumenta, s katerim bi lahko lažje obvladovali grožnje.

Kot izhaja iz Evropskih načel in smernic za odpornost interneta (European principles and guidelines for Internet resilience and stability 2011) naj bi EU v prihodnje načrtno razvijala in podpirala visoko stopnjo pripravljenosti, varnosti in razvoj zaščitnih zmogljivosti za zaščito informacijsko-komunikacijskih omrežij, tehnologij in digitalnih sistemov. Razlogov za tovrstno ukrepanje je več, glavni pa je, da vse več ključnih storitev temelji na digitalnih sistemih, katerih motnje v delovanju zaradi kibernetskih napadov (ali drugih vzrokov) lahko povzročijo ohromitev družbe kot celote. Zaradi čedalje kompleksnejše narave tovrstnih ogrožanj, njihovega povečanega vpliva ter napovedane pogostosti (O'Hara 2004, 19), ocenjujem, da je potrebno področje kibernetskega ogrožanja omrežij podrobneje preučevati ter neprestano spremljati njegov bliskovit razvoj. Opustitev tega področja kot manj pomembnega oz. manj poglobljeno preučevanje vključenih dejavnikov, bi bila usodna napaka pri zagotavljanju varnosti na vseh področjih. Brezmejna narava interneta nujno pogojuje čezmejno sodelovanje vseh vpletenih, zato so ključne aktivnosti mednarodnih in nadnacionalnih organizacij, na nacionalni ravni pa vseh internetnih akterjev, katerih sinergijsko delovanje ima potencial zmanjševanja ogroženosti omrežij.

Razvoj relevantne literature na tem področju je hiter, visoka strokovnost in nepoljudna narava pa omejujeta njen doseg. Obvladovanje tovrstnih groženj je zaradi zgoraj navedenih razlogov za širšo populacijo prezapleteno, točno ta populacija (oz. njena oprema) pa je zaradi navedenih razlogov lahko orodje v rokah zlonamernežev, saj s pridom zlorabljajo njihovo nepoučenost in izpostavljenost tovrstnim grožnjam. Izvirni znanstveni prispevek magistrske naloge je tako poizkus celovitega prikaza možnih ukrepov na področju pripravljenosti, preprečevanja, odkrivanja in odziva na kibernetske grožnje, poleg tega pa še omejevanje nastajanja škode in odprava posledic. S pomočjo zbranih ukrepov bo imel preučevalec kompetentno orodje in tako možnost povečati verjetnost obvladovanja groženj, ki tem sistemom grozijo.

Naj za zaključek povzamem še misel Davea DeWalta (McAfee 2008, 2), ki lepo oriše bistvo problematike kibernetske varnosti omrežij: »Bojevanje s kibernetskim kriminalom je neprestana bitka, globalni boj... in šele začel se je.«

2 Metodološki okvir

2.1 Opredelitev predmeta in ciljev preučevanja

Namen magistrskega dela je preučevanje kibernetske varnosti omrežij, spoznavanje groženj, akterjev, razsežnosti in drugih vzrokov za ogroženost omrežij in ključne informacijske infrastrukture ter razvijanje teorije na tem področju. Spoznavanju glavnih tipov groženj bo sledilo spoznavanje temeljnih ukrepov varovanja pred njimi ter optimizacija priporočil in navodil za preventivno ravnanje.

V sklepnem delu naloge bom na podlagi preučenih gradiv in sistemske preučitve teh kompleksnih groženj izdelal seznam priporočil in ukrepov, s katerimi bo moč bolje obvarovati omrežja, ki sestavljajo ključno informacijsko infrastrukturo, ki je nepogrešljiv element širše infrastrukture oz. še pomembneje širše ključne infrastrukture. V primerih kibernetskega ogrožanja pa je informacijska infrastruktura oz. omrežje kar bistven element ogrožanja in hkrati tudi neposredna tarča napadov.

Cilj dela je najprej vzpostaviti konceptualno-teoretični aparat s poznavanjem sodobnih vidikov ogrožanja in pojmovanja varnosti, med katerimi bo seveda poudarek na kibernetski varnosti. Nadalje imam namen elemente kibernetske varnosti poiskati v obstoječih teoretičnih varnostnih konceptih in definirati temeljne obravnavane pojme. Osrednji del naloge bo posvečen preučevanju groženj ter iskanju odgovorov na te grožnje tudi z institucionalnega vidika državnih in naddržavnih organizacij, temeljni cilj dela pa je vzpostaviti priporočil za mehanizme in ukrepe, ki lahko kibernetsko varnost omrežij izboljšajo.

2.2 Raziskovalno vprašanje

Temeljno raziskovalno vprašanje bo naslednje.

Katere so temeljne grožnje kibernetski varnosti omrežij in kateri so ukrepi za povečanje varnosti in preprečevanje oz. omejevanje negativnih posledic kibernetskih napadov?

Rezultat magistrskega dela bo na podlagi analize preučenih groženj in ukrepov ter izdelave priporočil hkrati tudi odgovor na osrednje raziskovalno vprašanje.

2.3 Uporabljena metodologija

Pri pisanju magistrskega dela nameravam uporabiti več različnih znanstvenih metod preučevanja problematike. Izbiro konkretne metode bom prilagodil posamičnem obravnavanem predmetu oz. segmentu. Osrednje uporabljene metode bodo zbiranje, analiza in interpretacija primarnih in sekundarnih virov, prednostno strokovnih knjig, internetnih virov, strokovnih člankov in prispevkov ter primarnih virov, prvenstveno priporočil in usmeritev evropskih in domačih institucij. Uporaba kvantitativnih metod bo namenjena predvsem analiziranju uradnih podatkov oz. že doslej zbranih merljivih stroškov in učinkov kibernetskega ogrožanja. V zadnjem delu naloge pa bom uporabil metodo inverzne dedukcije, s pomočjo katere nameravam skleniti to raziskovanje. Do vseh virov pristopam s kritične distance.

Magistrsko delo bo v osnovi raziskava, kjer bom (predvsem) s pomočjo kvalitativnih raziskovalnih metod sledil cilju razvijanja teorije in ukrepov na področju kibernetske varnosti omrežij in ukrepov za obvladovanje njenih groženj. Na podlagi preučevanja raznolikosti posamičnih groženj, protiukrepov in njihovih posledic oz. rezultatov bom z metodo sinteze spoznanj izluščil bistvene elemente, ki pripomorejo k uspešnemu varovanju omrežij. Analitični okvir obravnavane teme je tako omejen z vsemi oblikami kibernetskih groženj in ukrepi, ki te grožnje omejujejo, postavljen pa je na podlagi

preučenih družbenih teorij, predvsem koncepta človekove varnosti in kritičnih teorij varnosti.

2.4 Struktura analize

Izdelavo magistrskega dela lahko razdelim na naslednje segmente:

- V prvem delu bom s pomočjo analize virov, primarnih in sekundarnih, definiral in podrobneje pojasnil ključne koncepte, med njimi predvsem sodobno pojmovanje varnosti in relevantne teoretične koncepte ter temeljne pojme, kot so sodobna varnostna paradigma, informacijska in omrežna varnost ter ključna informacijska infrastruktura. Z uporabo pojasnjevalno-opisne metode in sinteze bom koncepte in pojme združil v konceptualno-teoretičen aparat, zaradi uporabe že obstoječih konceptov pa gre tu predvsem za deduktivno metodo.
- S pomočjo izdelanega aparata v prvem segmentu se bom najprej posvetil različnim vidikom in učinkom kibernetskih groženj na varnost omrežij. Zanimale me bodo temeljne razsežnosti ogroženosti kot tudi drugi vidiki, ki spremljajo kibernetske grožnje in njihov vpliv. V nadaljevanju bom predstavil najpogostejše pojavne oblike kibernetskih groženj, ki se jih akterji poslužujejo. S podrobnejšim poznavanjem tipov groženj se bom lahko posvetil naslednjemu delu naloge.
- Prepoznavanju groženj bo sledila analiza obstoječih ukrepov in aktivnosti, ki jih različne ravni institucij uporabljajo pri varovanju omrežij in ključne informacijske infrastrukture ter vpogled v organizacijsko logiko pristopa k tem izzivom. Omenil bom tudi nekaj ključnih standardov informacijske varnosti.
- V zadnjem delu sledi na podlagi predhodnih sklopov groženj in ukrepov izvedba primerjalne analize le-teh in interpretacija temeljnih struktur ukrepov, verifikacija raziskovalnih vprašanj ter na podlagi vsebinske analize, izdelava priporočil in primernih ukrepov za izboljšanje kibernetske varnosti omrežij informacijske infrastrukture.

Zadnji, sklepni del ima ključen pomen za relevantnost znanstvenega prispevka, saj bo šlo pri izdelavi priporočil za induktivno znanstveno metodo, i. e. za ustvarjanje sklepov iz zaznanih lastnih izkustev na širšo raven pri proučevanju problematike

kibernetske varnosti omrežij. Ker se zavedam omejitev induktivnih metod, imam namen v tem delu uporabiti tudi t. i. koncept inverzne dedukcije, v okviru katerega se gradi teorija skozi vzpostavljanje (teoretske) povezave med izkustvenimi posplošitvami in splošnimi teoretskimi trditvami kot to metodo oriše Hafner-Fink[3]. Z uporabo te metode bom združil dva temeljna elementa znanstvenega raziskovanja, i. e. logiko (razum) in opazovanje (izkustvo).

Menim, da je tovrstna struktura primerna, saj bo za zadnji del naloge potrebno poznavanje obsežnih informacijskih konceptov, družbenih teorij in predhodno izdelanih priporočil oz. predlaganih ukrepov s tega področja. Iz tega vidika je smiselno, da najprej spoznamo kibernetske grožnje in obseg ogrožanja, nato spoznamo obstoječe ukrepe in šele na koncu na podlagi vsega preučenega gradiva, izpeljemo metodo inverzne dedukcije pri iskanju rešitev. Ob tem velja opozoriti, da se zavedam metodoloških pomanjkljivosti uporabljenih metod in da je moj namen s priporočili pri preučevalcu prvenstveno vzbuditi zanimanje za tovrstno problematiko, vzbuditi razumevanje temeljnih konceptov tovrstnega ogrožanja, na podlagi kateri bo preučevalec sam lahko izpeljal manjše sklepe in ugotovitve za situacije, ki bodo šele nastale. Osnovna želja tudi ostaja, da bi preučevalec magistrskega dela na podlagi prebranega in dodatnih virov sam lahko osvojil veščine, s katerimi bo lahko aktivno sodeloval pri reševanju in preprečevanju bodočih izzivov s področja kibernetskega ogrožanja na sistemski ravni.

[3] Podrobnosti metode so opisane v dokumentu Nekatera temeljna vprašanja znanstvenega raziskovanja družbe, ki je na voljo na: http://www1.fov.uni-mb.si/mayer/MDR/Hafner%20Fink%20Mitja-Znanost%20in%20 znanstveno%20raziskovanje.pdf (28. maj 2011).

3 Konceptualno-teoretični aparat

3.1 Sodobno pojmovanje varnosti

Razvoj svetovnega političnega in družbenega življenja v zadnjih dveh desetletjih po koncu hladne vojne, je nezadržno vplival tudi na varnostne okoliščine. Te so bile prvič po skoraj pol stoletja drastično spremenjene, v novem okolju strateškega vakuuma[4] so postala (zastarela) teoretična orodja precej neprimerna za pojasnjevanje razmer in soočanje z novimi pojavi na področju varnosti. Grizold (2005, 7) tako ugotavlja, da je imelo varnostno okolje v preteklosti večinoma politične in vojaške razsežnosti, danes pa so v ospredju drugi vidiki širše socialne in kulturno-civilizacijske dimenzije. Razbrati je mogoče dva temeljna trenda (Grevi 2009, 9), ki spreminjata mednarodno in s tem varnostno okolje:

- prerazporejanje moči na globalni ravni, kar vodi do nove oblike multipolarne ureditve ter
- povečana medsebojna odvisnost, ki enakovredno vpliva na blaginjo in varnost tako velikih sil, kot širše mednarodne skupnosti.

Potreben je bil torej teoretski preskok oz. redefiniranje varnostne paradigme. Sodobna razprava o varnosti se tako usmerja predvsem na referenčne objekte **(na koga se varnost nanaša)**, kdo ali kaj to varnost ogroža **(grožnje varnosti)** in seveda na kakšen način to varnost zagotavljati **(varnostni mehanizmi).** To so tri osrednje dileme, ki definirajo sodobno varnostno paradigmo (Liotta v Svete 2005, 55). Tradicionalna varnost v smislu vojaške obrambe ozemlja držav je presežena, področja preučevanja varnosti pa so se razširila na več področij človekovega delovanja ter na različne ravni od mednarodne, nadnacionalne, državne, institucionalne, do posameznikove.

Različni avtorji (Malešič 1994, 97–104; Walt 1998, 29–44) delijo varnostno paradigmo na tri ključne teoretične perspektive. Prva je **politika moči in varnosti**, ki ima temelje v delih Hobbesa, Macchiavellija, Webra in drugih ter poudarja kvazianarhično naravo svetovnega političnega sistema, ukvarjanje držav z

[4] To novo okolje je imelo izreden pomen tudi za preoblikovanje organizacij (NATO), ki so temeljile na predhodnih ureditvah, potrebni so bili novi strateški dokumenti in širitve (Grizold 2005, 22).

nacionalno varnostjo, vojaško močjo (t. i. *might is right* pristop), bitko za naravne vire, nadzor ozemlja in monopolizira uporabo sile s strani države (realizem). Druga, **politika soodvisnosti in transnacionalnih odnosov,** temelji predvsem na idejah Smitha, Durkheima, Comta in drugih. Poudarja sožitje in interakcijo mnogih politično aktivnih skupin, omenja spreminjajočo se vlogo države, kompleksno politično in organizacijsko okolje, globalne finančne in komercialne tokove ter kot osrednji element poudarja demokratičnost in tržni kapitalizem v miroljubnem svetovnem okolju, čigar osrednja vrednota je svoboda v smislu odtujenosti omejitev s strani drugih akterjev (Wellings ur. 2009, 8–9) (liberalizem). Tretja pa je **politika nadvlade in odvisnosti**, ki temelji na delih Marxa, Engelsa in Lenina in vidi državo zlorabljeno s strani ekonomskih in političnih interesov, svet razdeljen na center in periferijo in težave družbe vidijo predvsem v imperializmu in kapitalizmu (marksizem). Vsaka od perspektiv uteleša različen pogled na svet, bistvene razlike pa se pokažejo predvsem pri odnosu med celoto in deli politične arene, pri možnostih spreminjanja svetovnega sistema (konservativni realizem, reformistični liberalizem in radikalni marksizem) ter odnosu do vrednot in politične akcije.

Tudi Walt (Svete v Malešič ur. 2006, 50) navaja, da so obravnavanje varnosti vseskozi determinirale tri ključne teoretične in politične paradigme: realistična, liberalna in radikalna. Za področje mojega magistrskega dela je ključna predvsem zadnja netradicionalna, radikalna paradigma, ki je v svojem bistvu nepozitivistična, nematerialna, zato dobro ustreza kibernetskemu okolju in je močno diferencirana od prvih dveh. Vsebuje pa tudi druge netradicionalne pristope od človekove varnosti do kritičnih teorij in odnosa človek-družba in človek-institucija. Pomemben je tudi konstruktivističen pogled, saj je vloga in pomen idej in znanja izredno pomembna v sodobni z informacijsko-komunikacijsko tehnologijo prepleteni družbi. Ker pa je delovanje idej in znanja oz. njihov vpliv na drugo stran kljub vsemu v določeni meri odvisno tudi od pozitivističnih dejstev[5], se zdi smiselno uporabiti t. i. integrativni pristop, kombinacijo realizma in konstruktivizma (Svete v Malešič ur. 2006, 64–65). Za kompleksno moderno družbo je tovrstna kombinacija teoretičnih pristopov verjetno najprimernejša.

[5] Prepletenost in odvisnost modernih družb od informacijsko-komunikacijske tehnologije in njihova vpetost v gospodarstva in materialnost, veča težo klasičnih pozitivističnih pristopov k preučevanju varnosti.

Posameznikovi varnostni problemi so tako prepoznani s strani višjih struktur in upoštevajo posameznika kot referenčni varnosti subjekt, i. e. element, na katerega se varnost nanaša. Vendar pa je problematika večplastna, saj je posameznik hkrati lahko tudi sam s svojim delovanjem vir ogrožanja varnostnih struktur in s tem varnostna grožnja. Pri obravnavi varnostne problematike, je tako potrebno posameznika upoštevati kot referenčni objekt varnosti in samega akterja nevarnosti, ključna je sekuritizacija[6] problematike.

Drugi avtorji (Prezelj v Malešič ur. 2002, 59) prav tako zaznavajo kompleksnost sodobnega ogrožanja varnosti, na katero vplivajo intenzivnost informatizacije, povezovalni procesi globalizacije, nastajanje novih držav po hladni vojni in tudi razvoj človekove zavesti. Kompleksna narava varnostnega okolja tako generira kompleksne grožnje varnosti, ki temeljijo na:

- hkratnem obstoju vojaške, politične, okoljske, gospodarske, zdravstvene, teroristične, kriminalne, informacijske, identitetne itd. razsežnosti ogrožanja varnosti in
- visoki povezanosti med temi razsežnostmi ogrožanja varnosti.

Prezelj (prav tam) še dodaja, da se je pojav kompleksnega ogrožanja varnosti oblikoval znotraj netradicionalnih pogledov na varnost, kjer je šlo za hkratno kognitivno širjenje razsežnosti varnosti in referenčnih objektov ogrožanja varnosti. Grizold (v Ferfila ur. 2002. 608) pa gre še dlje, saj naj bi zaradi kompleksnosti groženj, ki so neločljivo prepletene na individualni, lokalni, nacionalni, mednarodni, regionalni ter na globalni ravni, ter zaradi kompleksnosti vzrokov groženj (iz več dimenzij) in kompleksnimi posledicami (v drugih dimenzijah), lahko te eskalacije nevojaških groženj privedle celo do končnega vojaškega konflikta.

---

[6] Sekuritizacija je proces, ki preseže klasične postopke raziskovanja in analiziranja na drugih področjih znanosti in spreminja konceptualizacijo z namenom doseganja boljših rezultatov na varnostnem področju. Gre enostavno za prepoznavanje določene problematike skozi varnostno optiko. Tako proces sekuritizacije ne zmanjšuje pristojnosti in spodkopava klasičnih procesov raziskovanja, ampak sili varnostno analizo v bolj dinamičen premislek z namenom boljšega odziva na spreminjajoč se svet. Tako je potrebno na sekuritizacijo gledati kot na proces za vzpodbujanje razprav in analiz in ne kot na grožnjo starim konceptom preučevanja varnosti. Procesi sekuritizacije imajo sposobnost spodbuditi radikalno razmišljanje znotraj zelo tradicionalnih teoretičnih skupnosti in bi morali biti tudi zato prepoznani kot priložnost in ne kot grožnja (The Human Security Framework 2006, 10).

V spodnji shemi 4.1 so prikazane nekatere razlike med teoretičnimi pogledi na sodobno in tradicionalno varnost.

Tabela 4.1: Tradicionalni in moderni pogledi na varnost

POJMOVANJE VARNOSTI		
	tradicionalna varnost	**moderna varnost**
Varnost za koga oz. kaj?	• primarno države • ozemeljske celovitosti • nacionalne neodvisnosti • bitka za omejene vire	• primarno posameznika • družbo, institucije, okolje • osebne varnosti • svobode
Varnost pred kom?	• tradicionalne vojaške grožnje s strani drugih držav	• netradicionalne in tudi tradicionalne grožnje
Varnost kako in s katerimi sredstvi?	• zagotavljanje državne varnosti s silo (enostransko) • pomembnost ravnotežja (vojaške) moči • močno gospodarstvo • omejeno sodelovanje držav izven zavezništev • omejen pomen norm in institucij • igra ničelne vsote	• izredna pomembnost politike mehke moči • uporaba moči le kolektivno in v svetovljanske namene • splošen razvoj človeštva in blaginje dviga raven varnosti • sodelovanje držav z mednarodnimi inštitucijami in NVO je učinkovito tudi izven koalicij in zavezništev • norme in institucije so pomembne (demokratična reprezentativnost v njih dviguje legitimnost)

Prirejeno po Bajpai 2000, 48; Vogrin in drugi 2008, 20; Rančigaj 2010, 15; Malešič 1994, 97–102).

V postmoderni družbi je precej zahtevno določiti ustreznost posameznega koncepta oz. teorije pri preučevanju varnosti in mednarodnih odnosov. Svete (v Malešič 2006: 64, 65) opozarja na temeljni razkorak med realizmom in konstruktivizmom, saj se pri pojasnjevanju razhajata že v izhodiščih. Medtem ko klasični realisti izhajajo predvsem iz deterministične vloge človekove narave, ki naj bi bila konfliktna in nagnjena k vzpostavljanju moči nad drugimi subjekti ter njenega vpliva na oblikovanje države in mednarodnih odnosov, pa konstruktivisti prisegajo na družbeno določenost delovanja posameznih akterjev. Kljub precejšnjemu razkoraku med tema dvema teorijama pa so se pojavili predlogi, da bi za lažje razumevanje in razlago konkretnega stanja v mednarodni skupnosti in varnosti, upoštevali neke vrsto kombinacijo konstruktivizma in realizma, s čimer nastane že omenjeni t. i. integrativni pristop.

Svete (v Malešič ur. 2006, 64–65) tako zaključi, da je pri holističnem preučevanju varnostnega okolja v sodobni informacijski družbi nujno uporabiti realistično teorijo s katero preučujemo posredne vplive kot tudi konstruktivistično teorijo, s katero preučujemo predvsem zaznavanje stvarnosti in pojmovanje in zagotavljanje varnosti. Pogled na človekovo in posameznikovo varnost pa tako postaja ključni gradnik pri izgradnji varnih lokalnih, nacionalnih, regionalnih in globalnih okolij (Rančigaj 2010, 15).

Varnost, kot jo opredeli Edmonds (v Jelušič 1997, 70), je torej lahko sredstvo za dosego nekega cilja, oz. kar cilj sam. To vsekakor velja tudi za sodobno varnost ter. tudi za kibernetsko varnost omrežij, saj je njena zagotovitev pomembna neposredno za informacijska omrežja kot je hkrati tudi metoda zagotavljanja doseženega širšega blagostanja.

Drugi avtorji (Grizold in Bučar 2011, 847–849) pa ugotavljajo, da je sodobno varnostno okolje bolj zapleteno, ranljivo, nestabilno in ogroženo kot je bilo v preteklosti; vprašanje o ustreznem razmerju med varnostjo in svobodo v sodobni družbi pa je ponovno aktualno. Opazen je tudi premik pomembnosti referenčnega objekta varnosti od države k posamezniku. Vendar kljub temu nekatere države še vedno (oz. celo pogosteje) na račun svobode posameznika poskušajo zagotoviti lastno varnost (preiskave zasebne lastnine brez sodnega naloga, zadrževanje brez

pojasnila razloga in možnosti zagovora itd.) pogosto na podlagi suma povezanosti s terorizmom.

Iz vseh zgornjih tako jasno navedb izhaja, da je paradigma sodobne varnosti izredno kompleksna, njeno preučevanje pa vključuje mnogo področij, kar raziskave na področju varnosti postavlja v relevantno vlogo še za druga področja.

3.2 Relevantna teoretična koncepta

Po orisu sodobne varnostne paradigme želim nekaj besed nameniti tudi dvema konceptoma sodobnega pojmovanja varnosti, ki vsaj posredno posegata v področje kibernetske varnosti omrežij. Omemba kritičnih teorij varnosti je smiselna zaradi konceptualne širitve referenčnega objekta varnosti in idej ter motivov, ki so akterji delovanja. Koncept človekove varnosti pa zaradi ambivalentne vloge[7] posameznika v sodobni varnostni paradigmi in še posebno v kibernetski varnosti, ki v zadnjem času v temeljih pretresa razmerja moči in fokus varnosti in bo verjetno v prihodnosti še pridobival na pomenu, morda tudi iz percepcije posameznika kot grožnje.

3.2.1 Kritične teorije varnosti

Kritične teorije varnosti so svoje mesto med teorijami začele dobivati v 60ih in 70ih letih preteklega stoletja, ko so začele postavljati vprašanja, na katera je bilo praktično nemogoče odgovoriti s takratnimi teoretičnimi pristopi. Osrednje so tri dileme:

- Kaj je varnost?
- Koga imamo namen obvarovati in kaj so glavne grožnje subjektu varnosti?
- S čigavo varnostjo bi se morali ukvarjati in s katerimi strategijami bi ta varnost lahko bila dosežena.

Bistvo zgornjih vprašanj je bilo problematiziranje države kot osrednjega in ekskluzivnega subjekta varnosti. Razvoj te veje je pripeljal do ugotovitev, da je država lahko tudi akter ogrožanja (in ne samo ogrožan subjekt), da je potrebno fokus

[7] Po eni strani referenčni objekt varnosti, po drugi pa zagotovo tudi akter ogrožanja z uporabo IKT.

usmeriti še na druga področja (npr. spol) ter različne ravni ogrožanja recimo posameznika, državo in globalno raven. Prav tako so kritične teorije varnosti razprostrle nove pomene te besede kot so okoljska varnost, ekonomska varnost in socialna varnost. Termin kritične teorije je lahko zavajajoč, saj dopušča različne interpretacije; preprost pomen bi se lahko zožil le na kritičnost do tradicionalnega varnostnega diskurza, s tem pa bi postal le sinonim za nerealistične varnostne pristope. Globlja interpretacija pa ponazarja, da kritične teorije ne pomenijo le kritiziranja, temveč je njihov namen odstreti nove poglede, pokazati pomisleke in različne poglede (Sheehan 1999, 5).

Širjenje varnostnih perspektiv v okviru Kopenhagenske šole[8] je bilo sicer dobrodošlo, vendar avtorji zaradi navezanosti na državocentričen pogled na varnost, naletijo na množico omejitev. Buzan (v Sheehan 1995, 6) tako pravi, da naj bi države bile konceptualni center varnosti, ker so države tiste, ki naj bi se ukvarjale s celotnim varnostnim problemom. Danes to seveda ne drži več, sploh iz percepcije države kot edinega referenčnega subjekta varnosti. Ta varnostni model hladne vojne je tako presežen v celoti. Kritične teorije varnosti tako širijo področje varnosti v smislu raztezanja področja obravnave ter poglabljanja študij, tudi v smislu odmika od realistične varnostne perspektive in s tem prehoda od države kot osrednjega referenčnega objekta na druge subjekte (posameznik, institucije, okolje itd.).

Kritične teorije varnosti sicer v osnovi temeljijo na dveh analitičnih stališčih, poudarjajo zgodovinsko spremenljivost pojma varnost v času ter poudarjajo konstitutivno naravo kolektivnih podob o varnosti. Elemente varnostnega ogrožanja tako posredno določa tip družbene ureditve prek sekuritizacije in s tem sam določa referenčne objekte varnosti (Deibert v Svete 2005, 63–65).

Z uporabo kritične teorije varnosti je tako mogoče pojasnjevati pojave tudi v sodobnem okolju informacijske varnosti in varnosti ključne informacijske infrastrukture, saj le-ta (so)oblikuje sedanjo družbeno ureditev in s tem referenčne objekte varnosti.

[8] Ena od šol t. i. novih varnostnih študij, ki širi varnostni koncept na nevojaško in nedržavno perspektivo. Buzan je eden od vidnejši predstavnikov (Malešič v Svete 2005, 33).

3.2.2 Koncept človekove varnosti

Temeljni razlogi za nastanek koncepta človekove varnosti so predvsem v družbenem razvoju. Trenutni razvoj vodi v čedalje večje neenakosti v ekonomskih zmožnosti, zmanjševanje neobnovljivih virov, naraščanje proti tujcem nastrojenega razpoloženja, kot odgovor na pritiske migracij iz nerazvitega v razviti svet ter širjenje znotrajdržavnih konfliktov in pobude po človekoljubnem posredovanju (Bilgin v Svete 2005, 58). Razlogi pa seveda tičijo tudi v prenosu vrednot posameznika (kot so preživetje, kakovost življenja ter človekove pravice in svoboščine) v mednarodni sistem. Hkrati s prenosom vrednot pa je raslo tudi spoznanje, da so grožnje zaradi revščine in pomanjkanja razvoja, kršenja človekovih pravic[9], bolezni ter okoljskih katastrof, pomembnejše od tradicionalnih groženj miru in varnosti ter vprašanj o zadrževanju sovražnika (Nef v Vogrin in drugi 2008, 11). To vse so izzivi, ki jih s pomočjo tradicionalne varnostne paradigme ni bilo mogoče razjasniti, zato je bilo potrebno nekatere ideje razširiti. Svete (2005, 94) pravi, da je interes za človekovo varnost posledica zaznanega ogrožanja te varnosti[10], zato je za koncept človekove varnosti nujno potrebna osvoboditev od drugih struktur moči pa naj bodo globalne, nacionalne ali regionalne. Varnostne in razvojne politike so zaradi nastalih razmer morale vedno bolj upoštevati človeško dimenzijo. Fokus varnosti se je usmeril na zaščito ljudi in skupin ljudi pred grožnjami njihovemu preživetju. Poleg razpada blokovskih nasprotij po koncu hladne vojne pa so h krepitvi človeške dimenzije varnosti prispevali še:

- krepitev pomena človekovih pravic in svoboščin,
- naraščanje števila konfliktnih območij, v katerih je bilo prizadetih veliko število ljudi (humanitarne krize),
- vedno večje zavedanje pomena človekovega življenja, blagostanja ipd. (Vogrin in drugi 2008: 11).

---

[9] Kot eno od osrednjih nalog si zagotavljanje in odkrivanje novih groženj človekovim pravicam postavlja tudi Svet Evrope (The Council of Europe 2003, 25).

[10] Kot glavni vir ogrožanja nekateri vidijo globalizacijo, ki naj bi zmanjševala moč šibkih skupin, ogrozila domače gospodarske panoge ter povzročila družbeno neenakost, medtem ko drugi kot grožnjo človekovi varnosti zaznavajo predvsem državo in njene institucije (Svete 2005: 94).

Pristopov h konceptu človekove varnosti je več, vsak pa izhaja iz določenih družbenih, kulturnih ali geostrateških usmeritev. Prezelj (2008, 6–26), v okviru svojega prispevka za HUMSEC[11], navaja kot temeljna znanstvena prispevka pri razvoju koncepta človekove varnosti članka v revijah *International Security* in *Foreign Affairs*, oba z naslovom *Redefining Security*. Ta pionirski vidik koncepta človekove varnosti, je bil širši javnosti predstavljen šele nekaj let kasneje v Poročilu o človekovem razvoju.[12]

Podobno kot z drugimi temeljnimi koncepti (kot je človekova svoboda), je tudi človekovo varnost lažje definirati ob njeni odsotnosti, vendar pa je smiselno, da obstaja neka bolj definirana opredelitev. Tako lahko za človekovo varnost rečemo, da ima dva glavna vidika; prvi je varnost pred tako bistvenimi grožnjami kot so lakota, bolezni in represija, drugi vidik pa je varnost in zaščita pred nenadnimi in škodljivimi razdori v vsakdanjem življenju pa naj si bo v domovih, službah ali skupnostih (UNDP 1994, 24).

Newman (2001, 243) je poleg UNDP-jeve opredelitve človekove varnosti opredelil še tri najpomembnejše prepletajoče vidike, ki se bolj razlikujejo po poudarkih in osredotočenjih, kot po različnih zvrsteh. Med seboj se ne izključujejo, temveč so nekako različne veje iste misli. Dodajmo še, da bi se lahko nekatere koncepte človekove varnosti definiralo kot »netradicionalna varnost«, kjer bi referenčni objekt ostala država, izzivi pa bi bili nedržavni in nevojaški. Ti vidiki so:

- vidik temeljnih človekovih dobrin (UNDP),
- dogmatični vidik (intervencionistična smer),
- vidik družbene blaginje (razvojna smer) in
- nov varnostni koncept (angl. *new security concept*).[13]

[11] HUMSEC je projekt, ki ga podpira EU, ustanovljen z namenom boljšega razumevanja povezave mednarodnih teroristov s kriminalnimi organizacijami na zahodnem Balkanu (http://www.humsec.eu; 6.julij 2011).
[12] UNDP vsako leto izdaja poročila v katerem obravnava različne tematike. Poročila o človekovem razvoju so na voljo na njihovi spletni strani (http://www.undp.org/ 10. december 2010; http://hdr.undp.org/en/; 10. julij 2011).
[13] Več o tem na voljo (Newman v Dokl 2006, 11-15).

V novejših publikacijah pa HDR[14] definira človekovo varnost kot osredotočeno na ljudi, večdimenzionalno, medsebojno povezano in univerzalno. Koncept človekove varnosti tako predstavlja napor za rekonceptualizacijo varnosti v temeljnem smislu in je hkrati orodje, ki se osredotoča na zagotavljanje varnosti za posameznika in ne države (The Human Security Framework 2006, 5).

V drugih pristopih k preučevanju človekove varnosti je zaznati različno razumevanje varnosti kot tudi družbenega okolja. Poleg pristopa Razvojnega programa Združenih narodov pa drugi avtorji (Vogrin, Prezelj, Bučar, 2008: 11–24) izpostavljajo še pristope Kanade in Mreže za človekovo varnost, pristop Japonske in Komisije za človekovo varnost ter pristop Tajske. Pristopi imajo določene razlike pri definiranju referenčnega objekta, vprašanju vrednot in groženj ter sredstev za zagotavljanje človekove varnosti. Kljub mestoma različnim pogledom pa lahko sklenemo, da je koncept človekove varnosti še vedno v veliki meri v nasprotju s tradicionalnim konceptom varnosti in državno suverenostjo, ki je še vedno med najpomembnejšimi stebri zagotavljanja miru in varnosti.

Pomisleki drugih avtorjev (Krause v Toplišek 2010, 12) pa se nanašajo predvsem na porajajočo skrb, da bi ideja človekove varnosti lahko promovirala širšo agendo, ki bo omogočala neomejeno pravico do vmešavanja v notranje zadeve suverenih držav. Na kakšen način naj bi se to odražalo ni bistvenega pomena, ključno pa je, da obstajajo pomisleki, saj naj bi s tem svetovna politika, ki se osredotoča na ljudi in njihovo varnosti, tako postavljala posameznike proti svojim državam.

S konceptom človekove varnosti so stare ureditve, varovanje ozemlja pred varovanjem posameznika, v veliki meri postavljene na obrobje. Zaradi netipične narave modernih groženj, se je potreba po novi ureditvi varovanja pred temi grožnjami utelesila v modernejših varnostnih konceptih. Vendar pa nekateri avtorji (Grizold in Bučar 2011, 841) ugotavljajo, da je problem implementacija tega koncepta v prakso, za kar bi potrebovali sodelovanje mednarodnih, vladnih in nevladnih organizacij.

Povsem v ospredje je tovrstna problematika in človekova varnost prišla z izgredi na bližnjem vzhodu in v severni Afriki, kjer si prebivalstvo s protesti poskuša zagotoviti

[14] Human Development Reports (http://hdr.undp.org/en/ 11. julij 2011).

človeka vredno življenje v okviru demokratičnih sprememb in s tem odstranitev avtokratskih režimov. Žal pa mednarodna struktura in možnost veta v Varnostnem svetu OZN preprečuje ukrepanje mednarodni skupnosti in prekinitev nasilja v tem delu sveta[15]. Žal tako koncept človekove varnosti še vedno ostaja na ravni koncepta in si bo moral svoje mesto in pomembnejšo vlogo v konceptu sodobne varnosti še izboriti. Države in mednarodna skupnost pa morajo preskok na to raven še opraviti, saj se trenutno očitkom o dvoličnosti pri skrbi za varnost državljanov posameznih držav žal ni mogoče izogniti.

3.3 Informacijska in omrežna varnost

Razvoj sodobne varnostne teorije torej odraža prepletenost in množičnost referenčnih objektov, kompleksnejše grožnje varnosti ter zahtevnejše mehanizme s katerimi se poskuša varnost doseči. Informacijska varnost je tako le en od segmentov sodobnega varnostnega diskurza, (kibernetska) varnost omrežij pa le del tega segmenta.

Zaradi čedalje večjega pomena omrežij v sodobni družbi, tako postajajo kar omrežja sama referenčni objekt varnosti. Svete (2005, 105) prav tako ugotavlja, da omrežna varnost predstavlja eno novejših varnostnih perspektiv, ki izvira iz naraščajočega pomena omreženih informacijskih tehnologij iz vseh vidikov postindustrijske ekonomije, mednarodne proizvodnje in globalnih financ. Neločljiva povezanost bistvenih sprememb v ekonomskih organizacijah z novimi informacijskimi tehnologijami je le eno od področij vpletenosti IKT v sodobno družbo. Čedalje večja odvisnost družbe od omrežene informacijske infrastrukture (predvsem ključne informacijske infrastrukture) je vplivala na nastanek nove varnostne predstave, ki je usmerjena v zavarovanje omrežja samega, izgubo, krajo ali uničenje podatkov ter prekinitvijo informacijskih tokov.

[15] Dokument nastaja v času, ko sta Rusija in Kitajska izkoristila možnost veta na sprejem resolucije o Siriji, tako da mednarodna skupnost ostaja razklana na tej točki (Syria: Ban voices deep regret after Security Council fails to agree on resolution; 2012).

Prav ta, informacijsko komunikacijska tehnologija[16] (IKT), dejansko spreminja dojemanje realnosti in s tem v prvi vrsti tudi pojmovanje varnosti, nadalje pa njeno zagotavljanje. Uporaba IKT spreminja doživljanje vsakdana tako na ravni posameznika, podjetij, organizacij kot tudi mednarodne skupnosti[17]. Posameznik z uporabo IKT je tako neposredno povezan z varnostjo zlasti v smislu vplivanja na družbene konstrukte ter na zaznavanje varnosti prek različnih komunikacijskih tehnik (e-pošta, splet, blogi, forumi, novičarske skupine itd.). Prav tako se neposredne implikacije na varnost nanašajo tudi s strani zlorabe IKT v namene slabljenja varnostnih interesov posameznika (podjetja ali države) oz. drugih referenčnih objektov varnosti (zlasti v smislu vpliva na ključno informacijsko infrastrukturo in onesposabljanje le-te). Na drugi strani pa IKT posredno vpliva na zbiranje in obdelavo podatkov tako v civilni sferi kot v tradicionalnih varnostnih mehanizmih in tako postaja nov steber informacijske moči v družbi (Svete v Malešič 2006: 61).

Ta nov steber moči informacijsko-komunikacijske tehnologije pa je zaradi svoje razsežnosti in kompleksnosti podvržen tudi povsem novim grožnjam. Na RAND[18] konferenci so bile izpostavljene tri ključne skupine varnostnih groženj informacijskim sistemom, ki se do danes niso mnogo spremenile: fizične, elektronske in psihološke. Razporeditev vpliva je prikazan na shemi 3.1. Opazimo lahko, da ima dandanes posameznik zaradi uporabe modernih tehnologij možnost vplivanja na stabilnost IKT-sistemov (in s tem varnostnih sistemov ključne informacijske infrastrukture) prek vseh

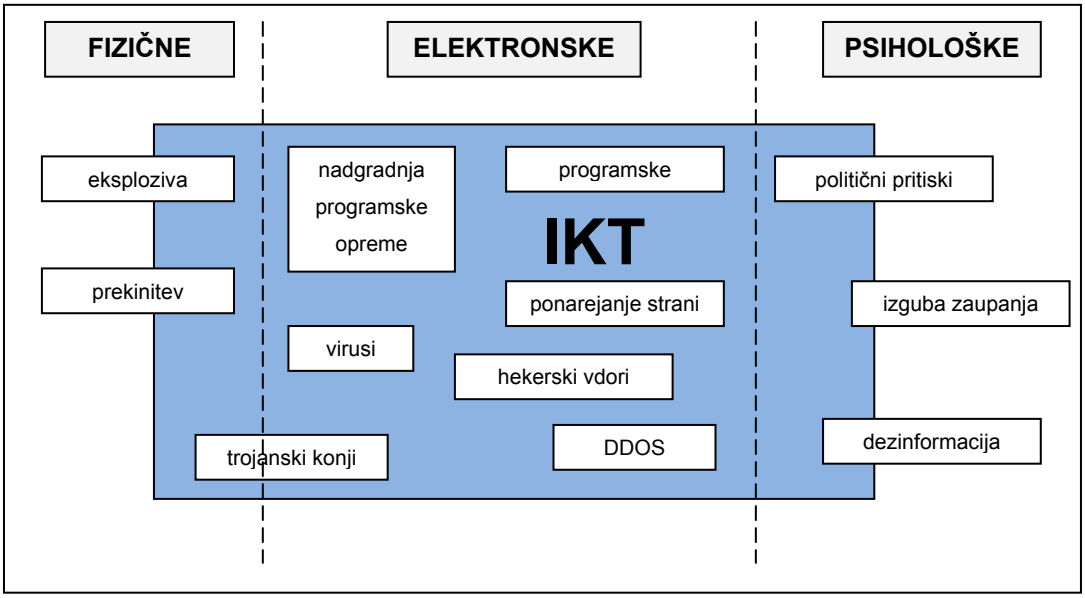
[16] Svete (2005, 16) odlično povzame več drugih strokovnjakov in opredeli IKT kot »sposobnost, znanje, spretnost oz. tehniko, da predvsem z uporabo strojev in naprav, ki omogočajo informacijske dejavnosti, dosežemo želene učinke«. Skozi celotno magistrsko delo se ta pojem večkrat pojavi, smiselno pa se vedno navezujem na zgornji oris.

[17] Aktualna problematika in nekdaj zaupni podatki, ki jih s pomočjo informacijsko-komunikacijske tehnologije (interneta) širša javnost prejema prek spletne strani Wikileaks. Njen avtor oz. eden od soavtorjev je tako deležen gonje različnih ustanov, mediji in širša javnost pa so na strani prostega pretoka informacij in seveda tako uhajanje informacij pozdravljajo v duhu odkritejšega delovanja držav in institucij v mednarodnem sistemu. Jasno pa ostaja, da z uhajanjem mednarodnih depeš lahko resno ogrozimo zaupanje v mednarodnih vodah, kar vsekakor lahko ima resne politično-varnostne posledice (http://www.bbc.co.uk/news/11932041, 10. julij 2011 in http://www.bbc.co.uk/news/uk-11930488, 10. julij 2011).

[18] RAND (angl. ***R**esearch **AN**d **D**evelopment*) je neprofiten globalni miselni trust (*think tank*), ki je bil sprva ustanovljen kot pomoč pri raziskovanju in analiziranju za potrebe ameriških oboroženih sil (http://www.rand.org/, 30. junij 2011).

treh oblik groženj, kar je za nekaj desetletij nazaj še povsem nepredstavljivo. Fokus moči se je tako od države močno nagnil k posamezniku[19].

Shema 3.1: Varnostne grožnje IKT-sistemom



Prirejeno po: *The Future of the Information Revolution in Europe*, 2001: 45.

Če je bila v začetnih fazah IKT v celoti v rokah države in institucij, so dandanes vloge vsaj izenačene, če ne že v prid skupinam oz. civilni družbi ter posamezniku. Uporaba IKT je do neke mere zamenjala vlogi nadzornika in predmeta nadzora, saj so danes z uporabo IKT pogosto pod nadzorom (oz. napadom) ravno države oz. institucije, nadzor (oz. napad) pa izvajajo kar državljani oz. druge družbene skupine, čeprav v (ne)organizirani obliki. Akterji ogrožanja so se razširili, s čimer se pozornost in sredstva tistih, ki sisteme varujejo, neizogibno razpršijo, kar poslabšuje nadzor.

Lahko ugotovimo, da se posameznik in drugi nedržavni akterji tako osvobajajo v odnosu do države, uporaba IKT pa v tem primeru igra eno odločujočih vlog. Za pojasnjevanje omenjenega procesa pa je gotovo najpomembnejša liberalna

[19] Primer medijske moči, ki jo trenutno ima (je imel) Julian Assange, ustanovitelj Wikileaksa, je precedenčen z vidika koncentracije moči na posamezniku (http://www.bbc.co.uk/news/world-11047811; 11. julij 2011).

varnostna paradigma, ki v ospredje varnostnih interesov postavlja posameznika (Svete v Malešič 2006: 64, 65). Torej prav v konceptu človekove varnosti in vlogi posameznika v njej, lahko najdemo ključne elemente postmodernega dojemanja varnosti. Več o konceptu človekove varnosti v nadaljevanju.

Na isti RAND konferenci so strokovnjaki predvideli tri tipe razvoja informacijske družbe v Evropi in nasploh (iz njih izhajajo potencialne varnostne implikacije):

1. **Pospešena evolucija brez drastičnih sprememb**; ta opcija naj bi predstavljala postopen razvoj, ki temelji na digitalni obdelavi procesov in ne več posameznikove vloge, ki pa naj ne bi imela drastičnih vplivov na razvoj družbe kot take.

2. **Družbena omrežja**; po tem scenariju naj bi omrežne skupine posameznikov delovale znotraj kratkotrajnih »koalicij« za doseganje partikularnih interesov v sodelovanju z nevladnimi organizacijami, interesnimi skupinami, idr., imele pa naj bi močan vpliv na družbo (v dobrem in v slabem smislu).

3. **Globalno vzdržna družba**: tudi ta scenarij vključuje omrežne skupine, ki naj bi v tem primeru delovale v smeri prihodnje družbe, ki je samozadostna, vzdržna in predvsem manj potrošniška.

(*The Future of the Information Revolution in Europe* 2001, 29–30)

Iz zgornjih scenarijev lahko izhaja, da naj bi imel posameznik povsod ključno vlogo, seveda v združevanju v interesne skupine. Desetletje po zgornjih predvidevanjih lahko ugotovimo, da je šel razvoj nekje med drugim in tretjim scenarijem, saj danes internetna družbena omrežja[20] predstavljajo velik del aktivnosti na svetovnem spletu, prav tako pa je ideja globalno vzdržne družbe prisotna skoraj na vsakem koraku v zahodnem svetu. Torej, hitrost in preprostost širjenja idej in s tem vpliv posameznika tako na podjetja, družbo kot tudi uradne institucije, je večji kot kdajkoli. Z objavo množice tajnih mednarodnih depeš lahko posameznik zatrese celoten svetovni mednarodni ustroj in postavi legitimnost delovanja svetovne velesile pod vprašaj; že

[20] Po podatkih spletne strani Facebakers, naj bi bilo v 2011 v Sloveniji več kot 600.000 uporabnikov registriranih samo na spletnem omrežju Facebook (najpopularnejši, obstajajo pa seveda tudi drugi), kar predstavlja skoraj tretjino populacije, oz. skoraj polovico "online" populacije (http://www.socialbakers.com/facebook-statistics/slovenia, 5. julij 2011).

sama ideja take moči v rokah posameznika je v okviru tradicionalnih varnostnih konceptov težko dojemljiva. Posameznik je tako s spretno uporabo informacijske tehnologije lahko državi oz. različnim institucijam in omrežjem resna varnostna grožnja in s tem so se vloge v nekaj desetletjih popolnoma zamenjale.

Raziskovalci v okviru RAND-a so pripravili tudi nekaj črnih scenarijev nadaljnjega razvoja informacijske družbe in s tem varnostnih tveganj za posameznika, mednarodni sistem, omrežja in družbo kot celoto, naštejem naj le nekaj največjih:

1. Uporaba umetne inteligence povzroči večje družbene nemire, saj je večina služb avtomatiziranih, kar ljudi sili v prekvalifikacijo ter jim hkrati znižuje vrednost na trgu.

2. Povečana družbena in posameznikova odvisnost od računalnikov in komunikacijskih sistemov postavlja te sisteme v vlogo specifičnih tarč za napad.

3. Naraščajoča kompleksnost omrežij pripelje do katastrofalnih prekinitev v delovanju. Izredna kompleksnost in medsebojna odvisnost omrežij, ki jih trenutno gradimo, nas pripelje do točke, kjer tudi največji strokovnjaki ne razumejo več delovanje sistema v celoti.

4. Strojna in programska oprema postane samorepliciraječa in povzroči verižno reakcijo, ki je neobvladljiva.

5. *Peer-to-peer* programska oprema in generični algoritmi dovoljujejo programski opremi, da se razvija in širi izredno hitro, kar jo prav tako naredi neobvladljivo in nerazumljivo za človeški um.

6. Naraščajoča odvisnost razvitega sveta od računalnikov in komunikacijske tehnologije ustvari asimetrijo varnostnih groženj v primerjavi z drugimi regijami in kulturami. Postanemo bolj ranljivi od tradicionalnih družb.

7. Naraščajoča razvitost robotike v povezavi z naprednimi programskimi orodji (umetna inteligenca, prepoznavanje govora itd.) zmanjša konkurenčnost človeka kot delovne sile tako v osnovnih delovnih panogah kot v visoko zahtevnih delovnih mestih.

8. Povečan obseg zbranih podatkov glede nakupovalnih navad, vzorcev uporabe mobilnega telefona, gibanja, nakupov s kreditno kartico itd. občutno zmanjša raven naše zasebnosti.

(*The Future of the Information Revolution in Europe* 2001, 71–72)

Iz zgoraj navedenih možnih varnostnih groženj izhajajo resni pomisleki, do kam nas razvoj informacijske tehnologije lahko pripelje in kakšne posledice bo to imelo za eksistenčni obstoj človeške vrste kot tudi družbenega sistema, ki smo si ga ustvarili. Zaenkrat ne obstajajo varnostni mehanizmi, ki bi preprečevali takšne scenarije; tudi na področju relevantne teorije[21] o tem ni veliko napisanega[22], saj se ta nova vrsta varnostne grožnje šele vzpostavlja; grožnja je v tem primeru tehnologija sama.

Drugi avtorji (Dunn 2004, 3–4) problematizirajo uporabo termina informacijska infrastruktura v teh okvirih, ravno zaradi njegove dvopomenskosti. Informacijska infrastruktura tako naj ne bi imela le fizične ravni, ki je relativno preprosta za razumevanje, temveč naj bi vsebovala tudi drugo, nematerialno (kibernetsko) komponento, to je informacije in vsebine, ki se prenašajo prek infrastrukture, znanje, ki ob tem nastaja in storitve, ki nam služijo. Ravno zaradi teh težko opredeljivih pojmov, nepredstavljivih situacij in odsotnosti preprostih determinant, je znanstveno preučevanje tega področja zahtevno. Tako nam informacijska varnost na svoj način s svojo kompleksnostjo in nepredvidljivostjo oriše omejitve znanja in raziskovalnih orodij (Dunn 2004, 23).

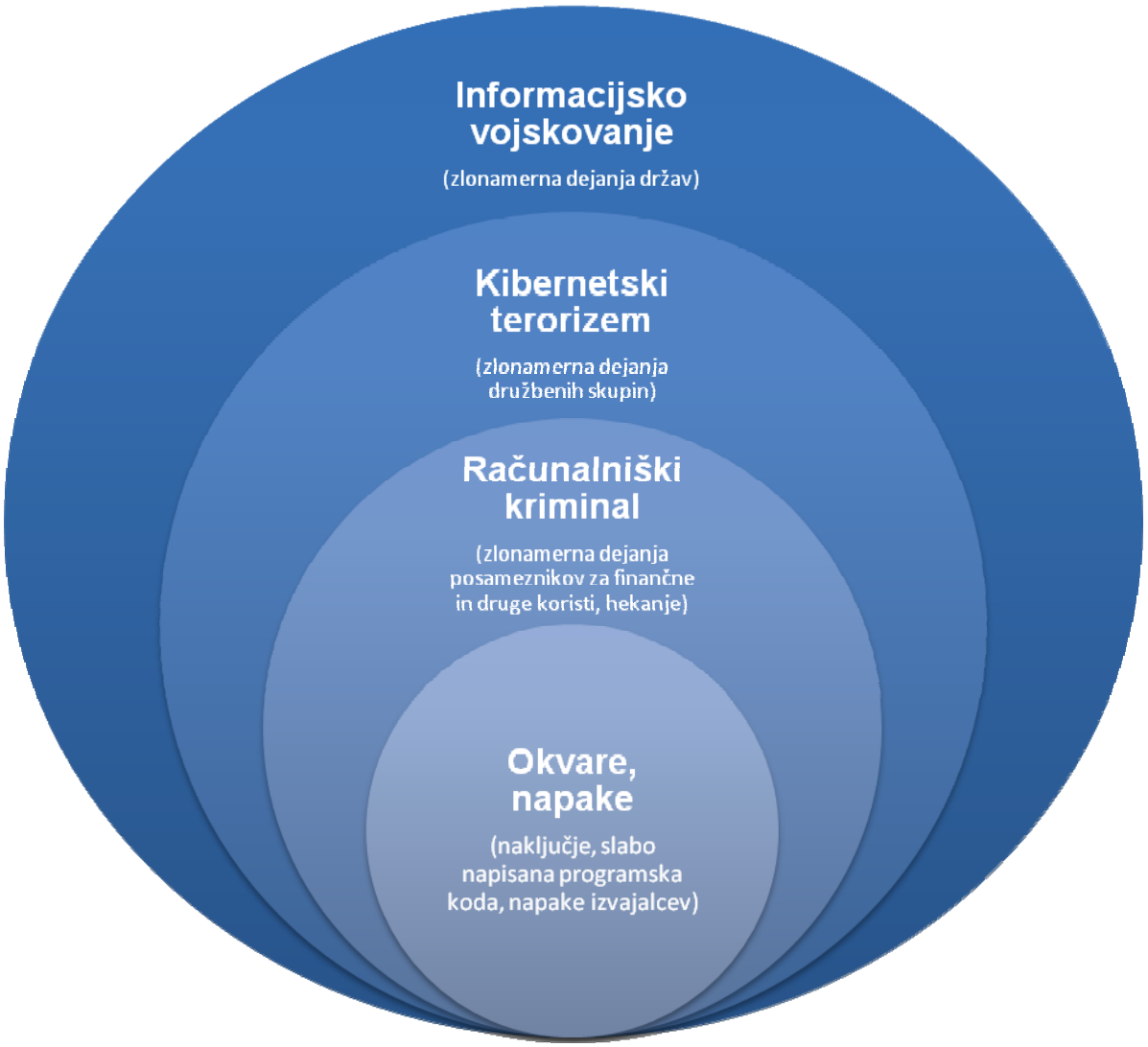
Zanimiva je misel, da informacijsko komunikacijska tehnologija na eni strani kreira varnostno problematiko sama po sebi kot grožnja in tako vzpodbuja razvoj novih varnostnih konceptov, po drugi strani pa je hkrati tudi orodje zagotavljanja varnosti v določenih situacijah. Ta dvojnost njene vloge, je lahko ključna gonilna sila, ki bi njen razvoj in zapletenost pognala do neobvladljivih ravni. Vendar pa sama grožnja ni

[21] Obstajajo sicer t. i. TTAT (***T**echnology **T**hreat **A**voidance **T**heory*) teorije, ki pa so bolj osredotočene na posameznika in njegove probleme z informacijsko tehnologijo.

[22] Še najbližje omenjenim situacijam so znanstvenofantastični filmi, recimo Terminator v režiji Jamesa Camerona, kjer je nazorno prikazana možnost razvoja umetne inteligence in končno spopad proti človeštvu ali film Umri pokončno 4 v režiji Lena Wisemana, kjer posameznik z izrednim poznavanjem nacionalno-varnostnega sistema in njegove IKT podstati in delovanja varovalk v primeru resnih groženj, spravi v nezavidljiv položaj najmočnejšo silo na svetu.

vedno v smeri posameznik-država ali država-posameznik oz. v skladu s starimi koncepti država-država; čedalje več je delovanja na ravni posameznik-posameznik oz. posameznik-institucija (omrežje). In ravno ta relacija, kibernetsko delovanje akterjev z uporabo IKT proti ključnim informacijskim omrežjem oz. infrastrukturi, je eden od osrednjih motivov mojega magistrskega dela. Ravni kibernetskega ogrožanja so ponazorjene na shemi 3.2. Več o ključni informacijski infrastrukturi v nadaljevanju.

Shema 3.2: Ravni kibernetskega ogrožanja



Prirejeno po: *The Future of the Information Revolution in Europe* 2001, 47.

Aktualnost problematike in prihodnji fokus lepo odraža govor predsednika ZDA, kjer je izpostavil, da je sedaj že povsem jasno, da so kibernetske grožnje ene najbolj resnih ekonomskih in nacionalno varnostnih izzivov[23] ter da je prihodnost blaginje naroda odvisna od kibernetske varnosti. V govoru je predsednik naročil izvedbo celovitega pregleda ukrepov zvezne vlade pri zaščiti informacijsko-komunikacijske infrastrukture in kot rezultat so ZDA izdelale dokument *Pregled politike kibernetskega prostora*[24], ki služi koordinatorju kibernetske varnosti in predsedujočemu Uradu za kibernetsko varnost in komunikacije[25] kot izhodišče.

Medtem pa EU sočasno z delovanjem ENISE, še vedno išče enoten in združen pristop h kibernetski varnosti, na srečanjih sodelujejo predstavniki Evropske komisije, predstavniki Evropskega parlamenta, Evropske obrambne agencije, ENISE, zveze NATO, zasebnih varnostnih organizacij ter drugi. EU ima namen ustanoviti Evropski center za kibernetski kriminal, ker trenutno relativno velik del odgovornosti pri zaščiti omrežij še vedno sloni na zasebnem sektorju, s tem pa okrepiti vlogo EU. Upravičeno pa je interes največji tam, kjer so kibernetski napadi že povzročili škodo[26], tako ima pomembno vlogo pri prizadevanjih Estonija, ki je bila žrtev obsežnega kibernetskega napada pred leti (*Estonia pushes for joint EU cyber response*, 2011).

3.3.1 Kibernetska varnost

Kljub vsemu pa preučevanje informacijske in omrežne varnosti in znotraj nje kibernetske varnosti še ne dosega prave, celostne ravni znanstvenega raziskovanja, saj večina ugotovitev še vedno izhaja iz spoznavne ravni preučevanja kibernetske varnosti. Vlada ZDA je tako zadolžila posebno skupino znanstvenikov - JASON[27], naj

---

[23] *»For all these reasons, it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation,«* je dobesedna navedba predsednika Obame v njegovem govoru o zaščiti nacionalne kibernetske infrastrukture v Beli hiši (Remarks by the President on *Securing our Nation's Cyber Infrastructure*, 2009).

[24] *Cyberspace Policy Review*

[25] Spletna stran Urada je na voljo na: http://www.dhs.gov/xabout/structure/gc_1185202475883.shtm (14. julij 2011).

[26] Napad na estonsko infrastrukturo v 2007 je onemogočil dostop do vladnih strani, spletnih strani bank, medijev in operaterjev ključne infrastrukture. Ocena škode se giblje med 30 in 40 milijoni $, napad naj bi bil izveden s strani ruskih hekerjev zaradi prestavitve spomenika ruskim žrtvam v Estoniji (*Estonia pushes for joint EU cyber response*, 2011).

[27] Več o statusu skupine JASON v poglavju aktivnosti ZDA na tem področju.

preuči možnosti za vpeljavo bolj znanstvenih metod pri preučevanju kibernetske varnosti. Kot rezultat je nastalo poročilo *Znanost o kibernetski varnosti*[28], ki poskuša odkriti še druge dimenzije kibernetske varnosti poleg obstoječe, zaznavno-spoznavne ravni preučevanja i. e. empirije.

V poročilu (JASON, 2010) znanstveniki že uvodoma ugotavljajo, da je zaradi umetne narave kibernetskega prostora, ki je le šibko povezan s fizičnim svetom, težko omejiti celotno problematiko, saj so pojavi v kibernetskem prostoru dinamični v svojem bistvu ter razvijajoči skozi čas, delno tudi zaradi odzivanja na obrambne ukrepe. Zaradi tega nobeno področje znanosti (matematično, fizikalno ali družbeno) ne more pokriti vseh pomembnih vidikov in izzivov, kljub temu pa obstajajo podobnosti, ki jih je mogoče prepoznati v drugih področjih preučevanja kot so recimo epidemiologija, ekonomija, klinična medicina. Študija identificira dve možni ravni preučevanja, prvo predvsem skozi tehnični pristop in uporabo metod, ki temeljijo na matematičnih in logičnih osnovah kot so teorija iger in kriptografija, druga možnost pa je preučevanje kibernetske varnosti kot analogija na imunologijo in biološke sisteme.

Ker enoznačnega odgovora na znanstveno preučevanje te problematike ni mogoče podati, študija kot primerno nadaljevanje razvoja znanosti predlaga vzpostavitev raziskovalnih centrov s področja kibernetske varnosti na univerzah in drugih organizacijah. Svoje magistrsko delo razumem predvsem kot raziskovalni prispevek na tem področju, zavedam pa se, da je Slovenija še precej oddaljena od raziskovalnih centrov na področju kibernetske varnosti, deloma je to možno upravičevati tudi z našo številčno majhnostjo.

Kibernetska varnost omrežij pa ni nov pojem. Združeni narodi so pomembnost kibernetske varnosti in kibernetske varnosti ključne informacijske infrastrukture zapisali v svojih resolucijah že leta 2002 (Resolucija ZN 57/239) in leta 2003 (Resolucija ZN 58/199). V njih so ZN izpostavili bistvene elemente pri vzpostavljanju varne informacijske družbe ter globalnost kibernetske kulture ter še posebej skrb za zaščito KII. Težava nastane pri definiranju kibernetske varnosti, ki je svojevrstna zloženka besed. Pojem varnost je relativno dobro poznan, torej ostane le še potreba po definiranju »kibernetskega«. Termin »kiber« izhaja kot predpona iz besede

[28] Angl. *Science of Cyber-Security*

kibernetika, ki jo SSKJ definira kot vedo, ki raziskuje podobnost med delovanjem strojev in živo naravo (SSKJ, 2011). Termin kiber se pogosto uporablja tudi kot sinonim za kibernetski prostor. Pridevnik »kibernetska« pred besedo varnost, tako pomeni varnost, ki se nanaša na kibernetiko. Kibernetska varnost se tako ukvarja z varovanjem kibernetskega prostora pred kibernetskimi in drugimi grožnjami.

Dunn (2005, 4) kibernetsko varnost v splošnem smislu opredeli kot nanašajočo se na tri temeljne stvari:

- Skupek aktivnosti in drugih ukrepov, tehničnih in netehničnih, katerih namen je zaščititi računalnike, računalniška omrežja, strojno in programsko opremo ter informacije, ki jih le-ta vsebuje in obravnava, kar vključuje programsko opremo in podatke kot tudi druge elemente kibernetskega prostora, pred vsemi grožnjami, tudi grožnjami nacionalni varnosti.
- Stopnjo zaščite, ki jo aktivnosti in ukrepi lahko zagotovijo.
- Združena področja profesionalnih naporov, vključno z raziskavami in razvojem na področju implementiranja in izboljševanja ukrepov ter dvigovanja kakovosti le-teh.

Kibernetska varnost tako presega informacijsko varnost ali varnost podatkov, vendar vključuje tudi ti dve panogi; informacijska varnost se tako nanaša na vse vidike zaščite informacij. Kot pa je pokazala študija ENISE (*Pobude za ozaveščanje o varnosti informacij* 2007, 1*)* o osveščenosti glede varnosti informacij, postaja sodobna družba zelo odvisna od delovanja informacijske tehnologije in še zlasti interneta, kar postavlja kibernetsko varnost v ospredje.

3.4 Zasebnost, nadzor in upravljanje z virtualnim prostorom

Poleg informacijske in omrežne varnosti pa je izrednega pomena tudi zasebnost v virtualnem prostoru. Zaradi same brezmejne narave in lastnosti interneta[29] je ta sprva veljal kot precej odporen proti nadzorovanju z različnih ravni, predvsem zaradi svoje velikosti[30]. Dandanes pa izkušnje uporabnikov pravijo drugače, delno se zasebnost izgublja zavestno pri uporabi socialnih omrežij, zagotovo pa ima pomembno vlogo pri zmanjševanju zasebnosti tudi želja po povečanem nadzoru v duhu preprečitve kriminalnih dejanj, tako kibernetske kot fizične narave. Sprva je sicer kazalo, da je internet prostor brezpravja oz. da tam oblasti ne bodo uspešne pri vpeljavi nadzorovalnih mehanizmov, ta »popolna svoboda« pa je pripeljala do zlorab in dejanske omejitve svobode posameznikov (Kovačič 2003, 39), saj so se v teh razmerah brezvladja najbolje znašli prav spletni nepridipravi, zato so različni vzvodi nadzora neizbežni. Težava z zasebnostjo pa je ravno v njeni dvojni vlogi, saj imajo države hkrati interes za več zasebnosti recimo potrošnikov pred ponudniki, hkrati pa zahtevajo več dostopa do uporabniških podatkov pod agendo nacionalne varnosti ali preprečitve kriminalne dejavnosti in si to tudi zakonsko omogočijo (*Privacy, Accountability and Trust – Challenges and Opportunities* 2011, 60).

Nadzor nad internetom je večpomenski in neoprijemljiv pojem, saj interneta nadzorovati v tem trenutku ne more nihče. Eno od bolj reguliranih področij je dodeljevanje imen in številk ter domen. Trenutno ima vlogo upravljanja s številskim prostorom internetnih protokolov (IPv4 in IPv6) in dodeljevanjem blokov naslovov regionalnim internetnim registrom ter upravljanjem z vrhovnimi domenami organizacija ICANN (angl. *Internet Corporation for Assigned Names and Numbers*) – Internetna korporacija za dodeljevanje imen in številk, pred tem (do 1998) pa je ta pomembna vloga pripadala vladi ZDA. Z rastjo interneta je primat ZDA na področju dodeljevanja IP-prostora ter domen postal nevzdržen, zato je vlada ZDA to vlogo dodelila zasebni instituciji (ostajajo pa ugibanja, čemu te vloge ni oddala recimo

[29] Boyle (v Kovačič 2003, 39) lastnosti interneta imenuje kar »sveta trojica«: tehnologija medija, geografska razpršenost in vsebina.
[30] V letu 2010 je število uporabnikov interneta preseglo dve milijardi (World Bank Data indicator, 2011).

Mednarodni telekomunikacijski zvezi[31]) (*ICANN vs. the World*, 2011). ICANN samo sebe definira kot neprofitno in v javno dobro usmerjeno korporacijo s predstavniki celega sveta, katere namen je prek nadzora edinstvenih identifikatorjev skrbeti, da internet ostaja varen, zanesljiv in interoperabilen (Internet Corporation for Assigned Names and Numbers, 2011).

Evropske institucije pa že problematizirajo vlogo ICANN in poudarjajo njeno nereprezentativnost in odsotnost nadzora mednarodne skupnosti nad njo. EU v svoji Resoluciji o upravljanju interneta tako ugotavlja, da je internet:

- temeljno globalno sredstvo za komuniciranje z velikanskim vplivom na celotno družbo,
- da upravljanje interneta vključuje vprašanje v zvezi z varovanjem in zagotavljanjem temeljnih pravic in svoboščin, dostopom do interneta, njegovo uporabo in ranljivostjo zaradi spletnih napadov in
- čedalje večjega ogrožanja s strani kibernetske kriminalitete zaradi odvisnosti naše družbe od IKT in zaradi povečanega napeljevanja k terorističnim napadom, kaznivim dejanjem spodbujanja sovraštva in otroške pornografije in
- ker se posamezni vidiki upravljanja interneta nanašajo na internetno naslavljanje in druga pretežno tehnična vprašanja, s katerimi se ukvarjajo Internetna korporacija za dodeljevanje imen in številk (ICANN), Organ za dodeljevanje internetnih naslovov (IANA[32]), Projektna skupina za internetno tehnologijo (IETF[33]), regionalni internetni registri in druge organizacije (Upravljanje interneta: naslednji koraki, 2009).

Zato in zaradi omejene pristojnosti drugih institucij (razen vlade ZDA) pri vpogledu v delovanje ICANN je želela Evropska komisija začeti razpravo v mednarodnem okolju z namenom izboljšati odpornost interneta v primeru naključnega izpada ali namernega napada. Želja EU je tako z razpršitvijo nadzora obdržati internet kot javno dobrino, gonilno silo inovacij, svobodnega izražanja in gospodarskega razvoja (*Evropska komisija poziva k odprtemu, neodvisnemu in odgovornemu upravljanju interneta*, 2009).

---

[31] *International Telecommunication Union* – ITU
[32] Angl. *Internet Assigned Numbers Authority*
[33] Angl. *Internet Engineering Task Force*

Seveda pa nadzorovanje interneta in s tem komunikacije med državljani ni vedno uporabljeno dobronamerno s strani države ali njenih institucij. Prevelika moč organov (tiranskih) držav se je tako pokazala za zlorabljeno v več primerih, zelo odmeven pa je bil internetni mrk v Egiptu v času t. i. egiptovske revolucije januarja 2011, ko je oblast poskušala na ta način[34] ustaviti koordinacijo in vzpodbujanje protestnikov k zborovanju proti takratnemu predsedniku Mubaraku. To je bil precedenčen primer, saj se je tokrat prvič v zgodovini interneta zgodilo, da bi se poskusilo ustaviti celotno komunikacijo prek interneta, medtem ko je do posamičnih blokad strani ali funkcionalnosti že prihajalo. Dolgoročno se seveda taka dejanje izkažejo za neuspešna, izpostavljajo pa pomembnost razpršenosti oz. ustrezne zaščitenosti in varovanega dostopa do ključne informacijske infrastrukture, o kateri več v naslednjem poglavju.

V zadnjem času pa se je razprava o svobodi posameznika in njegovi varnosti in zasebnosti na spletu razplamtela predvsem v okviru mednarodnega Trgovinskega sporazuma za boj proti ponarejanju (ACTA[35]). Medtem ko uradne institucije pojasnjujejo, da gre predvsem za skupne in učinkovitejše napore pri soočanju s kršitvami pravic intelektualne lastnine, usklajevanje mednarodnih pravil in okvirov za kazenski pregon ter zaščito delovnih mest in predvsem intelektualne lastnine, se v javnosti[36] poraja mnogo očitkov z različno argumentacijo. Bistvo očitkov leti predvsem na račun omejevanja osebne svobode, vendar iz samega besedila sporazuma težko opravičimo te pomisleke, ostaja pa trdna osredotočenost na zagotavljanje intelektualne lastnine (*Kaj je ACTA?*, 2012; *Trgovinski sporazum za boj proti ponarejanju*, 2011).

---

[34] Tehnično je to mogoče le v državah, kjer ima oblast nadzor nad vsemi ponudniki interneta, v Egiptu je tako oblast zahtevala začasen umik več kot 3500 BGP-jev (angl. ***B**order **G**ateway **P**rotocol* – protokol mejnih usmerjevalnikov) pri kar devetih ponudnikih, kar se je odrazilo v več kot 88% nedelovanju interneta. BGP-ji imajo izredno pomembno vlogo pri usmerjanju paketkov prometa prek interneta, ustavitev oz. blokada teh protokolov dobesedno odrežejo uporabnike, ki so v internet povezani prek tega protokola in postanejo za ostale »nevidni«, uporaba interneta pa je tako onemogočena. Edini ponudnik, ki je še imel možnost komuniciranja s preostalim svetom, je bil Noor Data Networks, ki povezuje Egiptovsko borzo s svetom (How Egypt shut down the internet, 2011).

[35] Angl. ***A**nti **C**ounterfeiting **T**rade **A**greement*

[36] Celo znana aktivistična skupina Anonymous je objavila poziv slovenski vladi naj zamrzne postopek podpisovanja tega sporazuma, sicer naj bi sledili napadi na vladne spletne strani in strani največje slovenske banke. V tem duhu so v januarju 2011 tudi potekali protesti proti sprejetju sporazuma, vlada pa se je odločila, da odpre širšo javno razpravo na to temo.

Popolnoma nov segment v področju kibernetske varnosti pa bo sprožila množična uporaba računalništva v oblaku. Avtorji (Seghal in drugi 201, 290) ugotavljajo predvsem, da je glavna varnostna dilema računalništva v oblaku na relaciji med varnostjo dostopa in učinkovitostjo storitve in sistema, saj je popoln varnostni sistem samo tisti, kjer dostop ni mogoč, pri računalništvu v oblaku pa je ravno neprestana dostopnost z različnih lokacij tista, ki ga definira in mu daje konkurenčno prednost. ENISA pa v svoji študiji (*Cloud Computing* 2009, 7–8) izpostavi kar nekaj koristi, ki jih prinaša računalništvo v oblaku, naj izpostavim samo varnostni vidik, i. e. da je za varnost na enem mestu potrebnih manj sredstev oz. da ista raven sredstev lahko zagotovi višjo raven varnosti in zasebnosti, če se le-ta uporabijo na enem mestu, ter druge prednosti računalništva v oblaku, kot so večje število lokacij strežnikov ter s tem razpršenost tveganj za trajno izgubo podatkov.

3.5 Ključna informacijska infrastruktura

Evropski svet je že leta 2004 predlagal pripravo splošne strategije varovanja ključne infrastrukture, takrat še predvsem v duhu zaščite pred terorističnimi napadi, predvsem pod vtisom napada na WTC v 2001 ter kasnejših v Madridu in Londonu. Komisija je tako v letu 2005 sprejela Zeleno knjigo o evropskem programu za varovanje ključne infrastrukture, ki je bila podlaga za začetek skupne politike zaščite ključne infrastrukture v EU.

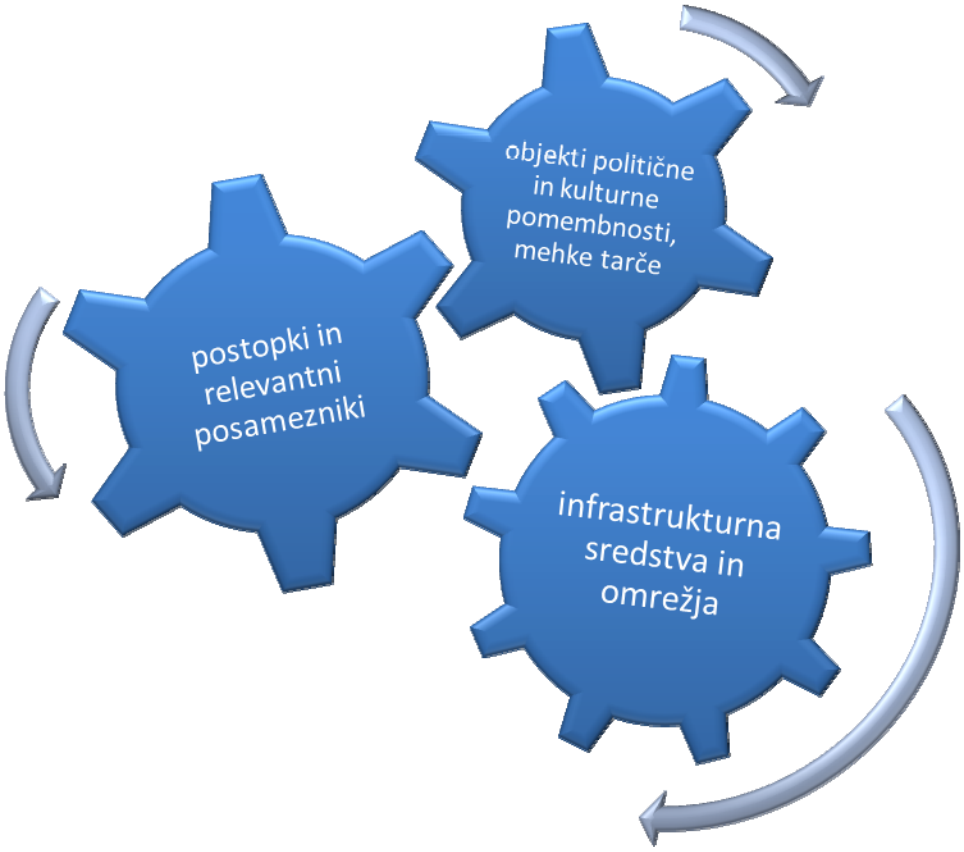
Uvodne ugotovitve Zelene knjige se tako nanašajo na potencialne grožnje ključni infrastrukturi, ki se lahko poškoduje, uniči ali okvari zaradi namernih terorističnih napadov, naravnih nesreč, malomarnosti, nesreč ali vdorov hekerjev, kriminalnih dejavnosti in zlonamernega vedenja. Osrednji namen ureditve tega področja pa je, »da bi življenja in premoženje ogroženih ljudi v EU zavarovali pred terorizmom, naravnimi in drugimi nesrečami ter da bi morale biti motnje ali manipulacije ključne infrastrukture čim krajše, čim manj pogoste, čim bolj obvladljive, zemljepisno omejene in kar najmanj škodljive za blaginjo držav članic, njihovih državljanov in Evropske unije« (*Zelena knjiga o Evropskem programu za varovanje ključne infrastrukture* 2005, 1).

Ključna informacijska infrastruktura je tako le en od sestavnih elementov ključne infrastrukture[37], zato je smiselno najprej opredeliti krovni pojem. V *Zeleni knjigi* (2005, 20) EU ključno infrastrukturo[38] definira kot »skupek fizičnih sredstev, storitev in objektov informacijske tehnologije, omrežij in infrastrukturnih sredstev, ki bi v primeru uničenja ali motenj v delovanju imele velik vpliv na zdravje, zaščito, varnost ali ekonomski dobrobit državljanov ali učinkovitega delovanja vlad«. Ločimo tri tipe infrastrukturnih sredstev: javna, zasebna in vladna infrastrukturna sredstva in soodvisna kibernetska in fizična omrežja; postopke in relevantne posameznike, ki izvajajo nadzor nad funkcijami ključne infrastrukture ter objekte politične ali kulturne pomembnosti ter tudi *mehke* tarče, ki vključujejo množične dogodke (športne, kulturne, aktivnosti v prostem času). Soodvisnost teh sredstev je ključna pri obravnavanju ključne infrastrukture. Svet Evropske unije pa je v svoji direktivi podal drugačno definicijo ključne (kritične) infrastrukture, in sicer jo opredeli »kot infrastrukturno zmogljivost, sistem ali njun del, ki se nahaja v državah članicah in je bistven za vzdrževanje ključnih družbenih funkcij, zdravja, varnosti, zaščite, gospodarske in družbene blaginje ljudi ter katerih okvara ali uničenje bi imelo v državi članici resne posledice zaradi nezmožnosti vzdrževanja teh funkcij« (*Direktiva Sveta o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite* 2008, 2). Slovenija je to direktivo implementirala v lastno zakonodajo v letu 2011 z Uredbo o evropski kritični infrastrukturi.

Za potrebe EU pa je bila definirana tudi ožja formulacija ključne infrastrukture, t. i. evropska ključna infrastruktura, kjer je bistvena razlika v pomenu čezmejnih posledic v dveh ali več državah članicah EU. Jakost ogrožanja ključne evropske infrastrukture se meri z geografskimi razsežnostmi grožnje izgube ali nedostopnosti ključne infrastrukture, časovne razsežnosti in ravni soodvisnosti pri posameznem elementu ključne infrastrukture (*Zelena knjiga o Evropskem programu za varovanje ključne infrastrukture* 2005, 20).

[37] Angl. ***C**ritical **I**nfrastructure* (CI)
[38] Med ključne sektorje spadajo: energetski, informacijsko-komunikacijske tehnologije, oskrba z vodo in hrano, zdravje, finance, javni red in mir, javna uprava, transport, kemična in jedrska energija, vesolje in raziskave (Zelena knjiga o Evropskem programu za varovanje ključne infrastrukture, 24).

Shema 3.3: Soodvisnost sredstev ključne infrastrukture



Ključna informacijska infrastruktura[39] (KII) pa je definirana kot »informacijsko-komunikacijski sistemi, ki so ključna infrastruktura sami zase ali so bistveni za delovanje druge ključne infrastrukture (telekomunikacije, internet, računalniki, programska oprema, sateliti itd.)«. Pomemben pojem je tudi zaščita ključne informacijske infrastrukture[40], ki ga EU definira kot »programe in aktivnosti lastnikov, upravljavcev, izdelovalcev, uporabnikov in regulatornih organov infrastrukture, katerih namen je vzdrževanje in zagotavljanje delovanja KII tudi v primeru okvar, napadov ali incidentov nad dogovorjeno minimalno ravnjo storitev in minimiziranje škode in potrebnega časa za okrevanje in odpravo ovir«. Zaščita KII je torej nadsektorski pojem in za uspešno izvajanje je bistven holistični pristop zaradi širine problematike (*Zelena knjiga o Evropskem programu za varovanje ključne infrastrukture* 2005, 19).

[39] Angl. ***C**ritical **I**nformation **I**nfrastructure* (CII)
[40] Angl. ***C**ritical **I**nformation **I**nfrastructure **P**rotection* (CIIP)

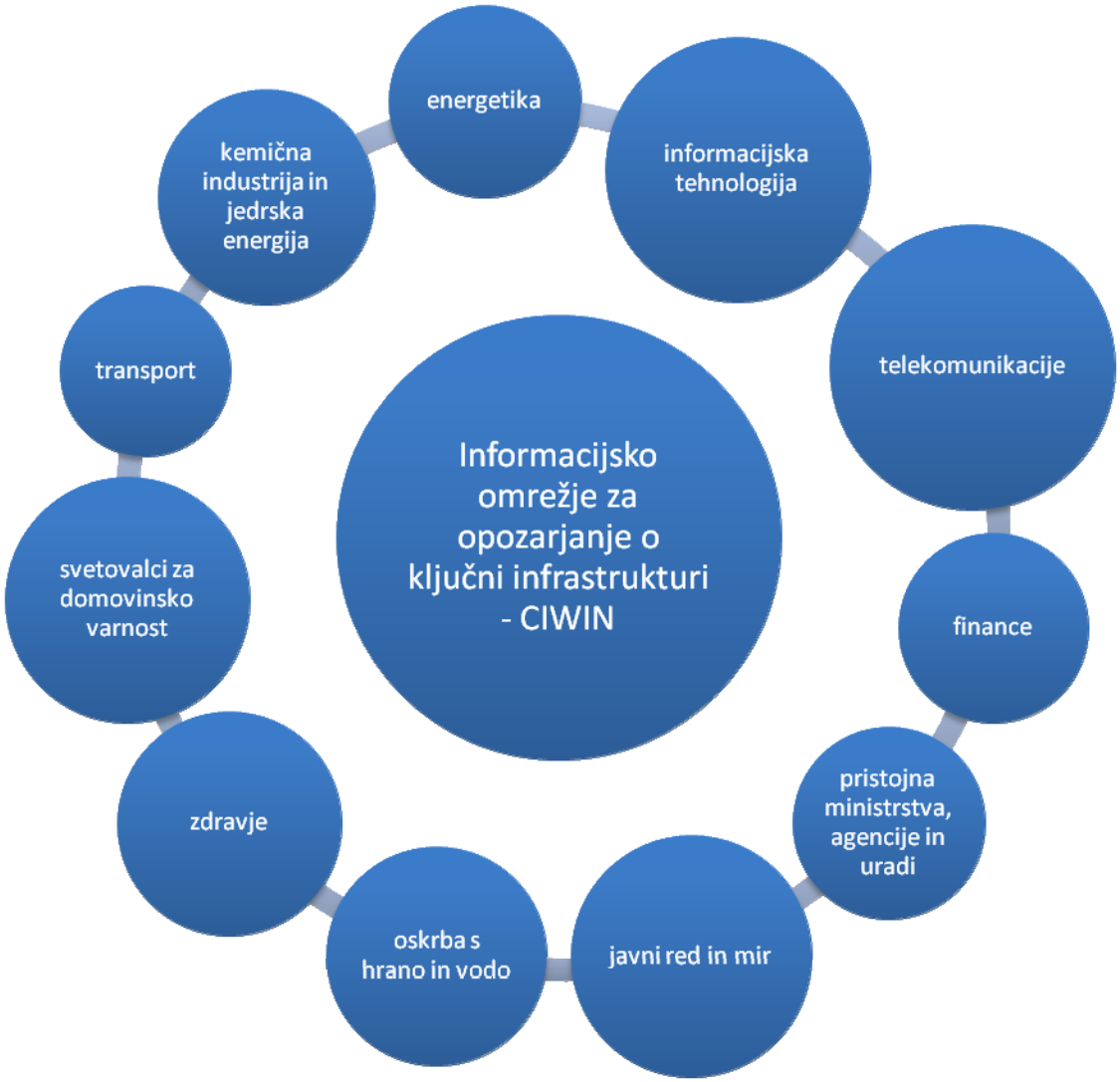
V Evropskem programu o varovanju ključne infrastrukture[41] (*Sporočilo Komisije o Evropskem programu za varovanje ključne infrastrukture*, 5) je opredeljeno tudi informacijsko omrežje za opozarjanje o ključni infrastrukturi[42], čigar namen je zagotoviti izhodišče za varno izmenjavo najboljših praks in dopolnitev obstoječih omrežij (CIWIN). Potencialno pa naj bi se CIWIN začel uporabljati tudi kot izhodišče za izmenjavo hitrih opozoril v kritičnih situacijah in pred njimi. V širšem smislu pa vzpostavitev CIWIN spada med ukrepe EU za olajšanje razvoja in izvajanje EPCIP.

Medtem ko se CIWIN v Evropi praktično šele vzpostavlja v okviru ENISE (EISAS, več o njem v naslednjih poglavjih), je bila v ZDA mreža za opozarjanje pred napadi na informacijsko omrežje aktivna že v 2002[43]. Na podlagi usmeritev Sveta za nacionalno varnost je bil v okviru Agencije za obrambne informacijske sisteme[44] vzpostavljen sistem zmogljivosti informiranja s časovno občutljivimi, ključnimi informacijami za ZDA na državni in lokalni ravni ter ključnimi zasebnimi institucijami. Osrednji cilj ameriškega CIWIN je vzpostavitev neodvisne mreže[45], ki povezuje ministrstvo za domovinsko varnost z vitalnimi sektorji, ki so bistveni pri vzpostavljanju državne ključne infrastrukture v primeru incidentov pomembnih na državni ravni. Povezani akterji so prikazani na shemi 3.4.

---

[41] Angl. ***E**uropean **P**rogramme for **C**ritical **I**nfrastructure **P**rotection* (EPCIP)
[42] Angl. ***C**ritical **I**nfrastructure **W**arning **I**nformation **N**etwork* (CIWIN)
[43] CIWIN naj bi bil znotraj ZDA dokončan v letu 2005 (*US Critical infrastructure Warning Information Network complete*, 2011).
[44] ***D**efense **I**nformation **S**ystems **A**gency* (DISA) deluje v okviru Ministrstva za obrambo (angl. *Department of Defense*). Poleg DISA pa je na tem področju v okviru Ministrstva za domovinsko varnost (angl. *Department of Homeland Security*) še množica drugih institucij, o katerih pa več v nadaljevanju.
[45] Kot ugotavlja Gorman (2004, 2–5) je bila v ZDA na prelomu tisočletja velika večina optičnih vlaken med ključnimi lokacijami v zasebni lasti, zato je bilo treba za celovit vpogled in možnost nadzora vzpostaviti tudi javno telekomunikacijsko infrastrukturo.

Shema 3.4: Povezanost sektorjev znotraj CIWIN



Opomba: prirejeno in smiselno združeno (*Critical infrastructure Warning Information Network,* 2 in *Zelena knjiga o Evropskem programu za varovanje ključne infrastrukture*, 1).

Drugi avtorji (Dunn 2005, 285) pa so mnenja, da ključna infrastruktura in ključna informacijska infrastruktura nista enostavno ločljivi, sploh pa ju ne smemo obravnavati kot različna koncepta. Varovanje ključne informacijske infrastrukture je tako bistven del varovanja ključne infrastrukture. Bistvo te povezanosti je, da osredotočanje izključno na kibernetske grožnje KII, ki zanemarja fizično ogrožanje ključne infrastrukture, je prav tako zmotno kot zagotavljanje zgolj fizične varnosti in zanemarjanje virtualnega, kibernetskega ogrožanja.

Globlje kot se pomikamo od splošne ravni ključne infrastrukture, večji pomen[46] se posveča informacijsko-komunikacijskih tehnologijam in njihovim akterjem, saj je ob povečani informatizaciji posameznega področja, vpliv z IKT opremljenega akterja lahko tem večji. Sistemi ključne infrastrukture so v zadnjih desetletjih zaradi uporabe IKT in globalizacije dobili novo razsežnost v infrastrukturi optičnih omrežij, ki je za gospodarstva in sisteme 21. stoletja ključna. Ta ista IKT, ki je omogočala hiter razvoj in zmanjševala pomembnost oddaljenosti različnih sistemov in je dandanes ključna v vseh pogledih, je v rokah zlonamernežev čedalje pogosteje[47] tudi orodje napada in ogrožanja. Zmanjšan pomen geografske lokacije, oz. uporabnost lokacije le od njene (dobre) povezanosti v kibernetski prostor je imelo mnogo pozitivnih razsežnosti. Navidezna »nepomembnost« geografske lokacije ter napačno asociiranje internetnih in IKT-groženj le na kibernetski prostor dopuščata veliko prostora za zlonamerno delovanje. Tudi izvršni direktor ENISE ugotavlja (*ENISA today and in the future*, 2011), da je uporaba IKT v namene kibernetske kriminalitete in politično motiviranih kibernetskih napadov v porastu.

Brezmejna narava IKT, njena globalnost, povezanost in soodvisnost z drugimi infrastrukturami naredi tudi grožnje globalne in kompleksne, zato njihova varnost in odpornost proti tovrstnim grožnjam, ne more biti zagotovljena zgolj z lokalnimi in nekoordiniranimi ukrepi, zato EU izpostavlja potrebnost celovitega okvira delovanja na ravni EU. Kibernetska varnost omrežij je tako vitalnega pomena za sodobne komunikacije, gospodarsko rast in razvoj ter družbeno povezanost.

---

[46] Zanimivo je, da EU v svojem strateškem dokumentu Evropa 2020, ugotavlja, da so vlaganja v inovacije premajhna, nezadostna uporaba informacijskih in komunikacijskih tehnologij pa naj bi vplivala na zmanjšano konkurenčnost in dolgoročno blaginjo. Torej, kljub dejstvu, da spadamo v razviti del sveta, se primerjalno gledano tuji gospodarski partnerji na področju IKT razvijajo hitreje, kar je zagotovo zaskrbljujoče, EU pa kot odziv na situacijo daje pobudo, da naj bi do leta 2013 vsa gospodinjstva imela dostop do širokopasovne povezave, do leta 2020 pa naj bi vsi imeli možnost dostopa do interneta z vsaj 30 Mbit/s ali hitreje (*Evropa 2020*, 7–14*).*

[47] Statistični podatki za Nemčijo prikazujejo čedalje večje število razrešenih kriminalnih dejanj in njihov splošen upad. Eno od redkih področij, kjer kriminaliteta narašča pa je področje kibernetskega kriminala, kjer so zabeležili več kot 8% porast v letu 2010. Številka se približuje četrt milijona zabeleženih incidentov letno, trend pa je vzpenjajoč (*Crime rates drops to record low*, 2011).

4 Kibernetska varnost omrežij

Kibernetski prostor se danes dotika vseh segmentov našega življenja. Širokopasovna omrežja pod nami, brezžična omrežja okoli nas, lokalna omrežja v šolah, bolnišnicah in v poslovnem okolju… in na koncu svetovni splet, ki nas je povezal bolj kot karkoli drugega v človeški zgodovini. Če želimo ohraniti varno okolje in trenutno kakovost življenja, je nujno potrebno zaščititi kibernetski prostor in njegove elemente, ki povezujejo naš vsakdan.

Pomembnost področja kibernetske varnosti omrežij odraža tudi raven pozornosti in prisotnost te problematike na najvišjih, strateških ravneh odločanja in načrtovanja. Sicer kibernetska varnost ni dobesedno omenjena v Evropski varnostni strategiji, vendar jo lahko prepoznamo v besedni zvezi »novih groženj« in v okviru varovanja ključne (informacijske) infrastrukture (Varna Evropa v boljšem svetu 2003, 2). Je pa kibernetska varnost svoje mesto dobila v strateškem dokumentu, ki je sledil strategiji. Kibernetska varnost je prepoznana kot eno od ključnih področij globalnih groženj in izzivov, tudi z vidika varovanja ključne informacijske infrastrukture ter odvisnosti celotne Evrope od IKT, v dokumentu pa je jasno zapisana potreba po celovitem pristopu EU k nadaljnjem preučevanju in spremljanju tega področja (Zagotavljanje varnosti v spreminjajočem se svetu 2008, 4). Omrežna in informacijska varnosti[48] pa je tudi eden od elementov Strategije za varno informacijsko družbo, kjer pa se omenja predvsem kibernetska kriminaliteta in boj proti njej (A Strategy for a Secure Information Society, 2006).

Prav tako je so tudi ZDA prepoznale kibernetsko varnost kot eno pomembnejših področij 21. stoletja. Predsednik Barrack Hussein Obama je tako že na začetku svojega mandata zahteval celovit vpogled v zvezne napore za zagotavljanje kibernetske varnosti na področju informacijske in komunikacijske infrastrukture ter

[48] Angl. ***N**etwork and **I**nformation **S**ecurity* (NIS) je v Strategiji definirana kot »zmožnost omrežja ali informacijskega sistema, pri določeni stopnji zaupanja, da se ubrani pred neželenimi dogodki ali zlonamernimi dejanji, ki ogrožajo dostopnost, avtentičnost, integriteto in zaupnost shranjenih ali prenesenih podatkov in odgovarjajočih storitev, ki so dostopne ali ponujene prek teh omrežij in sistemov« (*A Strategy for a Secure Information Society* 2006, 3).

določil koordinatorja kibernetske varnosti s stalnim dostopom do predsednika ter ustanovil Urad za kibernetsko varnost (Cybersecurity, 2011).

Informacijska doba in posledično informacijsko vojskovanje dopušča ogrožanje na več ravneh. Tako so dobila novo obliko orožja, prav tako tudi tarče. Arquilla in Ronfeldt (v Schwartzstein 1996, 157) že pred več kot desetletjem opazita dve ključni spremembi, prva je preskok od uporabe smrtonosnih materialnih orožij zgolj za napade na materialne tarče, tudi za napade na sisteme C3I[49] in RISTA[50], ki predstavljajo nasprotnikove elektronske senzorje oz. živčni sistem, drugi preskok pa je uporaba nesmrtonosnih elektronskih tehnik (orožij) za onesposabljanje nasprotnikovih smrtonosnih sistemov ali njegovih kibernetskih sistemov, ki hranijo, procesirajo ali prenašajo informacijo.

Tudi slovenski Center za posredovanje pri internetnih incidentih[51] je pred kratkim poročal (april 2011) o obsežnejšem vdoru v zbirko uporabniških podatkov. Vdor nepooblaščenih storilcev naj bi posredno oškodoval več kot 100 milijonov uporabnikov (SI.CERT 2011) po celem svetu. Razkriti naj bi bili osebni podatki od nazivov, naslovov elektronske pošte, vzdevkov, gesel in celo številk kreditnih kartic. Iskani termin »PlayStation Network« je v naslednjem tednu dosegel porast 2850 odstotkov na iskalniku Google ter tako postal najbolj iskan termin po spletnem napadu. Sony se je na napad odzval z blokado dostopa do zbirk podatkov in s tem svojih spletnih storitev, kar je ključen podatek (zanj, za konkurente in za uporabnike).

Podobni dogodki so v zadnjih letih vedno deležni precejšnje medijske pozornosti, širša skupnost pa se še ne zaveda dovolj prisotnosti tovrstnih groženj in potencialne škode, ki bi lahko s tem nastala. Svetovni gospodarski forum[52] je leta 2008 ocenil, da bi večja okvara omrežij oz. ključne informacijske infrastrukture lahko povzročila gospodarsko škodo v višini več sto milijard USD, verjetnost takega dogodka pa ocenil na 10-20% v naslednjih desetih letih (*A World Economic Forum Report* 2008, 24).

---

[49] Angl. ***C**ommand, **C**ontrol, **C**ommunications & **I**ntelligence* (poveljevanje, nadzor, komuniciranje in obveščanje).
[50] Angl. ***R**econnaissance, **I**ntelligence, **S**urveillance and **T**arget **A**cquisition* (izvidovanje, obveščanje, nadzorovanje in pridobivanje ciljev).
[51] SI-CERT; angl. ***S**lovenian **C**omputer **E**mergency **R**esponse **T**eam*. Naloga centra je koordinacija obveščanja in reševanje varnostnih problemov v računalniških omrežjih v Sloveniji, deluje pa v okviru Arnesa.
[52] V svojem poročilu *A global Risk Network Report*.

Forum je do teh sklepov prišel na podlagi ugotovitev, da neprestano prepletanje faktorjev ogrožanja (kompleksnost sistemov, množica ranljivosti, neuspešni oz. nepopolni popravki varnostnih lukenj, uporaba splošnih proti specialnim aplikacijam itd.) dodatno izredno otežuje napovedovanje posameznih napadov, poleg tega pa še splošno povečanje tovrstnega ogrožanja zaradi pomanjkanja pozornosti in sredstev, namenjenih kibernetski varnosti ter neprestanim prilagoditvam s strani napadalcev. Podobne ugotovitve navajajo tudi drugi avtorji (Owen v Janczewski in Colarik 2008, 35). Evidentirano je bilo, da se čedalje pogosteje kot napadalci pojavljajo predvsem državni akterji in akterji večjega obsega (Carr 2010, 1), tako naj bi bilo na področju kibernetskega vojskovanja trenutno aktivnih več kot sto dvajset držav.

Morebitno ogrožanje ključnih omrežij, če ga obravnavamo kot posamezen dogodek, izpolnjuje tudi vse kriterije, ki naj bi opredeljevali krizo (Malešič 2004: 436):

- ogrožanje temeljnih vrednot, še posebej varnosti kot instrumentalne vrednote,
- časovni pritisk pri sprejemanju odločitev za razrešitev razmer ter
- negotovost in stres, ki ju vsiljujejo razmere.

Kibernetska varnost omrežij ima zato pomembno vlogo tudi z vidika kriznega upravljanja in vodenja države ali institucij v izrednih razmerah[53] ter tudi z vidika uporabe kriznega komuniciranja[54] oz. omejenih možnosti v primeru izrednega dogodka.

Spopad z grožnjami kibernetske varnosti je vedno večplasten, bistveni pa sta dve prvini, ki se vseskozi pojavljata v večini strateških dokumentov:

- izboljšanje odpornosti KII proti kibernetskim incidentom in
- zmanjševanje kibernetske grožnje.

---

[53] Tudi v drugih uradnih dokumentih Republike Slovenije (Doktrina civilne obrambe Republike Slovenije, 11) je omenjena pomembnost različnih družbenih podsistemov, ki bi lahko bili z informacijskim ali drugim specialnim delovanjem onemogočeni, s čimer bi bilo onemogočeno delovanje informacijskih in komunikacijskih sistemov ter sredstev javnega informiranja, še zlasti radiodifuzije.

[54] Za učinkovito strategijo kriznega komuniciranja so predvsem pomembni štirje dejavniki: priprava in razširjanje informacij, identificiranje zainteresiranih strank, vzpostavljanje stika s skupnostjo in vzpostavljanje odnosov z množičnimi mediji (Malešič, Hrvatin in Polič 2006, 190). V primeru prekinjenega delovanja ključnih omrežij, bi bila resno ogrožena tudi zmožnost pristojnih za uspešno krizno komuniciranje, kar bi še dodatno poglobilo krizo.

Izboljševanje odpornosti ključne informacijske infrastrukture vključuje predvsem utrjevanje digitalne infrastrukture in njeno odpornost za predrtje in motnje, izboljšanje sposobnosti obrambe pred prefinjenimi in spretnimi kibernetskimi napadi in hitro okrevanje po morebitnih napadih. Zmanjševanje kibernetske grožnje pa se poskuša doseči z vzpostavitvijo pravil in dovoljenega v kibernetskem prostoru na mednarodni ravni ter z vzpostavitvijo ustreznih ukrepov na področju preganjanja kibernetskega kriminala in odvračanja potencialnih nasprotnikov od izkoriščanja preostalih ranljivosti. Kot je pokazala raziskava ENISE (Measurement Frameworks and Metrics for Resilient Networks and Services 2010, 11), je eden od izzivov tudi definicija odpornosti omrežij, saj je pogosta težava razlikovanje med odpornostjo in varnostjo ter odnosom (podrejenostjo kibernetske varnosti napram odpornosti[55]) med njima.

Ker pa ima varnost KII več aspektov je smiselno dogodke, ki bi imeli za posledico ogroženo varnost in stabilnost KII, razdeliti v nekaj temeljnih segmentov. V okviru ITU[56] avtorji (Dunn 2005, 8) tako potencialno ogrožajoče dogodke delijo na tri ravni:

- nedelovanje,
- nezgode in
- napade.

Nedelovanje je škodljivi dogodek, ki ga povzročijo pomanjkljivosti v sistemu ali v internem elementu od katerega je sistem odvisen. Nedelovanje lahko povzročijo napake v programski kodi, poškodbe strojne opreme, človeška napaka ali popačeni podatki. Nezgode vključujejo celoten spekter naključnih in potencialno škodljivih dogodkov kot so naravne nesreče. Praviloma so nesreče posledica zunanjih (i. e. zunaj sistema) dejavnikov, medtem ko je nedelovanje posledica notranjih dogodkov. Tretja raven pa so napadi z različnimi orodji, ki so potencialno škodljivi dogodki, praviloma povzročeni s strani nasprotnika. Ta kategorija je izrednega pomena za razprave okoli kibernetskega ogrožanja (prav tam).

---

[55] Kibernetska dimenzija ogrožanja omrežij je le ena od mnogih. Več o omogočanju in upravljanju z odpornostjo telekomunikacijskih omrežij je na voljo v publikaciji ENISE (*Enabling and managing end-to-end resilience*, 2011).

[56] Angl. ***I**nternational **T**elecommunication **U**nion* – ITU, več o ITU na uradni spletni strani (http://www.itu.int/en/Pages/default.aspx, 9. oktober 2011).

Pogosto je težko določiti kateri tip ogrožajočega dogodka je nastopil v konkretnem primeru, saj so posledice podobne; pomembneje je kakšne posledice je dogodek sprožil, vsaj kratkoročno. V prvi vrsti je tako pomembno kakšne so potencialne posledice, šele nato je smiselno določiti izvor dogodka; to pa seveda ne velja za srednjeročne in dolgoročne strategije varovanja KII (prav tam).

Nadalje Dunn (2005, 9) definira dva ogrožajoča scenarija, ki v temelju delita kibernetske grožnje po svoji naravi na dva pola.

- **Nestrukturirane grožnje** so naključne in relativno omejene. So posledica delovanja nasprotnikov z omejenimi sredstvi ter organizacijo in so praviloma kratkoročno usmerjene. Te akterji imajo omejena sredstva, orodja, veščine in financiranje, ki jim onemogočajo izvedbo prefinjenih napadov. Nestrukturirane grožnje tako ne morejo ogroziti državne varnosti oz. varnosti ključne informacijske infrastrukture. Lahko pa te napadi povzročijo precejšnjo škodo v določenih okoliščinah.
- **Strukturirane grožnje** so znatno bolj metodične in bolje podprte. Tovrstni nasprotniki imajo vsakovrstno obveščevalno podporo, obsežna sredstva, organizirano profesionalno podporo in dolgoročne cilje. Tuje obveščevalne službe, kriminalna dejanja, vključenost profesionalnih hekerjev, informacijsko vojskovanje in gospodarsko vohunjenje spadajo v to raven ogrožanja. Čeprav nestrukturirana grožnja ne predstavlja neposrednega ogrožanja, obstaja potencial, da se strukturirane grožnje odražajo prek aktivnosti, ki bi navzven delovale kot delovanje nestrukturiranih akterjev (prav tam).

S prepoznavanjem posameznega napada kot nestrukturirane grožnje bi mu lahko neupravičeno zmanjšali pripisano pomembnost, kar posledično lahko sproži verigo kasnejših napačnih odločitev, zato je smiselno vse napade obravnavati resno. Za kibernetsko varnost ključne informacijske infrastrukture pa so ključnega pomena strukturirane grožnje, ki lahko dolgoročno in trajno onemogočijo delovanje KII, zato bo njim namenjeno več pozornosti.

Napad na KII ima lahko več pojavnih oblik, od kibernetskih do fizičnih, zato je smiselno vsaj omeniti vse, tudi druge tipe ogrožanja, ki bi imeli podobno katastrofalne posledice. Prav tako je lahko KII ogrožena v obeh smislih, tako v smislu programske opreme ali podatkov kot tudi v smislu ogrožanja strojne opreme, ki poganja

programsko opremo ali fizične infrastrukture, ki omogoča prenos podatkov. V spodnji shemi 4.1 je mogoče razbrati različne kombinacije ogrožanja.

Shema 4.1: Matrika groženj KII

		CILJ	
		materialen	kibernetski
ORODJE	materialno	➢ fizična prekinitev telekomunikacijskega kabla ➢ fizično uničenje strojne opreme	➢ uporaba elektromagnetnega valovanja in radijskih frekvenc za destabilizacijo elektronskih komponent
	kibernetsko	➢ vdor v sistem oskrbe z vodo ➢ onemogočenje delovanja sistema nadzora prometne signalizacije	➢ vdor v ključne informacijske sisteme države ➢ vdor v javne komunikacijske storitve

Prirejeno po Dunn 2005, 10.

4.1 Različne ravni in učinki kibernetskega ogrožanja

4.1.1 Družbeno-politični vidik

Raziskovalci Züriškega Centra za varnostne študije poskušajo izpostaviti tudi druge vidike varovanja ključne informacijske infrastrukture, poleg pogledov inženirjev informatike in IT varnostnih specialistov. Zaradi množice družbeno političnih vidikov, ki vplivajo na to panogo in kompleksnega okolja, v katerem se ključna informacijska infrastruktura nahaja, je smiselno v preučevanje le-te vključiti tudi družboslovne

znanosti. Dunn (2005, 261) tako prepozna tri pristope k varovanju KII, ki so jih ubrale različne države:

- nacionalno-varnostni vidik (celotna družba in njene osrednje vrednote so ogrožene ob ogrožanju KII zaradi zanašanja družbe nanjo; ukrepi proti grožnjam potekajo na več ravneh: tehnični, zakonodajni, organizacijski ali mednarodni; glavni akterji politike varovanja KII so v tem primeru predstavniki varnostnega sektorja),
- ekonomski vidik (varovanje KII je predvsem varovanje poslovanja gospodarstva in produktivnosti v dobi e-oblik komuniciranja in poslovanja, ki pogojuje neprestan dostop do IKT in s tem ohranitev dosežene ravni produktivnosti; glavni akterji prihajajo iz zasebnega sektorja) in
- vidik kazenskega pregona (kjer je varovanje KII prepoznano predvsem z vidika zaščite družbe pred kibernetskim kriminalom, i. e. od kriminala pogojenega z uporabo IKT do kriminala usmerjenega proti individualnim računalnikom).

Omejevanje snovalcev politike varovanja KII zgolj na eno področje oz. prednostna obravnava nekega področja posredno zanemarja drugi dve področji, kar se odrazi v usmerjenem naporu, zastavljenih ciljih, strategijah in sprejetih instrumentih za varovanje KII. Myriam Dunn (prav tam) izpostavi še izredno pomembno, čeprav večkrat spregledano, vlogo posameznikov oz. ljudi kot akterjev varovanja KII. Človeški faktor je tako izrednega pomena, saj ljudje zagotavljajo, upravljajo in generirajo nove informacije, vzdržujejo in občasno tudi spodkopavajo druge elemente KII. Poleg tega je vloga človeka-posameznika, kot sem omenil že v teoretičnem delu naloge, pri varovanju KII bipolarna, saj se človek-posameznik pojavlja tudi na strani, ki KII s svojim delovanjem ogroža. Tako gre v nekem smislu predvsem za spopad posameznika s posameznikom oz. posameznika z družbo. Drugi avtorji (Lewis v Dunn, 2005, 263) in strokovnjaki prav tako postavljajo grožnjo posameznikov z dobrimi notranjimi informacijami ali celo pripadnike dotične institucije kot največje grožnje KII – to z drugimi besedami pomeni, da je človek-posameznik, ki je hkrati del ustroja varovanja KII, tudi njena največja grožnja.

Dunn (2005, 264–265) izpostavi še dva problematična vidika varovanja KII, ki se pojavljata danes. Najprej se zaustavi pri definiranju pojma *ključna* kjer omeni težavno prepoznavanje sektorjev kot ključnih, saj se definiranje le-teh vedno zgodi iz

percepcije opazovalca in dokler opazujejo le strokovnjaki določenega segmenta je jasno, da so prepoznane grožnje (prek sekuritizacije) le iz opazovalčevega področja, najsi bo tehnično ali ekonomsko. Ključno je, da te poglede razširimo še na družbeno-političen vidik, saj je obseg ogrožanja, ki je za družbo še sprejemljiv[57], bolj politično-družbeni pojem kot tehnično-sistemski. Poleg problema, ki izvira iz zaznavanja grožnje, Dunnova omeni tudi neprimernost orodij za ocenjevanje le-teh, saj naj bi bili primarno namenjeni ocenjevanju ogroženosti posameznih segmentov, sistema sistemov, posamezne infrastrukture, posameznih sistemov podjetij ali institucij oz. tehničnim komponentam. Večina pristopov varovanja KII se tako ukvarja z le ozkim delom problema, ne upošteva pa celostnih vzročno-posledičnih razmerij in morebitnih verižnih akcij pri tem kompleksnem ogrožanju. Za boljše rezultate pri problematiki varovanja KII je tako potreben holističen in interdisciplinaren pristop; torej podobno kot smo uvodoma že ugotavljali za koncept sodobne varnosti.

4.1.2 Fizični vidik ogrožanja

Drugi avtorji (Gorman 2004, 2 in Carr 2010, XIV) prav tako ugotavljajo, da percepcija zaznavanja groženj v kibernetskem prostoru še vedno ni zadovoljivo obravnavana v svojem celotnem pomenu, torej vključno z implikacijami v realnem prostoru, temveč se prepogosto še vedno obravnava le kot dodaten sektor, kot nov segment delovanja brez zavedanja, da ima ta segment zaradi uporabe IKT izreden vpliv na vse ostale »stare« segmente. Carr (2010, XIV) tako pravi, da do pravega zavedanja razsežnosti kibernetskega vojskovanja ne bo prišlo, dokler bodo vrhovni (politični oz. vojaški) odločevalci prihajali iz »predkibernetske dobe«.

Gorman (2004, 2) pa izpostavlja še obrnjeno logiko ogrožanja ključne informacijske infrastrukture, predvsem v fizičnem smislu, saj IKT-tehnologijam in medmrežju ne grozijo samo kibernetske grožnje, temveč tudi nevarnosti fizičnega okolja. Odvisnost delovanja IKT od optičnih omrežij, ki povezujejo različne lokacije, vlaken samih, vozlišč in usmerjevalnikov predstavlja temeljno področje ogrožanja. Različni podatki

[57] Posledice kibernetskega napada je potrebno preučevati tudi s psiho-socialnega vidika in ne le materialnega, saj recimo napad na neko institucijo večjega pomena za varnost in stabilnost družbe, lahko zamaje ugled celotne ureditve in stabilnosti sistema, kar ima lahko širše posledice (izgredi, družbena nepokorščina itd.).

(Albert, Callaway, Cohen v Gorman, prav tam) sugerirajo, da je izpostavljenost omrežij usmerjevalnikov za napade velika. Odzivnost interneta naj bi se kar prepolovila[58] v primeru, da bi bilo onemogočen le zgornji 1% najbolj obremenjenih usmerjevalnikov oz. vozlišč. Geografska razpršenost vozlišč in njihova redundantnost[59] sta zato ključni pri zagotavljanju ustrezne ravni storitev. Študija ENISE (Inter-X: Resilience of the Internet Interconnection Ecosystem 2011, 9) pa ugotavlja, da kljub visoki izpostavljenosti interneta na možne prekinitve, se je le-ta do sedaj pokazal kot izredno odporen. Izziv ostaja prepletenost omrežja omrežij, njegova kompleksnost in soodvisne ravni ter dejstvo, da kljub odsotnosti osrednjega centra upravljanja deluje dobro zaradi skupka posamičnih interesov. Odprta in decentralizirana organizacija je samo bistvo tega ekosistema in je hkrati ključna za dosedanjo uspešnost in odpornost interneta.

Fizični tip grožnje posredno povečujejo tudi različne tehnologije večkratnega koriščenja obstoječih kapacitet hrbteničnih optičnih omrežij. Tako recimo z uporabo različnih tehnologij, na primer WDM[60] ali MPLS[61], različni uporabniki koristijo isto optično vlakno oz. strojno opremo in v primeru fizične prekinitve vlakna ali okvare oz.

---

[58] Aktualnejši podatki pa zgornje analize postavljajo pod vprašaj, saj naj bi katastrofalni potres na Japonskem v 2011 le za nekaj ur zmanjšal dosegljivost določenih usmerjevalnikov, svetovni promet prek spleta pa naj ne bi utrpel večjih šokov. Zavedanje o nujnosti redundančnih prekooceanskih povezav in alternativnih vozlišč po potresu na Tajvanu v 2006 (pretrgani prekooceanski kabli) je očitno imelo učinek (Japonska: internet presenetljivo dobro preživel potres in cunami, 2011).

[59] Primer pomanjkljive vzpostavljenosti redundančnih povezav v tujino je sočasna prekinitev dostopnosti tujih strežnikov pri dveh večjih operaterjih (T-2 in Siol) v Sloveniji 22. februarja 2011. Vzrok napake je bila programska napaka na omrežnem usmerjevalniku v Frankfurtu. Izpad te povezave pa je povzročil večjo zgostitev prometa na drugih usmerjevalnikih in posledično izgubo paketkov (angl. *packet loss*) po celi Evropi in pri prometu, ki je Evropo le prečkal. Odkrivanje take napake lahko traja več ur, prav tako odprava le-te. V primeru fizične poškodbe mrežne opreme ali optičnega medija, pa se odkrivanje in odprava napake lahko zavleče tudi v več dni. Praviloma skrbniki mednarodnih povezav v takih primerih celoten promet preusmerijo na druga vozlišča, seveda pa v vsakem primeru nastane poslovna škoda (Pogovor z omrežnim strokovnjakom, 2011).

[60] Angl. ***W**avelength-**D**ivision **M**ultiplexing* je tehnologija, ki temelji na konceptu frekvenčne modulacije, kjer je pasovna širina razdeljena med več kanalov, vsak kanal pa zaseda le del večjega frekvenčnega spektra. V primeru WDM vsak kanal (tudi frekvenca, lambda) predstavlja svojo valovno dolžino, ideja WDM pa je, da različne pritočne signale s pomočjo multipleksa in prestavitve na točno določeno valovno dolžino pretočimo prek enotnega medija, ne da bi prišlo do kakršnekoli spremembe v informaciji pritočnega kanala. Več detajlov o WDM in drugih tehnologijah večkratnega koriščenja optičnih omrežij je na voljo v Rožman, 2005.

[61] Angl. ***M**ulti**p**rotocol **L**abel **S**witching*, večprotokolarna sprememba (vodenje podatkovnih paketkov od oddajnika do prejemnika, povezava med njima) z menjavo oznak je poseben protokol za usmerjanje in prenos podatkov med različnimi vozlišči, ki omogoča vzpostavitev navideznih povezav med posamičnimi vozlišči. Zaradi uporabe manjše količine strojne opreme, ki jo MPLS omogoča, je tak način prenosa podatkov cenejši (Pogovor z omrežnim strokovnjakom, 2011).

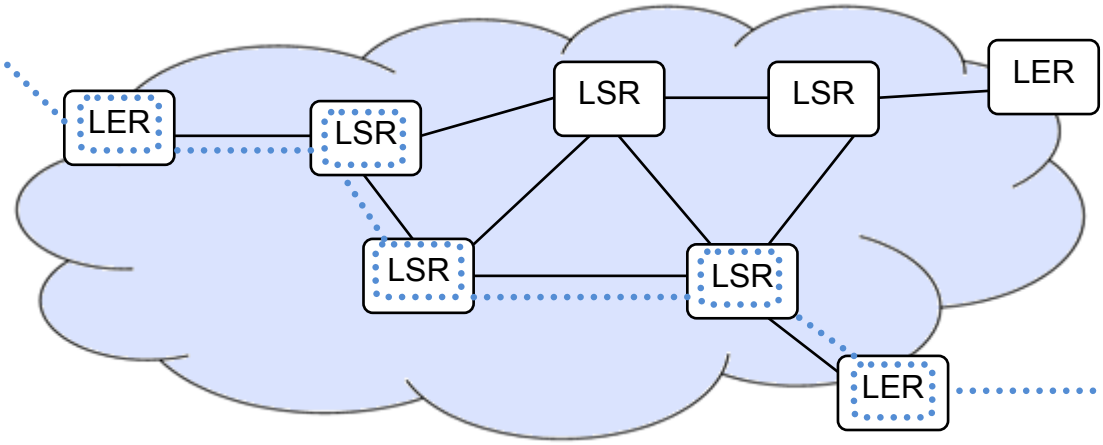
onesposobljene mrežne opreme na posamični lokaciji lahko sočasno preneha delovati več različnih kanalov komuniciranja od navidezno povsem neodvisnih ponudnikov. Razlog, da prihaja do tovrstnega načrtovanja, je ekonomske narave, saj najetje t. i. neosvetljenega vlakna[62] in uporabe obstoječih strežnikov predstavlja neprimerno nižji strošek, kot bi ga predstavljala vzpostavitev lastnega neodvisnega omrežja, v nekaterih primerih pa dodatna (lastna) izgradnja tudi ni mogoča (čezoceanske kapacitete). Obstajajo seveda tudi zaščitne sheme pri večkratnem koriščenju optičnih omrežij, vendar je njihova uporaba omejena z istimi, ekonomskimi razlogi.

Različne tehnologije pa imajo različne šibke točke oz. ozka grla. Pri MPLS-tehnologiji se uporablja več usmerjevalnikov (robni usmerjevalniki LER[63] in hrbtenični usmerjevalniki LSR[64]). Usmerjevalniki na osnovi podatka v glavi posameznega paketa podatkov in na osnovi omrežne topologije na omrežnem sloju[65] določijo (optimalno) pot (LSP[66]), po kateri bo paket potoval, paket pa opremijo s specifično prepoznavno oznako, ki bo paket poslal do naslednjega hopa[67] (MPLS v omrežjih ATM, 2011). LSR-usmerjevalniki pakete posredujejo naprej samo na podlagi oznake, kar ne zavzema dodatnih procesorskih kapacitet in je s tem ta tehnologija racionalnejša in ugodnejša. Arhitektura takega MPLS-omrežja je prikazana na spodnji shemi 4.2.

---

[62] Angl. *Dark Fibre*
[63] Angl. ***L**abel **E**dge **R**outer*
[64] Angl. ***L**abel **S**witch **R**outer*
[65] Angl. *Layer* je ena od omrežnih plasti pri OSI (angl. ***O**pen **S**ystems **I**nterconnection*) referenčnem modelu strukture protokolov. Referenčni model OSI ima sedem plasti: aplikacijska plast, predstavitvena plast, sejna plast, transportna plast, omrežna plast, povezovalna plast in fizična plast. MPLS-protokol deluje med povezovalno in omrežno plastjo. Ta model je potrdila tudi ISO, Mednarodna organizacija za standardizacijo.
[66] Angl. ***L**abel **S**witching **P**ath*
[67] »Hop« v telekomunikacijah pomeni preskok informacije od enega usmerjevalnika k naslednjemu.

Shema 4.2: Prikaz arhitekture MPLS-omrežja



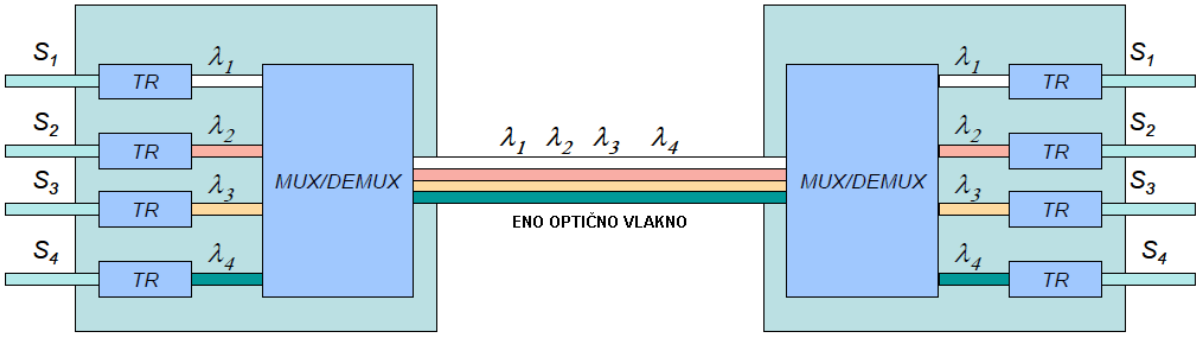
Vir: Prirejeno po *MPLS v omrežjih ATM*, 2011.

Ključna točka za prekinitev bi bil v tem primeru robni usmerjevalnik (LER), medtem ko drugi strokovnjaki (Bennet 2011) navajajo tudi druge potencialne težave, predvsem na področju zagotavljanja kakovosti odzivnosti in zanesljivosti prenosa podatkov[68] ter zanesljivosti in odpornosti programske opreme; le-ta je v MPLS-sistemih ključna, programska oprema pa je večinoma tudi prva tarča zlonamernih akterjev v kibernetski varnosti.

Princip koriščenja istega medija (optičnega vlakna) z uporabo WDM tehnologije pa je prikazan na naslednji shemi 4.3, kjer pritočni signali iz različnih vstopnih kanalov (S_1-S_4), ki so lahko različnih protokolov in različnih bitnih hitrosti, prek transponderjev (TR), ki opravijo pretvorbo v natančno določeno valovno dolžino (λ_1 do λ_4) in multiplekserja (MUX, DEMUX), ki omogoča, da se pritočni signali multipleksirajo tako, da se istočasno ter medsebojno neodvisno prenašajo prek istega optičnega vlakna. V sprejemni smeri je postopek inverzen (Rožman, 2005: 26).

[68] *»Concepts like five nines (99,999%) and 50ms protection are effectively the gold standard«* v angleškem izvirniku.

Shema 4.3: Prikaz večkratnega koriščenja s tehnologijo WDM



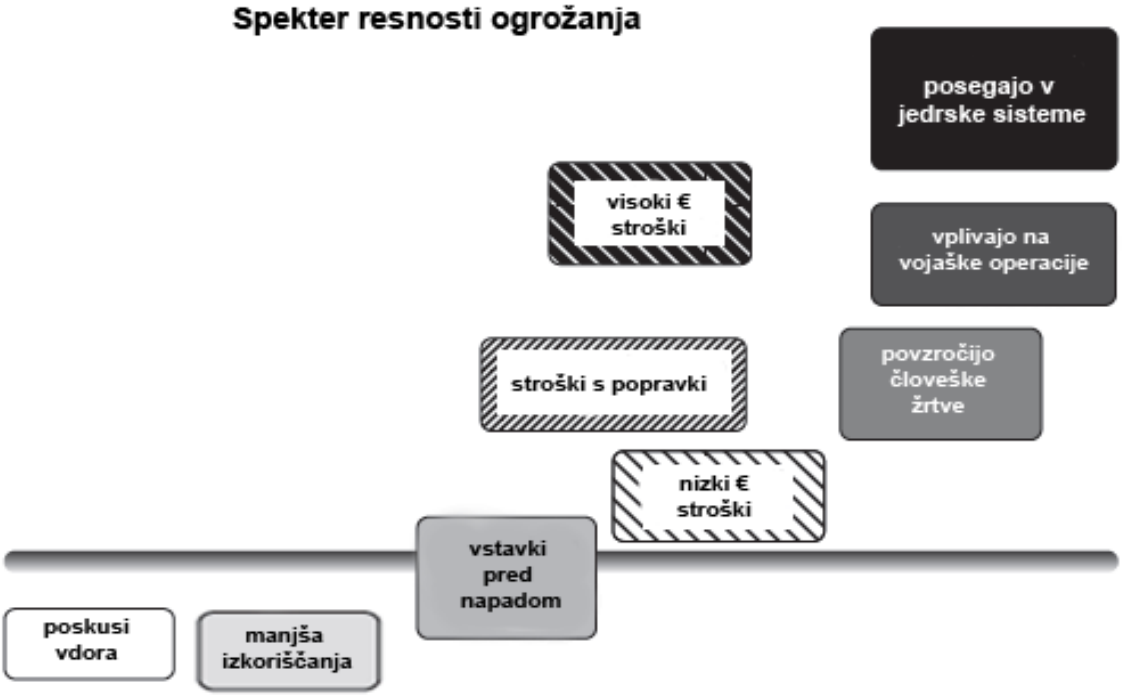
Prirejeno po Rožman, 2005: 26.

Iz sheme 4.3 tako evidentno izhaja, da se v primeru prekinitve enega optičnega vlakna lahko prekine več različnih poti informacij. Zato je pomembno, da poleg kibernetskih groženj KII izpostavimo tudi fizični vidik ogrožanja, v smislu enakega končnega učinka, nedelovanja omrežja. Zanimivo pa je tudi poigravanje z idejo, da lahko s kibernetskim delovanjem onesposobimo fizični del infrastrukture, posamezen usmerjevalnik ali strežnik, čigar delovanje je bistveno za delovanje širšega sistema. S prikazom zgornjih dveh tehnik prenosa podatkov se hitreje pokažejo ključne točke, kjer bi s kibernetskim delovanjem lahko onesposobili ključne elemente informacijske infrastrukture in tako dosegli želen rezultat.

4.1.3 Stopnje ogroženosti

Libicki (2009, 180–181) v okviru svojega raziskovanja za RAND različne stopnje resnosti kibernetskega napada oz. neprijetnosti razdeli na več ravni, predvsem z namenom ocenjevanja potrebnega odzivanja na tak napad. V določenih primerih je neposreden odziv na kibernetski napad neprimeren, sploh, ker še vedno ne obstaja splošen konsenz kakšno kibernetsko dejanje ali aktivnost lahko obravnavamo kot vojno dejanje. Prikaz različnih stopenj je ponazorjen na spodnji shemi 4.4.

Shema 4.4: Različne ravni ogrožanja v kibernetskem prostoru



Prirejeno po Libicki 2009, 181.

4.2 Druge perspektive kibernetskih groženj

Učinek kibernetskega ogrožanja, posreden in neposreden, lahko spremljamo na več načinov. Uporaba le ene percepcije, recimo neposredne finančne, bi bila zavajajoča in kratkovidna. Tako je recimo za neko podjetje lahko izguba ugleda ali zaupanja oz. neprijetnost ob kibernetskem incidentu večji »strošek« kot dejanska sanacija varnostne luknje oz. potencialna izguba podatkov. V očeh uporabnika-potrošnika je tak napad lahko prikaz nemoči oz. nesposobnosti podjetja, da se pred temi dejanji ubrani, kar ga na nek način prikaže kot drugorazrednega. Že uvodoma v to poglavje sem omenil primer Sonya, ki je zaradi kibernetskega vdora moral onemogočiti dostop do svojih strežnikov, s čimer je trpela predvsem uporabniška izkušnja. Večina vdorov

ostaja javnosti nerazkritih, kadar pa pride do razkritja, ugled napadene institucije ali podjetja trpi[69]. Zanimivo pa je nedavna raziskava (Gordon in drugi 2011, 51) pokazala, da se je odnos delničarjev do tovrstnih objav spremenil v zadnjem desetletju, in sicer so vlagatelji postali manj občutljivi na objave o kibernetskih napadih, tako da vrednost podjetij in njihovih delnic pade v manjši meri, kot je ob podobni objavi padla pred desetletjem. Seveda pa so tudi drugi, merljivi indikatorji, ki prikazujejo stroške, ki ob kibernetskem ogrožanju subjektov in njihovih omrežij nastajajo. V drugi raziskavi (Khansa in Liginlal 2009, 117) pa je bila ugotovljena pozitivna povezanost povečevanja sredstev za informacijsko varnost v podjetjih in s tem povezano odpornost na zlonamerne napade, kar že po prvem potencialnem napadu povrne začetni vložek.

V okviru Organizacije za gospodarsko sodelovanje in razvoj[70] so raziskovalci pripravili študijo za *Sistemsko zmanjševanje tveganj kibernetske varnosti*[71]. Avtorja študije (Sommer in Brown 2011, 81–82) tako ugotavljata, da so posamični napadi sicer lahko moteči v smislu povzročene škode in finančnih posledic, vendar ne predstavljajo sistemske grožnje. Sistemsko grožnjo bi lahko predstavljala do sedaj neodkrita pomanjkljivost v ključnih tehničnih protokolih interneta na katero bi bilo težko odgovoriti v nekaj dneh ali množica zaporednih kibernetskih napadov zlonamernežev z izjemnimi veščinami in odločenostjo z izključnim namenom uničevanja, ki bi se na koncu odrazila tudi v propadu napadalca in njegovega lastnega okolja. Avtorja še omenjata možnost nenavadno močnega sončnega izbruha, ki bi lahko povzročila večje prekinitve na električnih in IKT-sistemih. Kar bi snovalce politik moralo zadevati pa so kombinacije dogodkov, lahko več sočasnih kibernetskih dogodkov ali kibernetski napad v kombinaciji z drugimi oblikami napada ali ogrožanja. Možnost čiste kibernetske vojne le s kibernetskimi orodji je tako malo verjetna, gotova pa je uporaba kibernetskih orožij pred bodočimi spopadi, predvsem

[69] Pomenljivi so podatki, ki upoštevajo tržno kapitalizacijo podjetja pred in po kibernetskem napadu, saj naj bi se po nekaterih študijah kibernetski napadi odrazili tudi v ceni delnic napadenega podjetja. Različne študije so evidentirale padce delnic za od 2 % do 5 %, kar pri večjih podjetjih lahko pomeni tudi več deset ali sto milijonov dolarjev. Seveda je izrednega pomena tudi narava napadenega podjetja, internetno podjetje je neprimerno bolj ogroženo s strani kibernetskega kriminala kot neko drugo podjetje iz konvencionalnih panog (Cashell, Jackson, Jickling in Webel 2004, 9).
[70] Angl. ***O**rganisation for **E**conomic **C**o-operation and **D**evelopment*, OECD
[71] Angl. *Reducing Systemic Cybersecurity Risk*

v smislu motnje ali ojačevalca učinka, ki bo sočasen s konvencionalnimi napadi. Kibernetska orožja bodo pogosteje in z večjo intenziteto uporabljena tudi s strani ideoloških aktivistov z različnimi interesi.

Avtorja (prav tam) tako skleneta (sicer zaradi kratke zgodovinske podlage pri preučevanju interneta iz tega ni mogoče povzeti dolgoročnih ugotovitev), da so večje sistemske težave interneta sicer mogoče, vendar malo verjetne, ker:

- je narava interneta robustna (protokoli so narejeni tako, da iščejo alternative za prenos informacij),
- so kibernetski napadi, kjer je prišlo do fizičnih poškodb redki,
- so rešitve in popravki za programsko opremo relativno hitro na voljo,
- DDoS napadi le redko lahko uspešno trajajo dlje kot nekaj dni,
- ima mnogo organizacij in podjetij že lastne sisteme za zaščito in posebne postopke odzivanja na kibernetske incidente ter da
- mnogo najpomembnejših sistemov ni priključeno v internet ter uporablja posebne protokole in opremo ter ima zelo omejen dostop do teh sistemov.

Zaradi zgoraj navedenih argumentov tako grožnja sicer ostaja, sploh ker je internet produkt človeka, tako tudi največjo grožnjo internetu oz. IKT ali KII predstavlja človek. To je posameznik z ustreznimi znanji in ali notranjimi informacijami, ki bi lahko pripeljale do večjega incidenta.

4.2.1 Vpliv na poslovanje in stroške

Raziskave (*Information Security Breaches Survey* 2010) kažejo, da kljub povečanem številu vdorov, število zelo resnih vdorov relativno stagnira, povečano pa je število resnejših in manj resnih vdorov, tako naj bi kar tri petine večjih organizacije imelo vsaj en resnejši vdor v letu 2010. Osrednja škoda naj bi bila še vedno prekinitev poslovanja v primeru varnostnih vdorov, virusnih okužb ali delovanja druge zlonamerne programske kode. Zunanji napadi (večinoma DoS), zlorabe osebja znotraj delovnega časa in z uporabo službene strojne in programske opreme za različne druge aktivnosti ter včasih tudi varnostne nadgradnje same lahko tudi predstavljajo varnostno grožnjo omrežjem.

Že sam odziv institucije ali podjetja na kibernetski napad ali zlorabo se odrazi v stroških dela zaposlenih, ki se ukvarjajo z odpravo in/ali ponovno vzpostavitvijo delovanja omrežja ali sistema. Včasih je za evidentiranje (recimo internih zlorab) in dokazovanje zlonamernih dejanj ter kasnejše disciplinske postopke potrebno daljše obdobje raziskovanja in beleženja kršitev, v primerih neželenih sistemskih izpadov pa daljši napor za vzpostavitev delovanja in vzpostavljanja novih sistemskih procesov kot preprečevanje ponovnega sistemskega izpada.

Vdor v sistem ima lahko neposredne posledice, kot izgubo sredstev za poslovanje, razkritje zasebnih podatkov in posledične kazni regulatorjev ali pa povračila za nastalo škodo strankam. Direktni stroški nastajajo pri ponovni vzpostavitvi sistema na prvotno raven. Stroški so predvsem v dodatnem delu in tudi povečanih IT stroških, hitrejši naknadni nadgradnji programske ali strojne opreme. Drug sklop direktnih stroškov nastane zaradi prekinitve poslovanja, pokaže se lahko kot izpad prihodka oz. znižana produktivnost zaradi ukvarjanja kadra z incidentom. Izguba v prodaji je lahko le kratkoročna, lahko pa je izguba stranke tudi dolgoročna, če jo prevzame konkurenca. Pomemben segment je tudi izguba vrednosti informacijskih sredstev, ukradenih ali razkritih, recimo informacije iz področja raziskav in razvoja v rokah konkurence so lahko za podjetje pogubni. Na tem področju je ključnega pomena tudi časovna občutljivost, saj so določeni podatki (gesla) lahko ogrožajoči samo v določenem obdobju (*Information Security Breaches Survey* 2010 in *Impact Assessment, Part 3* 2009, 30–33).

Posrednih izgub in stroškov je več in so večja po obsegu, zavzemajo pa lahko vse od izgube oz. kraje intelektualne lastnine[72] do kasnejšega izpada potencialnih prihodkov oz. kasnejših nepredvidenih stroškov. Posredni stroški so lahko vse od izgube ugleda oz. oškodovanja blagovne znamke, prebega strank, finančni trgi lahko povečajo strošek zadolževanja, zavarovalnice strošek zavarovanja, možni so tudi tožbeni zahtevki proti napadeni stranki v primeru različnih razkritij. Napad na posamično

[72] Čedalje pogostejša je t. i. gospodarsko vohunjenje, seveda predvsem prek uporabe IKT, saj je s široko razširjenostjo osebnih (prenosnih) računalnikov, podatkovnih nosilcev in uporabe interneta izpostavljenost teh podatkov večja kot kdajkoli. Po nekaterih podatkih (*Chinese hackers blamed for cyber attack wave*, 2010) naj bi bilo kar 50.000 podjetij dnevno izpostavljenim različnim tipom gospodarskega vohunjenja, število teh napadov pa naj bi se vsako leto podvojilo. Potencialni stroški za gospodarstvo zaradi piratstva, vohunjenja, sabotiranja in izsiljevanja naj bi tako že presegali milijardo britanskih funtov.

podjetje ali institucijo ima lahko vpliv tudi na z njim povezane subjekte, tako je recimo kibernetski napad na finančno institucijo posledično lahko problematičen za kreditne kartice njenih strank, v primeru napada na internetnega ponudnika pa stabilnost povezave njegovih strank v splet. Ta vidik je prav zaradi povezanosti akterjev izrednega pomena tudi pri oblikovanju politike na področju CIIP. Raziskave ocenjujejo, da skupni stroški lahko presežejo več milijard britanskih funtov letno (*Information Security Breaches Survey* 2010 in *Impact Assessment – Part 3*, 2009, 30–33).

Tabela 4.2: Okvirni stroški organizacije ob incidentu

	manjše organizacije (do 250 zaposlenih)	**večje organizacije** (nad 250 zaposlenih)
Prekinitev poslovanja	£15.000–£30.000 2–4 delovne dni	£200.000–£380.000 2–5 delovnih dni
Čas porabljen za odziv na incident	£600–£1.500 2–4 delovne dni	£6.000–£12.000 2–5 delovnih dni
Neposredni stroški odgovora na incident	£4.000–£7.000	£25.000–£40.000
Neposredni finančni stroški/izguba	£3.000–£5.000	£25.000–£40.000
Posredni finančni stroški/izguba	£5.000–£10.000	£15.000–£20.000
Škoda povzročena ugledu organizacije	£100–£1.000	£15.000–£200.000
Povprečni skupni stroški največjega incidenta	**£27.500–£55.000**	**£280.000–£690.000**
(primerljivi podatki za 2008)	£10.000–£20.000	£90.000–£170.000

Vir: *Information Security Breaches Survey* 2010

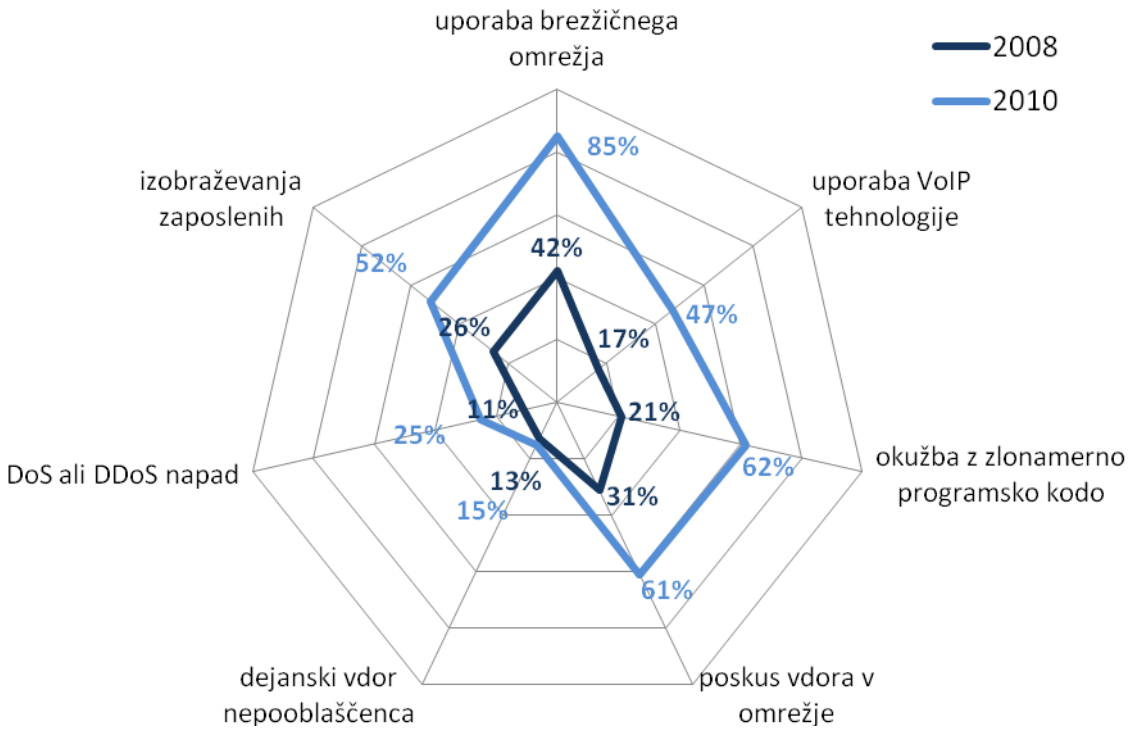
4.2.2 Spremenjeno poslovno okolje in nove tehnologije

Pomenljive so tudi ugotovitve organizacije Infosecurity Europe (*Information Security Breaches Survey* 2010), kjer v svoji raziskavi med zasebnimi podjetji po svetu ugotavljajo, da je spremenjeno poslovno okolje in implementacija različnih novejših tehnologij (WiFi, VoIP, VPN, FTTH[73], oddaljeni dostopi itd.) neposredno vplivala na odvisnost podjetij od povezave v splet, vzporedno z rastjo produktivnosti in večje učinkovitosti[74]. Različna socialna omrežja in gostovanje storitev programske opreme na zunanjih strežnikih, je uporabo interneta premaknilo dlje od le pošiljanja elektronske pošte in uporabe spletnih strani. Žal pa kljub povečanem zavedanju vodilnih kadrov v podjetjih glede kibernetske varnosti lastnih omrežij, varnostne mehanizmi še vedno zaostajajo za uporabo novejših tehnologij, ki odpirajo nova področja ranljivosti. Ta nova področja pa so sfera delovanja spletnih kriminalcev, katerih dejanja postajajo vse bolj vsakdanja praksa. Na shemi 4.5 je prikazan porast uporabe novejših tehnologij in vlaganj v znanje kadrov, posledica razvoja IKT-panoge v gospodarstvu, kot primerjava med letoma 2008 in 2010 ter hkrati porast različnih tipov poskusov vdorov in ogrožanja kibernetske varnosti kot posledica večje vpetosti podjetij v internet. Porast kriminalitete na posameznem segmentu je tudi več kot 100%, temu primerno pa naraščajo tudi stroški, posredni in neposredni. O tem pa več v enem od naslednjih poglavij.

[73] Naj kot zanimivost navedem, da je Slovenija po podatkih OECD-ja ena od držav (tudi Švedska in Portugalska), kjer je relativna penetracija tehnologije optike do doma (FTTH) najvišja (*Fibre Access* 2011).

[74] Podatki v raziskavah (*Growing Business Dependence on the Internet* 2007) kažejo, da naj bi uporaba interneta samo gospodarstvu ZDA v letu 2010 prihranila kar 500 milijard $ (izboljšano komuniciranje med podjetji, med podjetji in strankami, nižji stroški iskanja najugodnejših dobaviteljev, povečana učinkovitost, nižji stroški inventarja, povečana tekmovalnost zaradi dostopnosti podatkov, znižani stroški uporabniške podpore, nižji stroški osebja, nižji stroški računovodstva in financ itd.), prihodki pa naj bi bili zaradi interneta povečani za kar 1,5 bilijona $ (10^{12}).

Shema 4.5: Porast uporabe novih tehnologij in kibernetskih incidentov



Prirejeno po *Information Security Breaches Survey* 2011.

Druga raziskava (*Growing Business Dependence on the Internet* 2007) o poslovni odvisnosti podjetij od delovanja interneta, ugotavlja, da bi večja prekinitev dostopa do interneta posredno ali neposredno vplivala prav na vsako podjetje znotraj ZDA. Zato bi v takih situacijah prišlo do enormnih obremenitev drugih segmentov (potreba po gotovini, povečano povpraševanje po začasnih delavcih, povečana potreba po gorivu, nedostopnost alternativnih tehnologij, povečano povpraševanje po papirju in drugih pisarniških potrebščinah, večje potrebe po klasičnih telefonskih storitvah, prezasedeni transportni sistemi itd.), ker bi podjetja želela internetne poti nadomestiti s konvencionalnimi, kjer bi to bilo mogoče. Ublažitev posledic kibernetskega napada oz. prekinitve delovanja storitev je tako odvisno tudi od odpornosti ostalih »neinternetnih« segmentov gospodarstva na povečano povpraševanje po njihovih storitvah. Tipične poslovne funkcije, ki so v odvisne od delovanja interneta zavzemajo že velik del poslovanja, recimo oddaljeni klicni centri, potovalne storitve, internetne

prodajne točke, večkanalno komuniciranje s stranko, plačilno administriranje, ugodnosti zaposlenih, korporativni prenos sredstev, operativni nadzor električnega napajanja podjetja, državno in mednarodno sodelovanje, varnostno kopiranje in shranjevanje dokumentov, glasovno in podatkovno komuniciranje, računovodske storitve, upravljanje s stavbami. Težko si je predstavljati enakovredno produktivnost teh segmentov brez interneta, zato je tudi za poslovni svet le-ta danes ključen.

4.2.3 Izpostavljenost na različnih ravneh

Različni akterji imajo lahko različne stroške (*Impact Assessment – Part 3*, 2009, 68–80) z različnimi kibernetskimi napadi, prav tako niso vsi enako dovzetni za posamezno grožnjo, vsekakor pa lahko ogroženost enega od prepletenih akterjev vpliva tudi na stroške drugih, le posredno vpletenih. Naj povzamem le nekatere bistvene:

- **posamični potrošniki** (neposredna škoda v programski ali strojni opremi, namestitev novega operacijskega sistema, odstranjevanje virusov ali vohunskega programja, finančna škoda zaradi kraje podatkov, kraje identitete ali druge računalniške kriminalitete),
- **ponudniki hrbteničnih in internetnih storitev**[75] (neposredna in posredna škoda, ki nastane ob zlonamernem programju, zaradi stroškov podpore uporabnikom in odprave zlorab v mreži; stroški še narastejo, če ima ISP v svoji mreži t. i. uporabnike s črnih list[76], zaradi katerih drugi ponudniki blokirajo promet iz teh naslovov; raven potencialnih stroškov je odvisna tudi od zasedenosti omrežja, saj je zasedeno omrežje bolj izpostavljeno tveganju po prekomernem prometu zaradi zlonamernega programja, s tem pa tudi potencialni stroški za nove usmerjevalnike in prenosne kapacitete; potencialni strošek ponudnikov je tudi v preventivnih ukrepih, kot so filtri dohodnega prometa ali tehnologija za karanteno okuženih posameznikov ter morebitna škoda na ugledu, ki se lahko kasneje odrazi v odlivu uporabnikov),

[75] Angl. BSP – ***B**ackbone **S**ervice **P**rovider*, angl. ISP – ***I**nternet **S**ervice **P**rovider*
[76] Gre za črne liste (angl. *blacklisted*) oz. sezname uporabnikov, ki jim je onemogočena določena akcija v medmrežju.

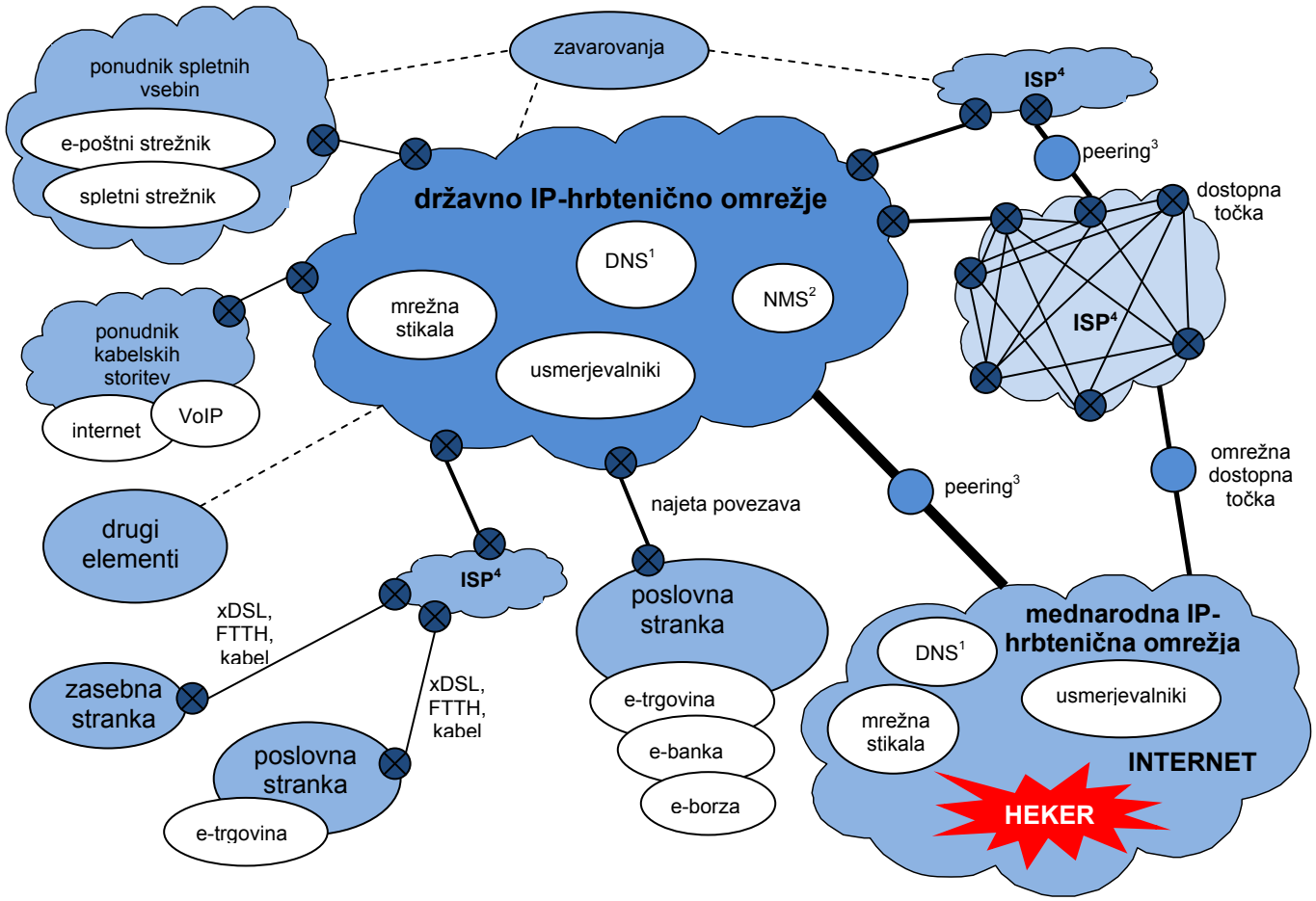
- **ponudniki spletnih storitev** (izpad delovanja interneta se pri njih odrazi kot potencialen izpad prihodkov iz naslova obračunanega prometa ali prostora strankam; odvisno od tipa strank rezidenčni ali poslovni so ponudniki spletnih storitev različno ogroženi, saj je ponudnik rezidenčnih storitev manj izpostavljen v primeru izpada v primerjavi s ponudnikom za poslovne stranke, kjer je pogost tudi t. i. dogovor o zagotovljeni ravni storitev[77]; ogroženost je podobna ISP/BSP),
- **ponudniki programske opreme** (zlonamerno programje ne vpliva neposredno na njih, vendar zaradi zlorabljanja programskih pomanjkljivosti in varnostnih lukenj v njihovih produktih škodo občutijo uporabniku njihovih storitev, kar se že kratkoročno odrazi v ugledu ponudnikov; morebiten dodaten razvoj in popravljanje teh ranljivosti pa se odrazi v neposrednih stroških oz. potencialni izgubi prihodkov zaradi zamujenega trženja produkta na trgu),
- **registrarji** (stroški nastanejo, ko je določena domena povezana z zlonamernim programjem, posledično pa se povečajo obvestila o zlorabah, na katere mora ustrezno usposobljeno osebje odreagirati, morebitne neupravičene ukinitve ali zamrznitve domen pa se lahko odrazijo tudi v kasnejših sodnih sporih in s tem povezanimi stroški),
- **internetna podjetja** (za zaščito pred DDoS napadi in drugimi oblikami kibernetske kriminalitete so potrebna sredstva ali storitve; ta segment je najbolj izpostavljen kraji potrošniških zasebnih podatkov zbranih v njihovih bazah, nezadovoljstvo uporabnika se odrazi v nezadovoljstvu s storitvijo, kar vpliva na poslovanje, ugled, v določenih primerih pa lahko uporabnik tudi zahteva odškodnino; v primeru izpada delovanja se pri internetnih trgovinah to odrazi tudi v izpadu prihodkov, saj potrošnik uporabi konkurenčnega ponudnika; pri ponudnikih z večjim številom zaposlenih in regijsko razpršenimi poslovnimi enotami so tako nastali stroški še večji iz naslova znižane produktivnosti v času izpada in s tem znižanih prihodkih),
- **zavarovalnice, banke, druga podjetja** (njihovi stroški nastajajo predvsem pri krnitvi ugleda, povečanem nezaupanju v poslovne poti in potencialnih odškodninskih zahtevkih),

[77] Angl. SLA – ***S**ervice **L**evel **A**greement*

- **vlade** (zanašanje modernih družb na delujočo IKT ima lahko resne posledice v eroziji zaupanja prebivalstva v ustrezno integriteto in tajnost pri prenosu informacij prek napadenih omrežij v primeru nedelovanja oz. omejenega delovanja le-teh v primeru napada z zlonamernim programjem; zaradi čedalje bolj razširjenih e-poti poslovanja z državo bi bil ta segment najprej ogrožen, potencial za zlorabo ogroženih ali razkritih podatkov pa je zaradi obsega in zaupnih podatkov v podatkovnih bazah precejšen),
- **ključna informacijska omrežja** (povezanost ključne infrastrukture v svet prek ključne informacijske infrastrukture je izpostavljena istim tipom groženj kot ostali uporabniki interneta, potencialne posledice pa so v tem primeru največje, saj lahko zaradi kibernetskih groženj, celotna omrežja na katerih temelji naša družba postanejo nedostopna oz. začasno neuporabna, ker bi se odrazilo v praktično nemerljivih stroških; čeprav odgovorni neradi razkrivajo podrobnosti napadov na ključno informacijsko infrastrukturo je očitno, da je **varovanje ključne informacijske infrastrukture, ki podpira celotno ključno infrastrukturo postalo izjemno pomembno**; kljub le nekaj znanim incidentom je sedaj jasno, da so ta omrežja tudi ranljiva za kibernetske napade) in
- **makroekonomske posledice** (stroški na tej ravni so bolj kot ne stvar špekulacij, saj računalniška in druga informacijska oprema praviloma nima neposrednega prispevka k proizvodnji dobrin in storitev na državni ravni, ni pa povsem jasno, v kolikšni meri bi drugi akterji proizvodnje, zaradi nedelovanja te opreme, postali neproduktivni; zato je najboljša determinanta obsega škode prav trajanje incidenta, škoda pa bi se v tem primeru merila kar v % BDP).

Prepletanje nekaterih zgoraj omenjenih akterjev je prikazano na shemi 4.6. Izpostaviti pa velja še eno dimenzijo ogrožanja, in sicer vzdržnost trenutnega poslovnega modela interneta. Internetne storitve so zelo ugodne zaradi relativno fiksnih stroškov in hitro rastočega obsega uporabnikov, težava pa nastaja pri ponudnikih tranzitnega prometa, ki kljub rastočim stroškom in potrebnim investicijam za vzdrževanje in nadgradnje ne generirajo dovolj prihodkov, kar bo verjetno zmanjšalo njihovo število (*Inter-X: Resilience of the Internet Interconnection Ecosystem* 2011, 9). Zmanjšanje števila ponudnikov, pa se hitro lahko odrazi v spremenjeni kakovosti ali cenovni dostopnosti storitve.

Shema 4.6: Povezanost akterjev internetnega modela



[1] angl. ***D**omain **N**ame **S**erver* – strežnik domenskih imen

[2] angl. ***N**etwork **M**anagement **S**ystem* – strojna in programska oprema za nadzor omrežja

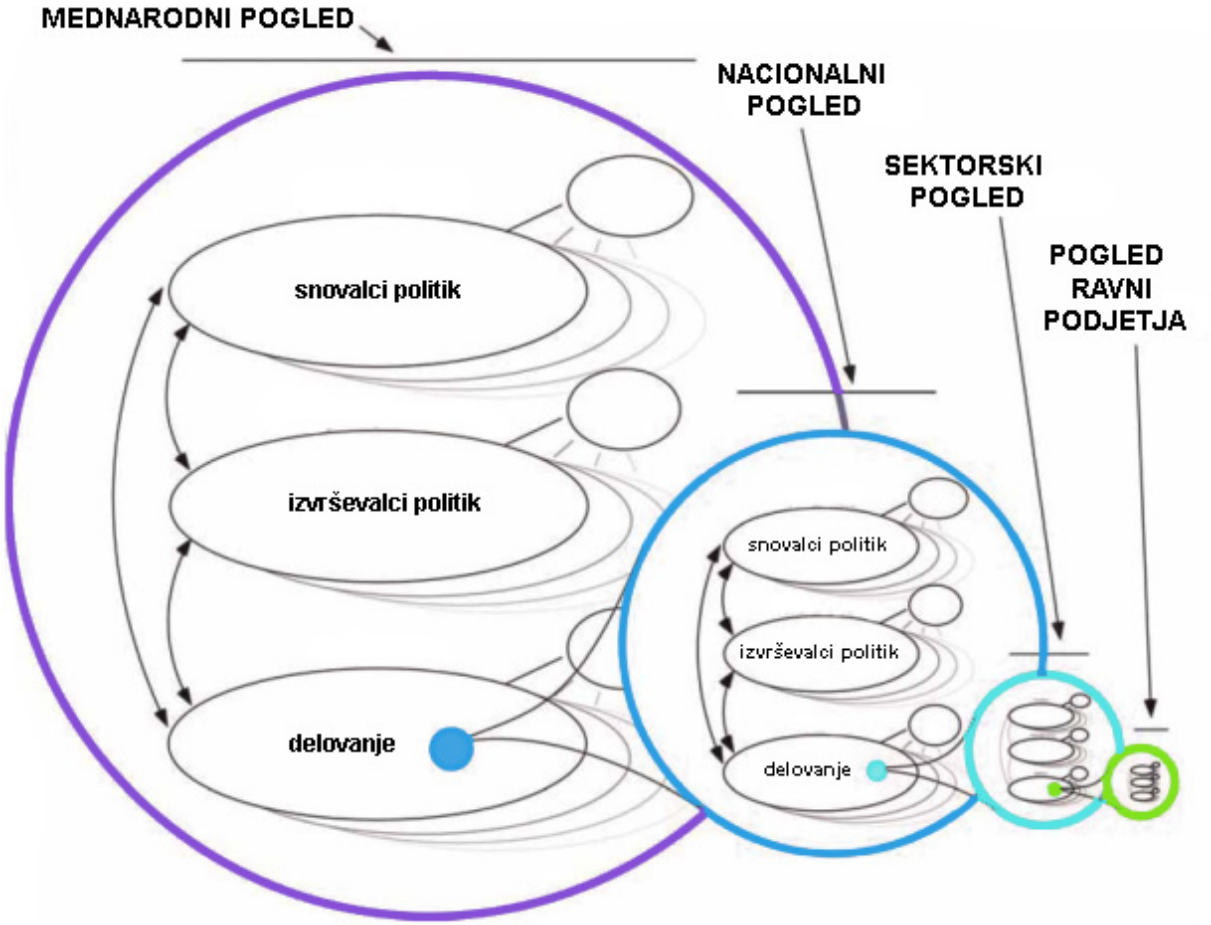
[3] enakovredno medsebojno povezovanje [4] angl. ***I**nternet **S**ervice **P**rovider*, ponudnik internetnih storitev

Prirejeno po *An Economic Damage Model for Large-Scale Internet Attacks*, 2004.

Podobno soodvisnost akterjev na področju kibernetske varnosti KII so ugotovili tudi avtorji (Brechbühl in drugi 2010, 84) v raziskavi o razvoju zakonodaje na področju kibernetske varnosti omrežij. Temeljna ugotovitev raziskave je vključenost vseh in vsakega v ogroženost pred kibernetskimi grožnjami, zato so ključne aktivnosti prav na vseh ravneh, tudi tistih, ki presegajo zakonodajo. Avtorji ugotavljajo, da kibernetske varnosti ni mogoče zagotoviti le na znanstvenoraziskovalni ravni ali ravni državnih varnostnih strokovnjakov ali ravni ponudnikov internetnih storitev. Večjo vlogo ima povsem heterogena skupina deležnikov, kjer vsak predstavlja unikatna

znanja in potrebe na svojem področju in lahko usklajeno ali neusklajeno ter formalno ali neformalno močno vplivajo na skupno raven varnostnih vlog v omrežju, ki kot rezultanta uspešno ščitijo interes vseh. Tovrstno omrežje deležnikov je nemogoče opredeljevati v okviru kibernetskih varnostnih politik. Izjemna prepletenost in razdrobljenost deležnikov in s tem poteka informacij ima podobne elemente na različnih ravneh. Bistvena pa je ugotovitev, da je za kibernetsko varnost kolektivni napor ključen ter da ima vsaka raven odgovornost do vseh drugih ravni. Prepletenost in podobni načini komunikacije na različnih ravneh so prikazani na shemi 4.7.

Shema 4.7: Prepletenost poteka informacij med različnimi ravnmi

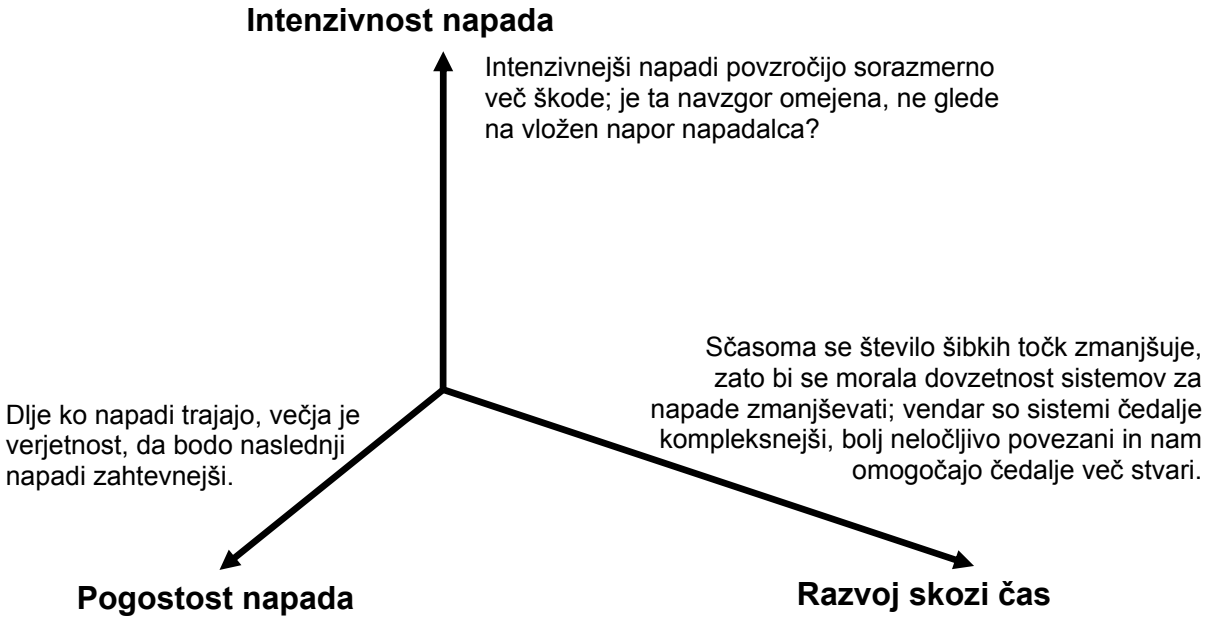


Prirejeno po Brechbühl in drugi 2010, 87.

4.2.4 Vpliv trajanja in intenzivnosti napada

Zanimiva so razmerja, ki so jih odkrili raziskovalci RAND-a (Libicki 2009, 58–60) ob preučevanju uspešnosti povračilnih ukrepov proti kibernetskim napadom in predpostavljajo, da so najuspešnejši tisti napadi, ki so izredno intenzivni ter trajajo kratek čas. Daljše trajanje napada zaradi aktivne obrambe in krpanja varnostnih lukenj ima tako manj možnosti za uspeh kot kratki in dobro načrtovani napadi. Prav tako ponovljeni napadi istega tipa nikakor ne dosegajo podobnih učinkov kot ob prvem napadu. Zmanjševanje potencialnih varnostnih lukenj pri tarči povzroči zahtevnejše iskanje novih varnostnih lukenj kar zahteva čas, s tem pa zaščita sistemov pridobi na pomembnem elementu varnosti, časovni okvir ogrožanja. Tak zamik pri izvedbi napada oz. ponavljanje identičnih napadov bo verjetno imel manj škodljive posledice in bo za izvedbo zahteval bolj rizične akcije ter bil uspešen le v ožjem segmentu okoliščin. Napačna aktivnost oz. neaktivnost sistemskih administratorjev ima lahko tudi ključen vpliv na varnost, saj z omejenim izborom znanj in orodij za preprečevanje napadov napadalec pridobiva tehnološko prednost in si širi polje možnih dejanj. Spodnja shema 4.8 tako prikazuje, da je učinkovitost kibernetskih napadov trirazsežna; učinkovitost napada odvisna od pogostosti napadov je drugačna od učinkovitosti napadov zaradi njihove intenzivnosti in učinkovitost napada v odvisnosti od razvoja skozi čas je drugačna od prvih dveh.

Shema 4.8: Tri dimenzije učinkovitosti kibernetskih napadov



Vir: Libicki 2009, 60.

4.2.5 Vloga zanesljivosti omrežij

V okviru programa CERT[78] so raziskovalci že pred leti prišli do spoznanja, da je zanesljivost omrežij ključna. Računalniške sisteme v temelju definira pet lastnosti: funkcionalnost, uporabnost, učinek, cena in zanesljivost. Zanesljivost sistema je upravičeno zaupanje v sposobnost sistema, da izvede storitev, torej je njen pomen pri varnosti KII bistven.

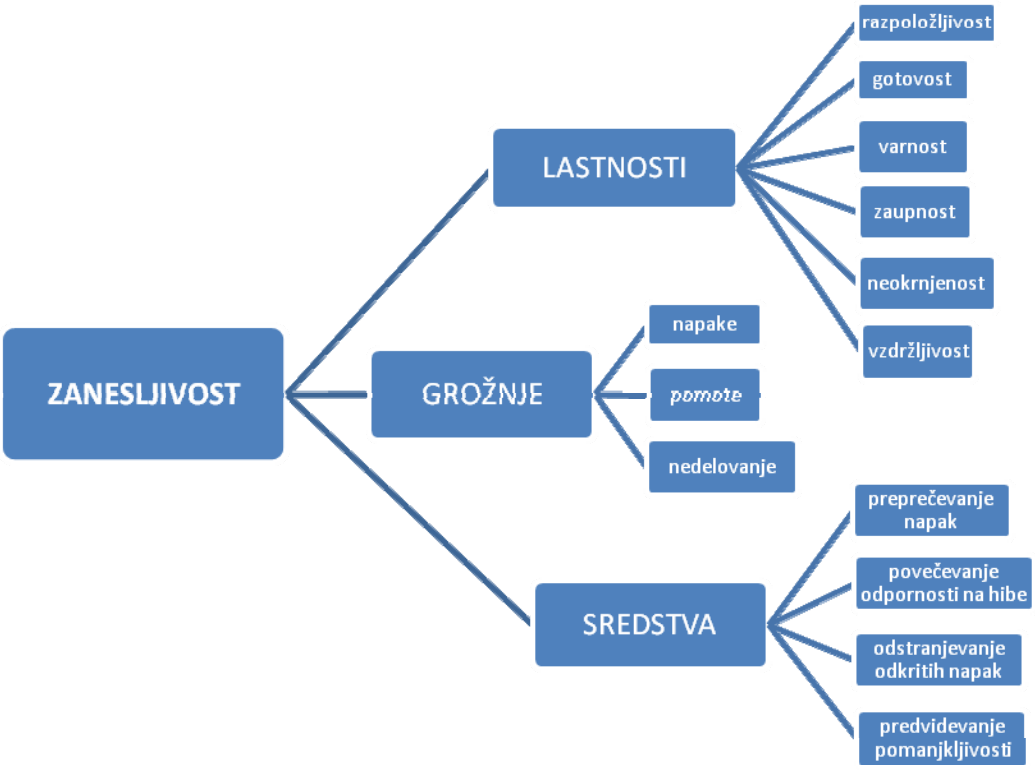
Pojem zanesljivost sestoji iz treh povezanih stebrov:

[78] Program CERT je del Inštituta za razvoj programske opreme na univerzi Carnegie Mellon v Pennsylvaniji, ZDA. Ukvarjajo se predvsem z varnostnimi pomanjkljivostmi interneta, znanstveno preučujejo dolgoročne spremembe v omrežnih sistemi in razvijajo postopke za povečevanje internetne varnosti. Uradna spletna stran: http://www.cert.org/ (9. oktober 2011).

- **lastnosti**: zanesljiv sistem naj bi vključeval lastnosti kot so razpoložljivost, gotovost, varnost, zaupnost, neokrnjenost in vzdržljivost;
- **ogrožanja**: sistem je v najširšem smislu izpostavljen trem tipom ogrožanj, in sicer napakam, pomotam in nedelovanju;
- **sredstva:** zanesljivost sistema pa je mogoče zagotavljati s preprečevanjem napak, povečevanje odpornosti na hibe, odstranjevanjem odkritih napak in predvidevanjem pomanjkljivosti (Avižienis, Laprie, Randell 2000, 1–6).

Vsako od področij so avtorji še podrobneje preučili, vendar je za mojo nalogo ključna sama ugotovitev pomembnosti zanesljivosti omrežij.

Shema 4.9: Zanesljivost računalniških omrežij



Prirejeno po Avižienis, Laprie, Randell 2000, 1.

4.3 Pogostejše pojavne oblike kibernetskih groženj

V celotnem poglavju, kakor tudi v celi nalogi, bom poskušal kar se da veliko uporabljati slovenske prevode za kibernetske grožnje in druge izraze za tehnologijo. Uporabljam slovenske prevode kot jih predlaga spletni terminološki slovar informacijske tehnologije (islovar, 2011).

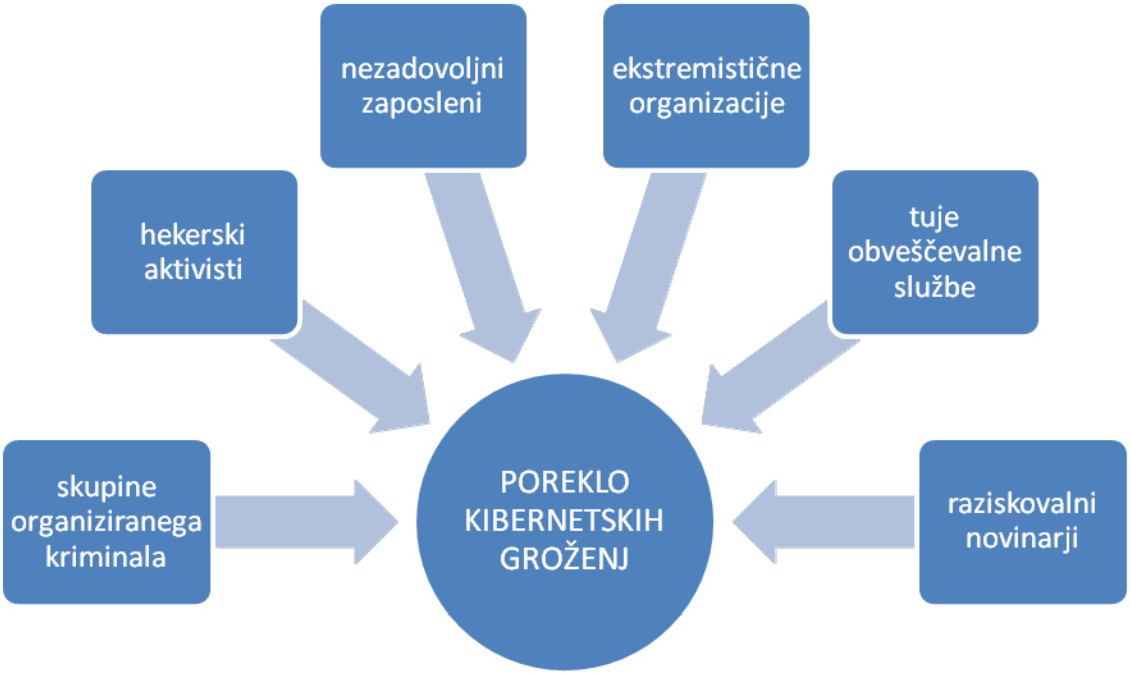
Preden omenim pogostejše in aktualne varnostne grožnje je smiselno prepoznati temeljne elemente in posebnosti kibernetskih groženj, kar vpliva na zahtevnost odkrivanja takih napadov, zahtevnost nadzorovanja in analiziranja ter zahtevnost odzivanja na njih. Dunn (2005, 11) tako opredeli pet temeljnih značilnosti kibernetskih groženj.

- **Anonimnost akterjev:** težavnost identifikacije akterjev je še posebno zahtevna na področju, kjer je ohranjanje anonimnosti relativno preprosto, še posebej zaradi časovnega zamika med akcijo, ki jo zlonamernež izvede, med dejansko spremembo ali vdorom ter med posledicami vdora. Nadalje otežuje odkrivanje storilcev razvoj sofisticiranih računalniških tehnologij med širšo internetno populacijo.
- **Odsotnost mej:** zlonamerni računalniški napadi niso omejeni s političnimi ali geografskimi mejami, napadi lahko izvirajo od koderkoli in iz več lokacij hkrati. Sledenje (načrtno) zavajajočim sledem napadov je potratno s časom in resursi.
- **Hitrost razvoja:** IKT se razvija izredno hitro, časovno okno med odkrito pomanjkljivostjo in razvitimi orodji za izkoriščanje le-te je vedno krajše.
- **Nizka cena orodij:** tehnologija uporabljena v tovrstnih napadih je (lahko) preprosta za uporabo, cenovno ugodna in široko dostopna. Orodja in napadalne tehnike so prosto dostopne prek spleta, prav tako orodja za anonimiziranje in kriptiranje.
- **Avtomatske metode:** čedalje več napadov je avtomatiziranih in sofisticiranih ter se odrazijo v večji škodi posameznega napada.

Ko pogledamo smer, v katero se grožnje IKT in posameznikom pri uporabi le-te razvijajo, so strokovnjaki[79] s področja kibernetske varnosti iz javnega in zasebnega sektorja ter raziskovalne sfere prepoznali nekaj glavnih trendov, in sicer: zlonamerno programje, prek medmrežja povezani avtomatizirani programi, spletno vojskovanje, grožnje VoIP-ju in mobilnim napravam ter nasploh razvijajoča se panoga spletnega kriminala.

Mednarodna telekomunikacijska zveza (ITU National Cybersecurity Strategy Guide 2011, 16) kot glavne akterje kibernetskih groženj prepoznava predvsem naslednje akterje: tuje obveščevalne službe, nezadovoljne ali odpuščene nekdanje zaposlene delavce, raziskovalne novinarje, ekstremistične organizacije, hekerske aktiviste (t. i. *hacktivist*) ter skupine organiziranega kriminala. Prikazani so na shemi 4.10.

Shema 4.10: Viri običajnih kibernetskih groženj



Prirejeno po ITU National Cybersecurity Strategy Guide 2011, 16.

[79] V tem primeru se navezujem na srečanje strokovnjakov v okviru Gruzijskega centra za informacijsko varnost (GTISC).

4.3.1 Zlonamerno programje

Zlonamerno programje[80] obsega izredno širok spekter programskih kod namenjenih zlonamernim dejanjem. Programska koda avtorju ali napadalcu omogoča škodljivo vplivati na delovanje informacijskega sistema, vključuje pa vse oblike programske kode, kot so virusi, črvi, trojanski konji, vohunsko programje itd.

Stare, poznane metode množičnega dostopa do uporabnika so postale preveč preproste in uporabniki so se jih naučili izogibati. Zato pisci zlonamernih kod uporabljajo čedalje bolj prefinjene metode socialnega inženiringa, s čimer zlonamerno programje zakamuflirajo oz. zakrinkajo v recimo povsem legitimno sporočilo med uporabniki. Okužba se navadno zgodi prek obiska strani ali sprejetja sporočila[81], ki naj bi mu ga poslal prijatelj, v njem pa je navedena povezava, kjer naj bi si ogledal zanimiv video posnetek, pred tem pa naj bi bilo potrebno namestiti še najnovejšo verzijo znanega predvajalnika ali neko drugo aplikacijo. Seveda ta aplikacija vključuje spretno zakrinkano zlonamerno programsko kodo, s pomočjo katere avtor te kode lahko recimo prevzame nadzor nad računalnikom.

Spletni kriminalci tako uporabljajo lokalne in poosebljene napade[82], ker s tem dosegajo večjo uspešnost, najbolj priljubljena pa so družbena omrežja, ki bodo tudi v prihodnje osrednji mehanizmi dostopa do uporabnikov. V preteklih letih je bila rast števila zlonamerne programske opreme skokovita, za 2011 in 2012 pa se napoveduje umiritev te rasti. Razlog za tako hitro širjenje v preteklosti je tudi v slabem odzivu korporativnih institucij pri pripravi popravkov varnostnih lukenj v programih, vendar se tudi na tem področju stanje izboljšuje, saj veliko izdajateljev programske opreme priporoča sprotno in avtomatizirano posodabljanje, ki zmanjšuje okno priložnosti za zlonamerne akterje (Emerging Cyber Threats Report 2009; 2).

---

[80] Angl. ***Mal**icious Soft**ware***, MALWARE

[81] Točno to se je zgodilo v 2010 tudi s slovenskim izvorom (*Analiza slovenskega Facebook botneta*, 2011).

[82] Do podobnih ugotovitev so prišli tudi razvijalci druge zaščitne programske opreme, saj skoraj vsi pričakujejo porast in osredotočanje na področje poosebljenih napadov (*Leto 2011 v znamenju hekerjev in kibernetskih vojn* 2011).

Naprednejša oblika zlonamernih kod, ki se uporablja za napade na večje sisteme in institucije, je bila pred kratkim odkrita za napad na iranske jedrske komplekse. Črv Stuxnet (Falliere, 2010) je tako prek okužbe operacijskega sistema Windows dostopal do industrijskih nadzornih in krmilnih sistemov, ki upravljajo s tehnološkimi industrijskimi procesi prek računalnika. Ti sistemi sestojijo iz posebnih programskih logični krmilnikov, ki jih lahko upravlja Windows operacijski sistem. Posebnost črva Stuxnet je bila, da lahko prikrito deluje in omogoča dostop do računalniškega sistema in uporabo skrbniških, administratorskih pravic ter da vrinjeno kodo sistematično skriva pred dejanskim skrbnikom. Z uporabo črva Stuxnet so tako programski logični krmilniki navidezno normalno upravljali s sistemom, dokler ni zlonamernež povečal pritiska v cevovodih prek zmogljivosti, kar se je na koncu odrazilo v eksploziji. To je dober primer kako lahko s kibernetskimi orodji povzročimo fizično škodo.

4.3.2 Napredne trajne grožnje

Znotraj tovrstnega zlonamernega programja, v zadnjem času osrednjo vlogo dobivajo t. i. napredne trajne grožnje[83], ki za doseganje uspešnosti zahtevajo visoko stopnjo neopaznosti in daljše obdobje delovanja. Cilji napada tako pogosto presegajo izključno materialno korist in imajo pogosto poslovne ali politične cilje. Sistem pa ostane ogrožen in izpostavljen tudi po izvedenem oškodovanju, saj ni nujno, da se tovrstna grožnja razkrije. Tovrstne grožnje opredeljujemo kot napredne, predvsem zaradi uporabe različnih naprednih orodij in zaradi različnih metodologij napada, napredna je torej kombinacija uporabljenih orodij. Trajna lastnost tovrstnih groženj je predvsem v odsotnosti iskanja kratkoročnih učinkov, predvsem finančnih, zato se napadalci poslužujejo počasnih in postopnih pristopov k razkrivanju in osvajanju tarče, tako da napad praviloma nima neposrednih učinkov, ki bi opozarjali napadenega na nenavadno dogajanje. Beseda grožnja v tej besedni zvezi pa se nanaša predvsem na dejstvo, da tovrstni napadi niso posledica neke pomanjkljivosti ali programske napake, temveč so posledica usklajenega delovanja posameznikov ali organizacij, ki so usposobljeni, motivirani, dobro organizirani in financirani ter

[83] Angl. ***A**dvanced **P**ersistent **T**hreat* (APT)

lahko sistematično obdelujejo tarčo na več področjih in skozi daljše obdobje. Napredne trajne grožnje uporabljajo in kombinirajo vse možne pristope med njimi predvsem:

- okužbe s prek interneta dostopnimi programi (priponke elektronske pošte, deljenje datotek, piratska programska oprema in generatorji kod, modifikacije preusmeritev povezav itd.),
- okužbe z zlonamernim programjem prek fizičnega nosilca (okuženi USB ključi ali drugi podatkovni nosilci) in
- izkoriščanje pomanjkljivosti od zunaj (profesionalno vdiranje, izkoriščanje programskih pomanjkljivosti, izkoriščanje gostovanja na kolokacijah, izkoriščanje ponudnika, ki dobavlja storitve v oblaku, vdori prek WiFi-omrežij in vdori prek pametnih telefonov).

Pogosta je tudi uporaba:

- notranje grožnje v korist napadalca, kjer zlonamerneži izkoristijo morebitnega nezadovoljnega zaposlenega, zlonamernega pogodbenika, dvonamensko programsko opremo ali socialni inženiring pri dostopu do podatkov ter
- zaupanja vrednih povezav, ki kljub ogroženi tajnosti in zaupnosti še naprej funkcionirajo; tovrstne grožnje so predvsem uporaba prisvojenih podatkov za dostop do virtualne privatne mreže[84], zloraba povezav med podjetji (B2B) ali vdor v partnerjeve sisteme (*Advanced Persistent Threat* 2011).

Mnogi strokovnjaki IT-podjetij (CISCO, McAfee, Symantec itd.) so mnenja, da so napredne trajne grožnje eden od osrednjih izzivov pri varovanju omrežij in večjih korporacij pred kibernetskimi napadi, ker za zaščito pred njimi ne obstaja nobena programska oprema, ki bi sistematično odpravljala vzroke za tovrstne napade. Ključno pri zaščiti pred tovrstnimi napadi je tako vzpostavitev kombinacije različnih orodij spremljanja, nadziranja, evidentiranja in preučevanja podatkovnega prometa, ki poteka skozi omrežje nadzorovanega subjekta, vzpostavitev tovrstne zaščite pa je izziv tudi za največje korporacije[85] (*Cisco 2Q11 Global Threat Report* 2011;

---

[84] Angl . **V**irtual **P**rivate **N**etwork (VPN)

[85] Omenim naj le *Operacijo Aurora* kot je bil poimenovan izredno prefinjen napad na Google v začetku 2010, kjer so napadalci poskušali pridobiti Googlovo intelektualno lastnino - izvorno kodo. Celo

Advanced Persistent Threats 2011; *Advanced Persistent Threats: A Symantec Perspective* 2011).

4.3.3 Porazdeljena ohromitev storitve

Porazdeljena ohromitev storitve (DDoS[86]) ali ohromitev storitve (DoS[87]) je za mnoge poznavalce trenutno najpogostejša operativno-varnostna problematika. Tovrsten napad ima samo en cilj, in sicer onesposobiti ali ohromiti storitev za njemu namenjene uporabnike. Načini, motivi in tarče se lahko razlikujejo, vendar temelj tovrstnega napada ostaja preprečitev internetne strani ali storitve k izpolnjevanju njene osrednje vloge ali namena. Tovrstna preprečite ali zmanjšanje učinkovitosti se doseže prek ogromnih količin podatkov in prometa, ki naslavljajo specifično storitev ali stran. Tovrstni napadi so pogosti predvsem iz naslova pridobivanja ekonomskih prednosti v zasebnem sektorju z onemogočitvijo spletne strani ali storitve pri konkurenci ali vladnih ali organizacijskih storitev zaradi političnih ali ideoloških interesov (*Impact Assessment – Part 3* 2009, 58). Raziskava s tega področja (Christensen in drugi 2010, 78) je na podlagi podobnih izhodišč in odvisnosti KII od IKT prišla do ugotovitev, da bo uskladitev zakonodaje in tehnologij uporabljenih za tovrstne napade prvi korak pri boju zoper akterje. Seveda pa ta korak nikakor ni dovolj.

Za lažjo oceno razsežnosti in rasti obsega tovrstnih napadov se pogosto uporablja uporabljena pasovna širina pri takem napadu (kot bomo videli spodaj, to ni edina klasifikacija). Raziskovalci opažajo (*Wordwide Infrastructure Security Report* 2010, 5) da je obseg tovrstnih napadov med letoma 2005 in 2010 dosegel kar tisoč odstotno

---

Google sam je napade na njihovo korporacijsko mrežo označil za izredno napredne in kompleksne, saj jih niso odkrili po več kot 14 dni od prvotne okužbe in kraje informacij Tovrsten napad je bil precedenčen za podjetje v zasebnem sektorju (Google Hack Attack Was Ultra Sophisticated, New Details Show, 2010).

[86] Angl. ***D**istributed **D**enial **o**f **S**ervice*
[87] Angl. ***D**enial **o**f **S**ervice*

rast uporabljene pasovne širine. Tako so največji napadi v letu 2010 presegali sto gigabitov[88] pasovne širine na sekundo.

Ollman (2011, 1) tehnike ohromitev storitev (DoS) razdeli v dve kategoriji, aplikacijske in omrežne. Aplikacijske omejitve se nanašajo na izkoriščanje znanih logičnih omejitev ali napak pri posamezni programski opremi, ki se v primeru napada odrazijo v napaki ali neželeni spremembi podatkov. Omrežna kategorija napadov pa je bolj poznana in vključuje ranljivosti, pri katerih je izkoriščana omrežna oprema ali pa internetni protokoli za usmerjanje prometa za onemogočitev dostopanja do strani ali storitve.

Uporaba porazdeljenih napadov za ohromitev storitve (DDoS) je smiselna pri napadih na večje in bolj odzivne tarče. Tovrstne napade pa Ollman (2011, 2) razdeli na tri kategorije.

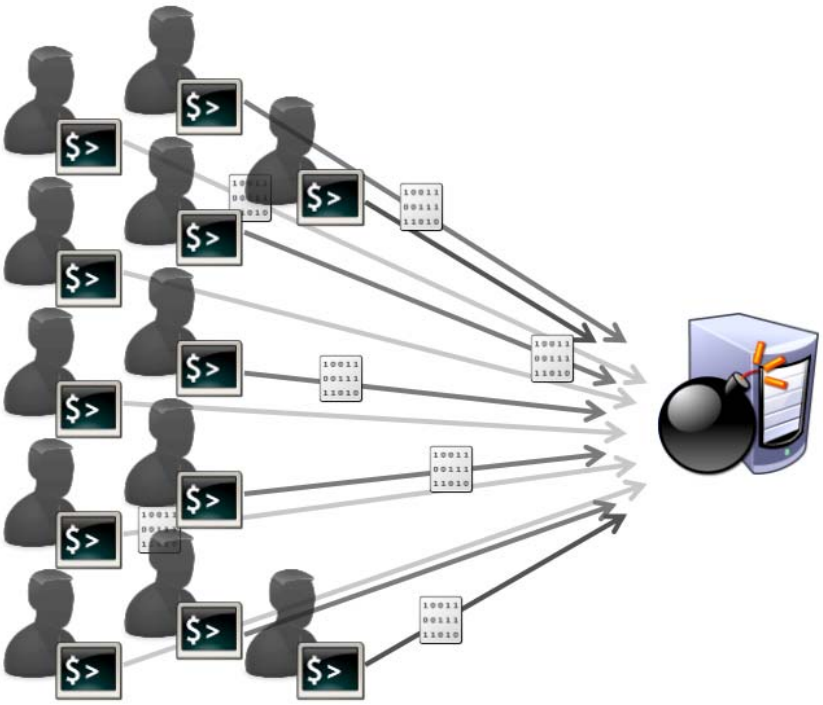
- **Porabo pasovne širine**, kjer udeleženci napada poskušajo poplaviti omrežje z več podatkovnega prometa, ko ga le-ta lahko prenese za učinkovito delovanje. Cilj takega preplavljanja s prometom je preprečiti legitimnemu prometu, da doseže cilj in prejme odgovor. To je temeljna in najpreprostejša oblika tovrstnega napada, ker zahteva samo preobremenitev podatkovne povezave tovrstnega sistema v internet.
- **Izčrpanje sistemskih zmogljivosti sistema**, je oblika napada pri kateri napadalci z nižjim obsegom pasovne širine poskušajo izčrpati sistemske zmogljivosti. Internetne storitve gostujejo na strežnikih s fizičnimi omejitvami sredstev namenjenih posamični storitvi, tako tak napad poskuša preseči te zmogljivosti in tako onemogočiti delovanje storitve. Primer take preobremenitve je odpiranje 500 sočasnih podatkovnih sej na strežniku, ki omogoča samo 500 sočasnih sej. Zaradi zasedenosti vseh razpoložljivih kapacitet, bi morebitna naslednja seja (legitimni uporabnik te storitve) bila onemogočena, s tem pa storitev nedostopna.

[88] Navedeno pomeni kar 100 milijard bitov prometa na sekundo, kar ponazorjeno s številko pomeni 100.000.000.000 bitov na sekundo, kar so težko predstavljive količine prometa. Za lažjo oceno obsega prometa lahko naredimo primerjavo z osebnimi računalniki (danes je sodoben trdi disk v velikostnem razredu 1 TB oz. 1000 GB), promet s tako hitrostjo bi zapolnil 12,5 TB velik trdi disk v sekundi ali kar 12 sodobnih diskov v sekundi.

- **Izkoriščanje aplikacijskih pomanjkljivosti** je kategorija napada pri kateri napadalec išče šibke točke in logične pomanjkljivosti ter napake aplikacij na gostujočem strežniku. Primer takega napada je izkoriščanje zgornje omejitve vpisovanja uporabnikov v storitev (kot oblika zaščite). Napadalec bi v tem primeru večkrat avtomatično presegal zgornjo omejitev vpisa z napačnimi podatki z namenom (varnostnega) zaklepanja aplikacije in s tem onemogočil dostop do storitve legitimnemu uporabniku.

Na spletu je množica orodij za tovrstne napade dostopna vsakomur, za še uspešnejšo kombinacijo napada pa se večinoma uporabljajo kombinacije različnih prijemov, torej napad porazdeljene ohromitve storitve v kombinaciji z omrežjem robotskih računalnikov, o čemer več v naslednjem poglavju.

Shema 4.11: Prikaz napada tipa porazdeljene ohromitve storitve



Vir: Ollman (2011, 2).

4.3.4 Omrežja robotskih računalnikov

Takoj za porazdeljenimi ohromitvami storitev so kot največja grožnja aktualni avtomatizirani povezani računalniki ali omrežja robotskih računalnikov[89]. Tako omrežje je množica slabo zaščitenih računalnikov, ki jih, brez vednosti lastnikov, napadalec prek zlonamerne programske opreme poveže v omrežje z namenom izvajanja zlonamernih dejanj. Napadalec je pogosto označen tudi kot *pastir robotov* ali *gospodar robotov*, ki do oddaljenih računalnikov dostopa prek odkritih pomanjkljivosti v računalniških sistemih ter jih osvoji z nameščanjem zlonamerne programske kode. Tovrstni osvojeni računalniki tako postanejo izvajalci zlonamernih dejanj, pogosto kot osvajalci drugih računalnikov po istih principih kot so bili zavojevani sami. Zlonamerna programska oprema v kombinaciji z omrežjem robotskih računalnikov pogosto vzpostavi samozadostno okolje obnavljajočih se računalnikov, ki so povezani v internet ter tako predstavljajo konstantno grožnjo pod vplivom upravljavca. Tako obstaja ciklično razmerje med zlonamernim programjem in omrežjem robotskih računalnikov, saj je zlonamerno programje uporabljeno za ustvarjanje omrežja robotskih računalnikov, to omrežje pa je uporabljeno za nadaljnje razširjanje neželenega smetenja s pošto ali drugih zlonamernih aktivnosti (*Malicious Software (Malware): A Security Threat to the Internet Economy* 2008, 22). Cilj zlonamernih uporabnikov pri ustvarjanju omrežja robotiziranih računalnikov je primarno dvojen, to je okužiti in osvojiti čim več naprav ter povečati njihovo nevidnost oz. zmanjšati sledljivost (*Botnets – The Silent Threat* 2007, 3).

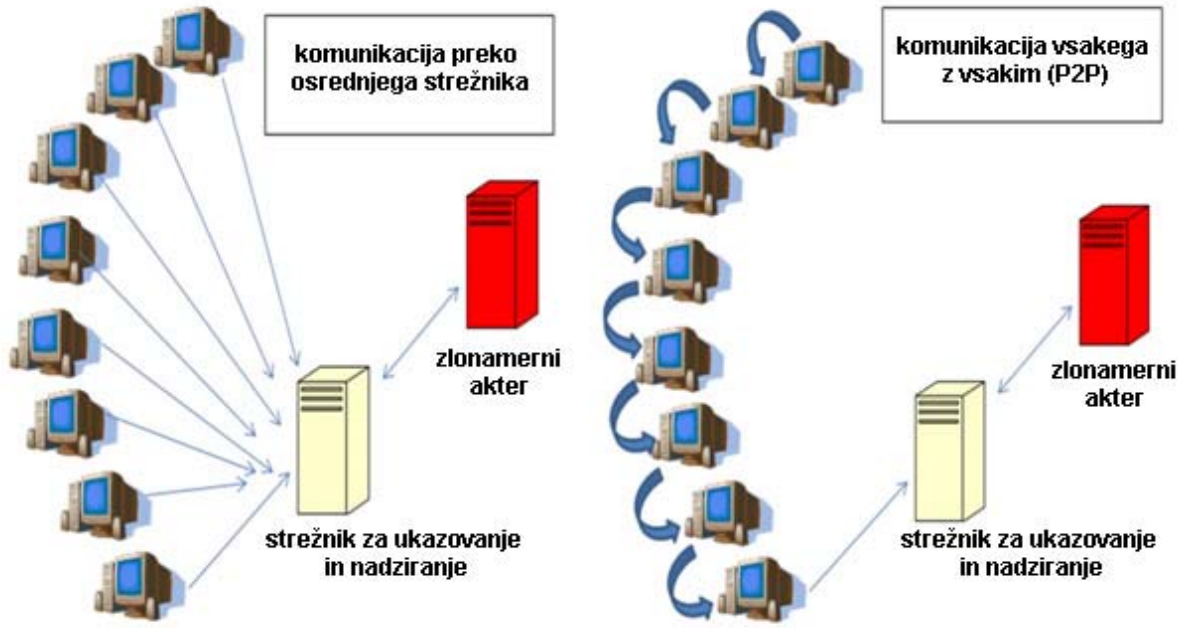
Omrežje robotskih računalnikov (v nadaljevanju tudi botnet) je lahko upravljano na dva načina, prvi je prek osrednjega centra za ukazovanje in nadziranje[90], drugi pa način, ki omogoča nadziranje vsakega z vsakim[91]. V prvem primeru omrežje komunicira prek osrednjega strežnika, ki je pogosto tudi sam okužen računalnik. Vsak od okuženih računalnikov se periodično ali po nekem drugem vnaprej določenem ključu povezuje na osrednji strežnik, kjer prejme navodila za delovanje. Čedalje več napadalcev uporablja protokole, ki omogočajo varne povezave (HTTPS),

---

[89] Angl. *botnet*
[90] Angl. ***C**ommand and **C**ontrol* (C&C)
[91] Angl. ***P**eer to **p**eer*, P2P

kar otežuje odkrivanje take povezave med osrednjim strežnikom in posameznim računalnikom, saj se promet skrije v množici vsakdanjega spletnega podatkovnega prometa. Drugi način ukazovanja in nadziranja pa je uporaba principa komuniciranja vsakega z vsakim (P2P). V primeru tega modela je hierarhija komuniciranja necentralizirana, kar otežuje odkrivanje dejanskega strežnika, ki je uporabljan kot osrednji center, s tem pa povečuje možnost njegovega preživetja (*Malicious Software (Malware): A Security Threat to the Internet Economy* 2008, 23).

Shema 4.12: Struktura ukazovanja in nadziranja omrežja računalnikov



Prirejeno po: *Malicious Software (Malware): A Security Threat to the Internet Economy* 2008, 23.

Po tem, ko uporabnik nevede namesti zlonamerno programje, njegov računalnik postane del omrežja, ki ga sedaj upravlja pisec zlonamerne kode, posameznik ali pa tudi organizacija. Seveda pa to ni edina pot do okužbe, saj se računalnik lahko okuži tudi prek elektronskega sporočila oz. obiska določene strani. Po oceni strokovnjakov naj bi bilo v medmrežju v letu 2009, kar 15 % računalnikov okuženih s t. i. botneti, kar predstavlja hitrejšo rast v primerjavi z virusi oz. nezaželeno pošto. Namen teh zlonamernih kod pa je predvsem prevzemanje nadzora nad napadenim računalnikom

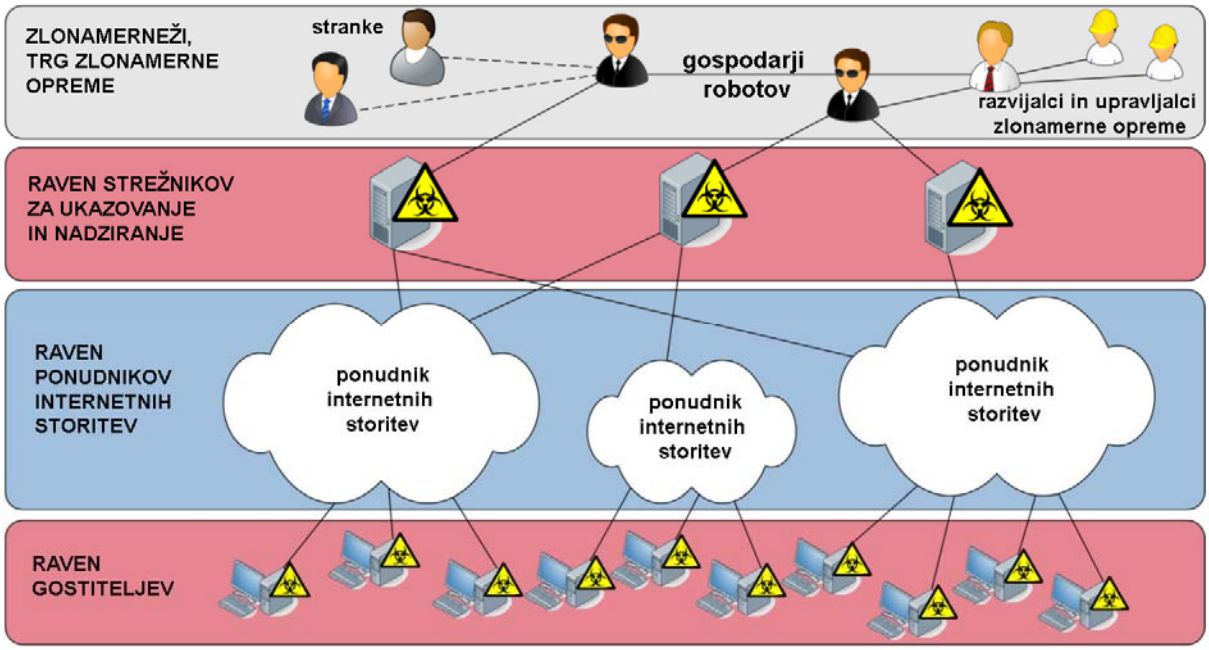
z namenom kasnejšega delovanja v skupini z ostalimi okuženimi računalniki; končni cilj pa je lahko različen, kraja osebnih podatkov, kraja poslovnih skrivnosti, porazdeljena ohromitev določene storitve, smetenje[92] in drugo. Obramba pred tovrstnimi grožnjami je precej težja, saj sam protivirusni program ne zadostuje, so pa v razvoju posebni algoritmi odkrivanja komunikacije med botnetom in upravljavcem botnetov in ob odkritju in uničenju te povezave, postane okužen računalnik za zlonamerneža neuporaben (*Emerging Cyber Threats Report* 2009; 3).

ENISA je izdala že več publikaciji na temo avtomatiziranih povezanih programov, torej tovrstne grožnje prepoznava kot pomembne. Zanimivi pa so razlogi za prihodnje trende avtomatiziranih povezanih programov, ki jih ENISA opredeli (*Botnets: 10 tough Questions* 2011, 16–17):

- motivacija za napade se povečuje, tako iz ekonomskih kot političnih razlogov ter iz razlogov promoviranja določenih stališč,
- kakovost in preprostost uporabe razpoložljivih orodij in opreme za razvoj napadalnih orodij se bo še naprej povečevala, torej bodo lahko tudi laiki s tako opremo povzročili precejšnjo škodo,
- koncepti ukazovanja in nadziranja, ki so uporabljani v primeri avtomatiziranih povezanih programov, bodo ponotranjili novejše tehnologije z namenom doseganja višjih ravni prevar in odpornosti na odkrivanje; to vključuje vpeljavo novih omrežnih protokolov in spletnih standardov, kot tudi komunikacije v živo in delovanja prek družabnih omrežij za razširjanje in prikrivanje zlonamernega prometa in programske opreme,
- kibernetski kriminal je postal dobičkonosen posel, raznoliko pravno okolje pa otežuje spopadanje z njim, kar pomeni, da bodo tudi preprostejše oblike avtomatiziranih povezanih programov lahko obstale dlje časa in bile razpoložljive za napade in zlorabe ter
- z razmahom uporabe pametnih telefonov in že odkritimi prvimi avtomatiziranimi povezanimi programi za pametne telefone in novimi načini dostopa do interneta, bo boj proti tovrstnim grožnjam dobil nove razsežnosti.

[92] Angl. *Spamming* (SPAM)

Shema 4.13: Plasti delovanja omrežij robotiziranih računalnikov



Prirejeno po *Botnets: Detection, Measurement, Disinfection & Defence* 2011, 103).

ENISA v svoji publikaciji namenjeni izključno omrežjem robotiziranih računalnikov (*Botnets: Detection, Measurement, Disinfection & Defence* 2011, 79–116) opredeli različne ukrepe in iniciative za zmanjševanje škode, ki jo tovrstna omrežja povzročajo. Ukrepe razdeli na tehnične, regulatorne in družbene ter na iniciativne ter institucionalne.

Kot tehnične protiukrepe ENISA tako predlaga:

- vpeljava in redno posodabljanje t. i. črnih list[93],
- razširjanje neuporabnih podatkov med sezname zbranih informacij[94], ki naredijo te informacije manj uporabne za naročnika,
- uporaba protokola mejnih usmerjevalnikov (BGP) za usmerjanje in zavračanje tovrstnega prometa[95],

[93] Angl. *Blacklisting*
[94] Angl. *Distribution of Fake/Traceable Credentials*
[95] Angl. *BGP Blackholing*

- ukrepi na področju sistema domenskih imen[96], kjer naj bi registrar[97] domene, ki je prepoznana kot zlonamerna, le to začasno ali trajno ukinil,
- neposredna razstavitev ali obglavljenje tovrstnega omrežja prek prekinitve povezave takega strežnika do omrežja, za kar so praviloma odgovorni ponudniki internetnih storitev (ISP),
- filtriranje paketov na ravni omrežja in aplikacij,
- blokada vrat 25,
- metoda nadziranja aplikacij, vsebine in omejevanja podatkov na strani ponudnika internetnih storitev ter še nekatere druge[98].

Med regulatorne in družbene ukrepa pa ENISA predvideva predvsem promocijo specialnih zakonov za kibernetsko kriminaliteto, dvigovanje zavedanja o škodljivosti robotiziranih omrežij pri končnih uporabnikih ter izvajanja posebnih usposabljanj, vzpostavitev centrov za pomoč uporabnikom ter izboljšati sodelovanje med vpletenimi deležniki.

4.3.5 Spletno vojskovanje in druge oblike

Splošna ugotovitev varnostnih strokovnjakov je, da bo spletno gostovanje čedalje bolj pogosto spremljalo vojaška posredovanja, pogosto pa se tudi omenja, da naj bi igralo še pomembnejšo vlogo na bolj živahnih bitkah na gospodarskem in infrastrukturnem področju. Razlogi, ki povečujejo aktivnosti na področju spletnega vojskovanja so predvsem:

- izredno nizki stroški spletnega vojskovanja v primerjavi s fizičnimi napadi,
- pomanjkanje spletne obrambe,
- izredno lahko zanikanje odgovornosti zaradi narave spleta in
- pomanjkanje spletnih »pravil spopadanja«[99].

---

[96] Angl. *DNS-based Countermeasures*

[97] Registrarji so posredniki med registrom domen (v Sloveniji ima to vlogo ARNES) in nosilci domen (registranti), pri njih je možno zakupiti domensko ime.

[98] Večino od predpisanih ukrepov večji slovenski ponudniki dostopa do interneta že izvajajo, težava pa je pri ponudnikih v manj razvitem delu sveta, kar posledično vpliva na učinkovitost in raven zaščite celotnega medmrežja.

Najbolj izpostavljene točke so predvsem sistemi transporta, telekomunikacijski sistemi, IT-podpora vodni in električni oskrbi itd.; zanimivost spletnega vojskovanja pa je predvsem v tem, da manj razvite sile in super-sile lahko sprožijo približno enako škodljive spletne napade z relativno majhnim vložkom (*Emerging Cyber Threats Report* 2009, 3–5). V sfero vojskovanja spada tudi kibernetsko izrabljanje virov. Avtorji (Denning in Denning 2010, 30) tako izpostavljajo tudi najbolj prikrito obliko vojskovanja, ki na kar se da neopazen način vstopa v tuje računalniške sisteme in zbira podatke brez odkritja aktivnosti; tovrstna dejanja sodijo med napredne trajne grožnje omenjene v prejšnjih poglavjih.

Na tem mestu je smiselno omeniti razsežnosti, ki jih v zadnjem času dosegajo akterji nedržavnega izvora. V ospredju se pojavlja predvsem skupina Anonimni[100], ki se identificira kot skupnost borcev za internetno svobodo, ki nimajo vodje, formalne strukture ali sprejetih določil ali kodeksa. Izvor oz. nastanek skupine se povezuje s sodelovanjem na oglasni deski www.4chan.org, kjer uporabniki lahko objavljajo slike in komentarje brez registracije in so v celoti anonimni, koordinacija delovanja pa se odvija na množici različnih portalov, tako da skupine ni moč evidentirati le z enim. Praktično edina skupna točka je ta, da so akterji anonimni in povezani v spletni skupnosti. V zadnjem času se je središčna točka akterjev selila med napadi na različne verske sekte, medijske hiše, glasbeno in filmsko industrijo do vladnih organizacij; primarna oblika napada pa so razpršeni napadi z ohromitvijo storitev, ki so za tak tip organizacije tudi zelo priročni (*The strange virtual world of 4chan* 2010; *Political hacktivists turn to web attacks* 2010; *4chan Users Organize Surgical Strike Against MPAA* 2010; *Music and film industry websites targeted in cyber attacks* 2010).

---

[99] Angl. ***R**ules **o**f **E**ngagement*
[100] Angl. *Anonymous*

Grožnje mobilnim napravam in pametnim telefonom

Mobilni aparati so danes več funkcijske naprave, ki združujejo funkcionalnosti še nedavno več in večjih naprav; vse to združeno z dostopom do interneta in povečanimi količinami prenesenih podatkov pa jih naredi še boljše tarče za spletni kriminal. Prenos celo finančnega poslovanja na pametne mobilne telefone[101], oz. koncept digitalne denarnice pa je lahko ključni dejavnik k povečanju napadov na te sisteme, saj praviloma napadalci iščejo finančne koristi. Uporaba pametnih programskih orodij pa lahko veliko pripomore k pravočasnemu razvoju varnostnih komponent, kar bo omogočalo varnejše rokovanje z mobilnimi aparati (*Emerging Cyber Threats Report* 2009, 5).

Druge študije (*Accompanying document to the Communication on Critical Information Infrastructure Protection* 2009, 53) pa izpostavljajo tudi nevarnosti ogrožanja poslovnega omrežja prek pametnih telefonov, saj se le ti danes uporabljajo tudi za uporabo poslovnih aplikacij in izmenjavo dokumentov. Z dejstvom, da je mobilni telefon postal prenosna pisarna, ki ima pogosto naložene tudi varnostne certifikate in kot brskalnik tudi piškotke[102], se je tveganje za varnost podatkov občutno povečalo ravno zaradi možnosti fizičnega dostopanja do aparata. Izpostavljenost različnih mobilnih platform pa je različna in vsaka ima svoje posebnosti in specifike. Odprtost Android® platforme za različne modifikacije jo hkrati naredi tudi zelo dovzetno za morebitne zlorabe[103], zato je ključno, da so uporabniki pametnih telefonov pozorni in dobro obveščeni o potencialnih nevarnostih (*Security threat report* 2011, 19).

---

[101] Raziskave kažejo, da je skoraj polovica brezplačne programske opreme, ki je na voljo za prenos prek različnih portalov okužena z neko obliko vohunske programske kode, saj naj bi izdajatelju sporočalo podatke o tipu telefona, ponudniku mobilnih storitev ali celo lokaciji uporabnika (*Skoraj vsa mobilna programska oprema je vohunska*, 2011).

[102] Angl. *Cookie*, podatek, ki ga na pobudo spletnega programa v spletni brskalnik shrani za poznejšo rabo, več o varnostnih in zasebnih vidikih piškotkov je na voljo v publikaciji ENISE (*Bittersweet cookies: Some security and privacy considerations* 2011).

[103] Proti koncu leta 2011 je odjeknila novica, da nekateri ponudniki mobilnih telefonov nameščajo programsko opremo, ki omogoča sledenje uporabnikovih akcij na telefonu, s tem pa posledično tudi vse ostale aktivnosti, vse z namenom kasnejše podpore uporabniku v primeru težav s telefonom. Seveda pa tovrstna programska oprema omogoča tudi manj dobronamerno sledenje aktivnostim, kar je omrežena skupnost jasno izpostavila in obelodanila, izpostavljen je bil tudi potencialni vpliv na poslovanje podjetij, saj bi bila zloraba informacij v tem primeru preprosta (*Carrier IQ Software Compromises Android Device Data Privacy* 2011).

Razvijajoča se panoga spletnega kriminala

Spletni kriminal in njegovi izvori bodo postajali čedalje bolj organizirani in gnani z dobičkom preteklih akcij. Gunther Ollman, glavni varnostni strateg pri internetni varnosti pri podjetju IBM, sodobne spletne kriminalce opisuje kot mednarodni konglomerat profesionalno izurjenih akterjev z motivacijo gnano z visokimi dobički. Danes je industrija spletnega kriminala tako razvita, da lahko »končne izdelke« kupite prek spleta, s katerimi je nato moč izvajati spletni kriminal. Obstaja celo spletna podpora tovrstnim izdelkom in garancija zadovoljive ravni delovanja, skratka trg se je v celoti razvil. Olmann je razdelil industrijo spletnega kriminala na tri glavne tipe:

- nizko razviti kriminalci, ki uporabljajo kupljene pakete, s katerimi dosežejo želene učinke za dosego njihovega ciljnega kriminala;
- izkušeni razvijalci in kolektivi tehničnih strokovnjakov, ki ustvarjajo nove komponente, ki jih nato vključijo znotraj njihovih komercialnih paketov in
- prvovrstni ponudniki novih vsebin, ki z uporabo najmodernejših storitev vzdržujejo najvišjo raven organiziranega spletnega kriminala na globalni ravni (*Emerging Cyber Threats Report* 2009, 6).

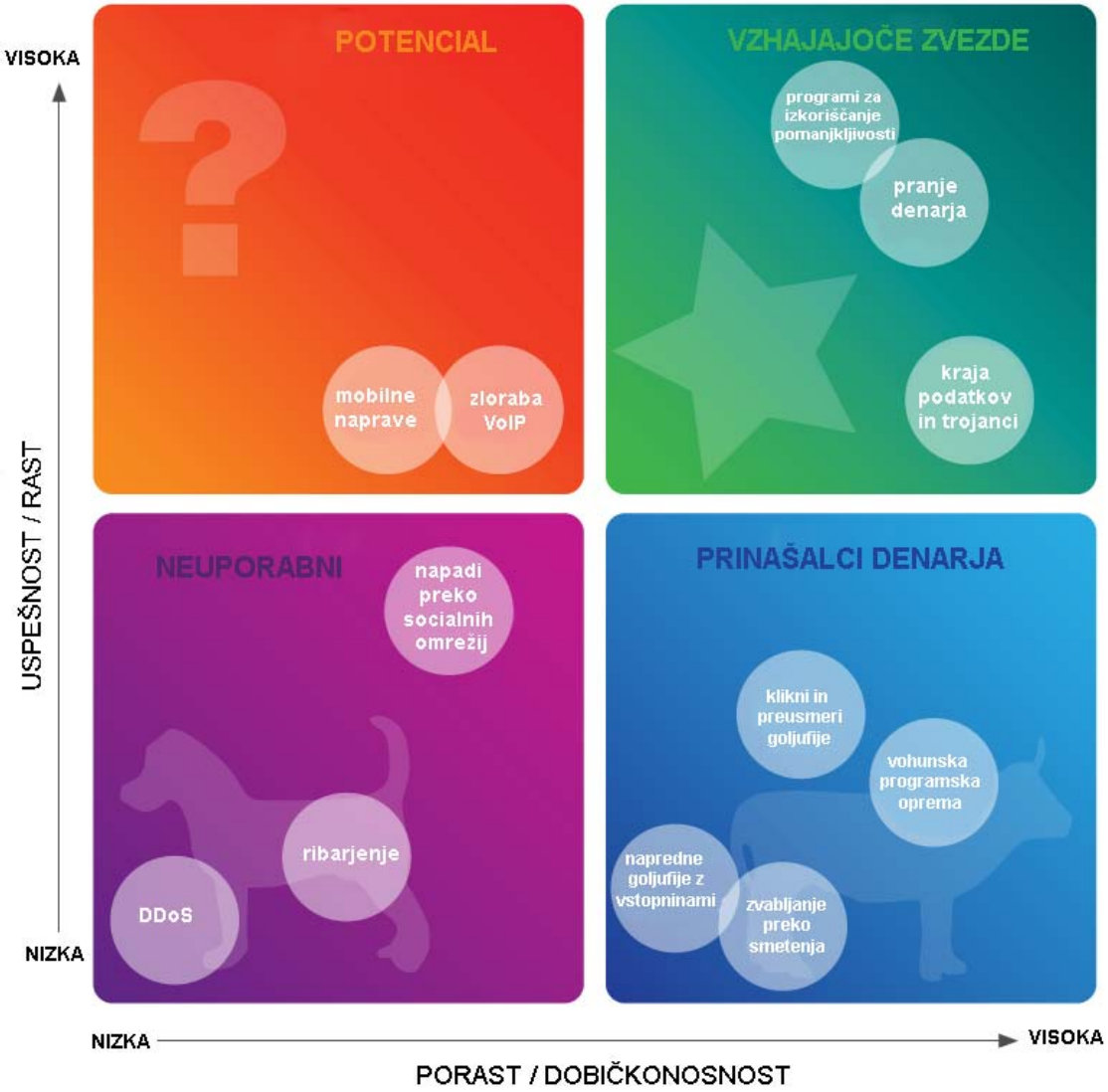
Zanimiva oblika ogrožanja je tudi nedavno odkrita, saj so spletni strokovnjaki ugotovili, da posamične skupine z uporabo izredno hitre strojne in programske opreme izrabljajo delniške trge, in sicer tako, da opravijo spremembo (prodajo ali nakup), še preden se le-ta vidi na delniškem trgu. Znano je, da tehnologija na marketih deluje na milisekundni ravni, zato ostanejo akcije na mikrosekundni ravni neevidentirane (*Hackers find new way to cheat on Wall Street* 2011; *The New Speed of Money, Reshaping Markets* 2011).

Strokovnjaki v okviru zasebnega podjetja (*Cisco 2010 Annual Security Report* 2010) spremljajo razvoj kibernetske kriminalitete in prek preteklih dogodkov predvidevajo trende razvoja le-te. Na podlagi uspešnosti in dobičkonosnosti je nastala spodnja matrika, ki prikazuje posamezne tipe kriminalitete v odvisnosti od njihove uspešnosti in rasti ter stopnjevanja ter dobičkonosnosti. Starejše oblike spletne kriminalitete, kot so onemogočanje storitev prek razporejenih napadov (DDoS), ribarjenje in napadi prek spletnih omrežij so v upadu. Kljub temu pa so tovrstni napadi še vedno prisotni

in ogrožajoči, vendar je verjetnost dobičkonosnosti takega napada nizka, torej postajajo neaktualni. Med aktualnimi prinašalci denarja ostajajo različne goljufije in vohunska programska oprema ter množično smetenje. Zaradi izredne rasti[104] trga pametnih telefonov in tabličnih računalnikov povezanih v internet je tudi priložnosti za tovrstne zlorabe čedalje več. Zlonamerni programi, ki zlorabljajo funkcionalnost SMS avtentifikacije za dostop do spletne banke, naj bi že povzročali milijonske škode pri korporacijah. Prav tako je v porastu zloraba telefonije prek internetnega protokola, kjer spletni kriminalci uporabljajo vdore v sisteme poslovne telefonije za pridobivanje finančnih koristi. Med kriminalnimi aktivnostmi, ki so v največjem porastu pa so programi za izkoriščanje spletnih pomanjkljivosti aplikacij, brskalnikov in programske opreme ter zlonamerni programi za krajo osebnih podatkov. V porastu je tudi zloraba internetnih uporabnikov za pranje denarja. Matrika dobičkonosnosti spletne kriminalitete, kot jo vidijo v podjetju Cisco, je prikazana na shemi 4.14.

[104] Po nekaterih ocenah naj bi že leta 2013 število mobilnih naprav, ki bodo dostopale do interneta, preseglo milijardo.

Shema 4.14: Matrika dobičkonosnosti spletne kriminalitete

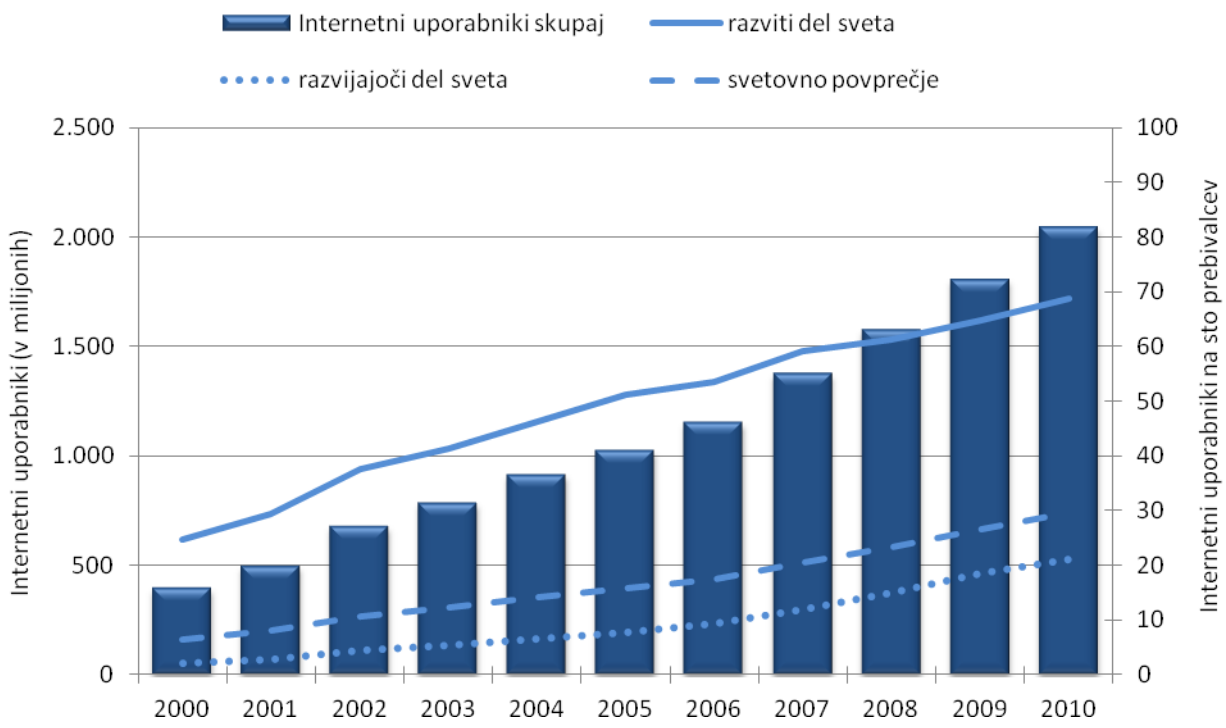


Prirejeno po *Cisco 2010 Annual Security Report* 2011, 8.

Brezmejna narava interneta, neizmerna rast novih uporabnikov (prikazana na grafu 4.1), težavno vzpostavljanje in preverjanje on-line identitete in pomanjkanje standardizacije na varnostnem področju vse to vpliva na težavno izgradnjo normativnega okolja. Toda uspehi spletnih kriminalcev in občutljive izgube dobička na račun tovrstnega kriminala že povzročajo določene spremembe v smeri regulacije na področju internetne varnosti. Strokovnjaki so si zato enotni, da bo tudi država oz. mednarodne institucije morale odigrati svojo vlogo pri uveljavljanju določenih pravil oz. omejitev; vsaj na področju varovanja kritične infrastrukture, ki v najhujših

scenarijih lahko povzroči tudi večjim entitetam izredno škodo, zaenkrat pa je problem spletnega kriminala večji kot so ga institucije, napori posameznikov ali kdorkoli sposoben omejiti. Žal tudi na področju varnostne teoretične misli tovrstna problematika ni dovolj dobro zastopana.

Graf 4.1: Število uporabnikov interneta skupaj in na sto prebivalcev



Prirejeno po *World Telecommunication/ICT Indicators Database* 2010 in *World Bank Data Indicator 2011*.

4.3.6 Prihodnji izzivi varnosti interneta stvari

Vse zgornje grožnje in njihove predpostavke temeljijo na povezanosti dveh ali več računalnikov, ki so se jim pred kratkim pridružile tudi druge naprave. Kar sledi že v bližnji prihodnosti in je v določeni meri na voljo že danes ter predstavlja prihodnost interneta pa bo povezanost vseh vsakodnevnih naprav in stvari, ki nas obkrožajo v

omrežje medsebojno povezanih stvari, s čimer bo nastal t. i. internet stvari[105]. Na tej ravni se nam odprejo nove možnosti komuniciranja med ljudmi in računalniki, ljudmi in stvarmi ter med stvarmi in stroji samimi. Odprla se je nova dimenzija v svetu komuniciranja in povezovanja, od povezljivosti kogarkoli, kadarkoli, kjerkoli se sedaj premikamo k povezljivosti česarkoli (*The Internet of Things* 2005, 2; *Internet stvari – akcijski načrt za Evropo* 2009, 2; *Sporočilo o prihodnosti omrežij in interneta* 2008, 3–5).

Z besedo česarkoli tako zaobjamemo tudi stvari, ki po lastni naravi niso elektronske naprave, temveč tudi povsem vsakdanje stvari, ki niso povezane z elektroniko, kot so hrana, materiali in infrastruktura; tako govorimo o številkah, ki po nekaterih ocenah presegajo petdeset tisoč milijard stvari. Tovrstno povečanje razsežnosti nemudoma porajajo vprašanja s področja varnosti in zasebnosti uporabnikov ter hkrati varnostnimi vprašanji za varnost in integriteto omrežij. Ker pa so nekatere pravice na področju varovanja osebnih podatkov in zasebnosti že v temeljnih dokumentih EU, je Evropska komisija na tem področju tudi pravočasno aktivna in je ob prepoznavanju pomembnosti radiofrekvenčne identifikacije[106] na področju interneta stvari, izdala ustrezne smernice o zakonitem, etičnem in družbeno ter politično sprejemljivem načinu uporabe te tehnologije (*Priporočilo Komisije o izvajanju načel varstva zasebnosti in varstva podatkov v aplikacijah podprtih z radiofrekvenčno identifikacijo* 2009, 1–3; Kunc 2011, 1–4). ENISA je v svojem poročilu (*Flying 2.0* 2010, 45–67), ki se med drugim nanaša tudi na uporabo storitev interneta stvari opredelila več potencialnih področij tveganj tehnične, organizacijske, družbene in normativne narave. Naštel bom le ključne kot so visoka odvisnost od tehnologije, možnost prekinitve dostopnosti storitve, možnost zlonamernih napadov z namenom onemogočanja sistemov, kraja identitet, onemogočanje transporta, tveganja za zasebnost, potencialno povečan nadzor in zaostajanje predpisov za dejanskim razvojem.

Vseprisotnost interneta stvari bo tako v temeljih preobrazila varnostne izzive s katerimi se soočamo danes, zato je ključno, da sisteme ključne informacijske

[105] Angl. ***I**nternet **o**f **T**hings*, IoT.
[106] Angl. ***R**adio **F**requency **ID**entification*, RFID; pri mobilnih napravah je pogosta tudi uporaba kratice NFC (angl. ***N**ear **F**ield **C**ommunication* – komunikacija bližnjih polj), ki uporablja tehnologijo RFID.

infrastrukture prilagodimo tako, da bodo pripravljeni na nove izzive, ki jih prinaša prihodnost.

4.4 Analiza normativnih okvirov na področju informacijske varnosti

Kibernetska varnost ima mnogo razsežnosti, več pojavnih oblik, več ravni zahtevnosti in predvsem več akterjev, zaradi česar je obvladovanje groženj na tem področju izredno kompleksno in zahtevno opravilo, rezultati pa težko merljivi. Glede na pretekle trende bi lahko ukrepe označili kot uspešne že, če bi se zmanjšala ali umirila letna rast kibernetskih napadov na ključna informacijska omrežja.

EU je na področju varovanja ključne informacijske infrastrukture in kibernetske varnosti omrežij opravila že precej formalnih korakov, vendar na področju zakonodaje in aktivnosti institucij še vedno zaostaja za ZDA, kjer so pravi razmah predpisov in institucij beležili po napadih 2001 v skladu z razvojem koncepta domovinske varnosti.

V tem poglavju želim izpostaviti nekatere ključne ukrepe in različne pristope ter dokumente državnih, naddržavnih in mednarodnih akterjev na področju kibernetske varnosti omrežij in ključne informacijske infrastrukture na različnih ravneh.

4.4.1 Evropska unija

Da bi lažje razumeli ukrepe in načrte EU za varovanje ključne informacijske infrastrukture in kibernetske varnosti omrežij, je potrebno omeniti nekaj temeljnih dokumentov s področja informacijske družbe. Čeprav je kibernetska varnost KII le majhen segment v celotnem ustroju dokumentacije in ukrepov na ravni EU pa postavlja močan pospešek v zadnjih letih to področje na osrednje mesto. Varna informacijska družba in vsi procesi, ki so vezani nanjo, kot predpogoj terja tudi varno informacijsko infrastrukturo, ki je praktično ustanovni kamen moderne družbe.

4.4.1.1 Ustvarjanje varne informacijske družbe

Evropska unija je svoj razmislek na temo varne informacijske družbe pričela z zavedanjem o nenehno rastoči pomembnosti omrežij in informacijske varnosti. Tako je bil prvi dokument z naslovom *Ustvarjanje varne informacijske družbe z izboljšanjem varnosti informacijske infrastrukture in bojem proti kibernetskemu kriminalu* sprejet s strani Komisije na začetku leta 2001. V njem Komisija spoznava naraščajočo pomembnost informacijske in komunikacijske infrastrukture in omrežne varnosti za sodobno družbo, hkrati pa te spremembe prepoznava tudi kot priložnosti za razmah kibernetske kriminalitete, zato oriše nekaj ukrepov in predlogov za ustvarjanje varne informacijske družbe. V dokumentu poskuša Komisija tudi definirati kibernetsko kriminaliteto v najširšem smislu, kot »vsako kršitev, ki vključuje informacijsko tehnologijo«, hkrati pa predlaga zakonodajne in nezakonodajne ukrepe (*Fight against cybercrime* 2011).

Evropska unija je tako svoje aktivnosti za varnejšo informacijsko družbo začela tudi na podlagi pobude organizacije Svet Evrope, ki je kot prva sprejela konvencijo, ki jo bom predstavil na koncu poglavja o Evropski uniji.

4.4.1.2 Varnost omrežij in informacij

Prav tako je EU leta 2001 sprejela dokument z naslovom *Varnost omrežij in informacij: predlog pristopa evropske politike*, kjer uvodoma ugotavlja rastočo vlogo IKT in njen pomen pri zagotavljanju ekonomskega in socialnega razvoja. Dostopnost IKT je že takrat bila ključna za podporne storitve in kot taka predpogoj za nadaljnji razvoj. Varnost IKT in omrežij je s povečano vlogo zasebnih akterjev postala kompleksnejša, prav tako zagotavljanje njene varnosti kot tudi razvoj ustrezne politike na ravni EU (*Varnost omrežij in informacij: predlog pristopa evropske politike* 2001, 3–5). Vloga politike na področju omrežne in informacijske varnosti naj bi tako pomenila most med obstoječimi pravnimi podlagami in jih smiselno povezovala. S tem dokumentom se je razprava o kibernetski varnosti omrežij prenesla na najvišjo, politično raven. Pristop pa lahko strnemo na osem ključnih ugotovitev: načelno soglasje za potrebo po ureditvi politike na tem področju, dvigovanje zavedanja obstoječe grožnje, evropski opozorilni in informacijski sistem, tehnološka podpora,

podpora tržno usmerjenim certifikatom in standardizaciji, izgradnja zakonske regulative, varno poslovanje lokalnih uprav in s tem zgled ter mednarodno sodelovanje.

Shema 4.15: Prepletanje področij različnih EU politik pred novim pristopom

Prirejeno po: *Varnost omrežij in informacij* 2001, 3.

4.4.1.3 Strategija za varno informacijsko družbo

Nekajletni razpravi po sprejetju predloga pristopa EU k omrežni in informacijski varnosti in vmesni ustanovitvi ENISE[107] v 2004, je sledilo osnovanje *Strategije za varno informacijsko družbo* z naslovom *Dialog, partnerstvo in povečanje vpliva in moči* v 2006. Strategija pri reševanju varnostnih izzivov informacijske družbe predvideva tridelni pristop, ki naj bi obsegal posebne ukrepe za varnost omrežij in informacij, regulativni okvir za elektronske komunikacije[108] in boj proti zasebnemu kriminalu. Kot izhaja že iz naslova, je v strategiji zapisan pristop na treh ravneh:

---

[107] ***E**uropean **N**etwork and **I**nformation **S**ecurity **A**gency*, več o Agenciji je dostopno na njihovi spletni strani (http://www.enisa.europa.eu/, 6. maj 2011).

[108] Širši javnosti je ta regulativni okvir poznan predvsem na področju urejanja stroškov mobilne telefonije za končnega uporabnika, saj je EU na tem področju dosegla veliko, z zmanjševanjem stroška komunikacij pa se je povečala dostopnost potovanj in dodatno razvil notranji trg EU.

- dialog (prvi predlog predvideva analizo obstoječih nacionalnih politik in s tem izbor najboljših praks iz javne uprave[109], ki naj bi postala gonilo najboljše prakse in varnosti);
- partnerstvo (za učinkovito oblikovanje politike je potrebno dobro poznavanje in razumevanje narave in obsega izzivov, zato naj bi v okviru ENISE vzpostavili zaupno partnerstvo z državami članicami in zainteresiranimi stranmi za razvoj ustreznega okvira zbiranja podatkov) ter
- povečanje vpliva in moči (se nanaša predvsem na posamezne interesne skupine, ki naj bi s svojimi aktivnostmi spodbujale ozaveščenost o problematiki varnosti omrežij in informacij (*Strategija za varno informacijsko družbo: Dialog, partnerstvo in povečanje vpliva in moči* 2006, 8–10).

4.4.1.4 Sklep o napadih na informacijske sisteme

Svet Evropske unije pa je v letu 2005 sprejel okvirni sklep o napadih na informacijske sisteme, ki ima namen pospeševati vlogo informacijske varnosti in predvsem izboljšati sodelovanje pristojnih sodnih in drugih institucij. V njem Svet poziva k vzpostavitvi zakonodaje, ki bi kriminalizirala vsak nezakonit dostop večjega pomena do informacijskih sistemov, nezakonito poseganje v sistem, nezakonito poseganje v podatke ter vsakršno napeljevanje, pomoč in podpiranje tovrstnih poskusov. Hkrati predlaga tudi minimalno zaporno kazen za tovrstna dejanja ter odgovornost pravnih oseb in njihovih vodilnih kadrov ter podeli sodno pristojnost državam članicam, kadar je bilo dejanje storjeno na njenem ozemlju ali je storilec državljan države članice ali ima pravna oseba sedež v državi članici (*Attacks against information systems* 2011).

[109] Tak pristop je po moji oceni nekoliko nenavaden, saj se čedalje večji del IKT-panoge odvija v zasebnem sektorju, zato je za pričakovati, da bo tudi na področju varovanja in razvoja najboljših praks zasebni sektor pred javnim.

4.4.1.5 Digitalna agenda

Evropska unija je z namenom boljšega izkoriščanja družbenega in gospodarskega potenciala ter vseh prednosti IKT, zlasti interneta, ter vzpostavitvijo enotnega digitalnega trga predstavila dokument z naslovom *Evropska digitalna agenda.* Z njo želi vzpostaviti okolje s katerim se vzpodbuja inovacije, gospodarsko rast in izboljšave v vsakodnevnem življenju tako državljanov kot podjetjih. Razširjena raba digitalnih tehnologij naj bi Evropi omogočila lažje soočanje s ključnimi izzivi prihodnosti. Panoga IKT tako danes predstavlja 5 % evropskega BDP, prispeva pa kar 30 % k rasti produktivnosti, hkrati pa skoraj vsak drugi Evropejec uporablja internet dnevno, zato je pomen IKT-panoge ključen za evropsko družbo (*Evropska digitalna agenda 2010,* 3–4*)*.

Vse te prednosti informacijske družbe pa so lahko ustrezno izkoriščene le v dobro delujočem in varnem IKT-okolju, zato se v Digitalni agendi izpostavlja pomembnost naraščajočega kibernetskega kriminala in s tem povezanega tveganja zaupanja v omrežja, ki so posledica novih oblik kriminala, vse od zlorabe otrok do kraje identitete in kibernetskih napadov. Zaradi množice dostopnih podatkov v podatkovnih bazah ter tehnologij spremljanja posameznikov na daljavo pa ta segment odpira tudi nove izzive za varovanje temeljnih človekovih pravic in zasebnosti. EU ima zato namen ohraniti oz. vzpostaviti stanje zaupanja in varnosti, ki bo omogočilo sprejemanje novih tehnologij in zaupanje vanje, naloga vseh vpletenih, od posameznikov, zasebnih in javnih institucij pa je, spopadanje s temi grožnjami in krepitev varovanja v digitalni družbi. Pravici do zasebnosti in varovanju osebnih podatkov je potrebno slediti že pri razvoju tehnologij z uporabo načela vgrajene zasebnosti[110]. Sodelovanje CERT in organov pregona je nujno pri preprečevanju kibernetskega kriminala in pri odzivanju na incidente. Komisija izpostavlja tudi pomembnost mednarodnega sodelovanja zaradi naraščajočih tveganj kibernetske varnosti (*Evropska digitalna agenda* 2010, *6, 16, 34)*.

V Evropski digitalni agendi so tako povzeti ključni pogledi EU za področje kibernetske varnosti, v kibernetsko varnost omrežij pa ta dokument detajlneje ne posega.

---

[110] To pomeni, da sta zasebnost in varnost ključni predpostavki že pri osnovanju in načrtovanju novih tehnologij, predvsem programske opreme.

4.4.1.6 Kako zaščititi Evropo pred obsežnimi kibernetskimi napadi

V okviru izboljšanja varnosti in odpornosti omrežij ter tudi v duhu Digitalne agende se je oblikoval skupek aktivnosti, ki so prepoznane pod pojmom zaščita ključne informacijske infrastrukture (KII). Temeljni dokument zaščite KII pa je nastal v 2010 z naslovom *Kako zaščititi Evropo pred obsežnimi kibernetskimi napadi in prekinitvami: izboljšati pripravljenost, varnost in odpornost.* V njem EU izpostavlja bistveno vlogo KII pri gospodarski in družbeni rasti skupnosti, za pomen IKT in pomembnost internetne ekonomije uporabi kar opis OECD-ja, ki internet navaja kot ključen »za povečanje gospodarske storilnosti in družbene blaginje ter krepitev storilnosti družb, da bi se izboljšala kakovost življenja državljanov po vsem svetu«[111]. Hkrati dokument izpostavlja tudi tveganja za KII, tako antropogena kot naravna ali tehnična. Ugotavlja, da kibernetski napadi postajajo kompleksnejši, njihov vzrok pa je čedalje večkrat denarna ali politična korist. Odvisnost družbe od KII tako terja sistematično obravnavanje njihove varnosti ter zavarovanje pred napakami ali napadi. Pogoj optimalnega izkoristka prednosti IKT in s tem vseh priložnosti informacijske družbe je povečanje zaupanja vanjo, zato so raznolikost, odprtost, interoperabilnost, uporabnost, preglednost, odgovornost, možnost presoje različnih komponent in konkurenčnost ključna gonila za razvoj varnosti ter spodbujajo uporabo izdelkov, procesov in storitev, ki krepijo varnost *(Kako zaščititi Evropo pred obsežnimi kibernetskimi napadi in prekinitvami: izboljšati pripravljenost, varnost in odpornost* 2009, 4–5).

Zanimivo pa je kako EU kljub izkazanem interesu za povečevanje varnosti ohranja distanco in se zaveda, da bi pretiran odziv onemogočal pojave inovativnih storitev in aplikacij, kar ocenjujem kot ključno in pravilno usmeritev.

V nadaljevanju dokumenta EU ugotavlja še razpršenost nacionalnih pristopov in potrebo po novem, evropskem modelu upravljanja s KII, spoznava lastno omejenost pri zmogljivostih zgodnjega opozarjanja in odzivanja na incidente in izpostavlja

[111] Izvirnik je na voljo v dokumentu OECD, Shaping Policies for the Future of the Internet Economy, 2008.

nadaljnjo potrebo po mednarodnem sodelovanju. Z namenom obvladovanja prepoznanih izzivov EU predlaga kot akcijski načrt pet področij ukrepanja, stebrov:

1. pripravljenost in preprečevanje na vseh ravneh,
2. odkrivanje in odziv ter zagotovitev ustreznih mehanizmov zgodnjega opozarjanja,
3. ublažitev in odpravo posledic ter krepitev mehanizmov EU na področju KII,
4. spodbujanje prednostnih nalog EU pri mednarodnem sodelovanju ter
5. razvijanje in izvajanje meril za KII za panogo IKT (*Kako zaščititi Evropo pred obsežnimi kibernetskimi napadi in prekinitvami: izboljšati pripravljenost, varnost in odpornost* 2009, 7–10).

4.4.1.7 Dosežki in naslednji koraki: h globalni kibernetski varnosti

Akcijskemu načrtu je v začetku leta 2011 sledilo sporočilo Komisije, kjer se opisuje naslednje korake na evropski in mednarodni ravni ter ponovno izpostavlja svetovno razsežnost problematike in v tem kontekstu potrebno sodelovanje na mednarodni ravni tako med subjekti javne kot zasebne sfere. Razvoj kibernetskih groženj tako terja od institucij aktivnejši odziv, zato je EU z namenom celovitejšega razumevanja razvrstila kibernetske grožnje v tri kategorije:

- **izkoriščanje** za gospodarsko in politično vohunjenje; v to področje sodijo napredne trajne grožnje[112], kraja identitete in napadi na vladne sisteme;
- **motnje ali prekinitev** komunikacij; sem spadajo različni napadi porazdeljenih zavrnitev storitev[113], množično pošiljanje neželene pošte in druga zlonamerna uporaba mreže računalnikov ter
- **uničenje**, ki predstavlja potencialni še ne uresničeni scenarij (*Dosežki in naslednji koraki: h globalni kibernetski varnosti* 2011, 2–4).

V nadaljevanju se v dokumentu ugotavlja posamezne izvedene ukrepe, v okviru akcijskega načrta ter zavezuje Komisijo k spodbujanju načel za odpornost in stabilnost interneta (več o tem v nadaljevanju), oblikovanju strateških mednarodnih

[112] Angl. ***A**dvanced **P**ersistent **T**hreats* – APT, omenjeno že v predhodnem poglavju.
[113] Angl. ***D**istributed **D**enial **o**f **S**ervice* – DDoS, omenjeno že v predhodnem poglavju.

partnerstev ter vzpostavljanje zaupanja za uporabo storitev v oblaku[114]. Poleg tega pa zavezuje države članice da:

- do leta 2012 vzpostavijo lastne CERT-centre ter s tem povečajo pripravljenost EU na kibernetske incidente,
- do leta 2012 vzpostavijo načrte odzivnosti na kibernetske incidente in sodelujejo pri rednih vseevropskih vajah ter
- usklajeno delujejo in si v mednarodnih forumih prizadevajo za povečanje varnosti in odpornosti interneta (*Dosežki in naslednji koraki: h globalni kibernetski varnosti* 2011, 7–8).

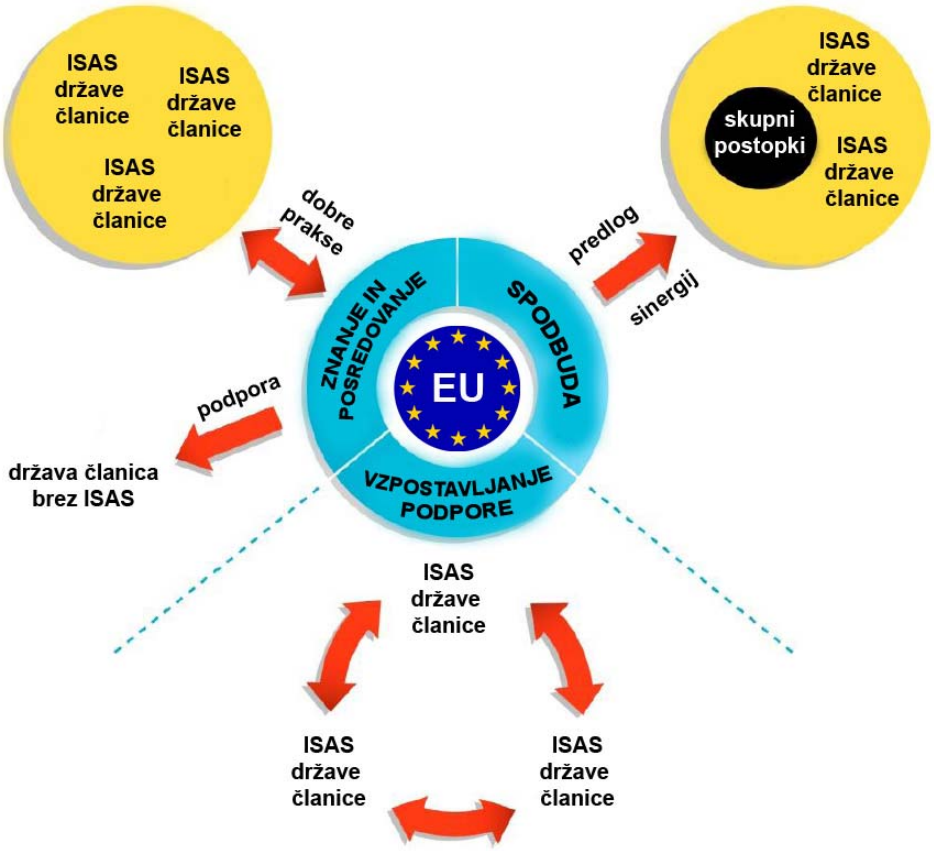
V okviru prvega stebra določenega v akcijskem načrtu se je tako že vzpostavil Evropski forum za države članice[115], čigar namen je pospeševanje razprave in izmenjave informacij o varnosti in odpornosti IKT ter izmenjave dobrih praks med uglednimi institucijami. Do leta 2011 je Forum že omogočil velik napredek na področju kriterijev pri identificiranju ključne infrastrukture predvsem v okviru Direktive o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite in pri identificiranju kriterijev za povečanje varnosti in odpornosti interneta, ki so bili strnjeni v dokumentu *Evropska načela in smernice za internetno varnost in stabilnost*[116] ter pri izmenjavi dobrih praks v zakonodaji in še posebno pri vajah kibernetske varnosti. Del prvega stebra akcijskega plana je tudi Evropsko javno-zasebno partnerstvo za prožnost[117] kot vseevropski okvir upravljanja za odpornost infrastruktur IKT, namen partnerstva pa je spodbujanje sodelovanja med javno-zasebnim sektorjem pri strateških vprašanjih politike EU ter predstavlja platformo za vprašanja javne politike ter gospodarskih in tržnih zadev, pomembnih za varnost in odpornost, zlasti za krepitev svetovnega obvladovanja tveganj, deluje pa v okviru ENISE. V okviru prvega sklopa so bili izdelani tudi minimalni sklopi osnovnih zmogljivosti in storitev ter priporočila za sprejetje ustreznih predpisov, da bi lahko

[114] Angl. *Cloud computing* – je smer v IKT-panogi, kjer so računalniška orodja in zmogljivosti na voljo kot storitve, do katerih se dostopa prek interneta; prednosti so predvsem velika fleksibilnost in znižanje stroškov za informacijske tehnologije.
[115] Angl. ***E**uropean **F**orum for **M**ember **S**tates*, EFMS
[116] Angl. *European principles and guidelines for Internet resilience and stability*
[117] Angl. ***E**uropean **P**ublic-**P**rivate **P**artnership for **R**esilience*, EP3R

nacionalni[118] CERT učinkovito delovali in bili hkrati ključni element nacionalnih zmogljivosti za pripravljenost, izmenjavo informacij, usklajevanje in odzivanje. S pomočjo teh usmeritev se naj bi do leta 2012 vzpostavilo omrežje nacionalnih CERT v vseh državah članicah. To omrežje pa bo temelj Evropskega sistema za izmenjavo informacij in opozarjanje[119] – EISAS, ki pa že sodi v okvir drugega stebra in je šele v vzpostavljanju (CIIP – angl. *Implementation activities* – Pillar 1 2011; *Dosežki in naslednji koraki: h globalni kibernetski varnosti* 2011, 7).

EISAS je še v vzpostavljanju, EU in ENISA pa njegovo vlogo vidita predvsem v podpornem smislu, povezovanju med nacionalnimi EISAS in kot pomoč državam članicam brez ISAS struktur.

Shema 4.16: Načrtovana povezovalna vloga EISAS



Prirejeno po EISAS Roadmap 2011, 7.

---

[118] Zaenkrat so le tri države objavile svoje strategije kibernetske varnosti na spletni strani ENISE, in sicer Nizozemska, Francija in Nemčija (*Dutch, French & German Cyber Security Strategies presented* 2011).
[119] Angl. ***E**uropean **I**nformation **S**haring and **A**lert **S**ystem*, EISAS.

V okviru ostalih stebrov so prav tako potekale različne aktivnosti, vendar oprijemljivejših rezultatov še ni. Morda velja izpostaviti le še dokument *Evropska načela in smernice za internetno varnost in stabilnost*, ki je rezultat mednarodnega sodelovanja (tretji steber) ter delovanja EFMS (prvi steber), cilj dokumenta pa je postati skupen okvir za mednarodna prizadevanja na področju dolgoročne odpornosti in stabilnosti interneta.

4.4.1.8 Strategija notranje varnosti EU

Kibernetska varnost omrežij je dobila svoje mesto tudi v notranji varnostni strategiji, saj si EU kot enega od petih strateških ciljev zadaja tudi dvig ravni varnosti za državljane in posle v kibernetskem prostoru, saj je kibernetska kriminaliteta v Evropi v porastu zaradi dobre informacijske razvitosti ter visoke stopnje vključenosti prebivalstva in gospodarstev v internet. Uvodoma se v njej ugotavlja, da je varnost omrežij informacijske tehnologije bistven faktor za delujočo informacijsko družbo, kar je zapisano tudi v Evropski digitalni agendi; brezmejna narava internetnih groženj otežuje odgovor na ogrožanja v okviru omejenih regionalnih pristojnosti znotraj držav članic zato so ključni ukrepi na ravni EU (*Izvajanje strategije notranje varnosti EU: pet korakov k varnejši Evropi* 2010, 4).

Evropska unija tako v svojem (tretjem) cilju k varnejši Evropi, dvigu varnosti prebivalstva in poslovanja v kibernetskem prostoru, načrtuje tri osrednje aktivnosti:

1. **Izgradnja večjih zmogljivosti kazenskega pregona in sodstva.** EU bo v okviru obstoječih zmogljivosti vzpostavila center za kibernetsko kriminaliteto, prek katerega bodo lahko države članice in institucije EU vzpostavile operativne in analitične zmogljivosti za preiskovanje in sodelovanje z mednarodnimi partnerji. Center bo izboljšal ovrednotenje obstoječih ukrepov proti kibernetski kriminaliteti, podpiral razvoj in usposabljanja za dvig zavedanja akterjev kazenskega pregona in sodstva, sodeloval z ENISO in lokalnimi CERT-i. Center za kibernetsko kriminaliteto naj bi postal osrednja institucija za boj proti kibernetski kriminaliteti. Na nacionalni ravni, naj bi države članice poskrbele za poenotenje standardov med policijo, sodniki,

tožilci in forenziki pri preiskovanju in preganjanju kibernetskega kriminal ter vzpostavile lokalne centre za boj s kibernetsko kriminaliteto, ki bodo tesno sodelovale z raziskovalnimi področji in gospodarstvom.

2. **Sodelovanje z gospodarstvom za krepitev zaščite prebivalstva.** Vse države članice naj bi zagotovile preprosto javljanje in sporočanje državljanov o zaznanih kibernetskih grožnjah oz. incidentih ter vzpostavile preprost dostop do informacij[120] o kibernetskih grožnjah in temeljnih ukrepih za preprečevanje le-teh. Sodelovanje javnega in zasebnega sektorja naj bi se krepilo tudi prek Evropskega javno-zasebnega partnerstva za prožnost (EP3R), ki naj bi nadaljeval z razvijanjem inovativnih ukrepov in instrumentov za izboljšanje varnosti, tudi ključne informacijske in mrežne infrastrukture, na evropski in globalni ravni s partnerji.
3. **Izboljšanje zmogljivosti za obravnavanje kibernetskih napadov.** Potrebnih je več ukrepov, vsaka država članica in vsaka evropska institucija naj bi vzpostavila lasten CERT (do konca 2012), ki bi tesno sodeloval z akterji kazenskega pregona pri preventivnih ukrepih in odzivih na dogodke kibernetske kriminalitete. Posamični CERT-i se morajo povezati skupaj z drugimi CERT-i na državni in mednarodni ravni ter tako povečati pripravljenost Evrope na incidente. Tu bo ključna vloga ENISE in njenega Evropskega sistema za izmenjavo informacij in opozoril (EISAS), ki bo vzpostavil mrežo kontaktnih točk med relevantnimi telesi in državami članicami. Kot zadnja točka pa je načrtovana izdelava načrtov za odzivanje v primeru izrednih dogodkov ter redno izvajanje vaj pri odzivanju na incidente ter okrevanja po njih na nacionalni in mednarodni ravni. Tu ima osrednjo vlogo ENISA (*Izvajanje strategije notranje varnosti EU: pet korakov k varnejši Evropi* 2010, 9–10).

4.4.1.9 Vaji Cyber Europe 2010 in Cyber Atlantic 2011

Kljub jasno zaznanim grožnjam pa so projekti, ki bi to problematiko obravnavali sistemsko oz. na višji ravni relativno redki. V novembru 2010 je Evropska unija in

[120] Na ravni EU deluje Program za varnejši internet, v okviru projekta tudi slovenski center za osveščanje o varni rabi interneta in novih tehnologij SAFE-SI in Spletno oko, ki je namenjeno prijavi nelegalnih spletnih strani in vsebin.

njena agencija ENISA izvedla obsežnejšo panevropsko akcijo *Cyber Europe 2010*, katere cilj je bil preizkus odzivanja držav članic na obsežnejši kibernetski napad (*Cyber Europe 2010 – Evaluation Report* 2011). Glavni namen vaje je bil predvsem povečati zavedanje o ranljivosti kibernetskih omrežij ter izboljšati sodelovanje držav članic in povezati njihove institucije, tako znotraj članic kot med njimi ter pridobiti pristojne kontakte ter oceniti sposobnosti odzivanja v primeru kibernetskega napada; izveden je bil neke vrste stresni test za evropske javne institucije (*ENISA Quarterly Review* 2010, 7). Simulacija je predvidevala bistveno zmanjšanje internetnih povezav med sodelujočimi državami, kar bi drastično otežilo dostop institucij, podjetij in javnih ustanov do osnovnih spletnih storitev. Vaja je vključevala le subjekte javne narave, vendar se v ugotovitvah predvideva že naslednjo vajo, ki bi vključevala več subjektov, tudi iz zasebnega sektorja, s tem povečala kompleksnost in simulacijo grožnje še bolj približala realnosti. Na tem primeru je dobro vidna vloga ENISE kot usklajevalnega in posvetovalnega organa za področje Evropske unije (*European principles and guidelines for Internet resilience and stability* 2011) in njena pobuda za priprave na dejanske grožnje.

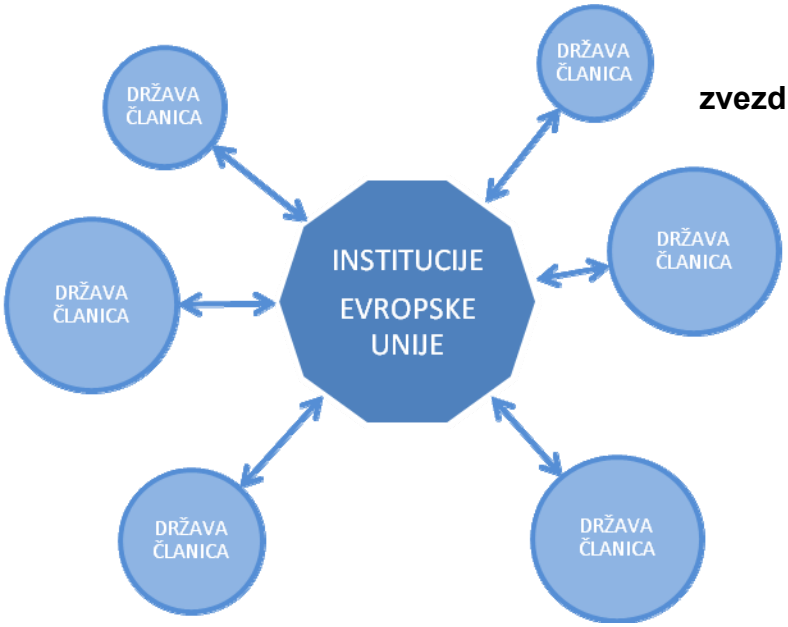
Usklajevala in posvetovalna vloga ENISE v organizacijskem smislu je pomembna, povezanost te agencije z drugimi EU institucijami in z institucijami v posameznih državah članicah (CERT-centri, zasebni sektor itd.) pa nikakor ne sme zavzeti arhitekturnega modela, kjer bi vsi vpleteni akterji komunicirali le prek osrednje agencije. Pomembno usklajevalno vlogo ENISE so potrdile tudi države članice (*Interim findings of CYBER EUROPE* 2010). Raziskave so pokazale, da je najprimernejša oblika povezanosti in komunikacije agencije in držav članic oz. njenih institucij v okviru prepletenega omrežja[121]. Za razliko od zvezdnate strukture, kjer se vse informacije pretakajo prek osrednjega telesa pa prepletena struktura vzpodbuja medsebojno komunikacijo vpletenih zainteresiranih akterjem. Omogočanje skupne rabe informacij, kjer obstaja zaupanje, se odrazi v bistveno večji količini dostopnih in

[121] Pojem *mesh network* je izhaja iz brezžičnih komunikacijskih omrežij (WiFi), kjer so različne oddajne-sprejemne naprave med sabo povezane v prepleteno brezžično okolje, kjer se vsaka od naprav lahko povezuje s katerokoli drugo napravo v njenem dosegu. V primeru izpada posamične povezave se tako prepleteno omrežje samodejno obnovi, informacije prek posebnih protokolov (usmerjevalnih, samodejne konfiguracije) poiščejo novo dostopno točko in promet z njimi steče z le krajšimi prekinitvami.

izmenjanih informacij (*Impact Assesment Part 2* 2009, 45). Različni strukturi povezav sta prikazani na shemah 4.17 in 4.18.

Shema 4.17: Zvezdnata arhitektura modelov povezav

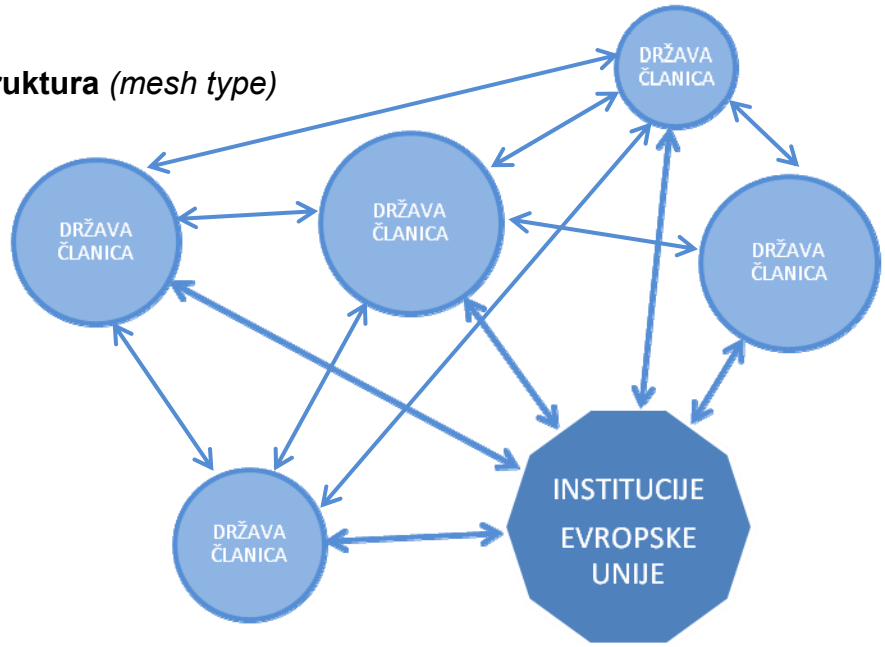
zvezdnata struktura *(star type)*



Prirejeno po *Impact Assesment Part 2* 2009, 45.

Shema 4.18: Prepletena arhitektura modelov povezav

prepletena struktura *(mesh type)*



Prirejeno po *Impact Assesment Part 2* 2009, 45.

Novembra 2011 pa je EU prek svoje agencije ENISA v sodelovanju z ameriškim Ministrstvom za domovinsko varnost opravila vajo z naslovom Cyber Atlantic 2011. Namen vaje je bilo spoznavati načine, prek katerih bi ZDA in EU lahko sodelovali v primeru kibernetskih napadov na njuna ključna informacijska omrežja. Vaja je simulirala prikrit napad, in sicer t. i. napredne trajne grožnje, ki naj bi razkrila pomembne informacije. Druga simulacija pa je predpostavljala prekinitev nadzora nad sistemom za nadzor omrežja za proizvajanje električne energije. Cilj vaje je bil lotiti se novih groženj globalnim omrežjem, od katerih je vse bolj odvisna varnost in blaginja naših družb (*First joint EU-US cyber security exercise conducted* 2011).

4.4.1.10 Konvencija Sveta Evrope o Kibernetskem kriminalu

Naj na koncu poglavja o Evropski uniji naj omenim še dokument, ki ga je že leta 2001 predstavila organizacija Svet Evrope, z naslovom Konvencija o kibernetskem kriminalu. V Konvenciji (*Convention on Cybercrime* 2001) so navedene različne oblike kršitev (po nekaterih nacionalnih zakonodajah tudi kaznivih dejanj) kot so dejanja zoper zaupnost, integriteto in dostopnost računalniških podatkov, kršitve povezane z računalniki, kršitve glede vsebin, kršitve povezane s kratenjem avtorskih in intelektualnih pravic ter druge. Konvencija poda še nekaj predlogov glede arhiviranja podatkovnega prometa, ki bi služilo kot dokazno breme v morebitnih kazenskih postopkih ter vzpostavitev ustrezne zakonodaje in mednarodnega sodelovanja.

Dokument omenjam predvsem iz razloga, ker je eden od prvih mednarodnih dokumentov, ki je podrobneje nagovarjal problem kibernetske kriminalitete in s tem prepoznal kibernetsko okolje kot potencialno grožnjo tudi za KII.

4.4.2 Združene države Amerike

4.4.2.1 Strategija za varen kibernetski prostor

Onkraj Atlantika so svojo Strategijo za varen kibernetski prostor sprejeli že leta 2003. V njej prepoznavajo pet prioritet, ki naj bi služile pri preventivi, odvračanju in zaščiti

pred kibernetskimi napadi ter vzpostavile proces zmanjševanja potencialne škode in pospeševanja obnove po napadih. Prioritete za varnost kibernetskega prostora so:

I. državni varnostni sistem za odzivanje na izzive kibernetskega prostora,
II. državni program za zmanjševanje varnostnih groženj in pomanjkljivosti v kibernetskem prostoru,
III. državni program za zavedanje in pripravo za kibernetsko varnost,
IV. zaščita kibernetskega medvladnega prostora in
V. sodelovanje na področju državne varnosti in mednarodne kibernetske varnosti (*The National Strategy to Secure Cyberspace* 2003).

Že pred skoraj desetletjem je tako obstajalo močno soglasje, da je kibernetski prostor in s tem posledično varnost omrežij KII, ki so del tega prostora, ključno za varnost naroda kot celote. Zaradi nenehnih sprememb in potrebnih prilagoditev državnega aparata je predsednik Obama v 2009 naročil pregled ukrepov na področju kibernetske varnosti, ki se je odrazil v dokumentu Pregled politike kibernetskega prostora.

4.4.2.2 Pobuda za celostno obravnavo kibernetske varnosti

Iz pregleda aktualne politike kibernetske varnosti je v okviru Sveta za nacionalno varnost[122] in Sveta za domovinsko varnost[123] v Beli hiši nastal nov dokument Pobuda za celostno obravnavo kibernetske varnosti s katero želijo ZDA opredeliti nove smernice na tem področju in katere sklepni del bo nova strategija za varnost kibernetskega prostora. Dokument je nastajal ob zavedanju, da je bistveno okrepiti tudi druga področja in zmogljivosti izvršne oblasti znotraj področij kazenskega pregona, obveščevalnih dejavnosti, obrambnega področja, preiskovanja kriminalnih dejavnosti, zbiranja informacij, procesiranja, analiziranja ter zagotavljanja informacij ključnih za prizadevanja na področju kibernetske varnosti. Osrednji cilji te pobude so:

1. **Vzpostavitev obrambne linije proti sodobnim neposrednim grožnjam** z izboljšanim zavedanjem o trenutnih situacijah, omrežnih ranljivostih, grožnjah

[122] Angl. ***N**ational **S**ecurity **C**ouncil* (NSC)
[123] Angl. ***H**omeland **S**ecurity **C**ouncil* (HSC)

in dogodkih na zvezni ravni ter lokalno z državnimi vladami in partnerji iz zasebnega sektorja ter sposobnostjo za hitro ukrepanje pri zmanjševanju ranljivosti in preprečevanju vdorov.

2. **Obraniti se pred celo vrsto groženj** z izboljšanjem protiobveščevalnih zmogljivosti in povečevanjem varnosti dobavnih verig za ključne informacijske tehnologije.
3. **Okrepiti prihodno okolje kibernetske varnosti** z razširitvijo izobraževanj o kibernetski varnosti, usklajevanjem in usmerjanjem raziskovalnih in razvojnih dejavnosti na zvezni ravni ter opredeliti in razviti strategijo za odvračanje sovražnih ali zlonamernih dejavnosti v kibernetskem prostor (*The Comprehensive National Cybersecurity Initiative* 2011, 2).

Vseskozi pa se naj bi si vlada ZDA tudi prizadevala za ohranitev zasebnosti in državljanskih svoboščin pri izvajanju ukrepov kibernetske varnosti. Z namenom transparentnega[124] izvajanja politike so tudi vsi dokumenti javno dostopni in večina jih ima povzetke[125] za državljane.

V Pobudi za celostno obravnavo kibernetske varnosti so si tako ZDA zastavile več podrobnejših segmentov in ciljev, na katerih bodo izvajali ukrepe, velika večina se jih nanaša samo na raven zveznih institucij ZDA, ti ukrepi so:

- Upravljanje zveznega omrežja institucij kot enotno omrežje z verodostojnimi točkami dostopa do interneta.
- Uvajanje sistema senzorjev[126] za odkrivanje vdorov.
- Prizadevanja za uvedbo sistemov za preprečevanje vdorov.

---

[124] Ravno to področje je eno od bolj delikatnih pri zagotavljanju varnosti, saj razkritje ukrepov usmerja napadalca tako, da se jim izogne.

[125] Podobno prakso uveljavlja tudi EU, ki ob obsežnejših resolucijah, strategijah in drugi dokumentaciji izdaja tudi kratke povzetke in bistvene sestavine dokumentacije v skrajšani obliki.

[126] Vpeljan je bil t. i. sistem za odkrivanje vdorov EINSTEIN, ki ga je razvil US-CERT, ki spremlja omrežne prehode vladnih služb in agencij v ZDA ter odkriva in prepoznava nedovoljen promet. Einstein je definiran kot program za avtomatiziran proces zbiranja, povezovanja, analiziranja in izmenjave informacij o računalniški varnosti na ravni zveznih institucij ZDA; namen programa pa je vzpostavitev zavedanja (skoraj v realnem času) zveznih organov o nevarnostih za njihovo infrastrukturo in posledično možnostjo hitrega ukrepanja (*Privacy Impact Assessment EINSTEIN Program* 2004, 4). Danes je v uporabi že EINSTEIN 2, ki ima sposobnost samodejnega posredovanja informacij o zaznanih grožnjah in v načrtu je že EINSTEIN 3, ki naj bi imel že sposobnost preprečevanja napadov (*Homeland Security seeks cyber counterattack* system 2008). Drugi priznani avtorji (Marcus J. Ranum, priznan strokovnjak varnostnih sistemov) pa problematizirajo tovrsten pristop k zagotavljanju varnosti z več vidikov, tako z vidika obsega kot načinov zagotavljanja varnosti. Več informacij je na voljo na njegovi spletni strani. (http://www.ranum.com/, 8. oktober 2011).

- Usklajevanje in preusmerjanje raziskav in razvoja.
- Povezovanje centrov za kibernetsko varnost za dvig zavedanja o razmerah.
- Razvijanje in izvajanje kibernetskega protiobveščevalnega načrta.
- Povečevanje varnostnih mehanizmov na tajnih omrežjih.
- Povečati izobraženost o kibernetskih grožnjah.
- Opredeljevanje in razvijanje tehnologij, strategij in programov naslednjih generacij.
- Opredeljevanje in razvijanje trajnih strategij in programov odvračanja.
- Razvijanje razpršenih globalnih dobavnih verig za lažje obvladovanje tveganja.
- Določitev vloge zvezne vlade pri zagotavljanju kibernetske varnosti na področju ključne informacijske infrastrukture.

(*The Comprehensive National Cybersecurity Initiative* 2011, 2–5).

Osrednjo operativno vlogo pri implementaciji Strategije za varen kibernetski prostor ima US-CERT[127], ki deluje v okviru Divizije za državno kibernetsko varnost[128] znotraj Urada za kibernetsko varnost in komunikacije[129], ki je del Direktorata za zaščito in programe[130] v okviru Ministrstva za domovinsko varnost[131], naloga US-CERT pa je operativno izvajanje nalog v okviru divizije, ki so bile nanjo prenesene s strani urada in ministrstva. Znotraj Direktorata pa deluje še Povezovalni center za državno kibernetsko varnost in komunikacije[132], ki ima predvsem povezovalno vlogo med zvezno, državno in lokalno ravnjo ter zasebnim sektorjem.

[127] Angl. ***U**nited **S**tates **C**omputer **E**mergency **R**eadiness **T**eam*, več informacij je dostopnih na njihovi spletni strani (http://www.us-cert.gov/, 8. oktober 2011).
[128] Angl. ***N**ational **C**yber **S**ecurity **D**ivision*
[129] Angl. ***O**ffice of **C**ybersecurity and **C**ommunications* (CS&C)
[130] Angl. ***N**ational **P**rotection & **P**rograms **D**irectorate*
[131] Angl. ***D**epartment of **H**omeland **S**ecurity*, več informacij je dostopnih na njihovi spletni strani (http://www.dhs. gov/index.shtm, 8. oktober 2011).
[132] Angl. ***N**ational **C**ybersecurity and **C**ommunications **I**ntegration **C**enter* (NCCIC)

4.4.2.3 Strategija za delovanje v kibernetskem prostoru

Znotraj Ministrstva za obrambo[133] v okviru Združenih bojnih poveljstev[134] znotraj Strateškega poveljstva[135] pa se je ustanovilo Kibernetsko poveljstvo[136], čigar namen je centralizirati poveljevanje kibernetskih operacij, organizirati in povezati obstoječa kibernetska sredstva in sinhronizirati obrambo vojaških omrežij. V okviru tega poveljstva je julija 2011 nastala tudi Strategija za delovanje v kibernetskem prostoru[137], ki predvideva več področij delovanja v kibernetskem prostoru, ključno pa je da kibernetski prostor prepoznava kot operativno domeno s katero je mogoče organizirati, vežbati in opremiti ministrstvo za polno izkoriščanje prednosti kibernetskega prostora in s tem učinkovitejše izvajanje svojih nalog. V okviru strategije namerava ministrstvo uporabiti nove obrambne koncepte pri varovanju svojih omrežij in sistemov ter se povezati z drugimi ameriškimi ministrstvi, agencijami in zasebnim sektorjem ter zgraditi trdna zavezništva z zavezniki in s tem ojačati kolektivno kibernetsko varnost (*Strategy for Operating in Cyberspace* 2011).

Pod okriljem Kibernetskega poveljstva naj bi bilo tako po nekaterih informacijah kar 90.000 osebja dobili pa naj bi tudi prvega »kibernetskega generala« (*US appoints first cyber warfare general* 2011). Prav tako se je razvila razprava na temo problematike dostopnosti novega profesionalnega osebja znotraj Kibernetskega poveljstva, Franz (2011, 93–94) tako pravi, da bo za učinkovito kibernetsko vojskovanje in obrambo potrebno razviti novo varnostno kulturo s strani strokovnjakov, saj naj bi se civilno upravljanje z omrežji močno razlikovalo od upravljanja in zaščite v času spopadov ter še posebno ravni pomembnosti, ki bi jo taka obramba lahko imela za celotno omrežje in druge potencialne posledice. Drugi avtorji (Hamilton v Van Derwerken in Ubell 2011, 47) prav tako izpostavljajo resne izzive pred katerimi je varnost KII prav zaradi pomanjkanja visoko usposobljenih strokovnjakov za kibernetsko varnost.

---

[133] Angl. ***D**epartment **o**f **D**efense*
[134] Angl. ***U**nified **C**ombatant **C**ommand*
[135] Angl. ***US Strat**egic **Com**mand* (STRATCOM)
[136] Angl. ***US Cyber Com**mand* (USCYBERCOM), v okviru poveljstva pa delujejo še kibernetska poveljstva kopenske vojske, marincev in druga (***Ar**my **Cyber** Command* - ARCYBER, ***Mar**ine **For**ces **Cyber** Command* - MARFORCYBER).
[137] Angl. *DoD **S**trategy for **O**perating in **C**yberspace* (DSOC)

Ne glede na problematičnost dokazovanja izvora napada in odgovornosti posameznika, pa je presenetljivo stališče ZDA, da naj bi v primeru kibernetskih napadov, ki bi imeli za posledico smrt državljanov ZDA ali večjo škodo, uničenje ali prekinitev večjega obsega kot praviloma izhaja iz vojaškega napada, imele pravico se na tak napad odzvati s fizično, vojaško silo. Argumenti za tako odločitvijo izhajajo iz stališč, da je zahtevnejše napade, ki bi ogrožali celotno državo ali večje sisteme, možno izvesti le ob podpori države agresorke. Ameriško ministrstvo za obrambo pa je večkrat izpostavilo, da beleži take napade že od leta 2003 ter da so napadi čedalje pogostejši in čedalje bolj prefinjeni. Nejasnost in odsotnost regulacije na tem področju dopuščajo možnosti različnih interpretacij, saj obstoječi predpisi in okviri spopadanja ne predvidevajo spopadov na kibernetski ravni, akterja napada (in tudi obseg posledic) pa je izredno težko določiti in dokazati (*Washington moves to classify cyber-attacks as acts of war* 2011; *Cyber Combat: Act of War* 2011).

Že sama strukturiranost in razvejanost institucij[138] s področja kibernetske varnosti v ZDA ponazarja pomembnost področja za politiko in širšo javnost, ki ga navedene institucije obravnavajo.

4.4.2.4 Mednarodna strategija za kibernetski prostor

Zanimivo in pomenljivo pa je dejstvo, da tudi velesile spoznavajo, da je zagotavljanje varnosti v kibernetskem omrežju prevelik izziv za posamezno državo, čeprav z aparatom in sredstvi na ravni ZDA.

Zato so ZDA v maju 2011 prvič predstavile *Mednarodno strategijo za kibernetski prostor*[139]*,* ki predstavlja koncepte in ideale v množici diplomatskih, tržnih in varnostnih izzivov katerim je globalni informacijski prostor izpostavljen. Strategija tako ni dokument o varnosti na internetu ali varnosti KII, vendar predstavlja širši okvir predpisov in pravil na splošnejši ravni. Namen je tako vzpostaviti kibernetsko okolje vredno zaupanja, ki ostaja odprt za poslovanje, vzpodbuja inovativnost in sprejema podjetništvo. Za doseganje teh ciljev pa je potrebno ohranjati kibernetski prostor

[138] Ob vseh naštetih delovnih telesih se poraja dvom v racionalnost take razvejanosti, saj so področja in zadolžitve organov podobni in bi optimizacija le-teh ameriškim davkoplačevalcem lahko prihranila marsikakšen dolar.
[139] Angl. *International Strategy for Cyberspace*

varen, zanesljiv in prožen, povečati pravna sredstva in vladavino prava v kibernetskem prostoru in poudarjati mednarodno sodelovanje za boj proti kibernetskem kriminalu. Treba je razvijati mednarodne standarde in ohranjati internetne trge kar se da odprte prek meja lokalnih interesov, hkrati pa ohranjati osnovne človekove pravice, zasebnost in svoboščine na najvišji možni ravni (*Translating the U.S. International Cyber Strategy Into Action* 2011; *International Strategy for Cyberspace* 2011)

4.4.2.5 Vaje Cyber Storm

Tudi ZDA so na področju kibernetske varnosti omrežij že izvedle nekaj vaj v okviru svojih institucij. Vaje naj bi izboljševale pripravljenost javnega in zasebnega sektorja na kibernetske napade in se izvajajo na dvoletni ravni, prva vaja pa je bila izvedena že februarja 2006, z naslovom Kibernetska nevihta I[140].

Namen teh vaj je pripraviti akterje na izvajanje naslednjih aktivnosti:

- preučiti organizacijsko sposobnost za priprave, zaščito in odziv na kibernetske napade in posledične učinke,
- opravljati strateško odločanje in medagencijsko koordinacijo pri odzivanju na incidente v skladu s politiko in predpisanimi postopki na državni ravni,
- utrditi razmerja pri izmenjavi informacij in komunikacijskih poti za zbiranje, odzivanje, obnovo ter razglašanje zavedanja o razmerah v primeru kibernetskih napadov ter
- preučiti načine in procese, prek katerih bi lahko uspešno delili občutljive informacije preko meja sektorjev, ne da bi s tem ogrožali državne ali zasebne varnostne interese (*Cyber Storm: Securing Cyber Space* 2011).

Do sedaj so bile opravljene že tri vaje (2006, 2008 in 2010) vsaka nadaljnja pa nadgradi zahtevnost in kompleksnost ogrožanja v skladu z ugotovitvami predhodnih

[140] Angl. *Cyber Storm I*

vaj. Posebnost ameriških vaj je v tem, da že vključujejo tudi mednarodne partnerje ter množico zasebnih[141] institucij z različnih področij.

Prav tako je zanimiv tudi projekt, ki želi dvigniti splošno zavedanje prebivalstva o kibernetski varnosti in poteka v okviru meseca za dvigovanje zavedanja o kibernetski varnosti, ki se odvija vsak oktober; prav tako pa vzporedno (od 2009) teče kampanja za osveščanje prebivalstva Stop.Think.Connect[142]. Poleg vaj in aktivnosti na državni ravni pa poteka še množica vzporednih projektov, denimo v okviru agencije FEMA[143] na področju brezplačnega izobraževanja prebivalstva o kibernetski varnosti, v okviru US-CERT pa izobraževanja za IT-specialiste in različne ravni zasebnega sektorja.

ZDA so tradicionalno zelo povezane z zasebnim sektorjem, zato tudi javne institucije precejšen del zahtevnih raziskovalnih projektov prepustijo zasebnim »neprofitnim« organizacijam in možganskim centrom, kljub lastni Agenciji[144] za to področje. V sodelovanju z Agencijo pa delujejo različne svetovalne korporacije, ena od bolj znanih je MITRE[145]. Pod okriljem te korporacije, čeprav izven formalne strukture pa deluje skupina neodvisnih znanstvenikov (delujejo tudi v okviru Zveze ameriških znanstvenikov[146]) pod nazivom JASON, ki ima svetovalno vlogo zvezni vladi ZDA na področju znanosti in tehnologije. V tem poglavju izpostavljam to skupino predvsem zato, ker je Ministrstvo za obrambo ZDA zaprosilo skupino JASON za preučitev teorije in prakse na področju kibernetske varnosti. Namen tega preučevanja je odkrivanje temeljnih načel, ki bi omogočile bolj znanstven pristop k preučevanju

---

[141] Visoka raven sodelovanja z zasebnim sektorjem je predvsem posledica dejstva, da velika večina vladne komunikacije poteka prek omrežij v lasti in upravljanju zasebnega sektorja. Prav tako se vlada skoraj izključno zanaša tudi na strojno in programsko opremo, storitve in vzdrževanje s strani zasebnih proizvajalcev. Gre torej za skoraj povsem prepleteno javno infrastrukturo z zasebno infrastrukture. Nekateri (McConnell v Jensen 2010, 1534) ocenjujejo ta delež kar na 98%.

[142] Projekt je osnovan na treh osrednjih načelih, ki s preprostimi nasveti dviguje splošno raven kibernetske varnosti v državi, ta načela so:
1. USTAVI SE: nastavi varna gesla, prenehaj širiti preveč zasebnih informacij, zaupaj lastnemu občutku, tudi na medmrežju se vedi primerno.
2. POMISLI, preden deliš z vsemi informacijo, kako lahko tvoja internetna dejanja vplivajo na tvoje vsakdanje življenje, ne klikaj na nepoznane povezave, s kom komuniciraš.
3. POVEŽI SE: prek varnih omrežij, z ljudmi, ki jih poznaš, bodi pozoren na potencialne grožnje.
Uradna spletna stran projekta je na voljo na: http://www.dhs.gov/files/events/stop-think-connect.shtm (8. oktober 2011).

[143] Angl. ***F**ederal **E**mergency **M**anagement **A**gency*, uradna spletna stran je na voljo na: http://www.fema.gov/ (8. oktober 2011).

[144] Angl. ***D**efense **A**dvanced **R**esearch **P**rojects **A**gency* (DARPA)

[145] Kot zanimivost lahko navedem, da je bila mitre.org prva domena, ki je dobila končnico ».org«, in sicer že leta 1985.

[146] Angl. ***F**ederation of **A**merican **S**cientist* (FAS)

kibernetske varnosti in vpeljavo znanstvenih metod. JASON je tako leta 2010 izdelal poročilo, ki poskuša odkriti še druge dimenzije kibernetske varnosti poleg obstoječe zaznavno-spoznavne ravni preučevanja, i. e. empirije.

4.4.3 NATO

Tudi NATO se je odzval na izzive, ki jih sodobno okolje prinaša mednarodnim organizacijam. V 2008 so ustanovili Center odličnosti za sodelovanje pri kibernetski obrambi[147], ki ga trenutno podpirajo samo nekatere države članice zavezništva. Osrednja vloga CCD COE je izboljšati sposobnosti, sodelovanje in izmenjavo informacij med članicami zavezništva ter partnerji za izboljšanje kibernetske obrambe. Gre torej za center, ki naj bi prek izobraževanj, razvoja in raziskav izboljševal pripravljenost na kibernetske incidente.

4.4.3.1 Center odličnosti

Center naj bi deloval v okviru štirih stebrov, od katerih je za moje delo najpomembnejši zadnji, zaščita KII. NATO prepoznava sodobno družbo kot omreženo, v kateri delujejo kibernetski kriminalci, nedržavni hekerji, hekerski aktivisti (t. i. *hacktivists*) in drugi z IKT opremljeni akterji. NATO kibernetski prostor prepoznava kot vzporedno digitalno bojišče prihodnjih (tudi sedanjih) konfliktov in ugotavlja, da bo v prihodnosti uglašenost napadov s konvencionalnimi orožji in napadov s kibernetskimi orodji postala standard, izključno kibernetski napadi pa prav tako ne bodo izostajali. NATO še izpostavlja strateški izziv, ki ga uporaba IKT-tehnologij predstavlja zaščiti informacij, saj se zlonamerneži lahko poslužujejo različnih tehnik zbiranja podatkov[148] in z izredno nizkimi stroški lahko dosegajo dobre rezultate, tehnologijo uporabljajo za komunikacijo, zbiranje sredstev in komunikacijo z

[147] Angl. ***C**ooperative **C**yber **D**efence **C**entre **o**f **E**xcellence* (CCD COE)
[148] Eno od njih je recimo OSINT (angl. ***O**pen **S**ource **Int**elligence*), kjer lahko s pomočjo spletnih orodij iz javno dostopnih informacij izdelamo precej dobro obveščevalno oceno.

javnostmi, pri čemer so izredno učinkoviti ter se praktično nevidno prepletejo s civilno družbo (*NATO Cooperative Cyber Defence* 2011).

NATO je kibernetske grožnje prepoznal tudi na najvišji ravni v novem Strateškem konceptu, kjer ugotavlja, da kibernetski napadi postajajo čedalje pogostejši, bolje organizirani in povzročijo čedalje večjo škodo vladnim službam, podjetjem in tudi ključni informacijski infrastrukturi ter lahko ogrozijo nacionalno ali evroatlantsko blaginjo, varnost in stabilnost. Kot potencialne vire ogrožanja NATO prepoznava tuje vojaške in obveščevalne sile, skupine organiziranega kriminala ter teroristične ali ekstremistične skupine (*Active Engagement, Modern Defence* 2010, 4).

Hkrati pa je v Lizbonski izjavi po vrhu v Lizboni leta 2010, NATO sprejel zavezo po ohranitvi nemotenega dostopa do medmrežja in neokrnjenost ključnih sistemov, kar naj bi dosegli z vključitvijo kibernetskih razsežnosti sodobnih konfliktov v obrambno doktrino ter izboljšanjem kapacitet za odkrivanje, oceno, obrambo in okrevanje po morebitnem kibernetskem napadu proti KII za NATO. Način za doseganje teh načrtov je v okviru CCD COE in vzpostavitvijo zavezniških sposobnosti za odzivanje na računalniške incidente[149] ter združevanjem vseh teles znotraj osrednje kibernetske zaščite; hkrati pa vzpostavljati centre v državah zaveznicah ter optimizirati sodelovanje, izmenjavo informacij ter medsebojno povezljivost posameznih elementov. Izpostavljajo tudi sodelovanje z drugimi mednarodnimi akterji kot sta EU in Združeni narodi (*Lisbon Summit Declaration* 2010).

V 2011 je nato sprejel področno politiko kibernetske obrambe z naslovom Zaščitimo omrežja, kjer so povzeta izhodišča iz strateškega koncepta in Lizbonske izjave ter dodani ukrepi. NATO bo pozornost kibernetske obrambe usmeril predvsem v:

- zaščito struktur in načrtovalnih procesov, ki bodo omogočili nemoteno delovanje kolektivne obrambe in kriznega delovanja tudi v času kibernetskih napadov;
- preventivo, odpornost in obrambo ključnih sredstev za NATO in zaveznice,
- razvil čvrste obrambne zmožnosti ter centraliziral zaščito zavezniških omrežij,
- razvil minimalne standarde za države zaveznice in njihova omrežja, ki so za delovanje zavezništva ključna,

[149] Angl. ***N**ATO **C**omputer **I**ncident **R**esponse **C**apability* (NCIRC)

- zagotavljal podporo zaveznikom pri doseganju minimalne ravni kibernetske obrambe in zmanjševal izpostavljenost njihovih ključnih informacijskih sistemov kibernetskim grožnjam ter
- sodeloval s partnerji, mednarodnimi organizacijami, zasebnim sektorjem in raziskovalnimi dejavnostmi (*Defending the networks* 2011).

4.4.3.2 Vaje Cyber Coalition

Tudi NATO prepoznava pomembnost vaj na področju kibernetske varnosti, saj z njimi testira in potrjuje svoje koncepte, postopke, sisteme in taktike delovanja. Vaje prav tako dvigujejo raven medsebojnega sodelovanja in preoblikujejo obrambne in varnostne strukture v bolj odzivne na tem področju.

Zadnja vaja je bila opravljena leta 2010 in je v simulaciji vključevala množične sočasne kibernetske napade na NATO institucije in države članice. Namen vaje je bilo preveritev proceduralnega delovanja institucij in množico tehničnih elementov in je nadgradila predhodni vaji iz 2008 in 2009. V letu 2010 pa je NATO in njegov CCD COE sodeloval tudi v mednarodni vaji *Baltic Cyber Shield* s švedskimi vladnimi institucijami. Namen sodelovanja pa je bil pridobiti boljši vpogled v zapleteno mednarodno kibernetsko okolje in dodatne ovire, ki se porajajo pri mednarodnem sodelovanju ter izboljšati sposobnosti zavezništva za delovanje v tem okolju *(»Cyber Coalition 2010« to exercise collaboration in cyber defence* 2011).

Kot je mogoče razbrati iz množice dokumentov, ki se dotikajo kibernetske varnosti, se tudi NATO dobro zaveda te dimenzije ogrožanja, ukrepi pa so podobni kot na drugih ravneh. Zanimiva razprava (Myrli 2011, 89–90) pa je bila sprožena tudi okoli interpretacije 5. člena Severnoatlantske pogodbe, saj je ukrepanje proti agresorju oz. akterju, ko je njegova identiteta lahko nejasna, izredno oteženo. Tudi v primeru, ko je identiteta jasno dokazana, pa se poraja vprašanje katera vrsta kibernetskega napada je lahko interpretirana kot dejanje napada na državo članico ter kako ravnati v primeru, ko je agresor dejansko skupina posameznikov izven držav članic, ki ni nujno povezana z njeno vlado. Drugi avtorji (Yost 2010, 509–511) ocenjujejo zastraševalno in preventivno vlogo NATO konceptov brez jasne opredelitve dejanja napada kot

omejeno, poleg tega pa sama narava kibernetskega prostora daje veliko prednosti napadalcu, kar je še dodaten izziv. Torej se tudi NATO podaja na področje, kjer bodo odločitve in ukrepi izredno zahtevni.

4.4.4 Druge institucije

Mednarodna telekomunikacijska zveza je najstarejša institucija s področja komunikacij, saj je bila ustanovljena že leta 1865 (kot Mednarodna telegrafska zveza). Združeni narodi so jo pod svoje okrilje umestili kot posebno agencijo za informacijsko in komunikacijsko tehnologijo. V okviru zveze in njenega sektorja za razvoj (ITU-D) danes deluje Divizija za uporabo IKT in kibernetsko varnost, ki promovira uporabo IKT-tehnologij po svetu (predvsem manj razvitem) in varno uporabo medmrežja. ITU organizira na svetovni ravni srečanja za informacijsko družbo[150], izdaja publikacije v pomoč državam v razvoju ter v splošnem sledi cilju povezovanja vseh ljudi z IKT.

Morda najpomembnejša aktivnost ITU na področju kibernetske varnosti pa je bila ustanovitev Globalne agende za kibernetsko varnost[151], ki predstavlja okvir za mednarodno sodelovanje s ciljem izboljšati zaupanje in varnost v informacijski družbi. GCA tako vzpodbuja sodelovanje z in med relevantnimi partnerji ter podpira delovanje v okviru obstoječih institucij, v želji preprečitve podvajanja le-teh (*Global Cybersecurity Agenda* 2011).

Agenda tako predpostavlja ukrepe na petih ravneh:

- zakonodaja (organizirani kriminal na spletu je v porastu predvsem zaradi pomanjkljive zakonodaje, ki onemogoča oz. otežuje ustrezno kazensko preganjanje tovrstnega kriminala; dodatna težava je brezmejna narava groženj in neusklajenost mednarodne zakonodaje na tem področju; ker je internet mednarodno orodje, je treba tudi zakonodajo na tem področju urejati na globalni ravni);

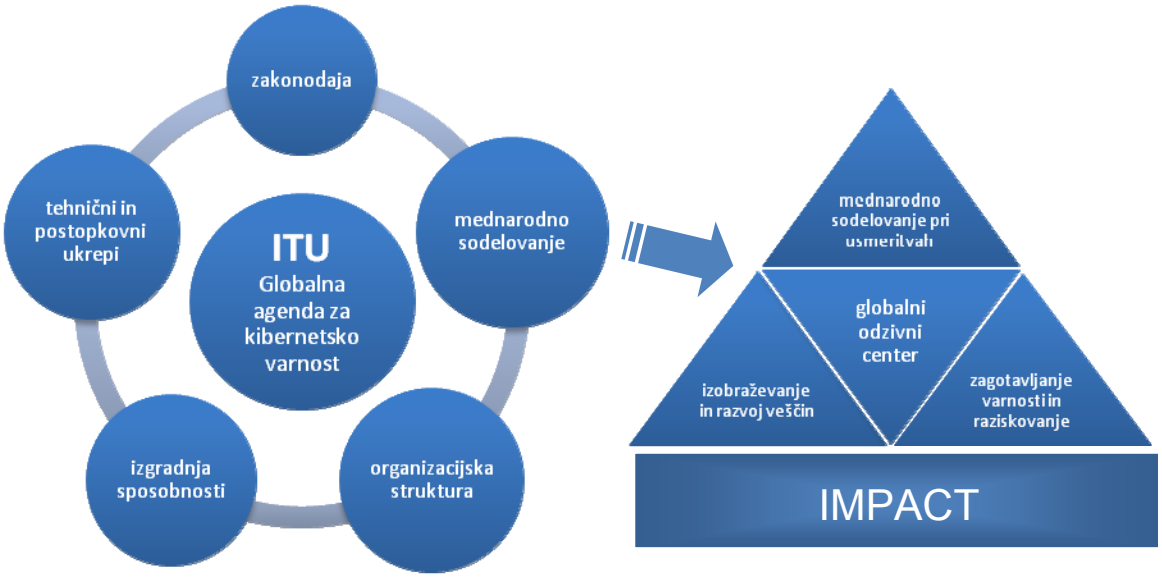
[150] Angl. ***W**orld **S**ummit on the **I**nformation **S**ociety* (WSIS)
[151] Angl. ***G**lobal **C**ybersecurity **A**genda* (GCA)

- tehnični in postopkovni ukrepi (izkoriščanje pomanjkljivosti v programski opremi v zlonamerne namene je podlaga za nepooblaščene vstope in spremembe, kar ogroža zaupnost, istovetnost in neokrnjenost IKT-omrežij in sistemov; tovrstne grožnje bi lahko imele resne posledice pri varovanju KII),
- organizacijska struktura (opazovalni in opozorilni sistemi so nujni pri odzivanju na kibernetske napade, prav tako je ključna tudi dobra izmenjava informacij znotraj in med organizacijami; IMPACT),
- izgradnja sposobnosti (ključni izziv je osveščanje končnega uporabnika za varno uporabo IKT, saj se s tem dviguje splošna raven varnosti v vseh segmentih uporabe IKT) in
- mednarodno sodelovanje (prav tako kot na področju zakonodaje, je potrebno za uspešno spopadanje z izzivi kibernetske grožnje vključiti vse akterje, zato je mednarodno sodelovanje ključno) (*Global Cybersecurity Agenda* 2011).

V okviru organizacijske strukture je ITU oblikovala tudi Mednarodno večstransko partnerstvo proti kibernetskim grožnjam[152], ki je največja svetovna institucija, ki združuje vlade, raziskovalne institucije, zasebni sektor, mednarodne institucije in možganske centre iz vsega sveta na področju kibernetske varnosti. Njena naloga pa je združevanje potencialov vseh deležnikov v boju proti omrežnim nasprotnikom za dvig kibernetske varnosti. IMPACT ima osrednjo vlogo pri analiziranju, zbiranju in razširjanju informacij v zvezi s kibernetskim ogrožanjem v realnem času, zgodnjem opozorilnem sistemu in nujnemu odzivanju na kibernetske grožnje ter izobraževanju in razvoju znanj na tehnični, zakonodajni in pravni ravni kibernetske varnosti (*IMPACT Alliance* 2011).

[152] Angl. ***I**nternational **M**ultilateral **P**artnership **A**gainst **C**yber **T**hreats* (IMPACT), sedež institucije je v kraju z zanimivim imenom Cyberjaya, ki je neke vrste silicijeva dolina Malezije.

Shema 4.19: Prepletanje vloge ITU in GCA z IMPACT



Prirejeno po IMPACT Alliance, 2011.

Kot zanimivost lahko dodam, da ITU aktivno deluje tudi na področju bolj ranljivih skupin, v ta namen je že leta 2008 vzpostavila iniciativo za zaščito otrok na medmrežju, ki se odraža tudi v lokalnih projektih, kakršen je tudi slovenski SAFE.SI.

Prav tako je tudi Organizacija za gospodarsko sodelovanje in razvoj aktivna na področju zaščite KII in je tudi sama izdala priporočila na dveh ravneh za to področje, opredelila je ukrepe na nacionalni ravni in ukrepe na mednarodnih ravni, niso pa posebej izpostavljeni ukrepi za zaščito pred kibernetskimi grožnjami (*OECD Recommendation of the Council on the Protection of Critical Information Infrastructures* 2008).

Seveda je aktivnosti na področju kibernetske varnosti mnogo tudi v okviru drugih institucij in raziskovalnih ustanov, vse večje imajo svoje oddelke oz. sektorje, ki se ukvarjajo s to pomembno problematiko. Vendar ni namen te naloge, da bi omenjal vse.

Zanimive pa so relacije do azijskih držav, ki jih je potrebno osvetliti predvsem z vidika izredne aktivnosti ter v luči potencialnih nasprotnikov. Dostopnost do informacij o aktivnostih azijskih držav je sorazmerno slaba, predvsem zaradi jezikovne in pisne

pregrade, zato so informacije težko dostopne. Kljub temu pa določene organizacije, ki sistematično preučujejo novice s tega področja in jih posredujejo zahodni javnosti, tokrat pa izpostavljam samo Kitajsko. Po njihovih ugotovitvah (*China's Cyberwarfare* 2011, 2–5) in izjavah kitajskih uradnikov je kibernetsko vojskovanje za Kitajsko najpomembnejše področje sodobnega vojskovanja in je tako postavljeno celo pred jedrsko varnost. Kitajska se je za tak pristop odločila predvsem z namenom zmanjševanja zaostanka za tehnološko razvitostjo ZDA, ki je nekakšna ugodnejša bližnjica do doseganja primerljive moči. Poleg tega poskuša Kitajska unovčiti še eno primerjalno prednost pred ZDA, to je njen kadrovski potencial[153], saj poskuša vplesti v delovanje celotno populacijo[154] in moč množic uporabiti za spletno mobilizacijo, spletno propagando, izgradnjo kibernetskih sredstev, novačenje aktivistov in zasebnih podjetij, kar močno razširi potencialne možnosti za kibernetski napad na nasprotnika. Podobno opažajo tudi drugi avtorji (Greengard 2010, 21), ki poleg navedenih prednosti izpostavljajo še proizvodnjo programske in strojne opreme v azijskih državah, ki jo uporabljajo uradniki in institucije v ZDA, s čimer se odpira dodatno okno priložnosti za nameščanje zlonamerne opreme ali kode in s tem olajšanje izvedbe potencialnih napadov. Še en vidik je dobava rezervnih delov v primeru množične okvare, saj so ZDA zaradi preseljene proizvodnje praktično odvisne od uvoza določenih tehnoloških komponent.

4.4.5 Standardi informacijske varnosti in OSI model

Pri opredeljevanju kibernetske varnosti so se v zadnjem času začeli uveljavljati tudi različni tehnični standardi, ki predpisujejo različne varnostne tehnike, ki omogočajo varnejše poslovanje in zmanjšujejo verjetnost uspešnega kibernetskega napada. Izpostavil bom le nekatere najbolj poznane v okviru Mednarodne organizacije za

[153] Kar ni novost, saj je bila podobna taktika uporabljena že s strani Mao Zedonga.
[154] Za populacijo, ki je zelo aktivna na medmrežju, se pogosto uporablja tudi angleški izraz *netizen*, kar je skovanka besed »cit**izen«** (državljan) in »inter**net«**, sinonim je tudi angleška beseda *cybercitizen*.

standardizacijo[155], ameriškega Državnega inštituta za standarde in tehnologijo[156] ter Projektne skupine za internetno tehnologijo.

V okviru standarda ISO 27001, ki je del skupine standardov ISO 27000, so določene zahteve za vzpostavitev, izvajanje, upravljanje, spremljanje, pregledovanje, vzdrževanje in izboljšanje dokumentiranja vodenja varovanja informacij v okviru celotne organizacije poslovnih tveganj. Glavno načelo sistema upravljanja z informacijsko varnostjo[157] je potreba po oblikovanju, vzdrževanju in izvajanju skladnega sklopa politik, postopkov in sistemov za upravljanje tveganj pri upravljanju s podatki, s čimer se zagotovi sprejemljivejše ravni tveganja za varnost podatkov. Standard določa zahteve za izvajanje varnostnih ukrepov prilagojenih potrebam posamezne organizacije ali njenih delov in je zasnovan tako, da zagotovi ustrezen nabor ukrepov varnostnih kontrol, ki dvigujejo zaupanje pri uporabnikih sistema. Uporaben je predvsem za oblikovanje varnostnih zahtev in ciljev znotraj organizacije, za opredelitev obstoječih in novih varnostnih procesov obdelovanja informacij in upravljanje z varnostjo le-teh, za uporabo in zagotovitev ustreznih informacij o politiki informacijske varnosti, skladnostjo z direktivami in standardi ter postopki za zunanje partnerje in druge organizacije s katerim je institucija povezana (ISO/IEC 27001:2005, 2011).

Del skupine standardov ISO so tudi standardi ISO 15408, ki so trenutno v treh delih. Prvi del 15408-1 predpisuje skupna merila, splošna načela in koncepte za ocenjevanje varnosti informacijske tehnologije[158] izdelkov in storitev. Ta del predstavlja temeljne pojme za vrednotenje varnosti informacijske tehnologije. Drugi del 15408-2 predpisuje različne varnostne funkcionalne zahteve in komponente, ki ustrezajo splošnim varnostnim potrebam. Zadnji del, 15408-3, pa določa ravni meril za ocenjevanje, zagotavljanje in vrednotenje stopnje varnosti informacijske tehnologije (ISO/IEC 15408: 2009, 2011).

Kot dopolnitev družini standardov ISO se pogosto pojavlja Standard dobrih praks za informacijsko varnost[159], ki ga izdaja Mednarodni varnostni forum[160]. Standard

---

[155] Angl. ***I**nternational **O**rganisation for **S**tandardization* (ISO)
[156] Angl. ***N**ational **I**nstitute of **S**tandards and **T**echnology* (NIST)
[157] Angl. ***I**nformation **S**ecuritiy **M**anagement **S**ystem* (ISMS)
[158] Angl. *Common Criteria for Information Technology Security Evaluation*
[159] Angl. *Standard of Good Practice for Information Security*

opredeljuje šest varnostnih področij, kjer je potrebna pozornost posameznih skupin, in sicer: okolje končnega uporabnika, razvoj sistemskih aplikacij, omrežje, umestitev strojne opreme, ključne poslovne aplikacije in varnostno upravljanje na ravni institucije. Standard ponuja informacije za vse ravni varnostne arhitekture, od osnovnih informacij, poglobljenih informacij, predlogov za izvajanje ter drugih navodil (*The Standard of Good Practice of Information Security* 2007, 1–4).

V okviru ameriškega Državnega inštituta za standarde in tehnologijo je bila že pred več kot desetletjem izdan *Priročnik za računalniško varnost*[161], ki ponuja temelje principe pristopa k izgradnji varnejšega računalniškega omrežja in vzpostavitvijo točk varnostnih preveritev. V naslednjih izdajah, ki so sledile priročniku so opisani različni varnostni principi na sodobnejših ravneh (*Special Publications – 800 Series* 2011).

Omeniti velja še Projektno skupino za internetno tehnologijo (IETF) in njihova izhodišča za varnejše spletne strani, ki je bil prav tako eden od prvih priročnikov za spletno varnost. Namen priročnika je bil zagotoviti praktične smernice za sistemske in omrežne administratorje pri naslavljanju varnostnih izzivov znotraj internetne skupnosti ter za sisteme, ki še niso bili priključeni na internet z namenom izboljšanja njihove izhodiščne varnosti na medmrežju (*Site Security Handbook* 2011).

Seveda so nekatere smernice in standardi danes že zastareli, vendar nekatera temeljna izhodišča ostajajo aktualna kljub ogromnemu preskoku IKT in strojne opreme. Tak primer brezčasne nevarnosti je recimo posameznik s specifičnimi znanji in notranjimi informacijami.

Pri standardiziranju omrežij je osrednji model povezljivosti odprtih sistemov – OSI, ki predstavlja temelj komunikacije med računalniki in je nastal na podlagi skupnih naporov Mednarodne organizacije za standardizacijo (ISO) in Mednarodne elektrotehnične komisije (IEC). Model je nastal z namenom vključevanja preteklih standardov in skupne osnove za razvoj standardov pri povezovanju različnih odprtih sistemov. »Odprtih« v tem kontekstu pomeni, da so sistemi na voljo za dostopanje s strani drugih sistemov (ISO/IEC 749-1: 1994, 1). OSI referenčni model ima sedem plasti: aplikacijsko plast, predstavitveno plast, sejno plast, transportno plast, omrežno

---

[160] Angl. ***I**nternational **S**ecurity **F**orum* (ISF)
[161] Angl. *The NIST Handbook: An Introduction to Computer Security*

plast, povezovalno plast in fizično plast (prav tam, 32–49). Za področje moje naloge je smiselna ugotovitev, da lahko do prekinitev oz. sprememb v delovanju prihaja praktično na vseh plasteh, zato je pozornost potrebna na vseh ravneh.

4.5 Temeljna področja preventivnega delovanja

V zadnjem desetletju je zaradi pomembnosti obravnavane problematike področje kibernetske varnosti dobilo izreden polet pri vzpostavljanju orodij in organizacijskih struktur za varovanje KII in omrežij pred kibernetskimi grožnjami. Vzpostavila se je kompleksna mreža prepletajočih se struktur na nacionalni, mednarodni, regijski ravni ter sodelovanje na ravni zasebno-javnega partnerstva. Vsi segmenti prepoznavajo pomembnost skupnih naporov in sodelovanja na področju kibernetske varnosti. Strokovnjaki zasebnega sektorja (Daley, 2001) prepoznavajo pomembno vlogo, ki jo na tem področju igrata EU in ZDA, predvsem s prevzemanjem iniciativ in pomembnostjo delovanja preko mej. Prepoznavajo vlogo, ki jo imajo zakonodajalci in regulatorji na splošni ravni ter spoznanje, da so ogrožene tako informacije kot ključni sistemi. Vsi akterji spoznavajo, da mora za uspešno odzivanje odgovor na kibernetske grožnje biti operativen, reaktiven in dinamičen.

Mednarodna telekomunikacijska zveza tako v okviru svojih raziskovalcev (Dunn, 2005) prepozna pet osrednjih področij, na katerih se prek različnih ravni države soočajo s kibernetskimi grožnjami.

4.5.1 Ključni sektorji

Države v odvisnosti od lastne percepcije prepoznavajo različne sektorje kot ključne, vendar nekaj temeljnih sektorjev ostaja ključnih na vseh ravneh, čeprav poteka neprestana razprava o pomembnosti posamičnih sektorjev. ITU izpostavlja pomembnost na dveh ravneh, in sicer sistemsko ter simbolno. Sistemsko je nek segment lahko ključen, ker povezuje različne sektorje in je tako vmesni člen med dvema pomembnima segmentoma. Simbolno pa je lahko nek element prav tako

ključen, ker je njegovo uničenje ali onesposobitev ključnega pomena za družbo ali njegov pomen v družbi (tak primer so recimo spomeniki ali vladne varnostne agencije). Široko sprejeta ključna področja pa so predvsem bančništvo in finančni sistem, osrednje vladne storitve, informacijska in komunikacijska tehnologija, reševalne službe in službe nujne pomoči, energetski sektor, zdravstvena oskrba, transport in logistika ter oskrba z vodo.

4.5.2 Organizacijska struktura

Razsežnost in kompleksnost varovanja KII pred kibernetskimi grožnjami se odraža v množici struktur in povezanosti le-teh. Pogosto ni le ena institucija odgovorna za varovanje KII, temveč so njihove pristojnosti deljene; zato je treba na državnih in naddržavnih ravneh vzpostaviti strukture, ki bodo sistemsko obremenjene izključno s kibernetsko varnostjo in zaščito KII. Pri naporih za varovanje v informacijski dobi so vlade soočene z novimi razsežnostmi pri zagotavljanju varnosti, saj je KII pogosto v rokah zasebnega sektorja, ki je izredno raznolik, prepleten in relativno nereguliran, njihova KII pa pomembna na ravni države. V tem smislu je zasebni sektor bolje opremljen z znanjem in dostopom do KII, torej je vloga skrbi za kibernetsko varnost KII pretežno na strani zasebnega sektorja[162]. Javno-zasebna partnerstva tako postajajo ključni temelj kibernetske varnosti omrežij.

4.5.3 Pristopi zgodnjega opozarjanja

Splošen trend je vzpostavljanje točk zgodnjega opozarjanja varnosti informacijskih sistemov in omrežij. Splošno razširjeni so različne oblike računalniških centrov za odzivanje na incidente, še posebno za vladna ministrstva in srednja ter velika podjetja in korporacije. Vloga CERT-ov je predvsem v odzivanju na računalniške incidente in pomanjkljivosti ter v tekočem objavljanju varnostnih opozoril ter s tem zmanjševanje verjetnosti uspešnih napadov.

---

[162] Zasebni sektor je po svoji naravi prvenstveno naravnan k ustvarjanju dobička, ki ga bodo povečana sredstva za zagotavljanje varnosti neposredno zmanjševala. Tako naletimo na temeljno razhajanje med imperativom učinkovitosti in dobičkonosnosti ter varnostnim zahtevam.

4.5.4 Aktualnost teme v pravu in zakonodaji

Učinkovit pregon kibernetskega kriminala ni mogoč brez ustrezne pravne podlage, zato so mnoge države začele s popravki obstoječe kazensko-pravne zakonodaje ali celo s samostojnimi zakoni na področju kibernetske kriminalitete. Področja ureditve zakonodaje so predvsem zaščita podatkov in elektronskega komuniciranja, vključno s prenosom podatkov, elektronskimi arhivi, varnost informacijske tehnologije in zahteve za informacijsko varnost, nezakonita uporaba računalnikov in sistemov, poškodovanje ali ponarejanje podatkov in podobne kršitve, zaščita osebnih podatkov in zasebnosti, identifikacije in digitalni podpisi, odgovornost v e-poslovanju in e-trgovinah, mednarodna uskladitev kibernetske zakonodaje, minimalni standardi na področju kibernetske varnosti za e-storitve javne uprave, ponudnike storitev in telekomunikacijske operaterje. Osrednja vloga pripada mednarodni standardizaciji zakonodaje, vendar to področje že zdaleč ni usklajeno.

4.5.5 Raziskovanje in razvoj

Kibernetska varnost ima in bo imela pomembno vlogo na področju raziskovanja in razvoja zaradi izrednega izziva, ki ga predstavlja. S to problematiko se ukvarjajo raziskovalni centri na ravni univerz, zasebnega sektorja in njihovih laboratorijev ter državnih raziskovalnih svetov. Mednarodna narava kibernetskih groženj terja raziskovanje in preučevanje na mednarodni ravni. Nekateri temeljni motivi za raziskovanje na mednarodni ravni so tako povečana omreženost sistemov in kompleksnejša struktura povezanih sistemov, naraščajoča soodvisnost ključnih infrastruktur, ter skupna ugotovitev, da so za globalne izzive potrebne globalne rešitve, povečana stroškovna učinkovitost s pomočjo večje učinkovitosti in hitrejših rezultatov ter dostopnost širšega kroga informacij preko nacionalnih meja.

Podoben pristop uporablja tudi *Mednarodni priročnik za varnost ključne informacijske infrastrukture* (Brunner in Suter 2009, 528) züriškega Centra za varnostne študije ter druge raziskave (Nicander 2010, 283–284), ki sistematično preučujejo pristope različnih držav k področju varnosti KII. Priročnik podrobno preučuje različne vidike,

med njimi: definiranje ključnih sektorjev, pretekle in sedanje iniciative ter politike, organizacijsko strukturo, pristope zgodnjega opozarjanja in javnega osveščanja ter področje zakonodaje. Omenjena je tudi vloga različnih mednarodnih institucij in organizacij kot so Evropska unija, OECD, G8, NATO, Združeni narodi in druge, ki sem jih tudi že omenil v poglavju o ukrepih.

4.6 Priporočila za izboljšavo kibernetske varnosti omrežij

Ob vseh preučenih iniciativah, pobudah, sklepih, usmeritvah, programih in strateških dokumentih, se poraja vprašanje kaj sploh dodati, kar še ni bilo povedanega ali zapisanega. Morda je odgovor ravno v množici in pestrosti predhodno zapisanega in združevanju navedenega v smiselno celoto. Poleg tega se mi zdi smiselna navedba nekaterih preprostih ukrepov za celostno izboljšanje varnosti kibernetskega okolja.

Verjamem, da ni več potrebno dodatno pojasnjevanje, da je kibernetska varnost omrežij interdisciplinarno področje, kjer je treba uporabiti holistični pristop, ki upošteva specifično naravo preučevanega področja in vpletenost deležnikov z različnih področij in ravni. Vsi vidiki morajo biti upoštevani, če želimo doseči zastavljen cilj, tj. dvig kibernetske varnosti omrežij. Namerno se bom distanciral od podrobnejših ukrepov tehnične narave, saj so metode in tehnike tako hitro razvijajoče, da je vsaka tiskana oblika navodil in smernic lahko kmalu zavajajoča ali celo povsem neuporabna, nekaj temeljnih tehničnih usmeritev za končnega uporabnika pa bom vseeno navedel.

4.6.1 Strateški pogled

Najprej se bom osredotočil na najvišjo raven zagotavljanja varnosti, torej na strateški pogled na problematiko. Izmed množice ukrepov za povečanje varnosti oz. preprečevanje in omejevanje negativnih posledic kibernetskih groženj sem izluščil nekaj bistvenih področij, ki so skupne mnogim usmeritvam in strateškim pristopom.

Sledenje tem smernicam naj bi pomembno vplivalo na izboljšanje kibernetske varnosti omrežij in s tem varnosti in neprekinjenega zagotavljanja storitev nam vsem.

1. **Odgovornost predpostavljenih za kibernetsko varnost**, kar vključuje iniciativo na področju in vzpostavljanje zavez k izboljševanju stanja ter po potrebi dodatno koordinacijo in podporo vsem podrejenim institucijam in organom.
2. **Vzpostavitev središčne točke za kibernetsko varnost** na ravni vseh struktur in nad njimi ter pospeševanje komunikacije med vsemi deležniki, kar se pogosto odrazi v konstituiranju centra za posredovanje pri omrežnih incidentih (CERT). Vloga takega centra je v koordinaciji državnih naporov za izboljšanje varnosti, analiziranje trendov groženj, koordiniranje odzivov in izboljševanju preventive. Pomembna je tudi javna objava morebitnih groženj in odziv zainteresirane strokovne javnosti, ki pogosto lahko pomaga pri odkrivanju pomanjkljivosti in tako prispeva k hitri rešitvi.
3. **Zakonodajni ukrepi**, ki vključujejo vzpostavitev ustrezne lokalne zakonodaje in omejitev nelegalnega kibernetskega delovanja, ki organom pregona omogočajo začetek postopka, odzivanje na kršitve, preganjanje kršiteljev in dosledno izvajanje zakonodaje na področju kibernetske kriminalitete.
4. **Vzpostavitev državnega okvira kibernetskega delovanja**, kar vključuje izdajo ustreznih smernic in ukrepov, ki bodo usklajeni na širši ravni ter predpostavljajo minimalne standarde upravljanja s tveganji in odzivanje na kibernetske incidente po dogovorjenih protokolih.
5. **Zaščita javnih institucij in sistemov**, ki naj bodo zgled vsem ostalim pri preventivnem delovanju in ukrepanju za povečanje kibernetske varnosti.
6. **Osveščenost in izobraževanje o kibernetski varnosti** na vseh ravneh in zahtevnostih. Potreba po programih s tega področja narašča, izobraženost in osveščenost prav vsakega omrežnega akterja posledično dviguje splošno raven varnosti in otežuje delovanje zlonamernih akterjev.
7. **Delujoče javno-zasebno partnerstvo** je ključno za kibernetsko varnost, predvsem zaradi množice strokovnjakov v zasebnem sektorju ter zasebnega lastništva nad omrežji in infrastrukturo, prek katere so (nekateri) ključni informacijski sistemi ali njihovi elementi povezani.

8. **Mednarodno sodelovanje na področju kibernetske varnosti** je prav tako ključno, saj sama brezmejna narava kibernetskih groženj terja mednarodno sodelovanje in koordinacijo pri varovanju in zaščiti pred kibernetskimi grožnjami.

4.6.2 Operativno-tehnična raven

Na bolj operativni ravni pa je množica ukrepov (tudi tehničnih), ki so primerni tako za končnega uporabnika kot tudi za skrbnike sistemov ter za vsesplošen dvig kibernetske varnosti omrežij nasploh. Najprej navedem nekaj splošnih smernic za zahtevnejše uporabnike in sistemske tehnike, nato pa še nekaj preprostejših za osnovno raven zaščite ter končnega uporabnika. Tu izhajam iz lastnih posplošenih izkustev in jih poskušam navezati na teoretske trditve glede varnosti omrežij, gre za t. i. inverzno dedukcijo.

Ta raven je prav tako zelo pomembna za celostno izgradnjo varnejšega kibernetskega okolja zaradi svoje množičnosti in s tem potencialnih tarč zlonamernih napadov, ki bi kasneje lahko bile uporabljene tudi za ogrožanje kibernetske varnosti omrežij in njihovih sestavnih elementov. Tudi za končnega uporabnika bi bila smiselna uporaba pristopa inverzne dedukcije, saj bi z globokim poznavanjem lastnega omrežja in sistema ter hkratnim poznavanjem teorije na področju kibernetske varnosti lahko sam prišel do uporabnih in učinkovitih zaključkov. Zato je razvoj kibernetske varnosti primarno v domeni zasebnega sektorja, kjer z induktivno metodo preučevanja posamičnih primerov napadov lahko sklepamo na celotno naravo problematike. Ob ustreznem poznavanju teorije tega področja ima zasebni sektor tako potencial in vlogo izgradnje novega teoretskega deduktivnega sistema smernic za varnejše kibernetsko okolje, kar se že odraža v pristopih t. i. vgrajene zasebnosti in vgrajene varnosti, ko so programska oprema in sistemi že ob načrtovanju grajeni tako, da omogočajo kar se da visoko raven zasebnosti in varnosti. Sedaj pa h konkretnim nasvetom.

NAPREDNA RAVEN

1. Omogočanje evidentiranja dostopa do storitev in zbiranje podatkov o sistemu ali uporabniku, ki dostopa do storitve.
2. Postavitev zgornje meje poskusov preverjanja pristnosti brez samodejnega odklepanja po določenem času ter vzpostavitev ročne preveritve neuspelih poskusov in povezovanje teh poskusov z drugimi nenavadnimi akcijami.
3. Omejitev oddaljenega dostopa do storitev na nujno potrebne in omejitev sočasnih dostopov istega uporabnika, če le-ta ni sistem, ki potrebuje več sočasnih dostopov.
4. Vzpostavitev poglobljenih tehnik varovanja s kompleksnostjo gesel in osebnih identifikacij na več ravneh dostopa.
5. Vzpostavitev zaščite pred beleženjem tipkanja ter samodejno zahtevo po pogostejšem menjavanju gesel uporabnika.
6. Redno potrjevanje istovetnosti in posodabljanje programske opreme ter digitalnih podpisov in ključev.
7. Uporaba sodobnih operacijskih sistemov in platform strojne opreme, ki omogočajo višje ravni varnosti. Pogosto so to operacijski sistemi, ki niso množično uporabljani.
8. Namestitev obsežne programske opreme za zaščito gostiteljskega sistema s protivirusno podporo, podporo varnega brskanja, preprečevanjem ribarjenja in požarnim zidom.
9. Omejevanje pravic posameznega uporabnika na operacijskem sistemu in ohranjanje ključnih pravic le za administratorja.
10. Fizično omejen dostop do sistemskih strežnikov, ki je omejen na pooblaščene osebe z evidentiranjem dostopov.
11. Dosledno odjavljanje administratorjev po opravljenem delu in vzpostavitev samodejnega odjavljanja po določenem času.
12. Po nameščanju operacijskega sistema je treba ohraniti število aplikacij na najmanjši možni ravni za delovanje storitev končnega uporabnika.
13. Odstranitev kakršnihkoli storitev, ki jih končni uporabnik ne potrebuje za delo.
14. Zapiranje neuporabljenih vrat in nadzor prometa[163] nad ostalimi.

[163] Angl. TCP/UDP, protokol za nadzor transporta, uporabniški podatkovni protokol

15. Uporaba supergesel na administratorski ravni, kar pomeni poseben poudarek na zahtevnosti gesla.
16. Arhiviranje vsebin in obnovitev podatkov v primeru katastrof, po možnosti na odročni lokaciji in podprto s procesnimi navodili za obnovo in dokumentacijo arhiviranja.
17. Ločevanje poslovnih vsebin od zasebnih ter vzpostavitev ustrezne zaščite pri upravljanju poslovnih vsebin na domačih (manj in slabše zaščitenih) omrežjih.
18. Uporaba storitev računalništva v oblaku za shranjevanje osebnih in informacij zaupnih narave naj bo pogojena s popolnim zaupanjem v ponudnika tovrstnih storitev.
19. Privzeto uporabljanje sloja varnih vtičnic[164], ki omogočajo šifriranje povezave med strežnikom in odjemalcem.
20. Sistem naj bi podpiral mehanizme za odstranitev določenih uporabnikov omrežja ter jim blokirati nadaljnji dostop do omrežja (recimo na podlagi MAC[165] naslova mrežne kartice).
21. Sistem naj bi omogočal mehanizme za filtriranje na osnovi IP naslova, protokola in TCP/UDP vrat.
22. Sistem naj bi za namene upravljanja in konfiguriranja podpiral varnostne protokole kot sta varna lupina[166] in protokol za varno internetno povezavo[167].
23. Morebiten oddaljen dostop do sistema mora biti mogoč le prek varnih protokolov (SSH, HTTPS), ki dodatno temeljijo na certifikatih in geslih.
24. Sistem naj bi omogočal filtriranje in posredovanje paketov.
25. Preveritev zaupnosti zunanjih sodelavcev in ponudnikov programske opreme.
26. Fizična omejitev dostopa do pomembnih sistemov ali dokumentov končnih uporabnikov na drugih lokacijah.
27. Klasifikacija pomembnosti in selektivno ohranjanje zbranih podatkov.
28. Redno šifriranje in arhiviranje pomembnih dokumentov ter varnostno kopiranje arhiva na oddaljene lokacije.
29. Redno evidentiranje dostopa do službenih delovnih postaj.

---

[164] Angl. ***S**ecure **S**ocket **L**ayer*, SSL
[165] Angl. MAC, ***M**edia **A**ccess **C**ontrol*, naslov, ki identificira uporabniško napravo.
[166] Angl. ***S**ecure **SH**ell*, SSH
[167] Angl. ***H**yper**T**ext **T**ransport **P**rotocol **S**ecure sockets*, HTTPS

30. Jasni protokoli uporabe elektronskih prenosnih naprav za šifriranje in arhiviranje poslovne dokumentacije.
31. Vzpostavitev protokola odzivanja na ugotovljen vdor ali napad.
32. Evidentiranje in sporočanje morebitnih incidentov odgovornim za informacijsko varnost.

OSNOVNA RAVEN

33. Uporaba brskalnikov s funkcijo nadzorovanega okolja za uporabo brskalnika.
34. Redno posodabljanje uporabniške programske opreme na najnovejše različice.
35. Programska samodejna zaščita uporabniških podatkov in gesel v primeru izgube prenosne računalniške opreme.
36. Uporaba lastnega usmerjevalnika za celosten nadzor nad domačim omrežjem in prometom, ki poteka po njem.
37. Uporaba WPA2[168] zaščite pri domačih brezžičnih omrežjih.
38. Skrivanje identifikacijskega oddajnega signala[169] brezžičnega omrežja.
39. Ročna nastavitev IP naslovov na uporabniških klientih pri brezžičnem omrežju.
40. Omejevanje nastavitev usmerjevalnika ali brezžične opreme na lokalno okolje, to je onemogočanje nastavitev na daljavo, kadar je le to mogoče.
41. Filtriranje fizičnega naslova klientov za dostop do brezžičnega omrežja na strani usmerjevalnika.
42. Uporaba močnih gesel na vseh omrežnih računalniških napravah.
43. Uporaba prenosnih računalniških naprav in pametnih telefonov na javno dostopnih internetnih točkah naj bo omejena na nujna opravila ali brskanje, po možnosti brez vnosa uporabniških podatkov.
44. Uporaba družabnih omrežij in deljenje osebnih informacij na tovrstnih omrežjih naj bo omejena na raven javnega.
45. Uporaba različnih uporabniških imen in gesel na različnih naslovih spletne pošte.
46. Uporaba varnih protokolov pri uporabi spletne pošte.
47. Gesla naj bodo raznolika in kompleksna. Geslo velja kot varno, ko vsebuje vsaj deset znakov, številk, posebnih znakov in simbolov, po možnosti različne velikosti in različne ravni na tipkovnici.

---

[168] Angl. ***W**iFi **P**rotected **A**ccess*, WPA
[169] Angl. ***S**ervice **S**et **ID**entifier Cloaking*, SSID

48. Vprašanja za izgubljena gesla naj bodo osebne narave in znana le uporabniku.
49. Onemogočitev izvajanja skript v brskalnikih s strani neznanih domen.

Pri zaščiti ključne informacijske infrastrukture in omrežij pred kibernetskimi grožnjami je tako smiselno govoriti o ukrepih na večih ravneh, ki vključujejo:

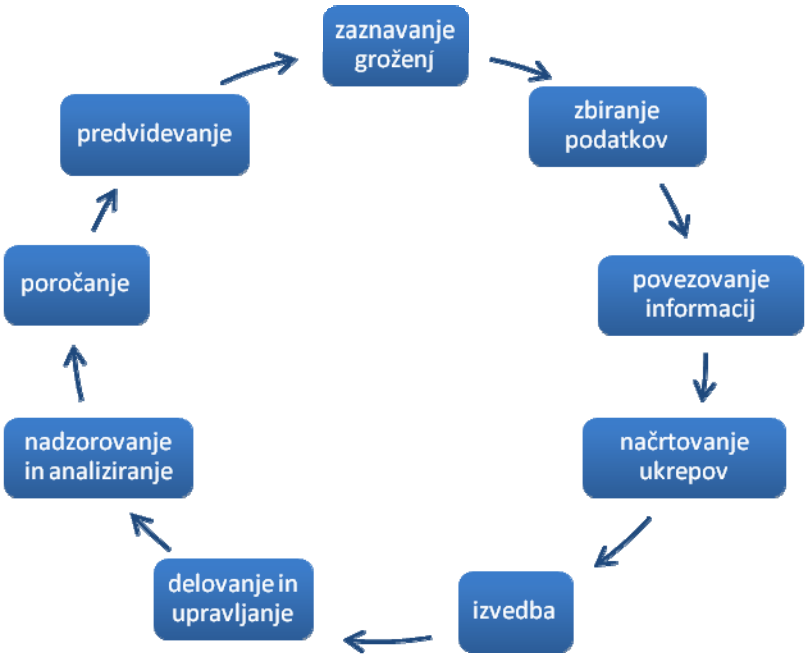
- **fizične zaščitne ukrepe**, ki z ustreznim načrtovanjem delovanja komunikacijskega in omrežnega sistema in natančno implementacijo izločijo ali omejijo potencialne priložnosti za kibernetsko ogrožanje sistema,
- **tehnične ukrepe** oz. ukrepe na ravni programske opreme, kar je pogosto prvi ukrep, na katerega pomislimo ob omembi kibernetske varnosti, še zdaleč pa ne pomenijo celovite rešitve,
- **družbene ukrepe** v smislu izobraževanja zaposlenih na področju kibernetske varnosti in osveščanja o potencialnih grožnjah ter preveritev osebja v smislu poznavanja njihovih preteklih zadolžitev in s tem potencialnih konfliktov interesov in
- **varnostno politiko**, ki ima jasno definirane namene in cilje zagotavljanja kibernetske varnosti omrežij ter ukrepe s katerimi bodo cilji doseženi, ključna pa je seznanjenost vseh akterjev s to politiko, saj je le tako mogoč celovit pristop.

Samo celostni pristop h kibernetski varnosti omrežij ima potencial omejevanja povzročene škode in stroškov ter izboljšati okrevanje po incidentih. Celovit in strateški pristop k ovrednotenju varnosti in tveganj na fizični, virtualni in psihološki ravni je osnova za celovito varnostno strategijo. Vsestranski in interdisciplinaren pristop k raziskovanju in vključenosti mnogih področij je tako nujen.

Ker pa je narava tovrstnih groženj neprestano spreminjajoča in kot taka predstavlja tudi največji izziv pri tovrstnem ogrožanju, je tako tudi odzive na grožnje potrebno neprestano posodabljati in spreminjati, nove grožnje pa preučevati. Delovanje vseh institucij in ukrepov na področju kibernetske varnosti, bi moralo tako slediti

spremembam tovrstnih groženj in varnostno strategijo neprestano prilagajati. Življenjski cikel tovrstnih ukrepov poskušam prikazati na shemi 4.20.

Shema 4.20: Življenjski cikel ukrepov za varnost na kibernetskem področju



5 Sklep

Vse več ključnih storitev v našem življenju temelji na informacijskih sistemih. Ti predstavljajo temeljni element naše sposobnosti, vse od hitrega komuniciranja in oskrbe z osnovnimi dobrinami do najbolj zapletenih in strukturiranih protokolov pri zagotavljanju varnosti. Ti informacijski sistemi pa za svoje delovanje potrebujejo različne oblike in velikosti omrežij, od lokalne do svetovne ravni. Varnost teh omrežij je torej ključna za delovanje informacijskih sistemov, ki nam lajšajo vsakdanje izzive. Skupek bistvenih omrežij in informacijskih sistemov tako lahko združimo pod okrilje pojma ključna informacijska infrastruktura.

V magistrskem delu sem se osredotočal predvsem na en, po moji oceni vse bolj pomemben, vidik varnosti teh omrežij in sistemov – kibernetsko varnost. Različne študije in tudi podatki kažejo, da ta segment varnosti ključne informacijske infrastrukture prevzema poglavitno vlogo, saj postopoma vsi ostali sistemi temeljijo na digitalnih procesih in omrežjih, ki bi morala biti odporna na kibernetske grožnje ter hkrati sposobna hitrega okrevanja po morebitnih incidentih. Motnje v delovanju sistemov ključne informacijske infrastrukture se lahko odrazijo v veliki gospodarski ali družbeni škodi, kibernetski izvor take motnje pa je tudi danes za marsikoga še vedno precej abstrakten, kar pa žal grožnje ne naredi nič manjše. Celo nasprotno, nepoznavanje tega segmenta groženj in napačno odzivanje lahko povzroči posledice, ki celo presegajo neposredno ogroženost ali omejeno funkcionalnost zaradi kibernetskega napada. Kibernetske grožnje postajajo kompleksnejše in pogostejše, zato je ključno, da odgovorni posamezniki in institucije prepoznajo ta vidik kot izredno pomemben.

V magistrskem delu tako predstavim nekaj pogostejših kibernetskih groženj in principov delovanja, s katerimi bi bila lahko ogrožena varnost omrežij. Na koncu naj izpostavim samo najbolj prikrito in kompleksno obliko ogrožanja, ki združuje več tehnik, t. i. napredne trajne grožnje. Tu napadalec s prefinjenim in organiziranim napadom brez vednosti tarče dalj časa sistematično spremlja in preučuje delovanje tarče, dostopa do njenih zaupnih informacij in si v nekaterih primerih celo prikrito pridobi nadzor nad sistemom in lahko celo skrije posledice takega nepooblaščenega

nadzora. Glavna značilnost teh groženj je vztrajnost napadalca in obsežna sredstva s katerimi lahko deluje in se izogiba morebitnim protiukrepom tarče. Ta dva pogoja tudi izločita morebitnega osamljenega akterja in v ospredje postavljata napadalce večjih razsežnosti. Tovrstni napadi so neposredna grožnja ključnim informacijskim sistemom in s tem njihovi varnosti. Okolje, v katerem sistemi delujejo, pa ni konstantno. Nenehen razvoj tehnologij in potreba človeštva po nadaljnjem razvoju sta zagotovilo, da se bo okolje sistemov spreminjalo tudi v prihodnje. Vseprisotnost interneta stvari in množica na novo vpletenih elementov, ki jih bo internet stvari vseboval, bo tako v temeljih preobrazila varnostne izzive s katerimi se soočamo danes, zato je ključno, da sisteme ključne informacijske infrastrukture prilagodimo tako, da bodo pripravljeni na nove izzive prihodnosti. Hkrati pa je potrebno že pri načrtovanju strukture in varnostnih principov predpostavljati razsežnosti omrežij prihodnosti, ki prihajajo.

V nadaljevanju dela izpostavim normativne okvire na različnih ravneh, ki so jih sprejele različne institucije in s katerimi želijo dvigovati raven varnosti omrežij. Naj izpostavim samo ukrepe Evropske unije, ki si je zaradi brezmejne narave kibernetskih groženj najprej zadala cilj premagati razlike v nacionalnih pristopih na področju varnosti in vzdržljivosti ključnih sistemov ter okrepiti vlogo evropskih institucij tako pri upravljanju s spremembami kot pri izboljšanju zmogljivosti Evrope na področju odzivanja na tovrstne dogodke. Temeljni cilj delovanja pa je vsesplošen dvig vzdržljivosti in stabilnosti svetovnega spleta ter s tem posameznih omrežij. Tudi ukrepi drugih institucij in organizacij gredo predvsem v smeri pripravljenosti, preprečevanja, odkrivanja in hitrih odzivov na kibernetske grožnje, predvsem skozi sisteme hitrega obveščanja, opozarjanja in osveščanja ter izmenjave informacij. Nadalje gredo ukrepi predvsem v smer zmanjševanja potencialne škode in hitrega okrevanja po morebitnih napadih, kar naj bi se doseglo s čezmejnim sodelovanjem in izvedbo mednarodnih vaj ter poglobljenim mednarodnim sodelovanjem na vseh ravneh. Ključna je proaktivnost predpostavljenih voditeljev, da z zgledom in pozivi ter primernimi poudarki postavijo kibernetsko varnost na ustrezno mesto. Tudi razvoj javno-zasebnega partnerstva, navkljub jasni potrebi po sodelovanju, brez obojestranske iniciative ne bo stekel, zato je pomembno, da vsi vpleteni prepoznajo dobrobiti sodelovanja. Le vsota vseh naporov in ukrepov na fizični in tehnološki ravni, podkrepljena z družbenimi ukrepi in ustrezno varnostno politiko, obeta rezultate.

Pri samem raziskovanju sem se opiral predvsem na tuje vire, saj je domačih relevantnih premalo. To dejstvo mi vzbuja dodatno skrb, saj je osveščenost in primerna izobraženost vseh akterjev pri spletni varnosti zelo pomembna. Že v tem desetletju bomo priča izrednemu razvoju na področju interneta stvari, kar bo v internetno okolje vpletlo tudi posameznike, ki do danes niso bili pretirano vešči oz. v stiku s tovrstno tehnologijo. Osveščanje in izobraževanje manj izobražene (starejše) populacije bo tako naša realnost in nuja za varnejše in stabilnejše sisteme. Ker pa je znanje jezika pri teh posameznikih lahko ovira, je nujno, da je ustrezna literatura na voljo tudi v njim razumljivem jeziku. Svoje delo vidim tudi kot prispevek na tem področju. V sklepnem delu naloge sem pokušal z uporabo metode inverzne dedukcije vzpostaviti povezavo med lastnimi izkustvenimi posplošitvami na področju informacijske varnosti ter splošnimi teoretskimi in normativnimi zapisi, ki so bili na voljo v literaturi. Rezultat te metode so priporočila za izboljšavo kibernetske varnosti omrežij, ki so zapisana v zadnjem delu.

V nalogi sem tako poskušal odgovoriti na osrednje vprašanje mojega raziskovanja: katere so temeljne grožnje kibernetski varnosti omrežij in kateri so ukrepi za povečanje varnosti in preprečevanje oz. omejevanje negativnih posledic kibernetskih napadov. V zadnjem delu naloge sem prek metode sinteze spoznanj in inverzne dedukcije izluščil bistvene elemente in ukrepe, ki pripomorejo k celovitem izboljšanju kibernetske varnosti omrežij. Ključna pa je ugotovitev, da posamezen ukrep ali celo skupina ukrepov na posameznem segmentu, ni in ne bo zadoščala za reševanje uganke kibernetske varnosti. Ključ in odgovor se skrivata v skupni vsoti vseh ukrepov, od izobraževanja akterjev na vseh ravneh do skupnih vztrajnih naporov vseh deležnikov za dosego sprejemljive in primerne ravni kibernetske varnosti omrežij.

6 Literatura

1. *4chan Users Organize Surgical Strike Against MPAA*. 2010. Dostopno prek: http://pandalabs.pandasecurity.com/4chan-users-organize-ddos-against-mpaa/ (10. februar 2012).
2. A World Economic Forum Report. 2008. Global Risks 2008. *A global Risk Network Report.* World Economic Forum Dostopno prek: https://members.weforum.org/pdf/ globalrisk/report2008.pdf (10. maj 2011).
3. Allen Julia. 2005. *Governing for Enterprise Security: Networked Systems Survivability Program.* Pittsburgh: Carnegie Mellon University.
4. *Analiza slovenskega Facebook botneta.* Dostopno prek: http://www.cert.si/ obvestila/obvestilo/article/analiza-slovenskega-facebook-botneta/44.html (13. avgust 2011).
5. ARBOR NETWORKS. 2011. *Wordwide Infrastructure Security Report 2010*. Dostopno prek: http://ipv6.org.sa/sites/default/files/World_Infrastructure_Security_ Report_2011.pdf (12. november 2011).
6. *Attacks against information systems.* 2011. Dostopno prek: http://europa.eu/legislation_summaries/information_society/internet/l33193_en.htm (26. november 2011).
7. Avižienis, Algirdas; Laprie, Jean-Claude in Randell, Brian. 2000. *Fundamental Concepts of Dependability.* Pittsburgh: Carnegie Mellon University. Dostopno prek: http://www.cert.org/research/isw/isw2000/papers/56.pdf (9. oktober 2011).
8. Baipai, Kanti. 2000. *Human Security: Concept and Measurement*. Kroc Institute Occassional Paper No. 19; OP: 1, 1-64. University of Notre Dame. Notre Dame, Indiana. Dostopno prek: http://www.hegoa. ehu.es/dossierra/seguridad/Human_ security_concept_and_measurement.pdf (16. julij 2011).
9. Bennet, Geoff. 2011. *Resilience, Reliability, and OAM in Converged Networks*. Dostopno prek http://www.heavyreading.com/details.asp?sku_id=528&skuitem _itemid=558&promo_code=&aff_code=&next_url=%2Fdefault.asp%3F (12. avgust 2011).

10. Bilgin, Pinar. Critical Theory. V: Williams, Paul D. (2008): *Security Studies (An Introduction). London* and New York: Routledge.
11. Brechbühl, Hans, Bruce, Robert, Dynes, Scott in Johnson, Eric. 2010. *Protecting Critical Information Infrastructure: Developing Cybersecurity Policy*. Information Technology for Development. Vol. 16, No.1: 83–91.
12. Brunner, Elgin M. in Suter, Manuel. 2009. *International CIIP Handbook 2008/2009*. Center za varnostne študije, Zürich. Dostopno prek: http://www.css.ethz.ch /publications/CIIP_HB_08 (26. november 2011).
13. Burkard, Schmitt, ur. 2005: Information *security: A new challenge for the EU*. Institute for Security Studies (ISS), European Union. Paris. Chaillot Papers. Dostopno prek: http://www.iss.europa.eu/uploads/media/cp076.pdf (22. maj 2011).
14. Carr, Jeffrey. 2010. *Inside Cyber Warfare*. Sebastopol: O'Reilly Media.
15. *Carrier IQ Software Compromises Android Device Data Privacy*. 2011. Dostopno prek: http://www.eweek.com/c/a/Security/Carrier-IQ-Software-Compromises-Android -Device-Data-Privacy-801615/1/ (30. december 2011).
16. Cashell, Brian, Jackson, William, Jickling, Mark in Webel, Baird. 2004. *The Economic Impact of Cyber-Attacks.* Congressional Research Service. The Library of Congress. Washington D.C. Dostopno prek http://www.cisco.com/warp/public/ 779/govtaffairs/images/CRS_Cyber_Attacks.pdf (21. avgust 2011).
17. *Center za varnejši internet SAFE-SI.* 2011. Dostopno prek: www.safe.si (3. september 2011).
18. *CERT – Software Engineering Institute.* 2011. Dostopno prek: http://www.cert.org/ (9. oktober 2011).
19. China's Cyberwarfare. 2011. *CHINASCOPE Analysis Series*. Dostopno prek: http://chinascope.org/main/PDF/CSA20110809.pdf (26. november 2011).
20. *Chinese hackers blamed for cyber attack wave.* 2011. Dostopno prek: http://www.thisismoney.co.uk/money/news/article-1687393/Chinese-hackers-blamed-for-cyber-attack-wave.html (17. avgust 2011).
21. Christensen, Sharon, Caelli, William, Duncan, William in Georgiades, Eugenia. 2010. An Achilles heel: denial of service attacks on Australian critical information infrastructures. *Information & Communications Technology Law*. Vol. 19, No. 1: 61–85.

22. *CIIP – Implementation activities – Pillar 1.* 2011. Dostopno prek: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/pillar_1/index_en.htm (5. oktober 2011).
23. *Cisco 2010 Annual Security Report.* Dostopno prek: http://www.cisco.com/en/US/prod/collateral/vpndevc/security_annual_report_2010.pdf (4. november 2011).
24. *Cisco 2Q11 Global Threat Report.* Dostopno prek: http://www.cisco.com/en/US/prod/collateral/vpndevc/cisco_global_threat_report_2q2011.pdf (9. november 2011).
25. Council of Europe. 2003. *The Council of Europe: 800 Million Europeans*. Strasbourg.
26. *Crime rate drops to record low.* Dostopno prek http://www.dw-world.de/dw/article/0,,15093336,00.html (25. julij 2011).
27. *CSI Computer Crime & Security Survey.* New York: Computer security institute. Dostopno prek: http://gocsi.com/sites/default/files/uploads/ CSIsurvey2008.pdf (20. maj 2011).
28. *Cyber Coalition 2010 to exercise collaboration in cyber defence.* 2011. Dostopno prek: http://www.nato.int/cps/en/natolive/news_68205.htm?selectedLocale=en (26. november 2011).
29. *Cyber Combat: Act of War.* 2011. Dostopno prek: http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html (24. avgust 2011).
30. *Cyber Europe 2010 Online Security Exercise.* Dostopno prek: http://www.security-technologynews.com/news/cyber-europe-2010-online-security-exercise.html (6. maj 2011).
31. *Cyber Security Strategy of the United Kingdom. Safety, security and resilience in cyber space.* 2009. Dostopno prek: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf (4. november 2011).
32. *Cyber Storm: Securing Cyber Space.* 2011. Dostopno prek: http://www.dhs.gov/files/training/gc_1204738275985.shtm (8. oktober 2011).
33. *Cybersecurity.* Dostopno prek http://www.whitehouse.gov/administration/eop/nsc/cybersecurity (3. september 2011).
34. *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 (3. september 2011).

35. Daley, Sue. 2011. Cyber Security Strategies and Approaches. 2011. Symantec. Dostopno prek: http://www.slideshare.net/vngundi/cyber-security-strategies-and-approaches-symantec (4. november 2011).
36. DAMBALLA. 2010. *Advanced Persistent Threats (APTs).* Dostopno prek: http://www.damballa.com/downloads/r_pubs/advanced-persistent-threat.pdf (9. november 2011).
37. *Defense Advanced Research Projects Agency.* 2011. Dostopno prek: http://www.darpa.mil/ (20. oktober 2011).
38. *Defense Information Systems Agency.* Dostopno prek http://www.disa.mil/ index.html (22. julij 2011).
39. Denning, Dorothy in Denning, Peter. 2010. Discussing Cyber Attack. *Communication of the ACM.* Vol. 53, No. 9: 29-31
40. *Department Of Defense.* Dostopno prek http://www.defense.gov/ (22. julij 2011).
41. *Department of Homeland Security.* 2011. Dostopno prek http://www.dhs.gov/ index.shtm (22. julij 2011).
42. Dokl, Jure. 2006. *Internet in koncept človekove varnosti*. Ljubljana: Fakulteta za družbene vede.
43. *Doktrina civilne obrambe Republike Slovenije.* 2002. Vlada Republike Slovenije. Ljubljana: Ministrstvo za obrambo.
44. Dübendorfer, Thomas, Wagner, Arno, Plattner, Bernhard. 2004. *An Economic Damage Model for Large-Scale Internet Attacks.* Computer Engineering and Networks Laboratory. Zurich: Swiss Federal Institute of Technology. Dostopno prek: http://thomas.duebendorfer.ch/publications/scientific/WETICE-ES-duebendorfer-economic_damage_model.pdf (21. avgust 2011).
45. Dunn, Myriam. 1995. *The socio-political dimensions of critical information infrastructure protection (CIIP).* Center for Security Studies. Zürich. Dostopno prek: http://www.environmental-expert.com/Files%5C6471%5Carticles%5C6388%5Cf4 12118326107915.pdf (24. avgust 2011).
46. --- 2004. *Securing the Information Age: The Twin-Forces of Complexity and Change and International Relations Theory*. Center for Security Studies, Zürich.

47. --- 2005. *A Comparative Analysis of Cybersecurity Initiatives Worldwide.* Geneva. International Telecommunication Union.
48. *Dutch, French & German Cyber Security Strategies presented.* 2011. Dostopno prek: http://www.enisa.europa.eu/media/news-items/cyber-security-strategies-of-de-nl-presented (5. oktober 2011).
49. Dvoršak, Andrej in Bojan Dobovšek. 2009. Pojavne oblike kriminalitete v informacijsko komunikacijski tehnologiji – računalniška in internetna kriminaliteta. *Transnacionalna kriminaliteta,* ur. Bojan Dobovšek, 433-495. Ljubljana: Fakulteta za varnostne vede.
50. *Emerging Cyber Threats Report.* Dostopno prek www.gtisc.gatech.edu /pdf/CyberThreatsReport2009.pdf (20. avgust 2011).
51. *Encyclopedia Britannica,* Inc.. http://dictionary. reference.com/ browse/cyberspace (29. april, 2011).
52. ENISA. 2007a. *Pobude za ozaveščanje o varnosti informacij: Sedanja praksa in merjenje uspeha.* Heraklion: ENISA. Dostopno prek: http://www.enisa.europa .eu/act/ar/deliverables/2007/kpi-study/sl (6. maj 2011).
53. --- 2007b. *Position Paper No. 3. Botnets – The Silent Threat*. Dostopno prek: http://www.enisa.europa.eu/act/res/other-areas/botnets/botnets-2013-the-silent-threat (12. november 2011).
54. --- 2009a. *Cloud Computing. Benefits, risks and recommendation for information security.* Dostopno prek: http://www.enisa.europa.eu/act/rm/files/ deliverables/cloud-computing-risk-assessment (11. februar 2012).
55. ---2009b. *Impact assesment (Part 3). Commission staff working document. Accompanying document to the Communication on Critical Information Infrastructure Protection.* Dostopno prek: http://ec.europa.eu/governance/impact /ia_carried_out/docs/ia_2009/sec_2009_0399_en_part3.pdf (12. november 2011).
56. --- 2010a. *Botnets: Detection, Measurement, Disinfection & Defence*. Dostopno prek: http://www.enisa.europa.eu/act/res/botnets/botnets-measurement - detection-disinfection-and-defence (15. marec 2011).
57. --- 2010b. *ENISA Quarterly Review*. Vol 6. No. 2. Dostopno prek: http://www.enisa. europa.eu /publications/eqr/issues (20. marec 2011).
58. --- 2010c. *Flying 2.0 - Enabling automated air travel by identifying and addressing the challenges of IoT & RFID technology.* Dostopno prek: http://www.enisa.

europa.eu/act/rm/emerging-and-future-risk/deliverables/flying-2.0-enabling automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology-2/flying-2.0-enabling-automated-air-travel-by-identifying-and-addressing-the-challenges-of-iot-rfid-technology (11. februar 2012).

59. --- 2010d. *Interim findings of CYBER EUROPE 2010; a successful 'cyber stress test' for Europe.* Dostopno prek: http://www.enisa. europa.eu/media/press-releases/cyber-europe-2010-a-successful-2019cyber-stress-test2019-for-europe (10. maj 2011).
60. --- 2010e. *Measurement Frameworks and Metrics for Resilient Networks and Services: Challenges and Recommendations*. Dostopno prek: http://www.enisa.europa.eu/act/res/other-areas/metrics/reports /metrics-survey (2. april 2011).
61. --- 2011a. *Bittersweet cookies. Some security and privacy considerations*. Dostopno prek: http://www.enisa.europa.eu/act/it/library/pp/cookies (22. april 2011).
62. --- 2011b. *Botnets: 10 tough Questions*. Dostopno prek: http://www.enisa.europa.eu/act/res/botnets/botnets-10-tough-questions (25. april 2011).
63. --- 2011c. *Cyber Europe 2010 – Evaluation Report.* Dostopno prek: http://www.enisa.europa.eu/act/res/cyber-europe-2010/cyber-europe-2010-report (10. maj 2011).
64. --- 2011d. *Enabling and managing end-to-end resilience.* Dostopno prek: http://www.enisa.europa.eu/act/it/library/deliverables/e2eres (20. marec 2011).
65. --- 2011e. *Inter-X: Resilience of the Internet Interconnection Ecosystem*. Dostopno prek: http://www.enisa.europa.eu/act/res/other-areas/inter-x/report/ interx-report (6. maj 2011).
66. --- 2011f. *Privacy, Accountability and Trust – Challenges and Opportunities.* Dostopno prek: http://www.enisa.europa.eu/act/it/library/ deliverables/pat-study (25. februar 2011).
67. *Estonia pushes for joint EU cyber response*. Dostopno prek http://homelandsecuritynewswire.net/estonia-pushes-joint-eu-cyber-response (14. julij 2011).

68. *European Network and Information Security Agency (ENISA).* Dostopno prek: http://www.enisa.europa.eu/ (6. maj 2011).
69. *Evropska komisija poziva k odprtemu, neodvisnemu in odgovornemu upravljanju interneta.* 2009. Dostopno prek: http://europa.eu/rapid/pressReleasesAction.do?reference=IP/09/951&format=HTML&aged=1&language=SL&guiLanguage=en (3. september 2011).
70. Evropska komisija. 2001. *Ustvarjanje varne informacijske družbe z izboljšanjem varnosti informacijske infrastrukture in bojem proti kibernetskemu kriminalu.* Bruselj. Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF (26. november 2011).
71. --- 2010a. E*vropa 2020. Strategija za pametno, trajnostno in vključujočo rast.* Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:SL:PDF (23. julij 2011).
72. --- 2010b. *Evropska digitalna agenda.* Dostopno prek http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245 :FIN:SL:PDF (23. julij 2011).
73. --- 2010c*. Izvajanje strategije notranje varnosti EU: pet korakov k varnejši Evropi 2010.* Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:SL:PDF (23. julij 2011).
74. --- 2011. *European principles and guidelines for Internet resilience and stability.* Dostopno prek: http://ec.europa.eu/information_society/policy/nis/docs/principles_ciip/guidelines_internet_fin.pdf (10. maj 2011).
75. Falliere, Nicolas. 2010. *Stuxnet Introduces the First Known Rootkit for Industrial Control System.* Symantec. Official Blog. Dostopno prek: http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices (26. november 2011).
76. Federal Emergency Management Agency. 2009. *Participant Guide - Comprehensive Cyberterrorism Defense Training Support Package.* Washington: U.S. Department of Homeland Security, Federal Emergency Management Agency. Dostopno prek: http://netacademy.iccms.edu/ courses/ networking/ security/manual.pdf (20. maj 2011).
77. *Federation of American Scientists.* 2011. Dostopno prek http://www.fas.org (20. oktober 2011).
78. *FEMA*. 2011. Dostopno prek: http://www.fema.gov/ (8. oktober 2011).

79. Ferfila, Bogomir ur. 2002. *Slovenija in Evropska unija.* Politični procesi in inštitucije. Ljubljana: Fakulteta za družbene vede.
80. *Fight against cybercrime.* 2011. Dostopno prek: http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/l33193b_en.htm (26. november 2011).
81. *First joint EU-US cyber security exercise conducted.* 2011. Dostopno prek http://www.enisa.europa.eu/media/press-releases/first-joint-eu-us-cyber-security-exercise-conducted-today-3rd-nov.-2011 (27. november 2011).
82. Franz, Timothy. 2011. The Cyber Warfare Professional. Realizations for Developing the Next Generation. *Air&Space Power Journal*, Summer 2011, 87-97.
83. *Global Cybersecurity Agenda.* 2011. Dostopno prek: http://www.itu.int/osg/csd/cybersecurity/gca/ (20. oktober 2011).
84. *Google Hack Attack Was Ultra Sophisticated, New Details Show*. 2010. Dostopno prek: http://www.wired.com/threatlevel/2010/01/operation-aurora/ (9. november 2011).
85. Gordon, Lawrence, Loeb, Martin in Zhou, Lei. 2011. The impact of information security breaches: Has therebeen a downward shift in costs? *Journal of Computer Security* 19: 33–56.
86. Gorman, Sean P. 2004.*The Revenge of Distance: Vulnerability Analysis of Critical Information Infrastructure.* Dostopno prek: http://arxiv.org/ftp/cond-mat/papers/0310/0310427.pdf (25. julij 2011).
87. *Green Paper on a European Programme for Critical Infrastructure Protection.* 2005. Comission. Dostopno prek: http://eur-lex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf (10. maj 2011).
88. Greengard, Samuel. 2010. The New Face of War. *Communication of the ACM*. Vol. 53, No.12: 20–22.
89. Grevi, Giovanni. 2009. *The interpolar world: a new scenario*. Occasional paper. European Union Institute for Security Studies (EUISS). Dostopno prek: http://www.iss.europa.eu/publications/detail/article/the-interpolar-world-a-new-scenario/ (20. avgust 2011).
90. Grizold, Anton in Bučar, Bojko. 2011. Izzivi sodobne varnosti: od nacionalne in mednarodne do človekove varnosti. *Teorija in praksa* 4/2011: 827–849.

91. Grizold, Anton. 2001. Nekaj izzivov izgradnji varnostne arhitekture v Evropi danes. *Teorija in praksa,* let. 38, 5/2001, 786–797. Dostopno prek http://dk.fdv.uni-lj.si /tip/tip20015Grizold.PDF (15. maj 2011).
92. Grizold, Anton. 2005. *Slovenija v spremenjenem varnostnem okolju.* Varnostne študije. Ljubljana: Fakulteta za družbene vede.
93. *Growing Business Dependenceon the Internet. New Risks Require CEO Action.* Business Roundtable. 2007. Dostopno prek: http://businessroundtable.org /uploads/news-center/downloads/200709_Growing_Business_Dependence_ on_the_Internet.pdf (16. avgust 2011).
94. *Hackers find new way to cheat on Wall Street.* Dostopno prek: http://www.infoworld.com/d/the-industry-standard/hackers-find-new-way-cheat-wall-street-everyones-peril-699 (16. avgust 2011).
95. Hafner-Fink, Mitja. *Nekatera temeljna vprašanja znanstvenega raziskovanja družbe.* Dostopno prek: http://www1.fov.uni-mb.si/mayer/MDR/Hafner%20 Fink%20Mitja-Znanost%20in%20 znanstveno%20raziskovanje.pdf (25. maj 2011).
96. Helmbrecht, Udo. 2011. *ENISA today and in the future*. ENISA. Dostopno prek: http://www.enisa.europa.eu/media/news-items/speech-in-the-european-parliament-may-2011 (25. julij 2011).
97. *Homeland Security seeks cyber counterattack system*. 2008. Dostopno prek: http://articles.cnn.com/2008-10-04/tech/chertoff.cyber.security_1_chertoff-government-cyberspace?_s=PM:TECH (3. september 2011).
98. *How Egypt shut down the internet.* 2011. Dostopno prek: http://www.telegraph. co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html (20. avgust 2011).
99. *Human development reports*. Dostopno prek: http://hdr.undp.org/ (10. julij 2011).
100. *ICANN vs. the World,* 2011. Dostopno prek: http://techland.time.com /2011/03/05/icann-vs-the-world/ (20. avgust 2011).
101. IETF. *Site Security Handbook*. 2011. Dostopno prek: http://tools.ietf.org /html/rfc2196 (24. oktober 2011).
102. *IMPACT Alliance.* 2011. Dostopno prek: http://www.impact-alliance.org/ home/index.html (20. oktober 2011).
103. *Impact Assesment Part 2. Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience.* Comission of the

European Communities. Brussels, 2009. Dostopno prek: http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2009/sec_2009_0399_en_part2.pdf (9. avgust 2011).

104. *Impact Assesment Part 3. Protecting Europe from large scale cyber attacks and disruptions: enhancing preparedness, security and resilience.* Comission of the European Communities. Brussels, 2009. Dostopno prek: http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2009/sec_2009_0399_en_part3.pdf (9. avgust 2011).
105. *Implementation of the CFSP and ESDP.* Dostopno prek: http://europa.eu/legislation_summaries/foreign_and_security_policy/cfsp_and_esdp_implementation/index_en.htm (5. april 2011).
106. Independent. *PlayStation Network becomes most Googled term after cyber attack.* Dostopno prek: http://www.independent.co.uk/life-style/gadgets-and-tech/playstation-network-becomes-most-googled-term-after-cyber-attack-2275543.html (6. maj 2011).
107. *Information Security Breaches Survey 2010, tehnical report.* Infosecurity Europe. London. Dostopno prek: http://www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf (17. avgust 2011).
108. *Information Security Forum.* 2007. The Standard of Good Practice of Information Security. London.
109. *Information Security Forum*. Dostopno prek: https://www.securityforum.org/ (5. julij 2011).
110. *Instrument for Stability 2007 – 2013.* Dostopno prek: http://europa.eu/legislation_summaries/foreign_and_security_policy/conflict_prevention/l14171_en.htm (7. maj 2011).
111. *Inštitut Evropske unije za varnostne študije*. 2011. Dostopno prek: http://europa.eu/agencies/ security_agencies/iss/index_sl.htm (1. april 2011).
112. *International Organization for Standardization*. 2011. Dostopno prek: http://www.iso.org/iso/home.htm (24. oktober 2011).
113. *International Strategy for Cyberspace.* 2011. Dostopno prek: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (9. oktober 2011).
114. International Telecommunication Union. 2005. *ITU internet Reports 2005: The Internet of Things*. *Executive summary.* Geneva. Dostopno prek:

http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf (11. februar 2012).

115. *International Telecommunication Union.* 2011. Dostopno prek: http://www.itu.int/en/Pages/default.aspx (9. oktober 2011)
116. International Telecommunication Union. 2011. *New GCA Brochure.* Geneva. Dostopno prek: http://www.itu.int/osg/csd/cybersecurity/gca/new-gca-brochure.pdf (20. oktober 2011).
117. *Internet Corporation for Assigned Names and Numbers.* Dostopno prek: http://www.icann.org/en/about/ (20. avgust 2011).
118. *Islovar*. Dostopno prek: http://www.islovar.org (28. april 2011).
119. *ISO/IEC 15408:2007.* 2007. Dostopno prek: http://www.iso.org/iso/search.htm?qt=15408&searchSubmit=Search&sort=rel&type=simple&published=on (24. oktober 2011).
120. *ISO/IEC 27001:2005.* 2005. Dostopno prek: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103 (24. oktober 2011).
121. *ISO/IEC 7498-1:1994*. 1994. Dostopno prek: http://www.ecma-international.org/activities/Communications/TG11/s020269e.pdf (9. februar 2011).
122. Janczewski, Lech J. in Colarik, Andrew M. 2007. *Cyber Warfare and Cyber Terrorism.* New York: Information Science Reference.
123. *Japonska: internet presenetljivo dobro preživel potres in cunami.* 2011. Dostopno prek http://www.monitorpro.si/41917/novice/japonska-internet-presenetljivo-dobro-prezivel-potres-in-cunami/ (25. julij 2011).
124. JASON. The Mitre Corporation. 2010. *Science of Cyber-Security*. Virginia, ZDA. Dostopno prek: http://www.fas.org/irp/agency/dod/jason/cyber.pdf (20. oktober 2011).
125. Jelušič, Ljubica. 1997. *Legitimnost sodobnega vojaštva.* Ljubljana: FDV.
126. --- 2002. Globalnost varnostnih interesov in groženj. *Teorija in praksa,* let. 39, 4/2002, 613-620. Dostopno prek http://dk.fdv.uni-lj.si/tip/tip20024Jelusic.PDF (10. maj 2011).
127. Jensen, Eric Talbot. 2010. Cyber Warfare and Precautions Against the Effects of Attacks. *Texas Law Review.* Vol. 88: 1533–1569.
128. *Julian Assange ready to meet police.* 2011. Dostopno prek: http://www.bbc.co.uk/news/ uk-11930488; (10. julij 2010).

129. Kaj je ACTA? 2012. Dostopno prek: http://ec.europa.eu/slovenija/hp/2012-0203-acta_sl.htm (11. februar 2012).
130. Khansa, Lara in Liginlal, Divakaran. 2009. Quantifyingthe Benefits of Investing in Information Security. *Communication of the ACM.* Vol. 52, No.11: 113–117.
131. Komisija evropskih skupnosti. 2001. *Varnost omrežij in informacij: predlog pristopa evropske politike.* Dostopno prek: http://eur-lex.europa.eu/LexUriServ/site/ en/com/2001/com2001_0298en01.pdf (29. september 2011).
132. --- 2003. *Varna Evropa v boljšem svetu: evropska varnostna strategija.* Dostopno prek: http://www.consilium.europa.eu /uedocs/cmsUpload/031208ESSIISL.pdf (5. maj 2011).
133. --- 2005. *Zelena knjiga o Evropskem programu za varovanje ključne infrastrukture.* Bruselj. Dostopno prek http://eur-lex.europa.eu/LexUriServ/site/sl/com/2005/com2005_0576 sl01.pdf (20. julij 2011).
134. --- 2006a. *Sporočilo Komisije o Evropskem programu za varovanje ključne infrastrukture.* Bruselj. Dostopno prek http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:078 6:FIN :SL:PDF (21. julij 2011).
135. --- 2006b. *Strategija za varno informacijsko družbo: Dialog, partnerstvo in povečanje vpliva in moči.* Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:SL:PDF(29. september 2011).
136. --- 2008. *Poročilo o izvajanju evropske varnostne strategije. Zagotavljanje varnosti v spreminjajočem se svetu.* Dostopno prek: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/SL/reports/ 104650.pdf (3. september 2011).
137. --- 2009a. *Internet stvari – akcijski načrt za Evropo*. Bruselj. Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do? uri=COM:2009:0278:FIN:SL:PDF (11. februar 2012).
138. --- 2009b. *Kako zaščititi Evropo pred obsežnimi kibernetskimi napadi in prekinitvami: izboljšati pripravljenost, varnost in odpornost* 2009. Comission. Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ. do?uri=COM:2009:0149:FIN:SL:PDF (10. maj 2011).

139. --- 2009c. *Priporočilo Komisije o izvajanju načel varstva zasebnosti in varstva podatkov v aplikacijah podprtih z radiofrekvenčno identifikacijo*. Bruselj. Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:SL:PDF (11. februar 2012).
140. --- 2009d. *Sporočilo o prihodnosti omrežij in interneta.* Bruselj. Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0594:FIN:SL:PDF (11. februar 2012).
141. --- 2011e. *Dosežki in naslednji koraki: h globalni kibernetski varnosti.* Dostopno prek:http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:SL:PDF (5. oktober 2011).
142. Kovačič, Matej. 2003. *Zasebnost na internetu*. Ljubljana: Mirovni inštitut, Inštitut za sodobne družbene in politične študije.
143. Kunc, Urban. 2011. Internet stvari: spodbujanje ali regulacija? Agencija za pošto in elektronske komunikacije RS. Ljubljana. Dostopno prek: http://www.ltfe.org/wp-content/uploads/2011/05/Internet-stvari_Urban_Kunc_APEK.pdf (11. februar 2012).
144. *Leto 2011 v znamenju hekerjev in kibernetskih vojn.* 2011. Dostopno prek: http://hack-protect.com/news.php?extend.205.1 (19. avgust 2011).
145. Libicki, Martin. 2009. *Cyberdeterrence and Cyberwar.* RAND Corporation. Dostopno prek: http://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (20. avgust 2011).
146. Malešič, Marjan ur. 2002. *Nacionalna in mednarodna varnost*. Ljubljana: Fakulteta za družbene vede.
147. Malešič, Marjan, Hrvatin, Sandra B. in Polič, Marko. 2006. *Komuniciranje v krizi*. Ljubljana: FDV.
148. Malešič, Marjan, ur. 2004. *Krizno upravljanje in vodenje v Sloveniji*. Ljubljana: FDV.
149. Malešič, Marjan, ur. 2006. *Varnost v postmoderni družbi*. Ljubljana: FDV.
150. Malešič, Marjan. Tri teoretične perspektive sodobne varnosti. *Public/Javnost, Vol.1,* (1994) 4, 97–104. Dostopno prek: http://www.javnost-thepublic.org/media/datoteke/Malesic_4-1994.pdf (16. julij 2011).
151. McAfee. 2009. *Virtual Criminology Report. Virtually here: The Age of cyber Warfare.* Santa Clara: McAfee, Inc.

152. --- 2010. *Advanced Persistent Threat.* Dostopno prek: http://www.mcafee.com/us/resources/solution-briefs/sb-advanced-persistent-threats.pdf (9. november 2011).
153. --- 2011. *In the Dark. Crucial Industries Confront Cyberattacks.* Santa Clara: McAfee, Inc. Dostopno prek: http://www.mcafee.com/us /resources/reports/rp-critical-infrastructure-protection.pdf (25. maj 2011).
154. *MITRE.* 2011. Dostopno prek: http://www.mitre.org/ (20. oktober 2011).
155. Morgenthau, Hans Joachim. 1995. *Politika med narodi: borba za moč in mir.* Ljubljana: DZS.
156. *MPLS v omrežjih ATM.* Fakulteta za elektrotehniko, Laboratorij za telekomunikacije. Ljubljana, 2011. Dostopno prek: http://www.ltfe.org/wp-content/pdf/mpls.pdf (12. avgust 2011).
157. *Music and film industry websites targeted in cyber attacks.* 2010. Dostopno prek: http://www.telegraph.co.uk/technology/internet/8013548/Music-and-film-industry-websites-targeted-in-cyber-attacks.html (10. februar 2012).
158. Myrli, Sverre. 2011. NATO and Cyber Defence. *Annual Cyberspace Focus MILTECH* 3/2011. 86–90.
159. *National Cyber Security Division.* Dostopno prek http://www.dhs.gov/xabout/structure/editorial_0839.shtm (22. julij 2011).
160. National Institute of Standards and Technology. 1995. *An Introduction to Computer Security: The NIST Handbook.* New York. Dostopno prek: http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (24. oktober 2011).
161. --- 2011. *Special Publications (800 Series).* Dostopno prek: http://csrc.nist.gov/publications/PubsSPs.html (24. oktober 2011).
162. *National Protection and Programs Directorate*. Dostopno prek http://www.dhs.gov/xabout/structure/editorial_0794.shtm (22. julij 2011).
163. National Protection and Programs Directorate. 2007. *Critical infrastructure Warning Information Network.* US Department of Homeland Security Headquarter Offices. Nebraska.
164. *NATO Cooperative Cyber Defence Centre of Excellence*. 2011. Dostopno prek: http://www.ccdcoe.org/ (18. oktober 2011).
165. NATO. 2010a. *Lisbon Summit Declaration*. Dostopno prek: http://www.nato.int/cps/en/natolive/official_texts_68828.htm#cyber (18. oktober 2011).

166. --- 2010b. *Strategic Concept fot the Defence and Security of the Members of the NATO. Active Engagement, Modern Defence.* Lisbon. Dostopno prek: http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf (18. oktober 2011).
167. --- 2011. *Defending the networks. The NATO Policy on Cyber Defence.* Brussels. Dostopno prek: http://www.nato.int/nato_static/assets/pdf/pdf_2011_09/ 20111004_110914-policy-cyberdefence.pdf (18. oktober 2011).
168. Newman, Edward. 2001. Human security and constructivism. *International studies perspectives 2* (3): 239-251. Dostopno prek http://people.cas.sc.edu/ coate/ Readings/Newman.pdf; (2. julij 2011).
169. Nicander, Lars. 2010. Shielding the net - understanding the issue of vulnerability and threat to the information society. *Policy Studies Vol. 31*. No. 3: 283-300. Centre for Asymemetric Threat Studies, Stockholm.
170. OECD. 2008a. *Malicious Software (Malware): A Security Threat to the Internet Economy.* Seul. Dostopno prek: http://www.oecd.org/dataoecd/53/34/ 40724457.pdf (12. november 2011).
171. --- 2008b. *Recommendation of the Council on the Protection of Critical Information Infrastructures.* Dostopno prek: http://www.oecd.org/ dataoecd/1/13/40825404.pdf (26. november 2011).
172. --- 2008c. *Shaping Policies for the Future of the Internet Economy*. Dostopno prek http://www.oecd.org/dataoecd/1/29/40821707.pdf (29. september 2011).
173. --- 2011d. *Fibre Access: Network Developments in the OECD Area.* OECD Digital Economy Papers, No. 182. Dostopno prek: http://www.oecd-ilibrary.org/science-and-technology/fibre-access_5kg9sqzz9mlx-en (20. avgust 2011).
174. *Office of Cybersecurity and Communications.* Dostopno prek http://www.dhs.gov/ xabout/structure/gc_1185202475883.shtm (14. julij 2011)
175. O'Hara, Timothy F. 2004. *Cyber warfare/cyber terrorism.* Carlisle: U.S. Army War College. Dostopno prek: http://www.dtic.mil/cgi-bin/GetTRDoc?Location= U2&doc=GetTRDoc.pdf&AD=ADA424310 (20. maj 2011)
176. Ollman, Gunther. 2011. *Understanding the Modern DDoS Threat*. Damballa. Dostopno prek: http://www.damballa.com/downloads/r_pubs/WP_Understanding_ the_Modern_DDoS_attack.pdf (12. november 2011).

177. *Organizacija za gospodarsko sodelovanje in razvoj.* 2011. Dostopno prek: http://www.oecd.org (20. oktober 2011).
178. Pogovor z omrežnim strokovnjakom. Prostori zasebnega telekomunikacijskega operaterja T-2 d.o.o., junij 2011.
179. *Political hacktivists turn to web attacks*. 2010. Dostopno prek: http://news.bbc.co. uk/2/hi/technology/8506698.stm (10. februar 2012).
180. Prezelj, Iztok. 2001. *Grožnje varnosti, varnostna tveganja in izzivi v sodobni družbi.* Teorija in praksa, let. 38, 1/2001, 127–141. Dostopno prek http://dk.fdv.uni-lj.si/ tip/tip20011Prezelj.PDF (2. maj 2011).
181. --- 2008. *Challenges in Conceptualizing and Providing Human Security*. HUMSEC Journal, Issue 2: 6–26. Dostopno prek http://www.etc-graz.at/cms/index.php?id=356, (6. julij 2011).
182. --- 2010. *Kritična infrastruktura v Sloveniji*. Ljubljana: Fakulteta za družbene vede.
183. Privacy Impact Assessment EINSTEIN Program. *Collecting, Analyzing, and Sharing Computer Security Information Across the Federal Civilian Government.* Department of Homeland Security National Cyber Security Division. ZDA. 2004. Dostopno prek: http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ eisntein.pdf (3. september 2011).
184. *Profile: Wikileaks founder Julian Assange.* Dostopno prek: http://www.bbc.co.uk /news/world-11047811; (11. julij 2011).
185. *Q&A's on the first, pan-European Cyber Security Excercise CYBER EUROPE 2010.* 2010. ENISA. Dostopno prek: http://www.enisa.europa. eu/media/news-items/faqs-cyber-europe-2010-final (10. maj 2011)
186. Ragin, Charles. 2007. *Družboslovno raziskovanje – Enotnost in raznolikost metode.* Ljubljana: Fakulteta za družbene vede.
187. Rančigaj, Katja. 2010. *Informacijska varnostna kultura v državni upravi*. Ljubljana. Fakulteta za družbene vede.
188. *RAND Corporation*. Dostopno prek: http://www.rand.org/; (30. junij 2011).
189. *Remarks by the President on Securing our Nation's Cyber Infrastructure. The* White House. Office of the Press Secretary. 2009 Dostopno prek: http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure (14. julij 2011).

190. Rožman, Marko. *Evalvacija novejših tehnologij za razširitev zmogljivejših optičnih omrežij.* Ekonomska fakulteta. Ljubljana. Dostopno prek: http://www.cek.ef.uni-lj.si/magister/rozman2570.pdf (25. julij 2011).
191. Schwartzstein, Stuart ed. *The Information Revolution and National Security. Information, Power and Grand Strategy: In Athena's Camp.* Washington, D.C. 1996. Dostopno prek: http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch6.pdf (3. avgust 2011).
192. *Security & Resilience in Governmental Clouds: Making an informed decision.* 2011. ENISA Dostopno prek: http://www.enisa.europa. eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds (25. februar 2011).
193. Seghal, Naresh, Sohoni, Sohum, Xiong, Ying, Fritz, David, Mulia, Wira in Acken, John. 2011. A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing. *IETE Technical Review*, vol. 28, issue 4: 279–291.
194. Sheehan, Michael. 1999. *Community, Anarchy and Critical Security.* University of Aberdeen. Scottish Centre for International Security Dostopno prek: www.anarchist-studies-network.org.uk/documents/ ECPR.doc (5. julij 2011).
195. *SI-CERT.* Dostopno prek: http://www.cert.si (5. maj 2011).
196. *Skoraj vsa mobilna programska oprema je vohunska.* 2011. Dostopno prek: http://hack-protect.com/news.php?extend.206.1 (13. avgust 2011).
197. *Slovar slovenskega knjižnega jezika.* 2011. Dostopno prek: http://bos.zrc-sazu.si/sskj.html (4. november 2011).
198. Sommer, Peter in Brown, Ian. 2011. *Reducing Systemic Cybersecurity Risk*. London School of Economics in Oxford Internet Institute v okviru OECD. Dostopno prek: http://www.oecd.org/dataoecd/57/44/46889922.pdf (20. oktober 2011).
199. *Sony Playstation Network Cyber Attack Revealed.* 2011. Dostopno prek: http://www.security-technologynews.com/news/sony-playstation-network-cyber-attack-revealed.html (6. maj 2011).
200. Sophos. 2011. *Security threat report 2011.* Dostopno prek: http://www.sophos.com/medialibrary/Gated%20Assets/white%20papers/sophossecuritythreatreport2011wpna.pdf (30. december 2011).

201. *Spletno oko*. 2011. Dostopno prek: http://www.spletno-oko.si/ (3. september 2011)
202. *STOP.THINK.CONNECT.* 2011. Dostopno prek http://www.dhs.gov/files/events/stop-think-connect.shtm (8. oktober 2011).
203. *Strategija razvoja širokopasovnih omrežij v Republiki Sloveniji.* Dostopno prek: http://www.mvzt.gov.si/fileadmin/mvzt.gov.si/pageuploads/DEK/Elektronske_komunikacije/Strategije/Strategija_BB_2008-03-25_SI.pdf (25. julij 2011) .
204. *Strategy for Operating in Cyberspace.* 2011. Dostopno prek: http://www.defense.gov/news/d20110714cyber.pdf (8. oktober 2011).
205. Svet Evrope. 2001. *Convention on Cybercrime.* Budimpešta. Dostopno prek http://conventions.coe.int/Treaty/en/Treaties/html/185.htm (26. november 2011).
206. Svet Evropske unije. 2005. *Okvirni sklep Sveta o napadih na informacijske sisteme.* Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:SL:PDF (26. november 2011).
207. --- 2008. *Direktiva o ugotavljanju in določanju evropske kritične infrastrukture ter o oceni potrebe za izboljšanje njene zaščite.* Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345: 0075:0082 :SL:PDF (5. oktober 2011).
208. --- 2011. *Trgovinski sporazum za boj proti ponarejanju med Evropsko unijo in njenimi državami članicami, Avstralijo, Kanado, Japonsko, Republiko Korejo, Združenimi mehiškimi državami, Kraljevino Maroko, Novo Zelandijo, Republiko Singapur, Švicarsko konfederacijo in Združenimi državami Amerike*. Bruselj. Dostopno prek: http://register.consilium.europa.eu/pdf/sl/11/st12/st12196.sl11.pdf (11. februar 2012).
209. Svete, Uroš. 2005. *Varnost v informacijski družbi*. Ljubljana: FDV.
210. *Symantec internet Security threat Report.* 2007. California: Symantec Corporation
211. Symantec. 2011. *Advanced Persistent Threats: A Symantec Perspective.* Dostopno prek: http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf (9. november 2011).
212. Syria: Ban voices deep regret after Security Council fails to agree on resolution. 2012. Dostopno prek: http://www.un.org/apps/news/story.asp?NewsID=41144&Cr=Syria&Cr1= (11. februar 2012).

213. *The 60 Minute Network Security Guid: First Steps Towards a Secure Network Environment.* 2006. Systems and Network Attack Center (SNAC). National Security Agency. Dostopno prek: http://www.nsa.gov /ia/_files/support/I33-011R-2006.pdf (20. maj 2011).
214. *The Comprehensive National Cybersecurity Initiative.* 2011. Dostopno prek: http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf (3. september 2011).
215. *The Future of the Information Revolution in Europe - Conference proceedings.* Dostopno prek: http://www.rc.rand.org/pubs/conf_ proceedings/CF172.html (30. april 2011).
216. *The Human Security Framework and National Human Development Reports.* Dostopno prek: http://hdr.undp.org/en/media/Human_Security _GN.pdf (11. julij 2011).
217. *The Internet Assigned Numbers Authority*, IANA. Dostopno prek: http://www.iana.org/ (3. september 2011).
218. *The Internet Engineering Task Force*, *IETF*. Dostopno prek: http://www.ietf.org/ (3. september 2011).
219. *The National Strategy to Secure Cyberspace.* 2003. Dostopno prek: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf (8. oktober 2011).
220. *The New Speed of Money, Reshaping Markets.* Dostopno prek: http://www.nytimes.com /2011/01/02/business/02speed.html?_r=1; (16. avgust 2011).
221. *The strange virtual world of 4chan*. 2010. Dostopno prek: http://www.bbc.co.uk /news/magazine-10520487 (10. februar 2012).
222. Toplišek, Alen. 2010. *Človekova varnost: med konceptom in prakso.* LE MONDE diplomatique – februar 2010, Ljubljana.
223. Toš, Niko in Hafner-Fink, Mitja. 1998. *Metode družboslovnega raziskovanja*. Ljubljana, Fakulteta za družbene vede.
224. *Translating the U.S. International Cyber Strategy Into Action.* 2011. Dostopno prek: http://www.worldpoliticsreview.com/articles/8900/translating-the-u-s-international-cyber-strategy-into-action (9. oktober 2011).
225. UNDP - United Nations Development programme. 1994. *Human development report.* New York. Dostopno prek http://hdr.undp.org/reports/ global/ 1994/en/pdf/ hdr_1994_ch2.pdf , (10. december 2010).

226. *United States Computer Emergency Readiness Team.* 2011. http://www.us-cert.gov/ (8. oktober 2011).
227. *Upravljanje interneta: naslednji koraki.* Resolucija Evropskega parlamenta. 2010. Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:236E:0033:0040:SL:PDF (3. september 2011).
228. *Uredba o evropski kritični infrastrukturi.* 2011. Dostopno prek: http://www.uradni-list.si/1/content?id=103668 (5. oktober 2011).
229. *US appoints first cyber warfare general.* 2011. Dostopno prek: http://www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare-general (8. oktober 2011).
230. US Army Training and Doctrine Command. 2005. *Cyber Operations and Cyber Terrorism, Handbook No. 1*.02. Fort Leavenworth: US Army Training and Doctrine Command.
231. *US Critical infrastructure Warning Information Network complete.* Dostopno prek: http://www.continuitycentral.com/news01838.htm (25. julij 2011).
232. Van Derwerken, Jay in Ubell, Robert. 2011. Training the Cyber Security Frontlines. *Training and Development.* Junij 2011: 46–50.
233. *Vdor v Sonyeve uporabniške zbirke.* 2011. Dostopno prek: http://www.cert.si/obvestila/obvestilo/article/vdor-v-sonyjeve-uporabniske-zbirke/35.html (5. maj 2011).
234. *Virtual Criminology Report. Cybercrime Versus Cyberlaw.* 2008. Santa Clara: McAfee, Inc.
235. *Virtual Criminology Report. Virtually here: The Age of cyber Warfare.* 2009. Santa Clara: McAfee, Inc.
236. Vogrin, Andreja, Iztok Prezelj in Vojko Bučar. 2008. *Človekova varnost v mednarodnih odnosih.* Mednarodni odnosi. Ljubljana: Fakulteta za družbene vede.
237. Walt, Stephen M. 1998. International relations: One world, manj theories. Washington, *Foreign Policy,* Št. 110, Special Edition: Frontiers of Knowledge. Dostopno prek http://faculty.maxwell.syr.edu/hpschmitz/PSC124/PSC124 Readings/WaltOneWorldManyTheories.pdf (16. julij 2011) .
238. *Washington moves to classify cyber-attacks as acts of war.* 2011. Dostopno prek: http://www.guardian.co.uk/world/2011/may/31/washington-moves-to-classify-cyber-attacks (24. avgust 2011).

239. Wellings, Richard ur. 2009. *A Beginner's Guide to Liberty.* Adam Smith Research Institute, London.
240. *Wikileaks: site list reveals US sensitivities*. Dostopno prek: http://www.bbc.co.uk/news/11932041 (10. julij 2011).
241. World Bank Data Indicator. 2011. Dostopno prek: http://data.worldbank.org/indicator (21. avgust 2011).
242. *World Telecommunication/ICT Indicators Database.* 2010. Dostopno prek: http://www.itu.int/ITU-D/ict/statistics/ (20. oktober 2011).
243. Yost, David. 2010. NATO's evolving purposes and the next Strategic Concept. *International Affairs* 86, 489–522.
244. Združeni narodi. 2002. Resolucija ZN 57/239. *Creation of a global culture of cybersecurity.* Dostopno prek: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf (4. november 2011).
245. Združeni narodi. 2003. Resolucija ZN 58/199. *Creation of a global culture of cybersecurity and the protection of critical information infrastructures.* Dostopno prek: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf (4. november 2011).