UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Maša Dobrina

Evropska unija in informacijska varnost

Diplomsko delo

Ljubljana, 2009

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Maša Dobrina

Mentor: asist. dr. Uroš Svete

Somentorica: doc. dr. Sandra Bašić – Hrvatin

Evropska unija in informacijska varnost

Diplomsko delo

Ljubljana, 2009

Zahvala

Staršem, sorodnikom in prijateljem, ker ste verjeli vame, me podpiral in spodbujali.

Evropska unija in informacijska varnost

V diplomski nalogi sem pregledala različne konstruktivistične pristope k pojasnjevanju (informacijske) varnosti. Vsem konstruktivizmom je skupna postavitev posameznika v ospredje, njegova kultura, interakcija z IKT, kar je pri obravnavanju informacijske varnosti pomembno, saj je prav uporabnik najšibkejša točka v tem tehničnem računalniškem sistemu. Predstavila bom tudi varnostne mehanizme, s katerimi lahko zagotavljamo informacijsko varnost glede na različne grožnje in referenčne objekte. Ti mehanizmi pa niso le tehnični, temveč tudi organizacijski in fizični. Kot primer varnostnega mehanizma sem šla še globlje in se prestavila na mikroraven varnosti. Varnostni mehanizem celice, ki ima anarhični pristop k varnosti sem primerjala s prav tako anarhično strukturo mednarodnega sistema in poskušala nadalje ugotoviti, ali je celični varnostni mehanizem aplikativen na makrosocialno raven. Praktični del naloge pa obsega pregled ureditve področja informacijske varnosti v EU ter nasvete za izbljšanje stanja na tem področju v prihodnosti.

Ključne besede: *konstruktivizem, informacijska varnost, Evropska unija, decentralizacija, omrežja.*

European Union and information security

In the paper, I reviewed the various constructivist approaches to explaining (information) security. All constructivist approaches have a common setting, positioning the individual as the starting point of explanation, his culture, interaction with information communication technology, which is in the debate about information security important as it is the user who is the weakest point of the technical computer system. The paper includes security mechanisms that provide information security depending on the various threats and referential actors. These mechanisms are not only of a technical nature but also organizational and physical. As an example of a safety mechanism, I went even deeper, and moved to micro level of tackling security. I compared security mechanism of cells, which have an anarchical approach to security, with the anarchical structure of the international system and attempted to further determine whether the cellular mechanism of protection is applicable to the macro social world. The practical part of the paper deals with the review of the current state of information security in the European Union and some suggestions for tackling security breaches in the future.

Keywords: *Constructivism, information security, European union, decentralization, networks.*

KAZALO

SEZNAM AKRONIMOV

CERT – orig. Computer Emergency Response Team (skupine za hitro odpravo škode kibernetskih napadov)
CFSP – orig. Common Foreign Security Policy (ali SZVP – skupna zunanja varnostna politika Evropske unije)
CI – orig. Critical Infrastructure (kritična infrastruktura)
CIIP – orig. Critical Informaciton Infrastructure Protection (zaščita kritične informacijske infrastrukture)
CIIRCO – orig. Critical Information Infrastructure Research Coordination (koordinacija raziskovanja kritične informacijske infrastrukture)
CIWIN- orig. Critical Infrastructure Warning Infromation Network (opozorilno informacijsko omrežje za kritično infrastrukturo)
CORDIS – orig. Community Research and Development Information Service (služba Skupnosti za informacije o raziskavah in razvoju)
EAPC – orig. Euro-Atlantic Partnership Council (evropsko-atlantski partnerski svet)
ECI – orig. European Critical Infrastructure (evropska kritična infrastruktura)
ENISA – orig. European Network and Information Security Agency (evropska agencija za omrežno in informacijsko varnost)
EPCIP – orig. European Program for Critical Infrastructure Protection (evropski program za zaščito kritične infrastrukture, t. i. »Green Paper«)
ESDP – orig. European Security and Defence Policy – evropska varnostna in obrambna politika
ESRAB – orig. European Security Research Advisory Board (svetovalni odbor za evropsko raziskovanje varnosti)
ESRIF – orig. European Security Research and Innovation Forum (evropski forum za raziskovanje varnosti in inovacije)
ESRP – orig. European Security Research Programme (evropski raziskovalni program za varnost)
EU – Evropska unija
EVS – evropska varnostna strategija
IDS – orig. Intrusion Detection System (sistem za odkrivanje vdorov)
IKT – informacijsko – komunikacijska tehnologija
IPv6 – internetni protokol verzija 6
ISP – orig. Internet Service Provider (ponudnik internetnih storitev)
IST – orig. Information Society Technology (tehnologije informacijske družbe)
MTP – orig. Multiannual Thematic Programmes (večletni tematski programi EU na področju informacijske varnosti)
NCI – orig. National Critical Infrastructure (državna kritična infrastruktura)
NVO – nevladne organizacije
OECD – orig. Organization for Economic Co-operation and Development (organizacija za gospodarsko sodelovanje in razvoj)
OIV – omrežna in informacijska varnost
RAS – orig. Rapid Alert System (sistem hitrega obveščanja o nevarnostih)
RFID – orig. Radio Frequency IDentification (identifikacija z radijskimi valovi)
VPN – orig. Virtual Private Network (virtualno zasebno omrežje)
ZN – Združeni narodi

1 UVOD

Koncentrirane specializirane enote informacij so disperzna in pluralna, med seboj povezana, nesimetrična središča, ki jih uporabniki iščejo glede na njihove identitete in interese. Cilj je vedno enak: najti ustrezno informacijo v sistemu. V mednarodnih odnosih je to lahko konsenz o rešitvi, ki zagotavlja zadovoljstvo obeh vpletenih strani ali na primer konsenz o nenapadanju med državama ali pa eliminacija virusa, ko gre za omrežno varnost. Tudi države iščejo rešitve v mednarodnem sistemu, če same niso kos varnostni grožnji, ki jim preti, posameznik lahko na internetu poišče politično skupino, ki zagovarja njegova stališča do določenega družbenega vprašanja. Skozi sodelovanje v taki skupini je posameznikovo delovanje, uresničevanje identitete ter interesov bližje temu, da se to mnenje uveljavi v pravni veljavi bodisi na državni ali naddržavni ravni.

V diplomskem delu bom poskušala povezati koncept nacionalne varnosti, družbene varnosti in globalne varnosti s konstruktivistično razlago mednarodnih (meddržavnih) odnosov. Komunikacijska teorija mednarodnih odnosov, ki povezuje kibernetske pojme z mednarodnimi odnosi, je po mojem mnenju visoko kompatibilna s konstruktivizmom, ki v ospredje postavlja kulturo. Kultura pa se v sodobnem času prenaša preko IKT, zato sem v razlago vključila tudi konstruktivistične teorije medijev. Koncept omrežne in informacijske varnosti bom preučila s konstruktivističnim razvojem računalniške znanosti. Kot navezavo na kulturo in oblikovanje interesov identitet (tako posameznika ali večjih družbenih skupin), pa bom v razpravo vključila tudi nekaj besed o semiotiki, ki razlaga konstrukcijo pomena na zelo podrobni, simbolno – idejni paradigmi. Tudi semantične prvine medijev in dojemanja (medijske) realnosti se pojasnjujejo s konstruktivizmom, vključila pa sem jih za to, ker je internet avtocesta različnih informacij in govorimo o konvergenci medijev, saj se televizija, radio in internet vedno bolj povezujejo, zato je tudi na mestu, da se medijski diskurz in njegovo percepcijo pojasni s konstruktivizmom.

Vsi koncepti pa so del pojma varnosti in odvisno je od ravni analize, kateri koncept se uporablja. Glavno sporočilo moje teoretične usmerjenosti pa je ravno filozofija, da je vse vzajemno odvisno, interaktivno in skonstruirano iz različnih prepletajočih se dejavnikov, ki se jih v realnosti ne da distancirati, pri teoretskih razpravah pa si lahko upamo poskusiti tako razločevanje (preučevanje) za poenostavljen prikaz družbenega odnosa do varnosti. Tako sem se odločila predvsem zaradi raziskovalnega vprašanja, ki se osredotoča na anarhično ureditev nekaterih struktur: anarhičnost interneta in anarhičnost mednarodnega političnega sistema nakazujeta na skupno točko (ahierarhična struktura sistema), iz katere izhaja osnovni

postopek za obravnavo groženj varnosti v sistemu, ki je podoben, ali pa vsaj teoretično in hipotetično primerljiv. Če ima sistem določeno strukturo, ima tudi glede na strukturo določeno logiko reševanja (varnostnih) problemov. Če torej ima določena osnovna struktura sistema tudi odzivni mehanizem na grožnje, potem imata tudi anarhična sistema primerljive metode upravljanja z grožnjami oz. imata tudi isti osnovni sistem za vzdrževanje in nadgradnjo varnosti, prvi je primer informacijske, drugi primer mednarodne varnosti, ki se med sabo prepletata, oz. sta soodvisni. Vzdrževanje ravnotežja sistema (varnosti) se vzpostavlja z upoštevanjem odziva ter nenehnim izboljševanjem in evolucijo sistema. Posodobitev protivirusnega programa lahko primerjamo z globalnim javnim mnenjem, raziskavami, izobraževanjem, komunikacijo in odnosi, ki nakazujejo nadaljnji razvoj (mednarodnega) sistema, če gre seveda za demokratične države Zahoda, ki za legitimizacijo vladanja potrebujejo podporo ljudstva.

Hierarhični sistem ima centralno direktivo reševanja problemov. Tok odzivanja je vertikalen, enosmeren (brez upoštevanja posameznika) in otežen z birokracijo. Medtem pa anarhični sistem, v katerem naj bi imeli vsi pravico do informiranosti[1] in dostop do informacij, pa se s pomočjo transparentne komunikacije (preko informacijsko komunikacijske tehnologije, v nadaljevanju IKT) lahko pride do informacij, ki pomagajo identificirati grožnjo, jo onemogočiti, preučiti vzroke ogrožanja, najti odgovore na vzroke, jih odpraviti in sanirati nastalo škodo ter preventivno nadgraditi sistem z redefinicijo (oz. preoblikovanjem) vzroka oz. grožnje, da postane integralni del procesov v sistemu. Na takšen način tudi protivirusni program zazna virus, ga da v karanteno ali ga izbriše in na koncu posodobi bazo virusov, ki hrani informacije o informacijski varnosti.

Država, ko zazna grožnjo iz strani druge države (na primer Slovenija pri Hrvaški), mora najprej preučiti vse možnosti za razrešitev grožnje. Ko pa problem ni nujno vedno pravilno in iskreno definiran, se pokaže vrednost resnične in transparentne komunikacije. Po rešitvi grožnje pa se bi naj po mojem mnenju sprejele še politike za vzdrževanje skupnih interesov, izboljševanje hrvaško slovenskih odnosov ter preprečevanje nadaljnjih konfliktov med državama. Upoštevati moramo delovanje držav v skladu z univerzalnimi normami in človekovimi pravicami, ki delujejo kot »osnovni fizikalni zakoni« mednarodnega (družbenega) sistema. Če bi vse države ravnale v skladu s temi normami in spoštovale osnovne človekove pravice, kot morajo računalniki imeti skupni protokol za povezovanje in komuniciranje, potem bi posameznikova varnost bila na višjem nivoju kot je danes. V

[1] Vsi seveda v realnosti nimamo svobodnega dostopa do vseh vrst informacij, vseeno pa se je ta sfera s pojavom interneta razširila. Še posebej pa se je razširila s pojavom črnega trga s hekersko programsko opremo.

diplomskem delu bom torej poskusila ugotoviti, ali obstaja osnovno vezivo, ki obstaja v vsakem anarhičnem sistemu (osnovni etični zakoni pri ljudeh oz. fizikalni zakoni v naravi). Pri tem je potrebno pripomniti, da vsak na prvi pogled anarhična struktura lahko ob podrobnejšem preučevanju izkaže kot funkcionalno dovršen sistem. Tak primer je lahko varnostni mehanizem v celicah, ki je tudi omenjen v diplomskem delu.

Menim namreč, da moramo najprej razumeti majhne stvari, da lahko razumemo večje; moramo poznati človekovo osebnost, da lažje razumemo njegove potrebe po varnosti in tako moramo tudi najprej natančno definirati kritično infrastrukturo referenčnega objekta varnosti, da bi lahko potem razvili primerno varnostno strategijo, pa naj gre za politike EU ali pa za tehnične ukrepe v podjetju z namenom povečanja omrežne varnosti.

2 METODOLOŠKO-HIPOTETIČNI OKVIR

2.1 Opredelitev ciljev preučevanja / analize

Namen te naloge je preučiti informacijsko varnost v Evropski uniji. V diplomski nalogi bom poskušala opredeliti glavne značilnosti pojmov: konstruktivizem, varnost, informacijska varnost, informacijski sistem, varnostni mehanizem. Nadalje bom poskušala ugotoviti, ali so trenutne smernice razvoja interneta primerne, na kakšne načine EU varuje svoje uporabnike in ali je ta način primeren glede na pričakovani razvoj v »informacijski dobi«, kot zelo radi govorimo današnjemu času. Ugotoviti želim tudi, katere so sodobne grožnje informacijski varnosti in kakšni so mehanizmi, s katerimi se spoprijemamo s temi grožnjami.

2.2 Raziskovalno vprašanje

Anarhični sistem (struktura)[2] *mora imeti tudi anarhično organizirane varnostne mehanizme. Internet in mednarodni politični sistem imata oba anarhično strukturo, torej morata imeti vsaj podobne in primerljive varnostne mehanizme. Ali se podobni mehanizmi kažejo tudi v trenutnih politikah Evropske unije? Vsebinske dokaze o takšnih dilemah pa sem poskušala opisati v diplomskem delu.*

[2] Pri tem je treba podariti, da nimam v mislih strukturo kot jo razlagajo strukturalisti. Moč ne izhaja iz strukture, ki je anarhična, moč pridobi celoten sistem, saj deluje usklajeno in optimalno glede na prihajajoče grožnje iz drugih, eksternih sistemov. Nekatere ideje v delu se vsebinsko nanašajo tudi na sistemsko teorijo. Preučuje se namreč odnos vplivanja med sistemom in strukturo, vprašanje pa je skoraj podobno tistemu, ki sprašuje »kaj je bilo prej, kura ali jajce?«, saj je vpliv obojestranski ter v kontinuiranem procesu, kot je družbeni sistem vedno »posodobljen« s kulturo, razvojem, komunikacijo in medsebojnimi odnosi.

2.3 Ključne metode dela

Pri oblikovanju diplomske naloge sem uporabila več metod, da bi raziskala problematiko, ki je z njo povezana. Preden sem pričela pisati nalogo, sem z *metodo zbiranja virov* zbrala in predelala razpoložljivo literaturo, ki je vključevala znanstvene monografije, strokovne članke, uradne dokumente. Pri pisanju teoretskega okvirja, pri opredelitvi ključnih pojmov in koncepta informacijske varnosti sem uporabila *metodo analize vsebine primarnih in sekundarnih virov*. Pri opisu dejavnikov, ki vplivajo na informacijsko varnost, sem uporabila predvsem *opisno metodo*, da bi opisala vse dejavnike, ki odločilno vplivajo nanjo. Opisno metodo sem uporabila tudi v nadaljevanju, ko sem predstavila obravnavanje informacijske varnosti v EU.

Ta naloga raziskuje vplive na področje informacijske varnosti z obramboslovnega vidika, vendar pa je za celovito razumevanje področja informacijske varnosti potrebno vključiti tudi tehnično znanje tega področja, kot primer varnostnega mehanizma pa sem vključila tudi poglavje o varnostnem mehanizmu celice. V nalogi se tako prepletata tehnični, celo biološki, psihološki in družboslovni (komunikološki) pristop. Vsekakor pa je tako kompleksen pojem kot varnost potrebno obravnavati z interdisciplinarnim pristopom.

Na podlagi *študije primera in primerjalnega raziskovanja* bom poskušala podati zaključke in nakazati trende nadaljnjega razvoja tega področja v EU. Prav tako bo predvsem na tej metodi slonelo iskanje odgovorov na raziskovalno vprašanje, saj bom s primerjavo trendov razvoja politik EU in ugotovitev v nalogi lahko opozorila na nekatere podobnosti v varnostnih mehanizmih in strukturo referenčnih objektov varnosti.

2.4 Struktura analize

V uvodu sem podala svoj pogled na problematiko in razloge za postavitev raziskovalnega vprašanja. Sledijo poglavja, v katerih sem opredelila metodološko-hipotetični okvir, kjer sem opisala cilje in namene preučevanja v nalogi, opisala pa sem tudi ključne uporabljene metode, ki sem jih uporabila pri pisanju in operacionalizaciji raziskovanja.

V prvem delu sem primerjala različne oblike »konstruktivizmov«, ki se pojavljajo pri pojasnjevanju družbenih pojavov, od kulture, komunikacije, interakcije, jezika, diskurza do norm, vrednot, identitet in interesov posameznih referenčnih objektov in vloga teh parametrov pri reševanju varnostnih problemov v današnji sodobni globalni družbi.

V drugem delu bom predstavila koncept informacijske oz. omrežne varnosti. Po razvoju varnostne paradigme bom analizirala nastanek koncepta omrežne oz. informacijske

varnosti. V analizi bom primerjala različne referenčne objekte, glede na vire ogrožanja, ogrožene vrednote in varnostne mehanizme, ki se uporabljajo pri varovanju teh vrednot. Kot primer anarhičnega sistema in njegovega varnostnega mehanizma, sem v diplomsko nalogo vključila tudi varnostni mehanizem celice, s katerim sem v zaključnem delu naloge primerjala mednarodni sistem in EU.

V zadnjem delu sem ugotovljeno aplicirala na makrosocialno raven in podala ugotovitve, kako se za informacijsko varnost danes skrbi v Evropski uniji. Kakšne raziskave so že bile izvedene, kakšne politike se implementirajo, kakšni ukrepi se sprejemajo, aplicirala pa bom tudi celični varnostni mehanizem, kot bi hipotetično deloval tudi na nivoju EU in s tem poiskala čim več možnih odgovorov na raziskovalno vprašanje.

V zaključku sem strnila ugotovitve ter podala sklep in predloge za morebitno izboljšanje stanja na področju informacijske varnosti v EU.

3 TEORETSKA RAZPRAVA O VARNOSTI

Pri preučevanju varnosti sem izhajala iz konstruktivističnih izhodišč, zato bom najprej predstavila konstruktivizem in njegovo široko povezljivost s sodobnimi teorijami in razvojni smermi.

Konstruktivizem na splošno

Sexton (v Raskin 2002, 2) je v historični analizi obravnavanja narave znanja razdelil človeško zgodovino na tri dobe: predmoderno, moderno in postmoderno. Tretjo dobo je označil kot postmoderno / konstruktivistično, ki poudarja ustvarjanje, ne pa na odkrivanje, osebnih in družbenih realnosti. Za razliko od prejšnjih obdobij, ni več tako pomembna univerzalna veljavnost znanstvenih trditev, temveč predvsem njihova sposobnost za razvoj skupaj z znanjem. Poudarja se tudi pomembnost epistemoloških vprašanj. Konstruktivisti raziskujejo, kakšna je vsebina znanja, pa tudi način kako se pride do znanja, je za njih pomemben (Raskin 2002, 2).

Gre za perspektivo, da sta opazovalec in objekt opazovanja neločljiva: narava pomena je relativna, fenomen je razlagan v kontekstu in proces znanja in razumevanja je socialen, induktiven, hermenevtičen in kvalitativen (Sexton v Raskin 2002, 2). Konstruktivizem se torej osredotoča na način, kako ljudje in družbe ustvarjajao (ne odkrivajo) konstrukcije realnosti, saj nimamo direktnega in natančnega dostopa do eksternega sveta. Konstruktivisti vidijo realnost kot numenološko – to je, da naše ambiciozne teorije (osebne ali znanstvene) ne

morejo pojasniti realnosti in zavračajo domnevo, da je naše mišljenje, verovanje in ideologije neodvisno od »objektivnih okoliščin« zunaj nas (Niemeyer v Raskin 2002, 2).

Epistemološki in hermenevtični konstruktivizem

Chiari in Nuzzo (v Raskin 2002, 2) menita, da konstruktivisti ponujajo most med realističnimi in idealističnimi pristopi k pojasnjevanju znanja. Realisti menijo, »da materialni objekti obstajajo zunaj nas in niso odvisni od našega zaznavanja,« idealisti pa menijo, da »materialni objekti ali eksterna realnost ne obstaja ločeno od našega znanja ali zavesti o njej, da je cel svet odvisen od naše zavesti o njem.« (Chiari in Nuzzo v Raskin, 3) Konstruktivistični pristopi pa poskušajo to realistično – idealistično dihotomijo razložiti povezano. Na podlagi tega Chiari in Nuzzo ponudita tri hibridne pristope:

1. EPISTEMOLOŠKI KONSTRUKTIVIZEM

Epistemološki konstruktivisti niso čisti idealisti, saj verjamejo v obstoj zunanje realnosti, ki je neodvisna od opazovalca, vendar menijo tudi, da opazovalci nimajo dostopa do te realnosti, ker jo poznajo samo preko svojih konstrukcij le-te. Zato je znanje kompilacija človekovih konstrukcij. Te konstrukcije so hevristične fikcije, ki nam pomagajo razumeti svet, v katerem živimo. V tem pogledu vidi epistemološki konstruktivizem sheme znanja kot klasificirane in bolj ali manj uporabne, kot pa bolj ali manj natančne glede na realnost. Ljudje ne morejo zagotovo vedeti, če njihove konstrukcije ustrezajo neodvisni realnosti, ampak lahko vedo, če njihove konstrukcije ustrezajo njim kot posameznikom. Torej so ljudje kognitivno zaprti sistemi: »S to idejo o zaprtem kognitivnem sistemu je dihotomija subjekt / objekt rešena in pojasnjuje več kot tradicionalne realistične perspektive (Chiari in Nuzzo v Raskin, 3).

Von Glaserfeldov radikalni konstruktivizem in Kellyjeva osebna konstruktivistična psihologija sta primera filozofije empiričnega konstruktivizma (Raskin 2002, 3).

2. HERMENEVTIČNI KONSTRUKTIVIZEM

Hermenevtični konstruktivisti ne verjamejo v obstoj neodvisne realnosti. Znanje je produkt jezikovne aktivnosti skupine opazovalcev. Tako lahko obstaja toliko sistemov znanja, koliko skupin se diskurzivno pogaja temi. V hermenevtičnem pristopu h konstruktivizmu so vloge jezika, diskurza in komunikacije postale osrednjega pomena pri razumevanju, kako se sistemi znanja razvijajo in ohranjajo (Raskin 2002, 3).

Čeprav izhajajo iz različnih zgodovinskih ozadij, imajo vsi ti pristopi skupni pogled na znanje (in resnico) kot interpretacijo, ki je zgodovinsko osnovana, ne večna, kontekstualno

veljavna, ne univerzalno aplikativna, izhaja iz jezika in je družbeno skonstruirana, ne pa kognitivno in individualno producirana (Chiari in Nuzzo v Raskin 2002, 3).

Gergenov socialni konstruktivizem in Maturanin radikalni konstruktivizem sta primera hermenevtičnega konstruktivizma (Raskin 2002, 3).

Socialni konstruktivisti opozarjajo na primat relaciske, pogovorne, socialne prakse kot vir konstrukcije individualnih pomenov (Stam v Raskin 2002, 3). V socialnem konstruktivizmu je vse znanje lokalno in likvidno. Gergen (v Raskin 2002, 4) meni, da obstaja toliko realnosti, kot obstaja kultur, kontekstov in načinov komuniciranja.

3. OMEJENI REALIZEM

Chiari in Nuzzo (v Raskin 2002, 4) pa obravnavata tudi tretji pristop k povezavi med realistično in idealistično dimenzijo. Zagovorniki omejenega realizma verjamejo v obstoj zunanje realnosti. Prav tako menijo, da je realnost možno dojemati direktno. Ampak, ker je človeško dojemanje nepopolno in omejeno, omejeni realisti domnevajo, da je **povezava med znanjem in realnostjo nepopolna**. Po mnenju Chiarija in Nuzza so kognitivni psihologi, kot sta Albert Ellis in Aaron Beck, omejeni realisti, ker poudarjajo pomembnost popravkov pri nelogičnem in zmotnem razmišljanju, ki popači realnost (DeRubeis in Beck v Raskin 2002, 4).

Ta konstruktivistični pristop je po mojem mnenju najbolj uporaben pri preučevanju vloge informacijsko – komunikacijske tehnologije (IKT) pri dojemanju realnosti. Kot je pri omejenih realistih možno dojemanje zunanje neodvisne realnosti, je tudi IKT sama po sebi popolnoma neškodljiva in objektivno neodvisna, dokler ne pride v interakcijo s človekom, ki si s pomočjo IKT ustvarja pomene in znanje o (medijski) realnosti. Omejeno je le naše poznavanje IKT in ostale realnosti. Računalnik sam ne bo nikoli naredil nič sam od sebe, dokler ne bo človek izvršil določenega ukaza, med tem procesom pa se zgodi interakcija, ki nedoločljivo (zaradi različnih dejavnikov) napoveduje rezultat ali konstrukcijo interakcije.

3.1 Konstruktivizem v mednarodnih odnosih

Okolje, v katerem delujejo države, je družbeno in materialno, ta predpostavka pa omogoča državam razumevanje njihovih interesov. Interesi države namreč niso eksogeni in od zunaj določeni, temveč so endogeni in so posledica interakcij držav z njihovim okoljem. Pri tem igrajo pomembno vlogo vrednote in norme, ki konstituirajo akterjevo identiteto ter interese in ne vplivajo zgolj na vedenje (Svete 2005, 46).

Glede varnosti je glavna konstruktivistična trditev, da je ne moremo opredeliti kot objektivnega stanja, **kajti grožnje varnosti niso preprosto zgolj stvar korektnega zaznavanja konstelacije oz. medsebojnega razmerja materialnih sil**, po drugi strani pa so objekti varnosti nestabilni in spremenljivi. Varnostne implikacije globalizacije konstruktivizem pojasni z učinki globalizacije na vrednote, prav tako pa jih ustrezno presoja. Njegova naloga ni oblikovanje objektivnih groženj, temveč razumevanje procesa oblikovanja deljenih zaznav o tem, kaj obravnavamo kot grožnjo in kakšni so kolektivni odgovori nanjo. V konstruktivističnem pristopu so razprave o grožnjah v veliki meri konstitutivni, sestavni del objekta, na katerega se varnost nanaša. Identitete držav, družb ali posameznikov pa izoblikujejo odnose razumevanja oz. sovražnosti v družbenem okolju. Zato akterji oblikujejo svojo varnostno identiteto kot proizvod priučenih običajev in navad. Njihova zaznava groženj je subjekt evolucije - razvoja. Države pa lahko spremenijo svoja zaznavanja groženj tako z razvojem v njihovem okolju, kakor tudi s spremenjenimi navadami, običaji oz. vrednotami. Novi referenčni objekti varnosti, kot so transnacionalne skupine ali nadnacionalne organizacije, lahko definirajo vire ogrožanja glede na njihove ključne vrednote, ki naj bi jih zaščitili. V tem smislu tudi potencialno negativne posledice globalnih pojavov, kot so okrepljene migracije ali degradacija okolja, avtomatično ne predstavljajo vira ogrožanja. Najprej morajo biti namreč zaznani kot izzivi ključnim normam referenčnih objektov varnosti (Goetschel v Svete 2005, 47). Tak pristop raziskovalcem omogoča razumevanje sprememb na področju varnosti med posameznimi družbenimi subjekti. Še posebej je v tem okviru pomembna relativizacija vloge nacionalnih držav v primerjavi z drugimi političnimi akterji na globalni, regionalni in poddržavni ravni.

Osrednje vprašanje konstruktivizma je torej povezano z vprašanjem, kako primarni akterji (nacionalne države v primeru nacionalne varnosti, uporabniki IKT v primeru informacijske varnosti) oblikujejo in sprejemajo svojo identiteto in interese. Ideje in norme so osrednji element konstruktivističnega razmišljanja. Njihovo delovanje pa ni zgolj regulativno temveč tudi konstitutivno. Norme tako niso zgolj refleksija materialne strukture iz okolja (kot je na primer razdelitev moči v mednarodnem okolju), temveč oblikujejo in definirajo osnovo za to materialno strukturo.

Anarhičnost mednarodnega sistema

Mednarodna politika je sprva določena s tem, da je mednarodni sistem anarhičen – manjka mu avtoriteta, namesto tega pa je sestavljen iz enot (držav), ki so formalno enakovredne; vse so suverene na svojem teritoriju. Anarhija pa po neorealističnem mnenju

sili države, da se obnašajo na določen način, saj za varnost odgovarjajo same (pomoči ne morejo pričakovati od drugih). Anarhija jih torej prisili, da branijo svoj interes za moč **(**Wendt 1999, 8–15; Brown 2005, 40–43).

Wendt ima dve ključni osnovni domnevi:obstoj anarhije in centralnost držav v mednarodnem sistemu. A Wendt zagovarja anarhijo *kulturnega* izvora, ne pa materialnega. Konstruktivizem upošteva pomen kulture, idej, ideologije in socializacije. Državni voditelji so ključni akterji v mednarodni politiki, toda kulturne norme, vrednote in identitete (v določenem zgodovinskem kontekstu) izoblikujejo oz. definirajo njihove politične preference. Konstruktivizem predpostavlja, da je mednarodni sistem družbeno določen na temelju ideologij, zgodovine in socializacije. Prav tako je družbeno določena tudi mednarodna anarhija (Peou v Svete 2005, 42).

Identitete in interesi napovedujejo ali bosta dve državi imeli prijateljske ali konfliktne odnose, ali bosta vzajemno priznavali suverenost, ali bosta imeli vladne povezave, ali bosta v revizionističnem odnosu ali bosta vzdrževali status quo itd. (Wendt 1992, 396) Ampak Wendt gre še dalje in pravi, da je način, kako anarhija usmerja države odvisen od načina, kako države dojemajo anarhijo, svoje identitete in interese. Anarhija ni nujno vase zaprt, rigiden in samoregulirajoč sistem. Anarhija sili države k samopomoči, samo če sprejmejo neorealistični pogled na varnost kot relativni, tekmovalni koncept, kjer več varnosti v eni državi pomeni manjšo varnost v drugi državi. Če namesto tega koncepta varnosti države sprejmejo alternativne koncepte varnosti, bodisi »kooperativno« varnost, kjer države lahko maksimizirajo svojo varnost brez da bi negativno vplivale na varnost druge države, bodisi »kolektivno« varnost, kjer države dojemajo varnost drugih držav tudi koristno za lastno državo, potem anarhija sploh ne pripelje države do tega, da bi morala ravnati egoistično v korist lastne varnosti na račun drugih držav (Wendt 1992, 399–403). Preučevanje procesov socialne konstrukcije pravzaprav opravi ključno pojasnjevalno delo pri konstruktivističnem pristopu k razlagi mednarodnih odnosov.

Jalal Alamgir uporabil konstruktivistično logiko tudi v mednarodni politični ekonomiji, ko je analiziral mednarodna nasprotovanja in indijsko ekonomsko politiko. (Alamgir 2008). Primer takšne aplikacije bom pokazala na koncu diplomskega dela z raziskavo Andersona in drugih avtorjev, ki predstavljajo ekonomski pristop k varnosti v notranjem trgu in podajo konkretne predloge za izboljšavo sistema omrežne varnosti v Evropski uniji.

3.2 Kibernetika in komunikacijska teorija v mednarodnih odnosih

Vukadinović (1978, 95) kibernetiko definira kot sistematsko preučevanje komunikacije in kontrole v organizacijah vseh vrst. Kot piše eden prvih, ki je preučeval elemente kibernetike v mednarodnih odnosih, profesor Karl W. Deutsch v knjigi »*Živčevje vlade: Modeli političnega komuniciranja in nadzora,*« je v osrednje vprašanje »upravljanja, sledenja instinktom do njihovih sistemskih manifestacij, regulacije in nadzora.« (Vukadinović 1978, 95)

Deutschu je kibernetika osnovni kalup, po katerem lahko splošno analiziramo in razumemo vse notranje in zunanje politične odločitve države ali organizacije. Po Deutschu je komunikacija živčevje vlade in tako je razumevanje teh najobčutljivejših niti omogoča neposredni vpogled v zunanjepolitično delovanje države in njenega zunanjepolitičnega mehanizma (Deutsch 1978, 77).

Osnovni zaključek se je oblikoval kot potrditev teze, da obstaja velika podobnost v tehnični naravi komuniciranja, ne glede na to, ali gre za sistem, ki uporablja elektronske signale (omrežje, internet), človeško živčevje, ali državni birokratski aparat. Vsi akterji v komuniciranju imajo skupne točke, ki se po Wieneru (1950, 175) vidijo po:

- njihovi sposobnosti pošiljati in sprejemati sporočila,
- sposobnosti obdelovanja in reproduciranja različnih vrst podatkov in
- pomnjenju vrednosti in formul.

Ti sistemi so, ne glede na to, da se razlikujejo, orientirani za doseganje nekih ciljev in vsi imajo možnost in sposobnost sortiranja različnih informacij, kombiniranja novih in starih podatkov in sestaviti končno rešitev.

Po Wienerju (1950, 176) imajo sociološke znanosti obravnavajo socialne skupine in organizacije, komunikacija med njimi pa je kot cement, ki ustvarja nadorganizacijo. Zaradi tega nam razumevanje logike in načina komunikacijskih procesov tudi poveča razumevanje obnašanja organizacij, kar nadalje omogoča postavljanje teoretskih postavk.

Meja med temi državnimi sistemi in zunanjo okolico se izkaže v neprekinjenem pretoku poslovnih kontaktov in procesov. V tem kontekstu Deutsch (1978, 78) postavlja pod vprašaj obstoj državne avtonomije in suverenosti, kar pa sta prva simptoma deetatizacije. Meja je torej medij med obema komunikatorjema. Avtonomija je odsotnost možnosti predvidevanja reakcij zunaj sistema, oblikuje se glede na kombinacije sprejemanja in brisanja informacij. Suverenost je samo bolj izražena oblika avtonomije.

Kibernetika se koncentrira na upravljanje kot osnovni proces vsestranskega značaja. Prisoten je v institucijah, družbenih skupinah in posamezniku, zato je preučevanje in analiziranje vseh teh institucij in posameznikov brez pomena, če ne upoštevamo tega karakterističnega elementa aktivnosti (Vukadinović 1978, 99).

John Burton izhaja iz teze, da so vsi komunikacijski modeli, ki razlagajo proces sprejemanja odločitev, mnogo bolj ustrezni od statičnih konceptov ravnotežja moči ali tradicionalnih političnih sil (Burton 1965, 147). Burton meni, da ima komunikacijski model veliko praktično uporabnost pri procesu sprejemanja zunanjepolitičnih odločitev. Politično življenje, zgrajeno na takih temeljih omogoča boljše poznavanje in razumevanje drugih državnikov oz. soustvarjalcev zunanje politike drugih držav in na ta način tudi sprejemanje odgovornosti za skupno preprečevanje in reševanje kriznih situacij. Burton piše: »Model sile ne nudi alternative konfliktu, ali politiki sile v takšni ali drugačni obliki, medtem ko komunikacijski model vsaj dopušča različne možnosti znotraj procesa sprejemanja vrednotnih odločitev in variante mednarodnega pogajanja, kakor tudi prilagajanja znotraj tega procesa.«

Pri komunikacijski teoriji je pozornost usmerjena na upravljanje in kontrolo, predvsem v smislu preoblikovanja ekonomije, izobraževanja, socialne in politične strukture. Vse to skupaj, po Johnu Burtonu, bi naj vodilo k praktični realizaciji politike, ki se bi na ustrezen način reševala tekoče probleme sodobnega sveta, da s svojimi akcijami prepreči uporabo sile, in da se na drugi strani prilagaja in pogaja za rešitve problemov na vseh ravneh političnega življenja.

Kot sem že omenila, so v temeljih komunikacijske teorije mednarodnih odnosov pojmi, ki so »izposojeni« iz kibernetike, zato se je v tem kontekstu tudi treba zadržati pri analizi osrednjih idej, ki izvirajo iz kibernetike. Znanost o kibernetiki se začenja z občim konceptom sistema, ki se ga da kontrolirati. Preučuje se tak sistem, ki ima dovolj visoko stopnjo organiziranosti, po sistemu poteka komunikacija in sistem je mogoče kontrolirati. To se lahko nanaša na elektronske signale in komunikacijo med računalniki, človeški govor ali pisanje ali živčne signale[3] v človeškem telesu. Skupne glavne črte pri teh sistemih se kažejo v tem, da obstaja baza podatkov (informacij), da imajo sistemi sposobnost prejemanja in kombiniranja novih informacij s starimi, enotno delovanje, s katerim je možno enopomensko odločanje, in sistem je istočasno sposoben spremeniti delovanje v skladu z rezultati z namenom, da se doseže želeni cilj.

[3] V nadaljevanju bom pokazala še eno podobnost s podobno analogijo, in sicer varnostni sistem celice, ki je enako večplasten in anarhično organiziran kot mednarodni sistem, kar je raziskovalna tema te naloge. Glej sliko 5.1 Komponente biološke celice in njihove ustrezne komponente v računalniški mreži. (Information Security Management Handbook 2005, 260).

Temeljne ideje kibernetike se nanašajo na informacijo, ki kroži v komunikacijski mreži (Deutsch 1966; Burton 1965, 146–149). Kibernetiki povezujejo informacijo tudi z materialnostjo, energijo ali električno napetostjo, da lahko tako natančno določijo njeno lokacijo v proučevanem sistemu. Informacija je lahko reproducirana, shranjena, množena, z merjenjem pretoka informacij, ki se preučujejo, izgubljajo v mreži ali se pojavljajo na novo, pa se računa indeks delovanja komunikacijskega kanala. Sam sistem medtem ne more prilagajati informacije svojemu okolju, saj je obstoj in prenos informacije takšne kot je, dokaz avtonomije sistema. Informacija, ki kroži v mreži sistemov, je negativna v odnosu na entropijo, oz. možnost zaprtega sistema, da se pokvari. Informacija je edina stvar, ki jo je mogoče modificirati, ima torej moč, da sistem uniči, zato pravijo, da ima negativen odnos do zaprtega sistema. Kot pravi Wiener, imajo živa bitja in stroji, ki imajo večjo stopnjo redu imajo nižjo stopnjo entropije (Wiener 1950, 175–176).

Prednost, ki jo imajo informacijski in družbeni sistemi, leži prav v sposobnosti prilagajanja spremembam v okolici na podlagi novih izkušenj, medtem ko bi entropičen sistem takim spremembam podlegel. T. i. »feedback« omogoča možnost prilagajanja obnašanja sistema na osnovi realnih odnosov v sistemu, ne pa nekega anticipiranega stanja. »Feedback ali odziv« lahko definiramo kot komunikacijsko vez, ki sproži akcije kot odgovor na prejem informacije in vključuje rezultate lastne akcije v novonastali informaciji, ki se ji menja predhodno obnašanje. Odziv je lahko definiran tudi s kvantitativnimi indikatorji uspeha ali neuspeha posamezne akcije ali obnašanja celotnega sindroma (Deutsch 1966, 88–89).

V nekaterih situacijah se odziv lahko meri in primerja v odnosu do predhodnih stanj posameznih odnosov. Na primer učinkovitost zunanje politike v zagotavljanju nacionalne varnosti se lahko primerja s preteklimi izkušnjami in obstoječimi podatki. Na osnovi obstoječih odnosov se tudi sistem lahko prilagodi tako, da modificira svoje akcije in da bolje uresničuje postavljeni cilj(Vukadinović 1978, 68).

Na področju ekonomije niz konkretnih kvantitativnih indikatorjev (npr. podatki o nezaposlenosti, gibanje inflacije, BDP) služi kot stalna osnova za sprejemanje odločitev ali prilagajanje državne monetarne ali fiskalne politike. Kombinacija novih in starih meritev se lahko spreminja in s tem popravlja obstoječo smer razvoja ekonomskega sistema, kar pomeni, da se tudi njegovi cilji lahko spreminjajo (Vukadinović 1978, 68).

Na področju zunanje politike je odziv seveda zaradi specifičnih lastnosti te aktivnosti in tudi zaradi velikega števila drugih akterjev težko določiti. Merjenje uspešnosti zunanje politike, tudi v kvantitativnem smislu je težko izraziti, saj je tudi zunanjepolitična aktivnost od začetka akcije pa do njenega rezultata podvržena nadzoru kreatorja, ki želi v vsakem trenutku

korigirati potek akcije in po možnosti doseči čim boljši rezultat glede na zastavljeni politični cilj. Učinkovitost procesa prilagajanja politične akcije ciljem se lahko po Deutschu meri glede na štiri faktorje:

- Prvi je **obremenjenost** – količina informacij, ki jih mora sistem sprejeti. Ta faktor posveča pozornost količini informacij in pritisku, ki se vrši nad državnim aparatom, da sprejema odločitve. Informacije morajo tudi biti točne, če bi naj komunikacija imela realen učinek.
- Drugi faktor se nanaša na **zaostajanje (šum)** sistema, ki ni v stanju, da hitro reagira na dobljene informacije o lokaciji cilja in ukrepov, ki se drugače kažejo v praktični akciji. Večje je zaostajanje sistema, manjša je verjetnost, da se bodo cilji realizirali.
- Tretji faktor je opazovanje **prilagajanja (interaktivnost),** ki se nanaša na t. i. »dobiček« oz. stopnjo korektivne akcije, ki že poteka, da bi se ukrepi usmerili v pravo smer. Vendar tudi tukaj obstaja nevarnost, da lahko preveliko prilagajanja sicer stanovitnim situacijam povsem spremeni ali odstrani cilj, na drugi strani pa premalo prilagajanja tudi ne pripelje do želenega cilja.
- Četrti faktor je sposobno **vodenje** glede na oddaljenost od predvidenega cilja. Naloga političnega sistema je, da je vedno sposoben predvidevati nove probleme. To praktično pomeni, da stalno pomikanje cilja zahteva tudi ustrezno reagiranje politične linije, ki sledi cilju ne glede na to, ali se cilj oddaljuje ali približuje (ibid.).

Glede na to, da vse vlade in vsi komunikacijski sistemi delujejo na podlagi odzivanja (feedbacka), se lahko uspešnost akcije meri s pomočjo četrtega faktorja, ki mu nekateri avtorji pravijo, da je faktor konstanten (a se vsebinsko s cilji in akcijami sproti nenehno spreminja). Če obstaja stalna diskrepanca med komunikacijskim bremenom, t. i. »količino informacij« in možnostmi, ki so na razpolago v političnih institucijah, potem sistem preide v situacijo, kjer težko ali sploh ne uresničuje svojih ciljev.

Pri proučevanju odnosa med komunikacijo in kontrolo je treba poudariti, da komunikacijska teorija z elementi kibernetike preučuje korelacijo med bremenom količine informacij in možnostjo sistema, da obvlada to količino informacij. T. i. »transakcija pretoka« pregleduje vso komunikacijo, tako notranjo kot zunanjo politiko. Te komunikacije se pregledajo in razvrstijo v kategorije izmenjave, lahko fizičnih stvari ali pa informacij.

Običajno se kot indikatorji komuniciranja na državnem nivoju štejejo transakcije vezane na trgovino, promet, migracije, turizem, kulturno izmenjavo ipd. (Vukadinović 1978, 77) Glede na nove grožnje, ki se pojavljajo s kibernetskim prostorom, pa bi se lahko beležile

tudi takšne informacije kot indikatorji za morebitni izvor grožnje. Z računanjem posebnega indeksa relativnega sprejemanja med državama se meri odnos transakcij med dvema državama, bodisi za področje transporta, kulturne ali znanstvene izmenjave ipd. Ta konkretna količina izmenjave se primerja s hipotetično, ki bi naj bila sorazmerna glede na splošno količino izmenjave transakcij države z ostalimi državami. Indeks relativnega sprejemanja lahko pokaže vzajemno preferenco za sodelovanje ali pa prizadevanje, da se sodelovanja zmanjšuje zaradi sodelovanje z drugo državo ali pa skupino držav(Vukadinović 1978, 77).

Glede na sodobna gibanja v Zahodni Evropi se z uporabo nekaterih analitičnih konceptov, ki izhajajo iz kibernetike, lahko pride do temeljev kibernetične logike. Primer je lahko raziskovanje ekonomske in politične integracije med Francijo in Zahodno Nemčijo v obdobju med 1950–1960. Izhodiščna predpostavka je, da integracija dveh ali več držav ustvari diplomatski sistem odločanja. Ko so sposobnosti tega sistema večje od bremena, sistem deluje v smeri doseganja cilja, realizacijo integracije. V tem konkretnem primeru je bil cilj oblikovanje današnje Evropske Unije (Puchála v Vukadinović 1978, 78).

Če pa je sistem odločevanja preobremenjen, ne funkcionira dobro, ker ni sposoben predelati vseh informacij. V našem primeru je skupni Francosko-zahodnonemški sistem dobro funkcioniral od 1954–1956, proces je nato nazadoval do leta 1962. Tega leta je bil prekinjena pravica veta za de Gaullove politike, ker do bili proti sprejemu Velike Britanije v evropsko ekonomsko združenje kot tudi zaradi vztrajanja, da se obdrži pravica veta pri odločanju znotraj evropske integracije. Po DeGaullovem odhodu je sistem spet oživel po stalnih kolebanjih (Vukadinović 1978, 87).

To vse kaže, da obstaja neposredna zveza med nizkim napredkom v realizaciji integracije in velikimi diplomatskimi stresi, oz. neuspešnih pogajanjih, nestrinjanjem. Prekinitve v ustvarjanju regionalne zahodnoevropske integracije so se pojavili zaradi preobremenjenosti diplomatskega sistema odločanja. Primer zahodne Evrope kaže na pomembnost visokih in pozitivnih transakcij kot predpogoj za ustvarjanje politične in ekonomske integracije (Vukadinović 1978, 87).

Za razliko od nekaterih drugih pristopov je kibernetski pristop odprt in postavlja komunikacijske možnosti kot neizčrpno polje vsake politike (notranje in zunanje) in potencialno nedefinirano prihodnost. Prav v prizadevanju, da se *poveča intelektualna kapaciteta* poznavanja zapletenih procesov, delovanja sistema in logike njegovega funkcioniranja leži vrednost kibernetičnih idej (Vukadinović 1978, 88).

Kot pravi profesor Deutsch moramo v obilici faktorjev, ki vplivajo na mednarodne odnose, ali priznati našo nemoč, da jih razumemo in obvladamo, ali pa si prizadevati, da

uporabimo vse metode in tehnike in si s tem ustvarimo možnost, da te procese bolje razumemo (Deutsch 1966, xvi).

3.3 Kulturalizem

Znotraj konstruktivizma lahko obravnavamo tudi kulturalizem (Farrell in Lantis v Svete 2005, 44). Konstruktivizem vidi kulturo kot izdelan sistem deljenih vrednot in pomenov, ki obvladuje in določa zaznave, komunikacije in delovanje samo. Siedschlag (v Svete 2005, 44) pa povezavo med kulturo in zunanjo politiko vidi kot primeren teoretični model za operacionalizacijo raziskovanja, kajti konstruktivizem ni izdelal teoretičnega pristopa, temveč zgolj analitično perspektivo. Zato mora, v kolikor želi na svoj način znanstveno preučevati konkretne politike, nujno uporabiti teoretične modele (kot je povezava med kulturo in zunanjo politiko – strateško kulturo). V varnostno-politični analizi je strateška kultura namreč zelo dobro izdelan koncept in se nanaša na izkušnje preteklih vojn in mirnodobnega stanja, predstave o vlogi oboroženih sil pri zagotavljanju miru, načine zaznavanja ogrožanja, podobe o nasprotnikih (nem. Feindbilder), načinih sodelovanja med akterji (unilaterizem, multilaterizem) ter na izkustvenih principih in principih na znanju temelječe vojaške strategije. Sicer pa kultura ni rezultat družbenih konstruktov realnosti, temveč osnova zanje. Je družbeno dejstvo, element konstituiranja akterjev in njihovega delovanja. *V tem smislu deluje kultura kot simbolno posredovana podlaga za upravljanje znanja neke družbene skupnosti in njenega odnosa do realnosti.* Na teh teoretičnih temeljih je mogoče primerjati in preučevati izkušnje družb in njihovega odnosa do okolja. Na področju raziskovanja strateške kulture so se pri tem izoblikovale štiri temeljne dimenzije analize in pripadajoči teoretični modeli (Ibid.):

- **Kultura kot repertoar (način) delovanja in svet izkustev.** V skladu s tem modelom strateška kultura omogoča delovanje varnostno-političnih elit neke države, ki potem oblikujejo tudi varnostne politike in mehanizme, tudi ko gre za informacijsko varnost. Mednarodni položaj sam kot tudi njegovo subjektivno zaznavanje namreč ne pojasnita, katere države, zakaj in kdaj razvijejo kakšne zunanje in varnostno-politične interese. Nanje v bistveno večji meri vplivajo strategije, oblikovane na temelju zgodovinskih izkušenj, identitetne predstave ter tipizacije (Svete 2005, 45).
- **Kultura kot sistem znanja za interpretacijo stvarnosti.** Odločevalci ne reagirajo neposredno na spremembe v okolju, temveč reagirajo primarno na kognitivno predstavo okolja, ki jo oblikujejo v duhu. Kar je v nekaterih državah objektivno in izjemno

pomembno, v državah z drugačno odločevalsko kulturo nima nobenega pomena. Da bi lahko ocenili mednarodne posledice svojih strategij, morajo odločevalci zmanjšati kompleksnost, zato pogosto razmišljajo na način zgodovinskih analogij. Kultura pa je tudi »software« za upravljanje odnosov med družbo in okoljem. Tako lahko pojasnimo preobrate v varnostnih politikah in sicer v smislu kognitivne evolucije, ki vključuje učenje in prisvajanje drugih interpretativnih načinov stvarnosti (Svete 2005, 45). Konkreten primer uporabe kulture kot sistema znanja pri informacijski varnosti je, da informatik oz. računalniški strokovnjak na grožnje informacijski varnosti reagira drugače, kot pa laik, ki nima tako obširnega znanja o delovanju omrežij.

- **Kultura kot vrednostni sistem oblikovanja identitet in interesov.** Ta model postavlja v ospredje identiteto ter na zgodovinskih kompromisih temelječe konstitutivne norme. Na določenih vrednostnih sistemih temelječe identitete se spreminjajo le počasi, zato se niso sposobne v hipu prilagoditi novim mednarodnim izzivom. Kjer pa so potrebni hitri odgovori, se zato prej razvijejo nove, dodatne identitete, kakor da bi se spreminjale stare. Druga možnost pa je, da se stvarnost interpretira na tak način, da ustreza predhodnim vrednotam in identitetam. V tem primeru govorimo med drugim tudi o družbeni konstrukciji zunanjih in varnostno-političnih interesov. Ti interesi so proizvod kolektivnega opisa situacije ter izključitve alternativnih predstav o stvarnosti, prav tako kot se oblikuje moč neke države, je moč družbenih akterjev in identitetnih predstav, sposobnost znotraj neke družbene strukture izoblikovati medosebne pomenske vzorce. (Svete 2005, 46). Države, ki so doživele kibernetski napad na kritično infrastrukturo, bodo seveda bolj poskrbele, da se bo to v prihodnje ne bi zgodilo, kot pa države, ki takšnih izkušenj do zdaj še nimajo.
- **Kultura kot družbena podlaga varnostne skupnosti in njenega odnosa do okolja.** V tem modelu so pomembni odnosi med skupinami držav in okoljem kakor tudi idejami in običaji, ki to razmerje (tudi občutek ogroženosti) določajo. Kot pravi Weiguang (v Svete 2005, 44) je kultura lepilo družbe in osnova, ki zagotavlja družbeno stabilnost. Človeška kultura prežema vsa področja socialnega življenja ter oblikuje družbene norme in socialne sisteme. Posamezniki, pripadniki določenega ljudstva, v določenem času živijo vsi v določenem kulturnem modelu. Tak odnos do pomena kulture torej popolnoma jasno nakazuje njeno relevantnost v sodobni varnostni razpravi.

3.4 Konstruktivistični pogledi na medije

Bistvene spremembe, ki jih je neposredna uporaba IKT prinesla na področje varnosti, so namreč povezane z **zaznavo stvarnosti**. Pa naj to velja tako za uporabo IKT, ki vodi k ogrožanju sodobnih družb, kot njeno uporabo v sodobnih konfliktih ali posameznih delih nacionalno-varnostnih sistemov sodobnih držav. Uporaba IKT je primarno povzročila predvsem drugačno predstavo o času in prostoru. Preučevanje varnosti v informacijski družbi se mora, zlasti kar zadeva IKT, primarno usmeriti na izvor sprememb (odnos človeka do tehnologije in njenih možnosti), nato pa šele na uporabo samo in strukturne družbene spremembe, ki jih je povzročila (Svete 2005, 54).

Interakcionistični konstruktivizem, največkrat uporabljen pri preučevanju medijev, sicer ne izhaja direktno iz tradicije realističnega konstruktivizma, ki preko naturalističnih ključev razlaga svet s pomočjo biologije (Maturana), psihologije (Piagert), ampak v tradiciji metodičnega konstruktivizma, ki ima izvor v fenomenologiji kulturnega konstruktivizma (t. i. kulturnih študij) in pragmatizma, s katerim ima skupna mnoga stališča (Reich in dr. 2005, 17).

Interakcionistični konstruktivizem se od drugih »konstruktivizmov« razlikuje v tem, da ima posebno dobro aplikativnost na diskurz (Reich in dr. 2005, 17) in izhaja iz subjektivne pozicije, saj je posameznik tisti, ki interpretira medijski diskurz.

Opazovalci, udeleženci in akterji so tri perspektive, skozi katere so Kersten Reich (2005, 26) in ostali avtorji preučevali možne interpretacije sveta skozi medijske reprezentacije tega sveta. Realnost, fikcija, domišljija in virtualnost so ključni pojmi pri preučevanju medijev, pri tem pa konstruktivistična razlaga pomembno loči in definira te pojme. Tako so z interpretacijo dualizma realnosti zunaj nas in »sliko« realnosti znotraj nas. (Reich in dr. 2005, 26) Tudi konstruktivizem pri razlaganju medijev sloni na kulturni osnovi in iz nje črpa kategorije in semantične razlike (Reich 2005, 27).

V svoji knjigi Reichova razloži tudi vpliv računalnikov in njihove napredne obdelave medijskih produktov kot prispevek k vedno bolj težki ločnici med realnostjo in virtualno realnostjo. Zdi se, da imajo fotografije, filmi in televizijski ekrani sposobnost upodabljanja realnosti. Opazovalci vedo, da lahko reprezentacija in realnost zamenjata, ampak ravno zaradi teh medijev menijo, da so te slike realnosti vsemogočne. Ta iluzija je s tehničnim razvojem samo še bolj resnična. Ne vidi pa se, kdo je primarni opazovalec, ker sekundarni opazovalec vidi le njegovo upodobitev realnosti.

Računalnik to iluzijo še nadgradi, saj ga lahko uporabljamo kot ekran, po drugi strani pa smo ravno preko uporabe računalnika zmožni generirati nove podobe. Kot orodje za

uprizoritev realnosti se prikaže računalnik kot prostor za simulacijo, kjer lahko naravo, »realnosti« znova izumimo in reproduciramo. Imitacija realnega življenja, generirana z računalniško simulacijo v začetku sploh ne obstaja, »simulira nekaj, kar ne obstaja,« ampak se vseeno sprevrže v eksistenco (Zizek v Reich 2005, 51). V nasprotju z imitacijo, simulacija generira predvsem videz neobstoječe realnosti. Z tehniko digitalne obdelave slik se lahko piksli, ki sestavljajo sliko poljubno animirajo, klonirajo in generirajo. Nekoč nespremenljiva realnost se tako izkaže za spremenljivo, zmožno novih kombinacij in realizacije poljubnih estetskih popravkov (Welsch v Reich 2005, 51).

Digitalizacija filma in računalniško simuliranih slik tako dovoljuje gledalcu v kinu, televiziji, video ali računalniških pomnilnikih, da vidi slike oz. zgodbe, ki prej niso obstajale *na tak način* (Reich 2005, 52). Gre za paradoks, da upodobitev sveta kot konstrukt in računalniško animiran trik deluje bolj realistično kot surova, neobdelana verzija oz. tehnična reprodukcija (film, fotografija) sveta. Računalniški ekran tako deluje kot kulturni instrument (Reich 2005, 52).

Kiberalizacija nam lahko nudi virtualizacijo identične reprodukcije dogodkov ter stanj. Računalniške animacije generirajo slike, ki imajo »avtentično« komponento iz realnosti. Tehnične slike kažejo dogodke, ki so po navadi neresnični delujejo resnično. Na primer, objekti, ki se trgajo, odpirajo, razstreljujejo, lebdijo, izginjajo, ali pa klonirani ljudje, živali in rastline delujejo enako avtentično kot v naših najbolj doživetih sanjah, ki si jih lahko zamislimo, te sanje, strahovi, želje itd. pa se prenesejo v naš notranji simbolni slikovni svet (Reich 2005, 53).

Preko medijskih reprezentacij se tudi konstruira in prenaša kultura iz generacije v generacijo, gradijo se naše identitete in interesi, naše dojemanje zunanjega sveta. Pri konstrukciji realnosti je zato pomembno **samoopazovanje uporabnika** (Reich, 2005, 55). Tako je oblikovanje in preučevanje svoje identitete (identitet) glede na različne vplive družbe, ne samo medijskega ampak tudi vpliva drugih socialnih skupin, pomembno za samozavest vsakega posameznika. Na to opozarjajo pojavne oblike različnih odvisnosti od virtualnega sveta, kjer posameznik lahko izgrajuje svojo idealno identiteto (odvisnost od računalniških igric, Facebooka ipd.).

3.5 Vpliv konstruktivizma na računalniško znanost - računalniška semiotika

Semiotika ali »znanost življenja znakov v družbi« kot jo je opredelil Saussure (1966), je splošen teoretski okvir za analizo in razumevanje različnih (družbenih) fenomenov: jezika, filma, gledališča, slik (podob), arhitekture, stila oblačenja, gestikulacije itn. Njihov skupni imenovalec je, da so vsi ti fenomeni razumljeni kot znaki; so še nekaj več kot samo oni.

Konstruktivizem je vplival tudi na načine programiranja in računalniško znanost. Nekateri znani programski jeziki so bili ustvarjeni v celoti, ali delno, za izobraževalne namene in so s tem potrdili Papertovo konstrukcionistično teorijo. Ti jeziki so bili dinamično napisani in refleksivni (Wikipedia 2009a). Z namenom podrobnejše razlage dojemanja medijskega (računalniškega) diskurza, sem v nadaljevanju prikazala tudi ugotovitve, ki jih prinaša računalniška semiotika, ki je nekako kolizija obeh zgornjih vej raziskovanja.

Definicija računalniške semiotike po semiotični raziskovalni skupini oddelka za Računalniški inženiring in industrijsko avtomatizacijo v sodelovanju z nekaterimi ameriškimi univerzami[4]: Računalniška semiotika poskuša sintetizirati semiotični cikel znotraj digitalnega računalnika. Med drugim poskušajo to doseči s konstruiranjem avtonomnih inteligentnih sistemov, ki so sposobni inteligentnega vedenja, kot percepcijo, modeliranje besed, vrednostne sodbe in generiranje vedenja. Trdijo, da velik del inteligentnega vedenja avtonomnega bitja obstaja zaradi semiotičnega procesiranja, ki se dogaja v bitju. V tem smislu bi moral biti inteligenten sistem razumljen kot semiotični sistem in kot tak tudi proučevan. Matematično modeliranje takih semiotičnih sistemov je predmet proučevanja raziskovalcev, ki preučujejo interakcije, ki potekajo med semiotiko in inteligentnimi sistemi. Pri tej definiciji se pozna poudarek na preučevanju umetne inteligence, v sklopu njihovega proučevanja pa najdemo tudi kognitivne procese generalizacije, združevanja, koncentracije, sploh pojmovanje inteligence same po sebi itd. (UNICAMP)

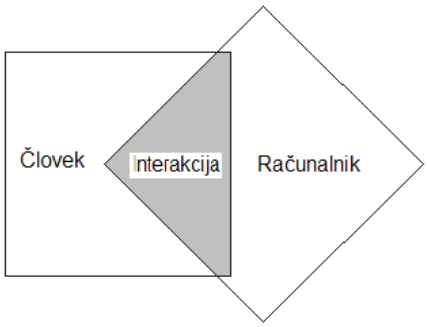
Semiologija je znanost o znakih. Njen predmet je vsaka vrsta znakov: verbalni jezik, slike, podobe, filmi, gledališče, telesna govorica itd. Računalniška semiotika pa je veja semiotike, ki preučuje specifično naravo računalniških znakov in kako funkcionirajo v praksi. Čeprav lahko računalniške sisteme po mnogih lastnostih primerjamo z ostalimi orodji, kot so tipkalni stroji, pisala, čopiči in aktovke, se razlikujejo od naštetih stvari po tem, da se primarno uporabljajo kot fizičen predmet in ne kot znak. Pisalo risarskega programa ni

[4] Natančneje fakultete za Električni in računalniški inžiniring (FEEC) in državne univerze v Campinasu (UNICAMP).

resnično pisalo, ki ga lahko žvečiš, ampak je samo znak za pisalo, ki je repretzentiran z množico pikslov na ekranu. Računalniški sistemi so podobni ostalim medijem predvsem po tem, da delujejo kot prenašalci pomena (Euphrates v Mihai 2001, 1).

Računalnike so na začetku uporabljali redki specialisti, danes pa računalnike uporabljajo na skoraj vseh delovnih mestih in tako je narastla tudi potreba po interpretaciji njihovih sistemov. Dober in razumljiv program (vmesnik) je postal predpogoj za dober računalniški sistem. Torej, ker so računalniki postali del vsakdanje rabe povprečnega posameznika, so postali programi in računalniške kode in znaki pomembni pojmi.

Slika 3.1 Človek, računalnik in interakcija



Vir: Mihai (2001).

Pri komunikaciji med človekom in računalnikom (v ang. je pogosto uporabljan izraz Human Computer Interface ali HCI), se računalniška semiotika ukvarja predvsem z osenčenim delom na sliki, z interakcijo.

Naša interakcija z računalniki je posredovana preko različnih sredstev, metod in protokolov. Ni načina, da bi se izognili temu pogoju semiotičnega posredovanja. V analognem svetu je direktna interakcija še vedno mogoča, medtem ko v digitalnem svetu stoji med uporabnikom in strojno opremo jezik (dve številki: 0 in 1) in »slovnica« (Booleanska logika).

Območje preseka (kjer se odvija mediacija oz. posredovanje), t. j. kako interakcije nastanejo, je raziskovalno področje mnogih znanstvenih disciplin: psihologije, kognitivne znanosti, tehnologije, izobraževanja, komunikacijske teorije, oblikovanja, ekonomije (kako učinkovita je interakcija, kakšne stroške prinaša), kulturnih študij (do kašne mere ustreza sistem kulturnemu kontekstu) (Mihai 2001, 1).

Področje računalniške semiotike je pojasnjevanje odnosa med pomeni, funkcijami in strukturo zankovnih sistemov na več ravneh računalniškega sistema (Clarke v Mihai 2001, 1). Vsaka definicija računalniške semiotike vsebuje tudi pojem znaka in znakovnih procesov, iz katerega izhaja. V tem kontekstu si je zato potrebno zastaviti ustrezno metodologijo in pregledati tri najbolj vplivne semiotične šole (Mehler v Mihai 2001, 2).

Peirce (v Mihai 2001, 2) predlaga dinamično, relacijsko semantiko, ki opisuje pomen kot rezultat cikličnih procesov interpretacije znakov, ki se kaže v konstituciji oziroma modifikaciji dispozicij obnašanja, ki zmanjšuje uporabo teh znakov prav v teh procesih. Ta cirkulacija je še posebej pomembna za računalniško semiotiko. O tem govori dejstvo, da znaki ne samo sodelujejo pri znakovnih procesih na podlagi dispozicij (regulacija uporabe), ampak tudi kot rezultat sodelovanja spremenijo te dispozicije. Implikacije tega pojma so za lingvistična pravila, ali bolj splošno regularnost pomamba, saj jih v Piercovi dinamični perspektivi ne moremo obravnavati kot kategorične in statične entitete.

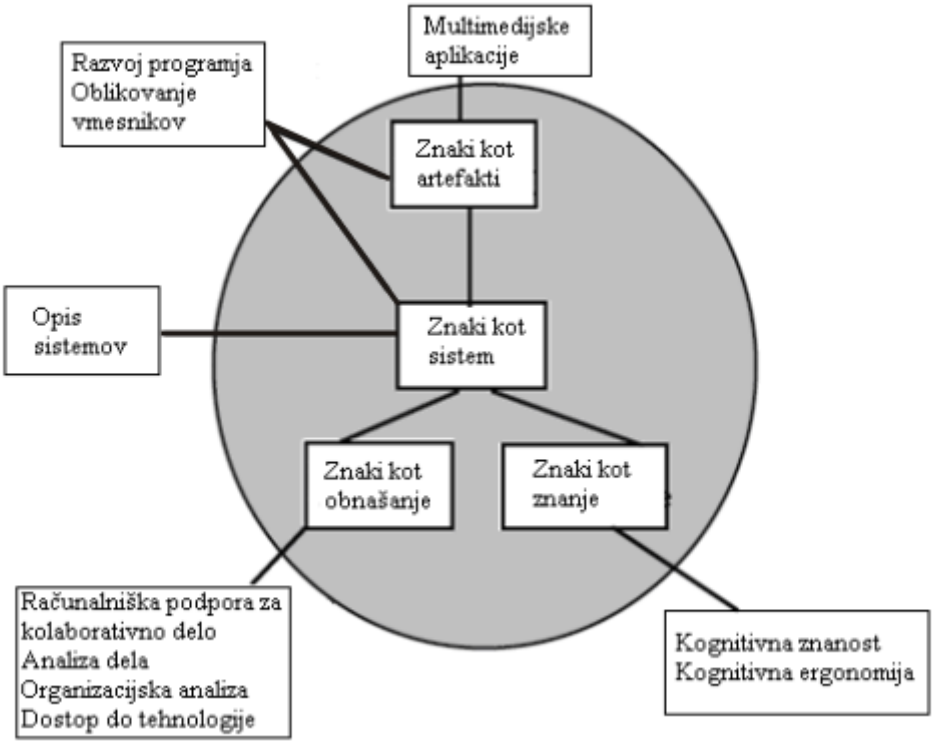
Medtem, ko Pierce (v Mihai 2001, 3) ne razlikuje med sintagmatsko in paradigmatsko analizo kot centralni osi filozofije znakov, pa je prav to razlikovanje, ki je podobno razliki med tekstovnim sistemom in jezikovnim sistemom, osnova Hjemlsleve glosemantike (Hjelmslev 1969). Tako Hjemlshlev opiše jezikoslovje kot formalni, deduktivni pristop, ki poskuša rekonstruirati sistem izbir, ki definirajo jezikovni sistem in realizacije teh izbir, ki pa nadalje definirajo sistemske tekstualne instance. Ne glede na deduktivni pristop glosemantike, je njegova dihotomija sintnagme in paradigme pomembna pri osnovanju računalniške semiotike.

V delu *Sistemsko funkcionalno jezikoslovje* (Halliday v Mihai 2001, 4) v nasprotju s Hjlemslevim statičnim pojmom jezikovnega sistema, Halliday poudarja njegovo dinamiko pri obojestranski konstituciji tekstovnega in jezikovnega sistema.. S tem opozarja na *kontekst* jezikovnih procesov. V tem primeru ima tekst, ki je produciran ali sprejet kot enota diskurza s strani sodelujočih v govorni skupnosti vsaj dve vrsti konteksta: sistem semantike / jezikoslovja, izbire znotraj njega in socialni kontekst, ki ga razlikuje kot ustreznega situacijskega faktorja, obstajajo pa še ostale socialne interakcije (opisane kot žanri) (Halliday v Mihai 2001, 3). Kot posledica konteksta ne more biti jezikoslovje popolnoma deduktivna disciplina, ampak mora nujno razvijati kvalitativne in kvantitativne analize sinhronih in diahronih vidikov dinamike jezikovnih struktur (Mehler v Mihai 2001, 3).

Teorija Petra Bøgha Andersena

Andersen v svojem članku podaja argumente za možno poddiscilplino semiotike, računalniško semiotiko (Andersen 1990; Figge 1991). Ta disciplina analizira računalniške sisteme in kontekst njihove uporabe skozi specifično perspektivo, torej kot sistem znakov, katerih pomen interpretirajo uporabniki računalniških sistemov (Andersen 1991, 1). Znotraj splošne perspektive Andersen definira štiri lokalne perspektive:

Slika 3.2: Zemljevid računalniške semiotike.



Vir: Halliday v Andersen (1990, 3).

V sredini je *znak kot sistem*. Individuum je kreator, interpret in referent znakov, se pravi, uporabnik in reproducent sprejetega, občega pomena in kode, hkrati pa uporablja rezultate semiološkega dela drugih individuumov. Ta kvadrat poudarja sistem znakov kot socialni fenomen s strukturo, ki je ni moč spremeniti po volji. Cilj sistemske analize, oblikovanja in implementacije pri ustvarjanju računalniških znakovnih sistemov je po navadi končna organizacijska uporabna vrednost (Andersen 1990, 3).

Znaki kot znanje. Tukaj je posameznik dojet kot skupek posameznih delov: njegova biološka in psihosocialna narava in psihološki mehanizmi, ki omogočajo učenje, so tisti, ki uporabljajo in razumejo znake. V tradicionalni lingvistiki te pojme obravnava psiholingvistika. Medtem v primeru računalniških znakov to vlogo prevzema kognitivna znanost in kognitivna ergonomija[5], ki preučujeta kaj se dogaja v mislih in telesu individuuma.

Znaki kot obnašanje. Posameznik je dojet kot sama, nedeljiva entiteta, poudarek pa je na njegovih interakcijah z okoljem, posebej komunikacija z ostalimi posamezniki. Sociolingvistika in pragmatika se tudi ukvarjata s podobnimi vprašanji. V zgornji shemi pa se s tem ukvarja kvadrat z računalniško podprtim kolaborativnim delom (Andersen 1990, 3).

[5] **Ergonomija** je veda, ki se ukvarja z raziskovanjem človekovih telesnih in duševnih zmožnosti in ustreznim prilagajanjem delovnih obremenitev (Wikipedia, 2009b).

Znaki kot artefakti. Pri tej perspektivi se posameznik dojema kot inovator kod in pomenskega potenciala, kot raziskovalec in inovator znakov. V tej kategoriji se razlikuje med ustvarjanjem kode na splošno (znak kot artefakt) in njegovimi različnimi variantami: ustvariti nov stil umetnosti (znake kot umetnost) ni enako kot ustvariti nove oblike vsakodnevnih artiklov. Ustvarjalni proces je pomemben pri oblikovanju novih izdelkov, še posebej pri ustvarjanju novih sistemov. Nova multimedijska tehnologija zahteva tudi znanje oblikovalca, ki zna odstraniti »oklepaje« in je sposoben prikazati resnične znake umetnosti (Andersen 1990, 3).

Po Andersenovem mnenju je semiotika globalna perspektiva o računalniških sistemih; vse ravni sistema se lahko obravnavajo semiotično, ampak – kot vse perspektive – lahko obravnava le podskupino vseh relevantnih elementov sistematično (Andersen 1990, 3).

4 OMREŽNA IN INFORMACIJSKA VARNOST

»Varnost lahko razumemo kot stanje, v katerem je zagotovljen uravnotežen fizični, duhovni ter gmotni obstoj posameznika in družbene skupnosti v razmerju do drugih posameznikov, družbenih skupnosti in narave.« (Grizold 1999, 23) O percepciji varnosti lahko govorimo z več vidikov: z vidika posameznika, družbe, države, mednarodne skupnosti in celo sveta kot celote ter predstavlja ravnotežje v odnosih med njimi, zaradi česar se v zavesti posameznika oblikuje občutek stabilnosti, homeostatičnosti, torej tudi zagotovljenih pogojev za življenje in preživetje (Jelušič 1997, 70).

Spremenjenim okoliščinam v svetu sledijo tudi zadovoljive spremembe tipologije varnostnih groženj kakor tudi konceptualnega razumevanja vsebine in oblik oz. virov družbenih sprememb (Svete 2005, 55). Prav tako ni konceptualnega konsenza o vsebini varnostnih groženj, oblikah, v katerih se pojavljajo ter viru teh groženj (Kirchner v Svete 2005, 55). Vsa sodobna razprava o varnosti se v zadnjem času usmerja predvsem na njene **referenčne objekte** (na koga se varnost nanaša - security from who), **kdo ali kaj to varnost ogroža** (grožnje varnosti - security from what) in seveda na kakšen način se varnost zagotavlja - **varnostne mehanizme** (kakšna oz. katera so sredstva za doseganje varnosti) (Liotta v Svete 2005, 55).

Zaradi vse večjega pomena IKT v sodobnih družbah omrežja sama referenčni objekt, na katerega se varnost nanaša. V tem primeru govorimo torej o omrežni, oz. v širšem smislu, o informacijski varnosti, ki naj bi se v skladu z varnostno teorijo nanašala na uravnotežen in stabilen razvoj in delovanje (Svete 2005, 105). Sporočilo iz leta 2001 opredeljuje varnost

omrežij in informacij kot *„zmožnost omrežja ali informacijskega sistema, da na določeni stopnji zaupanja prepreči naključne dogodke ali zlonamerna dejanja, ki ogrožajo razpoložljivost, verodostojnost, celovitost in zaupnost shranjenih ali prenesenih podatkov ter s tem povezanih storitev, ki jih ponujajo ta omrežja in sistemi ali so prek njih dostopne.“* V zadnjih letih je Evropska skupnost izvedla številne ukrepe za izboljšanje VOI (COM(2006) 251, 3). Omrežna varnost predstavlja eno novejših varnostnih perspektiv in izvira iz naraščajočega pomena omreženih informacijskih tehnologij v vseh vidikih postindustrijske ekonomije, vključujoč mednarodno proizvodnjo in globalne finance. Nove informacijske tehnologije so namreč neločljivo povezane z bistvenimi spremembami v naravi ekonomske organizacije kakor tudi drugih vidikov družbe. Ker je torej vse večji del družbe odvisen od omrežene informacijske infrastrukture, se je pojavila nova oblika varnostne predstave, ki je usmerjena v zavarovanje omrežja samega pred razpadom sistema (org. system crash), izgubo, krajo ali uničenjem podatkov ter prekinitvijo informacijskih tokov. Omrežna varnost pa ima dve dimenziji (Svete 2005, 105):

- Prva se nanaša na zaščito neokrnjenosti podatkov in interni pretok informacij do posameznih korporacij oz. delov sistema. Ker so korporacije in druge družbene organizacije spremenile obliko organiziranosti iz hierarhične v horizontalno ter iz fiksnih lokacij na geografsko dislocirana območja, je hiter in zanesljiv informacijski pretok postal bistvenega pomena za njihovo delovanje. Čeprav so številne korporacije oblikovale svoje lastne zasebne mreže (VPN- virtual private network) oz. intranet, pa narašča potreba po povezovanju teh mrež v internet. Tako postaja obramba pred omrežnimi napadi iz interneta vse pomembnejša. Prvi primer omrežne varnosti se torej nanaša na zanesljivo delovanje informacijske infrastrukture, ki je nujno potrebno za notranje delovanje organizacij. *Gre torej za notranjo omrežno varnost organizacije, ki tovrstno tehnologijo in infrastrukturo uporablja.*
- Druga dimenzija pa se nanaša na varovanje informacijskega toka med informacijskimi proizvajalci (ponudniki) in potrošniki (uporabniki). Danes je namreč vse več tako komercialnih kot javnih storitev, ki jih lahko uporabljamo v elektronski obliki, po drugi strani pa so določene klasične storitve dobile tudi svojo elektronsko obliko (elektronsko bančništvo, zavarovalništvo, e-javno upravo in e-volitve). Konvergenca komercialnega pritiska ter novih tehnologij je tako povzročila pravi vihar na internetu, zlasti pa so velika pričakovanja usmerjena v komercializacijo svetovnega spleta (orig. world wide web). Seveda pa mora temu napredku slediti tudi varovanje oz. zaščita informacijskega toka (povezav) med ponudniki storitev in uporabniki, kajti le na ta način je možno zagotoviti

dovolj visoko stopnjo zanesljivosti in hkrati tudi legitimnosti on-line storitev. To dimenzijo omrežne varnosti med ponudniki in uporabniki informacijskih storitev lahko zato opredelimo *kot omrežno varnost,* ***usmerjeno v zunanje okolje omrežene organizacije*** (Svete 2005, 106).

Ne glede na to, za katero dimenzijo omrežne varnosti gre (ali za komunikacije znotraj korporacij ali za tiste med korporacijami kot ponudniki storitev in njihovimi odjemalci), je učinkovito in zanesljivo delovanje informacijskih mrež najpomembnejše. **Mreža sama je zato referenčni objekt varnosti**. Upoštevajoč, da informacijska omrežja (še posebej internet) presegajo ozemeljske in birokratske omejitve ter zahtevajo mednarodno sodelovanje tako držav, kot posameznikov in korporacij, ki narekujejo tehnološki razvoj, pa moramo kot pomembno okolje omrežij upoštevati tudi državne in naddržavne jurisdikcije, ki poskušajo omejiti in sankcionirali grožnje, kar je vse prej kot lahko. Grožnje omrežni varnosti namreč vključujejo širok spekter aktivnosti, vključujoč programske napake, ki lahko vodijo do sesutja sistema; računalniške prevare in kraje; posameznike in zaposlene znotraj sistema, ki namerno onemogočajo delovanje sistemov; nedelovanje podpore fizične infrastrukture; aktivnosti hekerjev in drugih računalniških kriminalcev; industrijsko in drugo zasebno in državno vohunjenje ter zlonamerno kodo in programe kot so virusi, trojanski konji, črvi ipd. (Deibert v Rosenau in Singh v Svete 2005, 106).

Omrežna varnost izpostavlja torej komunikacijski (prenos podatkov) in uporabniški vidik IKT kot referenčni objekt, na katerega se varnost nanaša, koncept informacijske varnosti pa za cilj ogrožanja postavi v ospredje celotno IKT, vključujoč tudi njene zmogljivosti zbiranja in obdelave podatkov in delovanja strojne opreme nasploh.

Če izhajam iz teorije, potem lahko rečem, da prav akterji konstruirajo (mednarodne) odnose, družbe, interesne skupine, organizacije, oblikovanja politike, vsakdanji medsebojni odnosi, oblikujejo izmed vseh teh stvari tudi informacijsko družbo, ki mora imeti informacijsko varnost, saj so mnogi družbeni procesi danes povezani z uporabo IKT. Torej se bo tudi varnostna politika in ostali mehanizmi informacijske varnosti skonstruirani anarhično, glede na kulturo, interakcijo, odnose.

Akterji:

1. IKT.
2. Posameznik.
3. Naddržavne strukture (EU), NVO.

V diplomski nalogi bom podrobneje predstavila vidik posameznika, saj je tako zastavljena tudi teoretska podlaga, ki postavlja posameznika v ospredje ter vidik naddržavnih struktur kot je EU.

5 IKT kot referenčni objekt informacijske varnosti

Ko je govora o IKT sistemih, lahko ob pojmu varnosti dodam tudi pojem **zanesljivosti**, s katerim so se teoretično ukvarjali: Algirdas Avižienis (UCLA Computer Science Dept., USA), Jean-Claude Laprie (LAAS-CNRS, France) in Brian Randell (Dept. of Computing Science, Univ. of Newcastle, U.K.) in je predstavljen v njihovem skupnem delu z naslovom **Fundamental Concepts of Dependability (Temeljni koncepti zanesljivosti)**. Tudi ti avtorji že v uvodu izpostavijo, da je skrb za preživetje kompleksnih informacijskih sistemov, ki podpirajo infrastrukturo razvitih družb, med najpomembnejšimi nacionalnimi in celo svetovnimi nalogami.

Zanesljivost je opredeljena **kot lastnost nekega sistema**, ki vključuje naslednje atribute: *razpoložljivost oz. dostopnost, trdnost, varnost oz. zaščito, zaupnost,neokrnjenost, vzdržljivost.*

Struktura pojma zanesljivost se poleg atributov navezuje še na:

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

kar pa je enaka konceptualizacija kot pri opredeljevanju varnosti (grožnje in mehanizmi, ki zagotavljajo varnost referenčnega objekta).

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

- *zaupnosti* (preprečitve nepooblaščenih razkritij informacij),
- *neokrnjenosti oz. integritete* (preprečitve nepooblaščenih sprememb ali izbrisov informacij) in
- *razpoložljivosti* (preprečitve nepooblaščenih zadrževanj informacij).

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

5.1 Ogrožanje kritične informacijske infrastrukture

Splošno lahko rečemo, da kritično informacijsko infrastrukturo na različnih ravneh tvorijo informacijski sistemi z različno kompleksnostjo – od velikih računalniških mrež do

enega samega računalnika. Če torej začnemo splošno, lahko vidimo, da ločimo 3 vrste dogodkov, ki ta sistem lahko poškodujejo, in sicer (Dunn 2005, 14):

- *okvare* (failure) so posledice napak v zasnovi sistema ali zunanjega elementa, od katerega je sistem odvisen. Lahko so strojnega ali programskega izvora. Večinoma izvirajo iz sistema samega;
- *nesreče* vključujejo celoten razpon naključnih in morebitnih škodljivih dogodkov kot so naravne nesreče in splošno izvirajo iz okolja;
- *napadi* so morebitno škodljivi dogodki, ki jih pripravi nasprotnik.

Največ pozornosti se posveča zadnji kategoriji. Grožnje, s katerimi se soočajo informacijski sistemi, lahko pridejo tako od znotraj kot od zunaj. Tisti, ki ogrožajo sistem od znotraj, so škodoželjni uslužbenci in nekdanji zaposleni, ki imajo dostop do informacijskega sistema in ta dostop zlorabijo, da bi povzročili škodo. Verjetnost grožnje od znotraj je statistično pogostejša kot grožnja od zunaj (Dunn 2005, 14). Možnostim okvare in nesreče se lahko zoperstavimo predvsem z vzpostavitvijo nadomestnih sklopov ali celotnih nadomestnih informacijskih sistemov.

Kritično informacijsko infrastrukturo sestavlja poleg materialne tudi nematerialna komponenta. Zagotavljanje varnosti materialne komponente je relativno preprosto, saj je fizično in prostorsko omejena. V primeru velikih informacijskih sistemov je pogosto omejena v eni zgradbi, kar sicer olajša logistiko, vendar takšna centralizacija prinaša druge grožnje. V primeru velike naravne nesreče (potres, poplava ali požar), je verjetnost močnega fizičnega poškodovanja zgradbe, s tem pa narašča tudi možnost uničenja informacijskega sistema in podatkov, ki jih hrani. Varnostni mehanizmi, ki se tam vzpostavljajo, jamčijo delovanje informacijskih registrov tudi v primeru fizičnega uničenja osnovne lokacije. Varnostne implikacije za nematerialni del kritične informacijske infrastrukture so veliko bolj zapletene zaradi sledečih dejavnikov (Dunn 2005, 17):

- *anonimnost akterjev*: zagotavljanje anonimnosti je preprosto, dodaten problem predstavlja časovni razpon med dejanskim vdorom in učinki tega vdora. Prav tako razširjanje in dostopnost napredne računalniške tehnologije otežuje identifikacijo akterjev;
- *odsotnost meja*: škodoželjnih računalniških napadov ne omejujejo politične ali geografske meje. Napadi lahko izvirajo od kjerkoli na svetu in iz več različnih lokacij sočasno – teh je lahko tudi nad 10.000. Poizvedbe, ki sledijo nizu teh lažnih sledi, ki jih je nekdo nastavil namerno, so lahko zelo zahtevne v pogledu tega, koliko časa in

sredstev vložimo v to;

- *hitrost razvoja*: hiter razvoj tehnologije ima za posledico to, da je čas med razkritjem nove ranljivosti in orodjem, ki to ranljivost izkorišča, zelo kratek;
- *nizka cena sredstev*: tehnologija, ki se pri teh napadih uporablja, je preprosta, cenovno dostopna in zelo razširjena. Orodja za vdore lahko dobimo na različnih spletnih straneh, prav tako lahko dobimo orodja za šifriranje in za zagotavljanje anonimnosti;
- *avtomatizirane metode*: metode napadov so postale avtomatizirane in bolj napredne, kar se kaže v večji škodi, ki jo lahko povzroči en sam napad.

Po Dunnovi lahko grožnje razdelimo na nestrukturirane in strukturirane. *Nestrukturirane grožnje* so naključne in omejene. To grožnjo predstavljajo akterji, ki imajo omejena sredstva, orodja, znanja in finančno podporo, da bi uspeli izvesti zapleten napad. Ta tip grožnje ne predstavlja grožnje nacionalni varnosti. Vendar lahko takšni napadi povzročijo precejšnjo škodo, če jih spremlja sreča ali jim manjka presoje (Dunn 2005, 15). *Strukturirane grožnje* so veliko bolj sistematične in z boljšo podporo. Nasprotniki imajo obveščevalno podporo iz večjega števila virov, obsežno finančno podporo, organizirano profesionalno podporo in dolgoročne cilje. V to kategorijo spadajo tuje obveščevalne službe, kriminalni elementi in profesionalni hekerji, ki se ukvarjajo z informacijskim bojevanjem.

Čeprav nestrukturirana grožnja ne predstavlja neposredne grožnje, pa obstaja bojazen, da bi se akter strukturirane grožnje lahko predstavljal kot akter nestrukturirane grožnje (Dunn 2005, 15).

Po Schneierju so hekerji, osamljeni zločinci, škodoželjni zaposleni, industrijski vohuni, mediji, organizirane kriminalne združbe, obveščevalne službe in informacijski bojevniki dejansko tisti, ki bi lahko ogrozili informacijsko varnost (Schneier 2000, 43).

- *Hekerji; h*eker je oseba, ki eksperimentira z omejitvami sistema zaradi radovednosti ali samega užitka. Hekerji se po tej definiciji ukvarjajo z vdiranjem v sisteme predvsem ljubiteljsko in niso organizirani. Opiše jih tudi kot stereotipno mlade, moške in na družbenem robu. Hekerske skupnosti ne morete združiti, napadejo kar lahko. To je torej razpršena skupina ljudi, ki udari, kjer lahko in tudi tekmuje med seboj in ni homogena. Motivira jih pa predvsem lastni ego, uporništvo in izziv, ki ga vdor predstavlja (Wenger v Svete 2006, 37).
- *Osamljeni zločinci in organizirane kriminalne družbe;* ti povzročijo največ računalniškega zločina. Pogosto nimajo dovolj denarja, znanja ali dostopa. Napadli bodo poslovne sisteme, ker je tam denar. Njihov prvi motiv je pohlep. Kot taki ne predstavljajo grožnje

delovanju informacijskega sistema temveč denarju njegovih uporabnikov. Organizirane kriminalne združbe uporabljajo tehnologijo na dva načina. Po prvem načinu izvajajo zločinska dejanja tako, da uporabljajo orodja za vdiranje v bančne računalnike, po drugem pa tako, da tehnologijo uporabijo za vodenje in organizacijo drugih poslov. Skratka, uporabljajo bolj prefinjene metode kot posamezni zločinci, ker imajo več sredstev, s katerimi lahko kupijo znanje in dostop do sistema.

- *Škodoželjni zaposleni (Malicious Insider*); so je že znotraj sistema, obramba okoli sistema pa jih ne skrbi. Veliko računalniških sredstev se poskuša spoprijeti z zunanjo grožnjo, vendar so nemočni proti notranjemu nasprotniku. Kako daleč so te osebe pripravljene iti, je odvisno od njihove motivacije, torej preprost pohlep ali višji cilj. Razlog, zakaj notranja grožnja predstavlja takšno nevarnost, je v tem, da večina varnostnih mehanizmov, ki jih organizacije vzpostavljajo, ščiti pred zunanjimi grožnjami (Cole in Ring 2006, 8). Hkrati je tudi zaščita pred človekom, ki bi mu naj zaupali, zelo težavna. Obseg te grožnje nam prav tako ni znan, saj veliko primerov zlorab, ki jih povzročijo škodoželjni zaposleni, ni prijavljenih.
- *Industrijski vohuni;* cilj industrijskega vohunjenja je predvsem pridobiti prednost pred konkurentom, saj stroški vohunjenja predstavljajo le desetino tistega, kar bi porabili, če bi tehnologijo razvili sami. Povzročitelji niso pripravljeni veliko tvegati, kajti v primeru razkritja lahko vohunjenje povzroči veliko škode tistemu, ki se s to dejavnostjo ukvarja.
- *Mediji;* medije si lahko predstavljamo kot podvrsto industrijskega vohuna, s to razliko, da je njihov motiv pridobitev materiala za zgodbo, ki je vredna objave.
- *Podjetja;* podjetja, še posebej marketinški oddelki imajo velik interes v ustvarjajo profilov potrošnikov, zato raziskujejo povezave med preferencami posameznikov in jih razdeljujejo v skupine. Psihološkemu profilu teh ciljnih skupin pa potem priredijo bolj uspešno oglaševanje in posledično večjo prodajo (Facebook).
- *Policija;* policijo si lahko predstavljamo kot nacionalno obveščevalno službo, ker deluje na zakonski osnovi. Tukaj gre predvsem za problem zagotavljanja zasebnosti, ki je obravnavana v naslednjem poglavju.
- *Državne obveščevalne službe;* to je najbolj dostojen nasprotnik, ki ima zelo dobro finančno podporo, ker dostikrat deluje kot vojaška veja. Pogosteje je njihov namen pridobivanje informacij in ne povzročanje škode.
- *Informacijski bojevniki;* informacijski bojevnik je vojaški nasprotnik, ki poskuša spodkopati zmožnost cilja tako, da vodi vojno z napadi na informacijsko ali omrežno

infrastrukturo. Ta nasprotnik ima vsa sredstva obveščevalne organizacije, vendar se razlikuje v tem, da je osredotočen na kratkoročen cilj onesposabljanja nasprotnika in ne na pridobitev dolgoročnih obveščevalnih podatkov.

Kritično informacijsko infrastrukturo najbolj ogrožajo predvsem hekerji, škodoželjni zaposleni, teroristi in infobojevniki. Pri drugih gre bolj za problematiko ogrožanja zasebnosti posameznika. Hkrati to lahko povežemo z strukturo groženj, da edino informacijski bojevnik predstavlja obliko strukturirane grožnje. Vsi drugi (hekerji, škodoželjni zaposleni in teroristi) predstavljajo predvsem nestrukturirano grožnjo. Informacijski bojevniki uporabljajo metode nestrukturiranih groženj s to razliko, da te metode uporabljajo povezano in sistematično. Prav zaradi tega bi jih brez analize verjetno težko ločili od nestrukturiranih oblik groženj.

5.2 Varnostni mehanizmi IKT

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

- *tehnični:* zagotavlja se na tehnični ravni s poudarkom na omrežni varnosti. V tem pogledu se z grožnjami soočimo s tehničnimi sredstvi, kot so požarne pregrade, protivirusna programska oprema, avtentikacijski mehanizmi in ustanovitev CERT. Požarne pregrade oziroma »firewalls« si lahko razlagamo kot varnostnika na vratih, kjer ti prepuščajo le koristen podatkovni promet. Funkcija požarne pregrade je zavračanje in sprejemanje določenega podatkovnega prometa. Naloga CERT-a je preventivno delovanje. Podrobneje jih bom predstavila v nadaljevanju;
- *na ravni podjetja*: varovanje kritične infrastrukture se tukaj razume kot zagotavljanje neprekinjenega delovanja. To pomeni stalen dostop do informacijske infrastrukture in stalno delovanje poslovnih procesov, da bi se doseglo zadovoljivo poslovno delovanje. Sredstva za dosego teh ciljev, poleg organizacijskih in človeških dejavnikov, vključujejo tiste, ki so bili našteti pri tehničnem vidiku. Nekatere države na ta način pristopajo k varovanju informacijske infrastrukture;
- *vidik organov pregona*: organi pregona vidijo varovanje kritične informacijske infrastrukture predvsem v preganjanju kibernetskega kriminala, kar pokrije zelo širok razpon kaznivih dejanj. Vključuje kršitve avtorskih pravic, računalniške prevare, otroško pornografijo in kršitve omrežne varnosti. Proti takšni obliki kriminala se bori na klasičen način, še posebej s sprejemanjem nove zakonodaje in s spodbujanjem mednarodnega sodelovanja;

- *nacionalno-varnostni*: celotna družba je videna kot ogrožena, deluje se na več ravneh (tehnični, zakonodajni, organizacijski ali mednarodni). Akterji vključujejo državne uslužbence različnih organov ter predstavnike zasebnega sektorja in javnosti.

Pri zagotavljanju informacijske varnosti je vzpostavljanje mehanizmov zgodnjega opozarjanja. To nalogo opravljajo t.i. CERT (orig. Computer Emergency Response Team, računalniške skupine za urgentno reševanje kibernetskih groženj). Njihova naloga je, da se odzivajo na varnostne incidente v računalniškem omrežju, tako da jih rešujejo ali pomagajo pri njihovem razreševanju. Prav tako pa poskušajo preprečiti varnostne incidente v svoji sferi odgovornosti. Poznamo jih več vrst. Ločimo jih glede na področja, kjer delujejo. Ločimo CERT, namenjene majhnim in velikim podjetjem, vojaške, akademske, CERT za področje kritične (informacijske) infrastrukture, za področje javne uprave, državni, gospodarski in CERT dobavitelja programske opreme (GOVCERT.NL, s*etting up a CERT)*.

Ključno je tudi to, da ima vzpostavljeni CERT podporo vodstva (West-Brown 2003, 34). Dalje je potrebno določiti občinstvo oziroma odjemalce in odnos z njimi. Obstaja širok razpon storitev, ki jih CERT lahko izvaja, in sicer:

- *reakcijski*: to dejavnost sproži dogodek ali prošnja, kot na primer ogroženega strežnika, širjenje zlonamerne kode, programska ranljivost ali nekaj, kar zabeleži sistem za odkrivanje vdorov. Reaktivne storitve so ključni del nalog CSIRT-a;
- *proaktivni*: te storitve vključujejo pomoč in obveščanje, da bi pripomogli k pripravi, varovanju in zaščiti sistemov pred napadi, težavami ali dogodki. Izvajanje teh storitev bo zmanjšalo pojav teh dogodkov v prihodnosti;
- *postopki za zagotavljanje kakovosti*: ta storitev dopolnjuje obstoječe in uveljavljene storitve, ki so ločene od ravnanja z incidenti in jih izvajajo drugi oddelki, kot so IT, revizija in oddelek za izobraževanje. Če CERT pomaga s temi storitvami, lahko izboljša celokupno varnost organizacije in identificira grožnje in sistemske slabosti. Te storitve so proaktivne in posredno pripomorejo k zmanjšanju števila varnostnih incidentov.

Kot bomo videli v naslednjem poglavju, imajo storitve CERT-a podobne funkcije kot varnostni mehanizem v celicah.

5.2.1 Podobnosti med varnostnimi mehanizmi v bioloških celicah in omrežjih

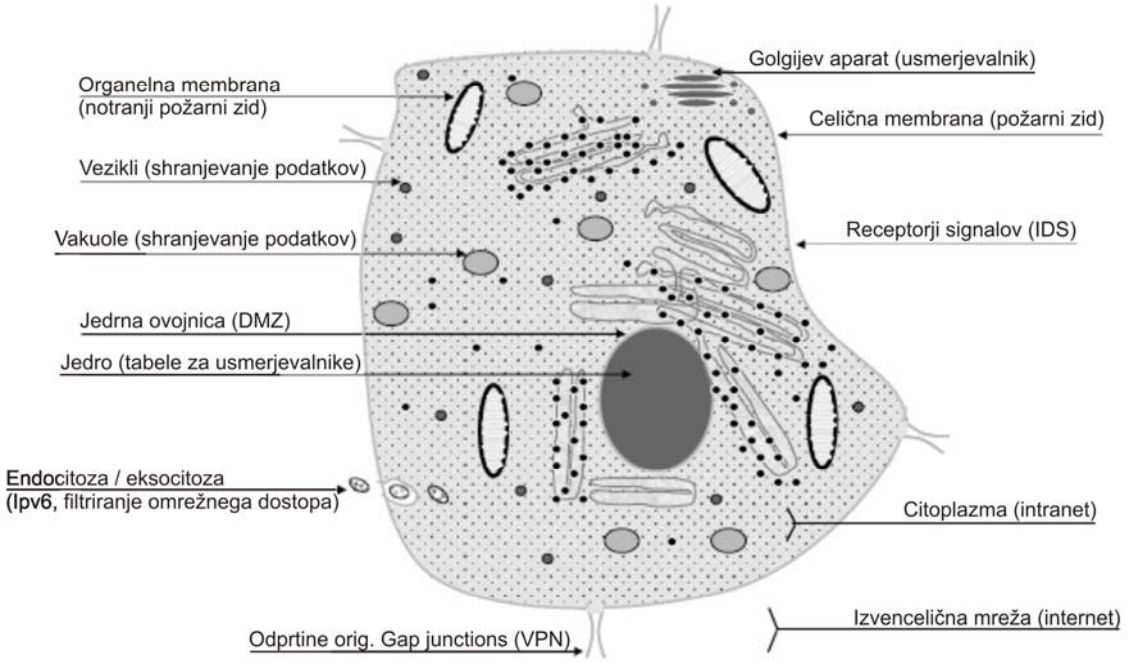
Pristop k varnosti v celicah je konsistenten s pojmom »podrobna, globinska obramba« (orig. Defense-in-depth notion), ki temelji na več tehnikah in slojih, kar pomaga zmanjšati tveganje, da bi karkoli ogrozilo eno izmed teh plasti (Knapp in dr. v Tipton in Krause 2008, 238).

Preučevanje varnostnih mehanizmov v celicah je pokazalo, da so ti mehanizmi prisotni skoraj v vsaki komponenti celice. Celice imajo večplasten in »podroben« pristop k varnosti. V današnjem visoko-tehnološkem okolju, kjer ima varnost vedno večji pomen, lahko takšno razmišljanje stimulira razmišljanje o varnosti in ponudi model oblikovanja varnostnih sistemov (Knapp in dr. v Tipton in Krause 2008, 238).

Razumevanje osnov celične teorije pomaga razložiti, zakaj so celice uporabne pri preučevanju varnostnega vprašanja. Premisa celične teorije je, da so vsa živa bitja zgrajena iz celic - to je osnovni gradnik strukture v vseh živih bitjih. Ena sama celica je lahko celoten organizem, ali pa se združujejo v skupine večjih večceličnih organizmov, kot je na primer človek. Tudi človek pa se nadalje združuje v družbene (interesne) skupine, države, organizacije, pri uporabi IKT pa se združuje v različne virtualne družbene skupine. Čeprav obstajajo razlike med vrstami celic (med živalsko in rastlinsko celico), obstajajo osnovne skupne značilnosti celic enake. Slika 5.1 kaže osnovno celično arhitekturo. Za vsako identificirano celično komponento na sliki je poimenovana tudi primerjalna komponenta v računalniškem omrežju. Komponente so podrobneje opisane v tabeli 5.2 (Knapp in dr. v Tipton in Krause 2008, 238).

Tabela 5.2 kaže ogrodje teh štirih analogij, ki primerjajo celično biologijo in računalniška omrežja. V levem stolpcu so opisi funkcij, ki so skupne obema. Sredinski stolpec vsebuje termin iz računalniških omrežij, v desnem stolpcu pa so ustrezni biološki termini (Knapp in dr. v Tipton in Krause 2008, 238).

Slika 5.1: Komponente biološke celice in njihove ustrezne komponente v računalniški mreži



Vir: Knapp in dr. v Tipton in Krause (2008, 239).

Tabela 5.2: Primerjava računalniške mreže in biološke celice

Analogna funkcija	**Primer enote v računalniški mreži**	**Primer enote v biološki celici**
Pregradna obramba	Eksterni usmerjevalnik, požarni zid, sistem za odkrivanje vdorov (orig. Intrusion detection system - IDS)	Plazma, membrana /celična stena, oligosaharidi
Prepuščanje delcev (podatkov) in komunikacija z zunanjim okoljem	Usmerjevalni protokoli (orig. Tunneling protocols), plasti varnostnih luknjic (orig. Secure Sockets Layer), virtualna privatna omrežja (VPN-ji), omrežna vrata	Variabilnost membranskih kanalov, Stik odprtin, olajšana difuzija, izvencelijska signalizacijska mreža (receptorji)
Notranja organizacija	Notranji požarni zidi, območje demilitariziranega omrežja (orig. Network demilitarized zone - DMZ)	Organeli, vezani na membrano, dvojna membranska ovojnica okoli celičnega jedra
Notranje usmerjanje in komunikacija	E-mail, instantno sporočanje, usmerjevalniki, IPv6, usmerjevalne preglednice (orig. Routing tables)	Endocitoza, eksocitoza, golgijev aparat, celično jedro

Vir: Knapp in dr. v Tipton in Krause (2008, 238).

Avtorji o študiji celične varnosti zato menijo, da se pojavi pet principov, ki predstavljajo zvijačo, ki jo je možno aplicirati na informacijsko varnost na družbeni ravni (Knapp in dr. v Tipton in Krause 2008, 243):

1. Brezhibna integracija komunikacije in varnostne funkcionalnosti. Varnostna funkcionalnost je zelo integrirana v celične mehanizme. To pomeni, da varnost ni ločena od komunikacijskega mehanizma, ampak je integralni del sistema samega. V celici ne najdemo posebnega organela, ki bi bil specializiran posebej za varnost. Gre torej za varnost, do katere imajo različni mehanizmi in organeli v celici direktno vgrajeno deljeno odgovornost.
2. *Proaktivni pristop* do membranske obrambe in prehajanja delcev. Celice imajo proaktiven pristop do prehajanja delcev skozi zunanjo celično membrano. Pristop identifikacije neželenih elementov, ki je značilna metoda sistema za odkrivanje vdorov (orig. IDS – intrusion detection system) pa je ravno nasproten od tistega, ki ga uporabljajo celice. S posvečanjem pozornosti na »prijazne« kemijske in električne signale, ki jih prinesejo obiskovalci zunanje membrane, celice tvorijo aktivno obrambo. Tako celice identificirajo želene elemente preden jim dovolijo prehod preko zunanje celične membrane. Neželeni in neidentificirani elementi pa so blokirani.
3. Visoka stopnja specializacije komunikacijskih metod. Celice imajo široko izbiro visokospecializiranih mehanizmov za prenašanje molekul preko zunanje celične membrane. Za vsako molekulo, ki jo celica potrebuje, obstaja poseben, po meri narejen mehanizem za komunikacijo in prehod te molekule skozi membrano. Celična membrana ni preprosto stena, ki blokira neželene ali nevarne elemente, ampak deluje kot kompleksni sistem, ki vsebuje številne transporterje in kanale, ki so vsi narejeni tako, da prepuščajo le določeno vrsto molekul.
4. Standardizirana uporaba notranjih membran, ki varujejo najbolj pomembne organele v celici. Celice imajo liberalno uporabo notranjih membran. Pomembnejši celični organeli (mitohondrij, vakuole in jedro) imajo vsi svojo lastno membrano (ali celo več membran), ki jim poleg zunanje celične membrane nudijo dodatno zaščito. Bolj pomembno funkcijo izvaja organel, bolj robustna je njegova interna membrana.
5. Na splošno lahko rečemo, da je varnost v celici integrirana, navzoča povsod in kontinuirana. Glede na to, koliko različnih inherentnih varnostnih mehanizmov ima celica, lahko rečemo, da je vzdržuje visoke varnostne standarde. Obrambni ukrepi so prisotni v zunanji membrani, znotraj celičnih organelov, med notranjim usmerjanjem molekul in na sploh skozi celotno celico. Varnostni mehanizmi v celici so tudi

neprekinjeno, kontinuirano aktivni. V celici je torej varnost del vsega, varnost je prisotna povsod in varnostni mehanizmi vedno funkcionirajo, torej je tudi varnost vedno na visoki stopnji (Knapp in dr. v Tipton in Krause 2008, 244).

Čeprav sem samo nakazala, kako delujejo procesi v celici, upam, da bo ta razprava stimulirala različne poglede na informacijsko varnost. Takšni pogledi lahko pripeljejo do idej, ki bi lahko na koncu prispevale k izboljšani varnosti (Knapp in dr. v Tipton in Krause 2008, 244).

6 Uporabnik kot referenčni objekt informacijske varnosti

6.1 Psihologija varnosti

Varnost je občutek in realnost hkrati, ampak ni nujno enake vrednosti. Naš subjektivni občutek, kako varno se počutimo v nekem okolju, se redko ujema z realnim stanjem varnosti v tem okolju. Govorimo lahko torej o našem občutku varnosti in realni varnosti, ki je v dejanskosti. Dejanska varnost je matematična, osnovana na verjetnosti različnih tveganj in učinkovitosti različnih protiukrepov. Če imamo dovolj statističnih podatkov o pogostosti kriminalnih dejanj, lahko izračunamo možnost, da se to zgodi nam (Schneier 2008, 1).

Varnost je tudi občutek, ki pa ne izhaja iz matematičnih verjetnosti, ampak iz naših psiholoških reakcij tako na tveganja kot na protiukrepe. Nekdo se lahko bolj ali manj počuti varno, ko vidi varnostnika na delu. Skratka, lahko smo na varnem, čeprav se tako ne počutimo in lahko se počutimo varno, čeprav nismo (Schneier 2008, 2).

Behavioristična ekonomika odgovarja na vprašanja o kod izvira občutek varnosti, kako deluje in zakaj občutek varnosti ne nujno sovpada z realno varnostjo. Ta veja proučuje človekove čustvene, socialne in kognitivne vzgibe, ter kako vplivajo na ekonomske odločitve. Naslednja veja je psihologija odločanja. Obstaja pa tudi direktno raziskovanje psihologije tveganj (Scneier 2008, 2).

Absolutne varnosti ni, vsako povečanje varnosti je kompenzacija za nekaj drugega. Varnost zahteva velike vsote denarja, časa, sposobnosti, neprijetnosti, svoboščin itd. Te vsakodnevne odločitve o kompenzaciji za varnost delamo intuitivno. Zaklenemo vrata, izberemo določeno pot v službo, izbor plačilnega sredstva itd. Čeprav delamo te kompenzacije intuitivno, lahko včasih pretiravamo ali pa minimiziramo dejanske grožnje (Scneier 2008, 2). Ljudje so manj usmerjeni k grožnjam, ko pričakujejo dobiček, hkrati pa so bolj dovzetni za grožnje, ko pričakujejo izgube (Schneier 2008, 3).

Po Schneierju (2008, 3) lahko napačno precenimo več aspektov grožnje:

- resnost grožnje,
- verjetnost grožnje,
- obseg stroškov,
- ocena efektivnosti protiukrepa in
- kako dobro primerjamo tveganja in stroške protiukrepov.

Primer iracionalne kompenzacije je dejstvo, da v Ameriki na leto umre 5000 ljudi zaradi zastrupitve s hrano, teroristi pa so 9/11 ubili le 2973 ljudi, Američani pa zapravljajo desetine bilijonov dolarjev na leto za obrambo pred terorizmom, proračun za hrano in zdravila pa je le 1.9 bilijona. Taki na pogled iracionalni primeri imajo pomemben evolucijski razlog (Schneier 2008, 3).

6.2 Ogrožene vrednote

Varnost posameznika se v prvi vrsti nanaša na njegovo zasebnost ter zagotavljanje ekonomskega blagostanja. Vrednotna in ekonomska sfera je pri širjenju uporabe IKT vse bolj ogrožena, saj je zasebne in zaupne podatke o posamezniku vse težje zavarovati pred zlorabami tako drugih posameznikov, podjetij kot tudi državnih institucij (Rogerson v Svete: 2005, 202). Po drugi strani pa je okolje IKT ter še posebej interneta postalo vse pomembnejši vir pridobivanja podatkov tako za državne kot zasebne obveščevalne in analitične službe (Boni in Kovacich v Svete 2005, 202).

6.2.1 Pravica do zasebnosti

Univerzalne definicije zasebnosti in pravice do zasebnosti ni. Vzrok za to je, da je zasebnost relativna, kontekstualna in subjektivna. Vsakdo ima drugačna pričakovanja glede zasebnosti in ta se spreminjajo tudi glede na družbeni kontekst. Problem definicije zasebnosti je tudi v tem, da zasebnost ščiti svobodo posameznika, "*individualna svoboda pa ne more biti ne napovedana, ne pogojena*" (Gutwirth v Kovačič 2006, 12), saj ima za vsakogar drugačen pomen (Kovačič 2006, 12).

Kljub temu da se zasebnost kot vrednota in posledično kot pravica začne uveljavljati šele v 18. stoletju, pri njenem priznanju ne gre za proces, katerega obseg bi se skozi čas širil, temveč prav nasprotno. Zasebna sfera se skozi zgodovino oži, pravica do zasebnosti pa v zadnjih letih postaja čedalje bolj omejena. Pravo pravico do zasebnosti sicer ščiti in na nekaterih področjih navidezno celo širi (čeprav gre pri teh "širitvah" večinoma zgolj za sledenje tehnološkemu in družbenemu razvoju, pogosto pa celo zgolj za legitimizacijo

uveljavljenih praks vdiranja v zasebnost), vendar zasebnost kot vrednota v družbi izgublja pomen (Kovačič 2006, 11).

Zasebnost ščiti svobodo posameznika, zato za tradicionalnega nasprotnika zasebnosti večinoma velja država, vendar se svoboda ne nanaša zgolj na odnos posameznika do politične oblasti, temveč tudi do družbe. Zato je danes pravzaprav poglavitni akter, ki ogroža zasebnost posameznikov, družba, država pa ima ambivalentno vlogo – po eni strani posega v zasebnost posameznikov, po drugi strani pa posameznika varuje pred vplivi družbe. V tem oziru se zasebnost nanaša na vzpostavitev meje med posameznikom in drugimi, ki po eni strani preprečuje odtekanje informacij o posamezniku k drugim, po drugi strani pa posameznika ščiti pred zunanjimi vplivi (Kovačič 2006, 11). Svoboda, avtonomija in samoodločanje so zato bistvene prvine zasebnosti (Gutwirth v Kovačič 2006, 12). Podobno stališče je glede pravice do zasebnosti zavzela tudi pravna stroka.

V sodobni družbi namreč postaja zasebnost tržno blago, s katerim je mogoče trgovati, in ne več pravica, ki jo je treba varovati. Poleg tega je v sodobni družbi zasebnost pogosto dojeta kot ovira, bodisi drugih posameznikov (npr. prostemu razpolaganju z zasebno lastnino v primeru zasebnosti na delovnem mestu, svobodi govora itd.), bodisi javnega interesa (v zvezi z vprašanji javne varnosti in javnega zdravja) ter drugih skupnih pravic in interesov (predvsem ekonomskih in množičnih medijev) (Gutwirth v Kovačič 2006, 12).

Čeprav zakonodaja ščiti zasebnost posameznikov, pa hiter tehnološki razvoj nadzorovalnih tehnologij in pritiski družbe zasebnost pravzaprav čedalje bolj ožijo. Zasebnost tako ostaja zgolj možnost za tiste, ki si jo lahko privoščijo, cena zanjo pa je vse višja (Kovačič 2006, 13).

Ko govorimo o zasebnosti, mislimo predvsem na pravico do zasebnosti. Banisar in drugi (v Kovačič 2003, 34) pravico do zasebnosti določajo kot mejo, »do katere družba lahko vdre v posameznikove zadeve«. Osrednja prvina pravice je možnost, da posameznik na določen način ravna, pravo pa pravice dodeljuje zato, da lahko posamezniki zadovoljujejo svoje interese. Cilj pravice je torej interes, pravo pa varuje tiste interese, ki so ovrednoteni kot pravno relevantni (Pavčnik v Kovačič 2006, 37).

Dosedanji prikaz pojmovanj zasebnosti kaže predvsem na to, da pravica do zasebnosti ni enodimenzionalen pojem. Po mnenju avtorjev poročila Privacy & HumanRights 1999 (v Kovačič 2006, 45) je zasebnost temelj človeškega dostojanstva in drugih vrednot, kot npr. svobode združevanja in svobode govora, iz česar tudi izhaja razumevanje zasebnosti kot temeljne pravice, iz katere izhajajo preostale pravice v sodobni družbi – po njihovem mnenju je zasebnost postala ena najpomembnejših (pa tudi najbolj ogroženih) človekovih pravic v

sodobni družbi. Sodobne klasifikacije pravice do zasebnosti le-to delijo glede na njene dimenzije, nekateri pa težijo tudi h klasifikaciji pravice do zasebnosti glede na možne vdore vanjo (Lampe v Kovačič 2006, 45).

Avtorji poročila Privacy & Human Rights 2003 (v Kovačič 2006, 46) ločijo naslednje vrste zasebnosti: *informacijsko zasebnost*, ki se navezuje na obdelavo osebnih podatkov, oziroma je znana tudi kot zaščita (osebnih) podatkov; *zasebnost telesa*, ki posameznika ščiti pred postopki, ki zadevajo njegovo fizično telo, npr. genskimi testi, pregledom telesnih odprtin ter testi telesnih tekočin (krvi, urina); *zasebnost komunikacij*, ki ščiti posameznikove komunikacije ne glede na obliko pred prestrezanjem s strani drugih; *prostorsko zasebnost*, ki ščiti posameznika v njegovih prostorih, kar zajema preiskovanje in opazovanje njegovih domačih, pa tudi službenih prostorov.

V komentarju Ustave RS pa se pravica do zasebnosti deli na:

1. **Zasebnost v prostoru**, ki se odraža v možnosti posameznika, da je sam, torej ločen od fizične navzočnosti drugih ljudi;
2. **Zasebnost osebnosti**, ki se odraža v svobodi misli, opredelitve in izražanja;
3. **Informacijsko zasebnost**, ki se odraža v možnosti posameznika, da obdrži informacije o sebi, ker ne želi, da bi se z njimi seznanili drugi (Šilc 2007).

Kot rečeno, je k razvoju pravice do zasebnosti precej pripomogel razvoj tehnologije. Tehnološke spremembe namreč prinašajo nove oblike in načine posegov v zasebnost, pravo pa je na te spremembe prisiljeno reagirati. Pravzaprav pravni sistem tem tehnološkim spremembam večinoma le sledi (Sykes v Kovačič 2006, 46), zato gre pri razvoju pravice do zasebnosti za nenehno prilagajanje načel varstva zasebnosti tehnološkim spremembam, kar velja zlasti za 20. stoletje (Gellman v Kovačič 2006, 46).

Večina avtorjev je mnenja, da se zasebnost ljudi danes zmanjšuje.

Problematika osebnih podatkov

Osebni podatek je vsak podatek, ki se nanaša na določeno ali določljivo fizično osebo tako, da kaže na njegove lastnosti, stanja, razmerje, ne glede na obliko, v kateri je izražena. Pri nas imamo na tem področju dobro dodelan Zakon o varstvu osebnih podatkov (ZVOP – 1). Smisel tega zakona je varovanje zasebnosti in dostojanstva posameznikov, ki sta lahko ogrožena pri obdelavi njihovih osebnih podatkov.

Zakon o varstvu osebnih podatkov načelno določa, da je varstvo osebnih podatkov namenjeno preprečevanju nezakonitih in neupravičenih posegov v informacijsko zasebnost posameznika na vseh relevantnih področjih. Določa tudi, da je na ozemlju Republike

Slovenije vsakemu posamezniku, ne glede na državljanstvo in prebivališče, zagotovljeno varstvo osebnih podatkov. Smisel varstva osebnih podatkov torej ni varovanje osebnih podatkov kot takih, temveč varovanje pravic posameznika, na katerega se podatki nanašajo.

Osebni podatki se lahko obdelujejo le, če je njihova obdelava določena z zakonom, ali če ima upravljavec zbirke podatkov pisno privolitev posameznika. Za pravne ali fizične osebe, ki opravljajo javno službo ali dejavnost po zakonu, ki ureja gospodarske družbe, pa velja, da lahko že neposredno na podlagi tega zakona, torej brez izrecne podlage v nekem drugem zakonu ali pisne privolitve posameznika, obdelujejo osebne podatke oseb, s katerimi so v pogodbenem razmerju, vendar le, če gre za osebne podatke, ki jih potrebujejo za izpolnjevanje pogodbenih obveznosti ali uveljavljanje pravic iz pogodbenega razmerja. Za državne organe, organe lokalnih skupnosti in nosilce javnih pooblastil je ureditev drugačna, saj lahko obdelujejo le tiste osebne podatke, za katere je tako določeno z zakonom. Posameznik, čigar osebni podatki se obdelujejo na podlagi njegove pisne privolitve, mora biti predhodno pisno seznanjen z namenom obdelave podatkov, njihove uporabe in časom shranjevanja.

Obseg podatkov, ki se lokalno, nacionalno in internacionalno pretakajo skozi elektronska omrežja stalno narašča (Lyon 2006, 16). Današnja družba meji na shranjevanju podatkov, opazovanju in nadzorovanju s strani različnih agencij in organizacij. Osebni podatki se pretakajo povsod, ob nakupu v trgovini z bančno kartico, pri brskanju po internetu in po ostalih storitvah, ki jih ponuja, z uporabo RIFD etikete, mobilnega telefona, skratka podatki konstanto krožijo in se beležijo. Zaradi tega so možne tudi zlorabe osebnih podatkov, npr. kraja identitete (angl. *identity theft*), ki je zelo pogost pojav v ZDA. Seveda pa osebni podatki krožijo tudi na mednarodni ravni, za izmenjavo policijskih podatkov ali za zunanje izvajanje (angl. *outsourcing*) (Lyon 2006, 17-19).

Najostrejša zakonodaja o osebnih podatkih je značilna ravno za Evropo, ki so precej razlikuje od »milejše« zakonodaje v ZDA. Dejstvo je, da imajo ZDA in EU različne poglede na informacijsko zasebnost. Prva očitna razlika je, da imamo države znotraj EU varstvo osebnih podatkov urejeno enotno, največkrat v enem predpisu, ki zajema vse oblike obdelave osebnih podatkov, ZDA to področje ureja zelo parcialno in nepopolno (Lavrenčič, 2007). V ZDA velja načelo, da je lastnik osebnih podatkov, tistih ki jih je zbral, v Evropi pa so posameznik na katere se osebni podatki nanašajo njihovi lastniki. Torej diametralno nasprotni pogledi na informacijsko zasebnost (Lavrenčič 2007).

Danes se tako pojavlja nova tehnologija za zbiranje osebnih informacij, ki prodira globlje, širše, bolj sofisticirano in posamezniku bolj prijazno kot tradicionalne metode. Moč

nadzorovanja pa je ravno v tem, da je vse zbrane podatke možno povezati, in s tem pridobiti nove vredne podatke in informacije, ki so lahko škodljive ali celo nevarne za posameznika (Čebulj v Kovačič 2003, 27). Pri zbiranju podatkov pa obstajajo tudi druge nevarnosti, kot so »nenatančnost, nepopolnost ali neažurnost zbranih podatkov«, preventivno zbiranje podatkov, obstoj baz podatkov, za katere posamezniki sploh ne vedo ali pa vanje nimajo vpogleda (Kovačič 2003, 36). Tako se podatki danes ne samo zbirajo in popravljajo, ampak tudi analizirajo, iščejo, združujejo, trgujejo, znotraj in med organizacijami (Lyon 2006, 22), pri tem pa so možne tudi različne zlorabe in druge nevarnosti.

Med pomembnejšimi oblikami ogrožanja varnosti posameznika, Cronin (v Svete 2005, 203) izpostavlja zlasti **kibernetski kriminal** (cyber-stalking), **digitalno obrekovanje** (digital defamation) ter **krajo identitet** (identity theft). Pri tem pa je pomembna ugotovitev, da so lahko posamezniki žrtve različnih vrst napadov tako s strani informacijskega terorizma kot kibernetskega kriminala. Z vidika varnosti posameznika je sicer manj pomembno, kdo ogroža njihovo varnost, je pa vir ogrožanja pomemben pri izvajanju varnostne politike. Poleg dejanskega ogrožanja posameznika je izredno pomemben tudi psihološki vidik, kajti posamezni uporabniki lahko izgubijo zaupanje v uporabo IKT, kar lahko predstavlja resen gospodarski in celo politični problem. Kot ugotavlja Cronin (Ibid.), je bilo po nekaterih podatkih nekaj deset oz. celo sto tisoč uporabnikov žrtev kibernetskega kriminala[6]. To pa je dovolj velika številka, da se je problema lotila tudi že država in celo mednarodna skupnost, ki postopoma določa pravila obnašanja v kibernetskem prostoru ter tudi ustrezne sankcije (Svete 2005, 204).

KIBERNETSKI KRIMINAL; opredelitev Cyber-stalking oz. kibernetskega, ki jo predlagata D'Ovidio in Doyle (v Svete 2005, 203):

Cyber-stalking je v tem primeru definiran kot uporaba interneta, elektronske pošte oz. drugih primernih digitalnih elektronskih komunikacijskih naprav in sistemov z namenom ovirati, škoditi oz. ogrožati posameznika ali skupino posameznikov. V ta namen se lahko uporabljajo različne oblike groženj, kraje identitet in podatkov, poškodovanje podatkov in opreme ter navajanje mladoletnikov na pornografijo. Eden izmed najnovejših primerov kibernetskega kriminala je kodiranje datotek s trojanskimi konji. Na ta način je uporabnikom onemogočen dostop do vsebin trdih in mrežnih diskov, v zameno za dekodiranje le-teh pa morajo avtorjem trojanskih konjev plačati odkupnino.

[6] Glej podatke za obseg takih groženj za države članice EU v prilogi.

DIGITALNO OBREKOVANJE; digital defamation oz. digitalno obrekovanje bi lahko poimenovali kot sodobno obliko psihološkega bojevanja tako na lokalni kot globalni ravni, ki se lahko izvaja na različne načine (zloraba imen domen, ko se zamenja le del, navadno končnica, t. i. sovražne strani - hate pages, obrekovanje oz. širjenje laži z uporabo elektronske pošte - email alerts). Organizirane kampanje digitalnega obrekovanja imajo potencialno zelo veliko ciljno publiko, ki jo dosežejo v zelo kratkem času, prav tako pa lahko povzročijo velike frustracije uporabnikov zaradi sitnosti, ki jih povzročijo. Ponovna vzpostavitev zaupanja in prvotnega ugleda podjetij ali posameznika, pa predstavlja velik izziv za prizadete uporabnike IKT, kajti premagati morajo še posttravmatski učinek, ki nastopi s časovno zakasnitvijo (Svete 2005, 204).

Posameznikove informacijske dobrine oz. omrežno identiteto pa lahko poleg vojaških in komercialnih virov ogrožajo tudi **hekerji**, kljub temu pa lahko rečemo, da bo nekaj posameznikov vedno tarča sistematičnih oblik delovanja informacijskih bojevnikov oz. omrežnih teroristov (Svete 2005, 203).

KRAJA IDENTITETE je naslednja zelo pogosta oblika ogrožanja varnosti posameznika, pri čemer izvajalec črne PR kampanje doseže znatne asimetrične učinke v svojo korist. Cilj je tako prisiljen na defenzivno delovanje, pri čemer ga napadalec lahko pusti v stanju negotovosti, kajti pri kraji identitete je praktično nemogoče ugotoviti napadalčevo identiteto, njegove motive, lokacijo, namene, prav tako pa ne moremo ugotoviti, ali gre za skupino ali za delovanje posameznika. Nadalje pa lahko izvajalec tovrstnega napada prevzame ciljno omrežno identiteto ter jo prilagodi svojim potrebam in interesom, pri čemer pa se cilj takšnega delovanja sploh ne zaveda, da njegovo identiteto v kibernetskem prostoru uporablja nekdo drug (Cronin v Svete 2005, 205).

Digitalno obrekovanje in kraja identitet sta torej dva zelo pomembna vidika ogrožanja varnosti posameznika, ki nastaneta pri uporabi IKT. Za obe obliki je značilno, da si napadalec brez vedenja in soglasja napadene osebe prisvoji njeno identiteto oz. jo z neresničnim prikazom v internetnem prostoru poskuša omadeževati. Glavni cilji tovrstnega delovanja pa so gotovo povezani s finančnimi zlorabami, pridobivanjem osebnih dokumentov ter drugimi premoženjsko - pravnimi koristmi.

Med človeškim dejavnikom, ki namerno ogroža omrežno varnost na nivoju posameznika, moramo še posebej izpostaviti krajo identitete, izsiljevanje ter grožnje, oblikovanje in posredovanje virusov ter drugih pritajenih programov. Prav tako pa ima pomembne predvsem psihološke implikacije onemogočanje dostopa do storitev, kraja zaupnih podatkov in uporaba nelegalne programske opreme (piratstvo), ki ga sodobne države vse

pogosteje kazensko preganjajo tudi na ravni posameznih uporabnikov (orig. Denial of Service) (Petrović v Svete 2005, 205).

6.3 Varnostni mehanizmi za zagotavljanje informacijske varnosti posameznika

Wray (v Svete 2005, 207) tako predlaga, da se pri preučevanju sodobnih konfliktov, ki naj bi bili popolnoma odvisni od uporabe IKT, v središče preučevanja postavi posameznik. Posameznik je namreč vse bolj pomemben dejavnik, ki ni zgolj žrtev informacijskega delovanja, temveč lahko s svojo uporabo IKT bistveno vpliva na prihodnje konflikte. Zato je potrebno pri razpravi o informacijskem bojevanju izhajati od posameznika in njegovih interesov navzgor (Svete 2005, 207).

Pri obravnavanju informacijske varnosti posameznika se pojavi vprašanje, kdo točno naj skrbi za njeno zagotavljanje. »Ali naj za varnost pri uporabi IKT skrbi država, razvijalci IKT tehnologije in druge nedržavne institucije ter organizacije (npr. nevladni CERT), ali pa celo posamezniki sami.« (Svete 2005, 206) Tu namreč naletimo na osnovno vprašanje, ki ga izpostavlja že koncept človekove varnosti: ali lahko država sploh zagotovi varnost posameznika, ali pa predstavlja enega izmed najpomembnejših virov ogrožanja njegove varnosti, kot trdijo radikalni predstavniki varnostnih teorij, v skladu s katerimi varnost izhaja iz posameznika, ne pa iz države (oblasti) ali nacije (Svete 2005, 206).

Ukrepe za zavarovanje posameznika med njegovo uporabo IKT lahko razdelimo na **samozaščitne, ukrepe nedržavnih akterjev** (predvsem komercialnih ponudnikov IKT) in na **ukrepe države.** Slednje sprejema država za zavarovanje varnosti posameznika, razdelili pa bi jih lahko na normativne, fizično - tehnične ter logične (Petrović v Svete 2005, 209). Od vsake države pa je odvisno, kakšne bodo konkretne rešitve na omenjenih področjih.

Med *normativne ukrepe* sodijo netehnični ukrepi, med katerimi so najpomembnejši pravni, organizacijski in kadrovski. Ti ukrepi se sicer neposredno ne nanašajo na sam sistem zaščite, pač pa bistveno izboljšajo učinkovitost njegovega delovanja. Na ta način namreč določimo zaščitno politiko, ki odreja, kaj je dopustno, na drugi strani pa določimo tudi sankcije za nedopustno delovanje. Normativni ukrepi so temelj, ki se nato finalizira s *fizično-tehničnimi* in *logičnimi ukrepi* v učinkovit zaščitni sistem. Prav tako pa normativni ukrepi kohezivno vežejo vsa ostala sredstva v enoten zaščitni mehanizem (Svete 2005, 209).

Druga vrsta ukrepov se nanaša na *fizično-tehnični vidik*[7], ki zahteva finančne investicije vnaprej, torej še preden se kažejo prvi učinki, vendar pa se lahko stroški natančno ocenijo in jih je mogoče prilagoditi finančnim zmožnostim.

Logični ukrepi predstavljajo vrsto avtomatiziranih informacijskih sistemov edino in obenem zelo učinkovito zaščitno sredstvo. Visoko stopnjo učinkovitosti je mogoče doseči še posebej z uporabo logičnih ukrepov v paketu (Svete 2005, 209).

Brez sodelovanja države, nedržavnih organizacij, stroke in laične javnosti je nemogoče zagotoviti celovit pristop za zagotovitev varnosti posameznika pri njegovi uporabi IKT. Le na ta način je namreč mogoče zagotoviti ravnotežje med razvojem tehnologije in njenih možnosti ter varnostnimi mehanizmi in varno uporabo na drugi strani (Svete 2005, 208).

V nadaljevanju bom predstavila primer biometrije kot sistema za varovanje posameznikove integritete, ter zagotavljanje pravilne avtentikacije. Gre torej za kontrolo dostopa, ki pa je, kot bomo videli, tudi marsikdaj na žalost popoln sistem, ki se ga da pretentati.

6.3.1 Biometrija kot napredni varnostni mehanizem identifikacije posameznika

Biometrija spada med najnovejšo nadzorovalno tehnologijo. Sama beseda biometrija izhaja iz starogrške besede »bios« (življenje) in »metron« (meritev) (Lavrenčič, 2007). Njena značilnost je uporaba telesnih značilnosti kot načina identifikacije in nadzorovanja. Gre torej za »proces zbiranja, procesiranja in shranjevanja podatkov o posameznikovih fizičnih lastnostih z namenom identifikacije.« (Kovačič 2003, 103) Z biometrijo smo identificirani skozi fizične značilnosti kot je glas, obraz, oči, prstni odtis, DNK itd. Med seboj se najbolj ločimo po DNK, šarenici, mrežnici in prstnih odtisih, manj pa po obliki dlani, obrazu, govoru, podpisu, hoji, načinu tipkanja. Uporabimo jo lahko v dveh primerih: *za identifikacijo* ali prepoznavanje posameznika z vsemi, ki so v bazi, ter *za verifikacijo* oz. potrditev, torej ali gre res za tisto osebo, za katero se izdaja.

Biometrija dlani se sicer uporablja že vrsto za let, vendar je za splošno rabo neprimerna, saj se dlani med sabo ne razlikujejo dovolj. Prav tako tudi 5 % ljudi nima

[7] Med take ukrepe spadata recimo kriptografija in kontrola dostopa. Kriptografija ali »skrite kode« so osnovno orodje informacijske varnosti. Kriptografija se uporablja na različnih področjih, tudi pri zagotavljanju zaupnosti in integritete, ki spadata med vitalne funkcije informacijske varnosti. Kontrola dostopa se izvaja z avtentikacija, avtorizacija in biometrijo. Pri kontroli dostopa do informacij govorimo o avtentikaciji in avtorizaciji. Alternativa geslom je biometrija in t. i. »pametne kartice«. Avtorizacija pa je omejitev določenega dela podatkov pred avtentičnimi uporabniki. To se uravnava s seznami ljudi, ki imajo kontroliran dostop in pooblastila do ravnanja s podatki. (Tipton in Krause, 2006)

čitljivega prstnega odtisa, bodisi zaradi genskih napak, zaradi obrabe ali nesreč, elektronske čitalnike pa je mogoče prelisičiti s pomočjo toplega in vlažnega zraka ter z drugimi načini, npr. želatine iz katere so narejeni gumi-medvedki[8]. Prepoznavanje obraza temelji na 30-ih obraznih točkah, vendar tudi ta sistem ne deluje brezhibno. Za ugotavljanje identifikacije je tako najbolj primerno analiziranje DNK, šarenice in mrežnice. Ravno odčitavanje šarenice je dovolj zanesljiva metoda, kjer hkrati tudi ni potreben fizični stik kot pri oddajanju prstnih odtisov (Miko 2004). Za večjo verodostojnost se raziskovalci nagibajo k multibiometričnim sistemom, torej kombinaciji različnih biometričnih metod. ZDA so izbrale skeniranje prstnih odtisov in prepoznavanje obraza (Miko 2004), temu sledi Evropa, tudi Slovenija z novimi potnimi listi zaradi zahtev ZDA. S preverjanjem več biometričnih podatkov hkrati se tako poveča zanesljivost preverjanja ljudi. Kovačič (2003) pravi da »ni dvoma, da biometrija izrazito povečuje možnosti nadzora posameznikov.«

Evropska komisija je leta 2005 izvedla študijo o vplivih biometrične tehnologije na družbo (Evropska komisija 2005).

Dokument navaja primere komercialne distribucije in izmenjave biometričnih podatkov, do katerih je že prišlo: " *Nekatera ameriška podjetja strankam že ponujajo možnost uporabe sistema prstnih odtisov za hitrejšo dostavo hamburgerja.*" (Kodelja in Banovič 2005)

Biometrični sistemi za vstop v šolsko jedilnico, vžig avtomobila s pomočjo skenerja prstnih odtisov ali sistemi prepoznavanja obraza na avtobusih lahko kmalu postanejo realnost v vsakdanjem življenju Evropejcev.« (M. B. STA 2. 4. 2005) Čeprav je Evropa v primerjavi z ZDA veliko bolj zadržana in trenutno ne zaseda dominantnega položaja na tem področju, naj bi hitro dohitela ZDA, predvsem v bančnem sektorju. Študija omenja tudi negativne učinke: negotovost glede stroškov, zaščite zasebnosti in velika akumulacija moči tistih, ki bodo nadzirali biometrične podatke, in opozarja evropske politike, da se začnejo pripravljati na novo tehnologijo čim prej, pri tem pa morajo biti pozorni na možnosti zlorabe podatkov in vdora v zasebnost.

Skeniranje šarenice naj bi se v večji meri uporabljalo za dostop do dragocenih podatkov (glej M. B. / STA 2. 4. 2005). Lahko bi imeli tudi popolni nadzor nad bivalnim

[8] Japonski kriptograf Tsutomu Matsumoto je iz želatine (kupljene v obliki gumi-medvedkov) naredil obliko prsta. Želene prstne odtise je pobral iz kozarca, nad odtise pa spustil pline iz tube sekundnega lepila, da je odtis postal bolj kontrasten. Odtis je fotografiral ter v Photoshopu povečal kontrastnost, nato pa odtis natisnil na prosojnico, vzel foto-občutljiv PCB, nanj položil prosojnico ter pustil, da se je v baker izrezljala oblika odtisa. To je pritisnil na želatino in tako ponaredil prstni odtis, s čimer se lahko pretenta kar 80 % vseh naprav za prepoznavanje prstnega odtisa (Slo-Tech.com 2002). Tudi Marie Sandström je v magistrski nalogi preverjala čitalce prstnih odtisov. S pomočjo umetnih prstnih odtisov iz želatine je preverila devet čitalcev na sejmu CEBIT v Nemčiji, kjer pa je bilo vse sisteme možno pretentati (glej Slo-Tech.com 2004).

okoljem s t. i. »inteligentnimi hišami«, ki se že pojavljajo tudi v Evropi. Takšna hiša poveže vse sisteme, kot so ogrevanje, razsvetljavo, alarmno napravo in ostalo. Vse funkcije so daljinsko vodene in jih je mogoče nadzirati preko interneta ali mobilnega telefona (glej T. S. 7. 10. 2003). Nekoliko hitreje, že leta 2007, pa želi britanska policija in notranje ministrstvo uvesti tudi elektronsko identifikacijo vozil (orig. electronic vehicle identification – EVI). Gre za senzorje ob cestah, ki bodo beležili vsako kršitev mimo vozečih vozil na tistem odseku ceste. Vozila bodo imela vgrajena mikrovezja, katera bodo dolžni izdelovalci avtomobilov vgraditi v vsa nova vozila, v stara vozila pa bodo to vgradili ob prvem tehničnem pregledu. S pomočjo senzorja se bodo tako ob vsakem prekršku samodejno izpisal plačilni nalog. Še bolj zaskrbljujoče pa je, da o takšnem elektronskem načinu identifikacije vozil razmišljajo tudi na sedežu EU v Bruslju (glej Triglav 2004, 65 – 66).

Eden takih primerov v praksi so tudi biometrični potni listi in nadzor na slovenskem letališču. Pogoj za takšno izdelavo so določile ZDA za vse tiste države, ki za njen obisk ne potrebujejo vizuma (glej Piano 25. 4. 2004). Med njimi je tudi Slovenija, katere državljani lahko do 90 dni po ZDA potujejo brez vizuma. V novih potnih listih imamo dva biometrična identifikatorja: posnetek obraza in prstni odtis, shranjen v posebnem čipu (glej Miko 1. 6. 2004). Slovenija je prve potne liste začela tiskati 28. 8. 2006. Sprva bo v njem shranjen le posnetek obraza, prstni odtis bi naj dodali leta 2009. Prav tako bo imel vsak potni list tudi navodila za uporabo, saj bo potni list zaradi priloženega čipa bolj ranljiv. Čeprav vlada trdi, da bodo podatki zelo dobro varovani, je Evropo prestrašil nemški raziskovalec, ki mu je uspelo kopirati in prenašati podatke v evropskih potnih listih, ki so se v Nemčiji začeli izdajati že leta 2005. Pri tem je uporabil standarde, ki so objavljeni na spletni strani Mednarodne organizacije za civilno letalstvo. Na Cetisu, ki naše dokumente tudi izdeluje, pravijo, da je v tem trenutku biometrični potni list 100 % varen, varnost pa bodo okrepili in nadgradili še ob dodanem prstnem odtisu. Dodali so tudi, da bodo imeli »pošteni ljudje z biometričnim potnim listom manj težav, kriminalci pa vsekakor več«. Tako naj bi biometrični sistemi za preverjanje potnih listov, legitimacij in vizumov državam pomagali v boju proti ponarejanju osebnih podatkov, nezakonitemu priseljevanju in terorizmu. Nasprotniki pa opozarjajo, da so napake pri vsaki biometriji še vedno mogoče. Gre tudi za globok poseg v zasebnost, saj tukaj ne gre za običajno geslo, ampak podatke, ki so unikatni vzorec posameznika (glej Miko 1. 6. 2004). Bojan Lučovnik, vodja varnosti in zaščite pri Aerodormu Ljubljana, je za Nedelo (glej Sušnik 22. 2. 2004) povedal, da na letališču Jožeta Pučnika za zdaj še ni standardov za biometrijo, ki bi »postopek kontrole verjetno precej poenostavila in pospešila.« Strinja pa se, da bodo biometrične meritve v prihodnosti igrale pomembno vlogo, ker je s tem sistem skoraj

nemogoče prelisičiti. Tako EU že pripravlja tehnične standarde za biometrijo, na nekaterih letališčih pa že potekajo testne faze takšnega uvajanja. Drugače je nadzor celotnega letališča podprt z video nadzornim sistemom, ki je usmerjen na prehode, del kamer pa nadzira tudi širšo okolico. Lučovnik tudi dodaja, da njihov »namen vseeno nikoli ni bil iz letališča narediti trdnjavo.«

Na podlagi konkretnih primerov lahko vidimo, da se nadzorovalna tehnologija res zmeraj bolj integrira v vsakdanje življenje ljudi.

7 EU KOT REFERENČNI OBJEKT INFORMACIJSKE VARNOSTI – INFORMACIJSKA VARNOST V EVROPSKI UNIJI

Pomembnost sektorja IKT za evropsko gospodarstvo in za evropsko družbo v celoti je neizpodbitna. IKT predstavlja pomemben del inovacij in je zaslužen za skoraj 40 % rasti proizvodnje. Poleg tega je ta izjemno inovativen sektor zaslužen za več kot četrtino celotnih evropskih prizadevanj v zvezi z raziskavami in razvojem in igra ključno vlogo pri ustvarjanju gospodarske rasti in delovnih mest v celotnem gospodarstvu. Vedno več Evropejcev živi v resnično informatizirani družbi, kjer se je uporaba IKT naglo povečala kot bistvena funkcija človeškega družbenega in gospodarskega vzajemnega delovanja. Po podatkih Eurostata je leta 2004 89 % podjetij v EU aktivno uporabljalo internet in približno 50 % potrošnikov je pred kratkim uporabilo internet (Eurostat, *Internetne dejavnosti v Evropski uniji*, 40/2005).

Kršitev OIV ima lahko vpliv, ki presega gospodarske dimenzije. Obstaja splošna zaskrbljenost, da bodo varnostni problemi vodili k odvrnitvi uporabnikov in manjši uporabi IKT, saj so razpoložljivost, zanesljivost in varnost predpogoj za zagotavljanje temeljnih pravic „on line“(COM(2006) 251, 5).

Poleg tega zaradi večje povezljivosti med omrežji tudi druge ključne infrastrukture (kot so promet, energija itd.) postajajo vedno bolj odvisne od neoporečnosti njihovih zadevnih informacijskih sistemov (COM(2006) 251, 5).

Zaradi vsesplošne razširjenosti IKT in informacijskih sistemov predstavlja varnost omrežij in informacij izziv za vsakogar (COM(2006) 251, 6):

- **javna uprava** mora obravnavati varnost svojih sistemov, ne samo zaradi zaščite informacij javnega sektorja, ampak tudi zato, da bi služila kot zgled dobre prakse za druge udeležence;
- **podjetja** morajo obravnavati OIV bolj kot pridobitev in element konkurenčne prednosti in ne kot „negativni strošek“;

- **posamezni uporabniki** morajo razumeti, da so njihovi domači sistemi odločilni za celotno „verigo varnosti“.

Pomembno je, da programi ozaveščanja, namenjeni osvetlitvi primerov ogrožanja varnosti, ne spodkopavajo zaupanja potrošnikov in uporabnikov z osredotočanjem na samo negativne vidike varnosti. Zato bi morala biti OIV, kadar je to mogoče, **predstavljena kot prednost in priložnost** in ne kot obveznost in strošek. Treba jo je obravnavati kot pridobitev pri gradnji splošnega zaupanja in zaupanja potrošnikov, kot konkurenčno prednost za podjetja, ki delajo z informacijskimi sistemi, in kot vprašanje kvalitete storitve ponudnikov storitev v javnem in zasebnem sektorju (COM(2006) 251, 6).

7.1 Identifikacija groženj in kritičnih sektorjev v EU

Pobuda Evropske komisije iz 20. oktobra 2004 vsebuje definicijo kritičnih infrastruktur (CI), našteje identificirane kritične sektorje in poda kriterije za določanje CI. V pobudi je kritična infrastruktura definirana tako: »*Kritično infrastrukturo sestavljajo fizična in informacijska tehnologija, omrežja, storitve in ugodnosti, ki bi v primeru ogroženosti ali prekinitve delovanja imele vpliv na zdravstvo, varnost in ekonomsko dobrobit državljanov ali celo na učinkovito delovanje vlad držav članic.*« Kritična infrastruktura zajema tudi ekonomski sektor in ključne funkcije vlade (COM(2004)702, 3).

V naslednji publikaciji Evropske komisije, t. i. »Green Paper« o evropskemu programu za zaščito kritične infrastrukture (Green Paper o EPCIP 2005, 19), pa je CIIP definirana takole: »*Programi in aktivnosti lastnikov infrastrukture, operaterjev, izdelovalcev opreme, uporabnikov in regulativnih avtoritet, katerih namen je obdržati definirano minimalno stopnjo storitev v primeru napadov ali odpovedi sistema, ter minimalizirati obnovitev in škodo*.« Na CIIP je zato treba gledati kot transsektorski fenomen, ne pa da se ga preučuje samo po posameznem sektorju. CIIP mora biti koordinirana skupaj z CIP iz holistične perspektive.« (Green Paper on EPCIP 2005, 19) Green Paper o EPCIP identificira naslednje kritične sektorje in njihove izdelke ter storitve:

- *energetski sektor* (produkcija, obdelava in shranjevanje goriv in plina, rafinerija, plinovodi; generiranje elektrike; transport elektrike, plina in nafte; distribucija goriv, plina in elektrike);
- *IKT* (zaščita informacijskih sistemov in omrežij; internet; fiksne in mobilne telekomunikacije; radijska in satelitska komunikacija in navigacija; oddajanje televizijskih programov);

- *voda* (skrb za pitno vodo; kontrola kvalitete vode, uravnavanje količine vode);
- *hrana* (skrb za zdravo hrano);
- *zdravstvo* (medicinska in bolniška nega, zdravila, serumi, cepiva in farmacevtiki, bio-laboratoriji in bio-agenti);
- *finančni sistem* (plačilne storitve / plačilne strukture (zasebne); vladni finančni aparat);
- *javni red in varnost* (ohranjanje javnega redu in varnosti, sodišča in zapori);
- *javna administracija* (funkcije vlade, oborožene sile, storitve javne administracije, urgentne storitve, poštne storitve);
- *transport* (cestni promet, železniški promet, zračni promet, plovni promet, morski promet);
- *kemična in jedrska industrija* (izdelava in shranjevanje / procesiranje kemičnih in jedrskih snovi in njihovo prenašanje) in
- *vesolje in raziskave* (Green Paper on EPCIP 2005, 24).

Čeprav je večina sektorjev v privatni lasti in upravljanju, je Evropska komisija v Pobudi 574/2001, 10. 10. 2001 razglasila, da mora »država poskrbeti za implementacijo nekaterih varnostnih ukrepov«, saj se pojavljajo napadi, ki so namenjeni družbi kot celoti, ne samo udeleženim v določenem sektorju. Javni sektor ima pri OIV tudi pomembno vlogo (COM(2004)702, 4).

Določiti kateri deli infrastrukture so kritični je kompleksna naloga. Evropska komisija predlaga, da se pri identifikaciji morebitne kritične infrastrukture upoštevajo naslednji dejavniki (Dunn in dr. 2008, 467):

- *Področje delovanja*: izguba elementa kritične infrastrukture je povezano z obsegom geografskega območja (mednarodno, nacionalno, regionalno, lokalno), ki ga ta izguba ali nedostopnost dosega.
- *Moč ogrožanja*: stopnja vpliva ali izgube lahko kategorizirana kot »ni izgube«, »minimalna izguba«, «zmerna izguba«, »velika izguba«. Med kriteriji za ocenjevanje potencialne moči ogrožanja nesreče so: vpliv na javnost (število ogroženih državljanov, izguba življenja, bolezenskih znakov, resnih poškodb, evakuacija); ekonomski vpliv (učinek na BDP, količina ekonomske izgube ali degradacija produktov in storitev); vpliv na okolje (vpliv na javnost in okolje); soodvisnost (z ostalimi elementi kritične infrastrukture); politični vpliv.

- *Čas ogrožanja*: ta kriterij pove, kdaj bi izguba elementa lahko imela resne posledice (na primer takoj, v roku 24 do 48 ur, en teden).

Kakorkoli, v večini primerov je potrebno upoštevati tudi psihološke učinke (COM(2004)702, 3 – 5).

7.2 Iniciative in politike EU na področju informacijske varnosti

Na kibernetsko varnost so opozorili že pri poročilu o implementaciji Evropske varnostne strategije (v nadaljevanju EVS), ki jo je predlagal SG/HR Javier Solana decembra 2008 evropskemu Svetu. V seminarju so razmišljali o možnih implikacijah EU na kibernetsko varnostno agendo in podobne grožnje (IESUE/SEM(09)04, 1).

Javna diplomacija je osnovni in najbolj značilen element pristopa EU k varnosti in tako bi naj zavzela tudi osrednje mesto pri pristopu k kibernetski varnosti v okviru skupne zunanje in varnostne politike (v nadaljevanju SZVP) EU. EU se mora zavedati, da odzivanje na kibernetske grožnje ne sme biti omejeno samo na kolektivno akcijo 27-ih držav članic, ampak mora vključevati aktivno sodelovanje z ostalimi partnerji in relevantnimi mednarodnimi institucijami (IESUE/SEM(09)04, 3).

Sodelovanje in razvoj mednarodnih pravnih režimov je lahko eden izmed vidikov SZVP. Že znotraj EU niso vse članice podpisnice Evropske konvencije o kibernetskem kriminalu Sveta EU. Mednarodni pravni sestav vključuje tudi bilateralne pogodbe, vendar številčnost teh pogodb lahko vodi do nasprotovanj ali obojestranske nekompatibilnosti, kar je še eden razlog več za globalno pravno ogrodje. Ko bi tak sporazum bil zaključen, lahko stranke začnejo premestitev ukrepov v državno-pravno okolje, da postane pogodba praktično uporabna in aplikativna (IESUE/SEM(09)04, 3).

Osrednjega pomena pri razvoju evropske kibernetske varnostne politike bo razvoj kibernetske varnostne strategije, bodisi iz strani EU ali iz skupne operacijske vizije, ki bo združila agencije in postopke. Glede ustanovitve *organa za kibernetsko-varnostno koordiniranje* EU je bilo podanih več predlogov. En tak predlog je bil za ustanovitev evropskega *Sveta za kibernetsko varnost* ali pa *Kibernetsko varnostno agencijo*, po vzoru Evropske agencije za omrežno in informacijsko varnost (ENISA). Izražena je bila tudi zaskrbljenost za prekomerno rast specializiranih institucij, ki bi se ukvarjale z novimi grožnjami, kar pa tudi ni primerno. Po drugi strani obstaja resnično tveganje v luči hitro nastajajoče varnostne grožnje, da bo reakcija EU bila prepočasna, še posebej, če bodo poskusi oblikovani tako, da bodo naravnani proti široki in splošni politiki EU. Alternativa temu

predlogu je, da se razišče, kateri organi EU imajo odgovornosti, povezane z kibernetsko varnostjo in bi dali centralnemu organu splošno odgovornost. Še ena izmed bolj decentraliziranih možnosti je, da bi maksimizirali in združili prispevke kibernetski varnosti vsake institucije in agencije EU (IESUE/SEM (09)04, 3). Ta zadnji predlog je s konceptom anarhične organizacije varnosti v celicah najbolj skladen.

Medtem ko so bili udeleženci bili složni pri vprašanju o potrebi po skupnem evropskem pristopu, so nekateri opozorili na relevantnost držav članic pri razvijanju nacionalnih strategij kot dodatek k možnim evropskim direktivam (IESUE/SEM(09)04, 3). Tudi ta predlog je skladen na mikro-ravni, saj imajo celični organeli dodatno membrano, ki jih ščiti pred škodljivimi molekulami.

Naslednja možnost je subsidiarnost, pri čemer bi se EU najprej spoprijela z lastno kritično infrastrukturo in potem nudila pomoč, znanje in svetovanje državam članicam. Po drugi strani pa so mnogi udeleženci seminarja menili, da bi moral biti primarni odziv in odgovornost za spopad s kibernetskimi grožnjami vseeno pri državah članicah. Diskusija se je dotaknila tudi aktivne udeležbe privatnega sektorja znotraj držav članic. Mnogi so poudarili pomembnost sodelovanja javnega in zasebnega sektorja kot bistvenega elementa protiukrepov iz strani držav članic (IESUE/SEM (09)04, 3).

Na državnem nivoju varnosti so udeleženci seminarja poudarili pomembnost sodelovanja med državo članico in CERT. Pomembna je ne samo njihova vključitev v strukturno sodelovanje z vladami, temveč so CERT pomembne tudi iz stališča preučevanja takšnega sodelovanja na evropski ravni (IESUE/SEM (09)04, 4).

Udeleženci seminarja so bili mnenja, da se mora *sodelovanje z mednarodnimi organizacijami* kot so ZN, NATO, OSCE, Mednarodna telekomunikacijska unija (orig. ITU), Svet Evrope za regionalne skupine in pobude povečati. Predlagano je bilo tudi, da naj EU premisli o sodelovanju z ZDA, ki že ima pripravljenih več iniciativ za kibernetsko varnost. Sodelovanje EU z zvezo Nato, ki ima politiko kibernetske varnosti že od leta 2007, pa se bo nadaljevalo z znanimi omejitvami (IESUE/SEM (09)04, 4).

Do neke mere bi se v oblikovanje varnostne politike EU vključila tudi vloga vojaških struktur oz. *evropske obrambne agencije* (orig. EDA, European Defence Agency). To bistveno vprašanje se ne more prezreti, ker so številni kibernetski napadi bili izvedeni proti EU kot celoti. Mnenja so se delila glede na to ali bi bilo bolje imeti eno globalno zaščito ali pa več različnih pobud (nacionalne ali EU skupaj z ostalimi regionalnimi pobudami). Mnogi udeleženci seminarja so bili mnenja, da je kombinirani pristop najboljša izbira: narediti

najboljše kar je možno na državni in regionalni ravni, hkrati pa delovanje z drugimi državami, da bi po koraki prišli do globalnega konsenza (IESUE/SEM (09)04, 4).

Še ena dimenzija politik EU v domeni kibernetske varnosti je preprečevanje pretiranega varovanja osnovnih vrednot kot so svoboda dostopa do informacij in svoboda izražanja, saj *pretirano varovanje lahko pomeni kratenje teh osnovnih vrednot* (IESUE/SEM (09)04, 4). Obe omenjeni svobodi sicer lahko imata različni interpretaciji v različnih družbah, a pomembno je, da EU v boju proti kibernetskim grožnjam promovira te osnovne človeške vrednote, ne pa, da jih ogroža pod pretvezo »varovanja«. Vendar so demokratične vlade prostovoljno sprejele določene omejitve svobode, da bi lahko bolj ustrezno reagirale na grožnje in zagotavljale varnost svojih državljanov.

7.2.1 Green Paper o evropskem programu za CIP (EPCIP)

Ta pobuda za evropski program za CIP v boju proti terorizmu vsebuje predlog Komisije o dodatnih ukrepih za ojačitev obstoječih instrumentov, z ustanovitvijo *Evropskega programa za zaščito kritične infrastrukture* (EPCIP). Novembra 2005 je Komisija objavila Green Paper o EPCIP, ki opozarja na možnosti za izboljšanje preprečevanja, pripravljenosti in odzivanja pri varovanju kritične infrastrukture EU. Green Paper prinaša možnosti, kako naj Komisija reagira na prošnjo Sveta, da bi ustanovili EPCIP in opozorilno informacijsko mrežo za kritično infrastrukturo (CIWIN) ter konstituira drugo fazo posvetovalnega procesa, ki se je začel s Pobudo Komisije o CIP, ki je bila sprejeta oktobra 2004. Green Paper se dotika ključnih vprašanj (Dunn in dr. 2008, 470):

- cilj varovanja EPCIP,
- ključni principi,
- vrste ogrodij, ki jih potrebujemo,
- definicije in razumljiv seznam kritične infrastrukture EU (ECI),
- ECI v odnosu do državnih kritičnih infrastruktur (NCI),
- vloga lastnikov, operaterjev in uporabnikov kritične infrastrukture,
- vloga CIWIN in ocena ter nadzor kritične infrastrukture (soodvisnost).

Možnosti, ki jih predlaga Green Paper o EPCIP, je kombinacija ukrepov, ki bi naj bili dopolnilo k trenutnim ukrepom držav članic (Dunn in dr. 2008, 470).

7.2.2 Opozorilno informacijsko omrežje za kritično infrastrukturo (CIWIN)

Da bi olajšali izmenjavo informacij o skupnih grožnjah in ranljivostih v EU, je komisija uvedla CIWIN. To omrežje EU je namenjeno pomoči državam članicam, institucijam EU in lastnikom, operaterjem, da delijo informacije o grožnjah, ranljivostih in primernih ukrepih ter strategijah za zmanjšanje tveganja in zaščiti CI. Natančna definicija vozlov tega omrežja še ostaja odprto vprašanje in bo najverjetneje vključevalo avtoritete na različnih nivojih.

Evropska komisija je predlagala naslednje tri možnosti za razvoj CIWIN v Green Paperu (Dunn in dr. 2008, 47):

- CIWIN bi lahko oblikovala forum, ki bi bil namenjen izključno na izmenjavo idej o CIP in dobrih praks kot podpora lastnikom in operaterjem CI;
- CIWIN bi lahko bil hiter sistem opozarjanja (orig. Rapid Alert System – RAS), ki bi povezoval države članice;
- CIWIN bi lahko bil več nivojski komunikacijski alarmni sistem z dvema določenima funkcijama: sistem hitrega obveščanja, ki bi povezoval države članice s Komisijo in forum za izmenjavo idej in najboljših praks o CIP-u.

Ne glede na to, katero možnost se bo izbralo, CIWIN bo dopolnjeval obstoječa omrežja, ne bo pa jih podvajal.

7.2.3 Evropska agencija za omrežno in informacijsko varnost (ENISA)

ENISA je bila ustanovljena marca leta 2004. Ko se je junija 2003 EU odločila za ustanovitev ENISE kot legalne entitete, je izboljšala pobude za evropsko koordinacijo informacijske varnosti (Dunn in dr. 2008, 472).

Cilj ENISE je zagotavljanje visoke stopnje omrežne in informacijske varnosti znotraj skupnosti. Tako pripomore k razvoju omrežne in informacijske varnosti v dobro državljanov, potrošnikov, podjetij in organizacij javnega sektorja EU. Njena dejavnost pa prispeva tudi k nemotenemu delovanju notranjega trga (ibid.).

Agencija pomaga Komisiji, državam članicam in posledično poslovni skupnosti, da vzdržujejo omrežno in informacijsko varnost, vključno s sedanjo in prihodnjo zakonodajo na tem področju. ENISA torej služi kot center ekspertnega znanja tako za države članice, kot za institucije EU, ko iščejo nasvete, povezane z OIV (ibid.).

ENISINI delovni programi so razvili »Seznam pomembnih oseb« z njihovimi kontaktnimi informacijami za področje OIV v državah članicah. Prav tako je izdala

»Inventory of CERT Activities in Europe« in periodično izdaja novice iz tega področja. ENISA organizira delavnice za razširitev dobrih praks v državah članicah. ENISA med drugim tudi definira prilagodljive informacijske pakete, ki vključujejo dobre prakse za specifične dotične skupine (na primer za SME in domače uporabnike). ENISA je ustvarila omrežno povezavo sodelavcev, ki izmenjujejo informacije in sodelujejo vsak dan z državami članicami (Dunn in dr. 2008, 472).

ENISIN zadnji delovni program iz leta 2008 nosi naslov »Build on Synergies – Achieve Impact,« izdan novembra 2007. Osredotoča se na povečanje vpliva agencije pri OIV v sodelovanju z relevantnimi udeleženci. Delovni program je bil razvit kot nov pristop k določanju prioritet in bolj poglobljenem sodelovanju z vsemi udeleženci. Predstavi pa tudi tri nove ključne elemente pri definiciji t. i. »večletnih tematskih programov« (MTP – orig. Multi-annual Thematic Programmes). Trenutni MTP pokriva naslednje teme (Dunn in dr. 2008, 473):

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

MTP ponuja tudi pregled ENISINIH aktivnosti, vključujoč ozaveščanje in promocijo dobrih praks in nadgradnja sodelovanja. ENISA se zaveda pomembnosti svoje vloge in podpira strategijo Evropske komisije. Z željo po maksimiranju vpliva svojih aktivnosti, agencija stremi po vzpodbudi obstoječih sinergij in pobud na državnem in evropskem nivoju ter bo tudi naprej sledila bolj osredotočenemu vplivno-orientiranemu pristopu (Dunn in dr. 2008, 473).

7.3 Pravo in zakonodaja EU

Z zakonodajo o CIIP je EU ponovno poudarila pomembnost osnovnih principov, ki jih evropsko pravo že vsebuje, t. j. zaupnost komunikacije in zakonite pogoje za prekinitev te zaupnosti, pridržanje prometa podatkov, legalnost vsebin in intelektualne lastnine (Schmitt v Dunn 2008, 476). V nadaljevanju sem na kratko opisala pomembne pravne dokumente EU, ki pokrivajo področje informacijske varnosti.

7.3.1 Direktiva o varovanju podatkov 1995 (95/46/EC)

Direktiva o varovanju podatkov (95/46/EC) prinaša regulativni okvir, za zagotavljanje varnega in svobodnega pretoka osebnih informacij preko mej držav članic in tudi uveljavlja

osnovno linijo varnostnih kontrol, ki varujejo te informacije. Direktiva o varovanju podatkov zahteva, da katerakoli tretja država, v katero se podatki pošiljajo uredi ustrezno zaščito teh podatkov (*ExportGOV*).

7.3.2 Direktiva o elektronskih podpisih 1999 (1999/93/CE)

Direktiva o elektronskih podpisih (I999/93/CE) je področje e-trgovine pravočasno uredila z implementacijo v zakonodaje držav članic. Ta direktiva poudarja pomembnost certifikatov, ponudnikov certifikatnih storitev in naprav za varno elektronsko podpisovanje ter prinaša nasvete za varno preverjanje podpisov. Direktiva upošteva potencial različnih tehnologij, ki se uporabljajo za izdajo podpisov, a ne uveljavlja natančnih tehničnih standardov in prav tako ne predlaga najboljše prakse. Je pa podlaga za mednarodno prepoznavnost certifikatov.

7.3.3 Direktiva o varovanju zasebnosti v sektorju elektronskih komunikacij 2002 (2002/58/CE)

Direktiva 95/46/EC je bila dopolnjena z Direktivo 97/6650 o varovanju osebnih podatkov na področju telekomunikacij in z Direktivo EU o zaščiti zasebnosti v sektorju elektronske komunikacije (2002/58/CE).

Direktiva razloži politike o spamanju, zbiranju in shranjevanju elektronskih podatkov ter zahteva od držav članic, da sprejmejo zakonodajo, ki omogoča zaupnost podatkov, omejuje kontrolo in shranjevanje prometa podatkov in podaja izjeme v primeru, ko gre za ogrožanje nacionalne varnosti. Direktiva tudi natančno določi, da je potrebno podatke, pridobljene s kontrolo prometa depersonalizirati ali izbrisati, kakor hitro niso več potrebni za pošiljanje in pripravo faktur, vseeno pa dopušča državi možnost, »da sprejme zakonodajne ukrepe, ki dovoljujejo shranjevanje podatkov v omejenem časovnem obdobju.« (2002/58/CE, čl. 15) Ti ukrepi morajo biti primerni in sorazmerni, v okviru demokratične družbe, z namenom obvarovanja nacionalne varnosti, obrambe, javne varnosti, preiskav, odkrivanja in kazensko-pravnega pregona kriminalnih napadov ali neavtorizirane uporabe sistemov elektronske komunikacije.« (ibid.)

7.3.4 Okvirna direktiva iz leta 2002 (2002/21/EC)

Cilj okvirne direktive (2002/21/EC) je ustanovitev uravnoteženega okvirja za regulacijo elektronskih komunikacijskih omrežij in storitev. Polaga osnovni temelj v obliki horizontalnih ukrepov, ki dopolnjujejo ostale ukrepe: obseg in splošni principi, osnovne

definicije, splošne ukrepe pri državnih regulativnih avtoritetah, koncept nove sile tržišču, in pravila za zagotovitev nepogrešljivih sredstev kot so na primer radijske frekvence (Dunn in dr. 2008, 480).

7.3.5 Okvirni sklep Sveta EU o napadih na informacijske sisteme 2005 (2005/222/JHA)

Okvirni sklep Sveta Evrope o napadih proti informacijskim sistemom (2005/222/JHA) februarja 2005 predvideva boljše sodelovanje na področju kriminalitete in prava o napadih na informacijske sisteme ter razvoj učinkovitih orodij in postopkov. Kriminalni prestopki, ki so kaznivi v okviru tega sklepa so: nelegalen dostop do informacijskih sistemov, nelegalno motenje sistemov (namensko oviranje ali prekinjanje funkcioniranja informacijskega sistema z dodajanjem, prenašanjem, poškodbo, brisanjem, odstavljanjem, spreminjanjem, tajenjem ali prikazovanjem nedostopnih računalniških podatkov) in nelegalno motenje samih podatkov. Države članice so morale sprejeti ukrepe za take napade, da so ti napadi ustrezno kaznovani z učinkovitimi, sorazmernimi in posvetovalnimi kriminalnimi kaznimi. Da bi povečali sodelovanje, morajo države članice ustanoviti operacionalne točke kontakta, ki so dostopne 24 ur na dan in sedem dni na teden (Dunn in dr. 2008, 481).

7.3.6 Pobuda i2010

Sporočilo „i2010 – Evropska informacijska družba za rast in zaposlovanje“ (COM(2005) 229 konč., 1. 6. 2005) je poudarilo pomembnost omrežne in informacijske varnosti pri vzpostavitvi enotnega evropskega informacijskega prostora. Razpoložljivost, zanesljivost in varnost omrežij in informacijskih sistemov postaja vse bolj pomembno za naše gospodarstvo in družbeni sistem (COM(2006) 251, 3).

Na podlagi izkušenj držav članic in izkušenj, pridobljenih na ravni Evropske skupnosti, je cilj nadalje razvijati dinamično, globalno strategijo v Evropi, osnovano na *kulturi varnosti* ter utemeljeno na **dialogu, partnerstvu ter povečanju vpliva in moči** (COM(2006) 251, 3).

Pri reševanju varnostnih izzivov informacijske družbe je Evropska skupnost razvila tridelni pristop, ki obsega: **posebne ukrepe** za varnost omrežij in informacij, **regulativni okvir za elektronske komunikacije**, ki zajema vprašanja zasebnosti in zaščite podatkov in **boj proti kibernetskemu kriminalu** (COM(2006) 251, 3).

EU je dejavna tudi v mednarodnih forumih, ki obravnavajo ta področja, kot so OECD, Svet Evrope ali ZN. Na svetovnem vrhu o informacijski družbi v Tunisu je EU močno

podprla razprave o razpoložljivosti, zanesljivosti ter varnosti omrežij in informacij. **Tuniska strategija** (COM(2006) 181), ki skupaj s tuniško obvezo določa nadaljnje ukrepe za politično razpravo o globalni informacijski družbi, kot so potrdili svetovni voditelji, poudarja potrebo nadaljnjega boja proti kibernetskemu kriminalu in nezaželeni elektronski pošti ob hkratnem zagotavljanju varovanja zasebnosti in svobode izražanja. Opredeljuje potrebo po skupnem razumevanju vprašanj internetne varnosti in po nadaljnjem sodelovanju, s čimer bi pospešili zbiranje in razširjanje informacij, povezanih z varnostjo, in izmenjavo dobre prakse med vsemi zainteresiranimi stranmi o ukrepih za boj proti ogrožanju varnosti (COM(2006) 251, 4).

V sporočilu je omenjena tudi preučitev izvedljivosti **vzpostavitve evropskega večjezičnega sistema za delitev informacij in opozarjanje**, ki bi gradil na podlagi obstoječih ali načrtovanih nacionalnih in zasebnih pobud in jih povezoval med seboj, bi zato lahko bila eden od glavnih ciljev ENISE (COM(2006) 251, 7).

Ob primerni strukturiranosti bodo rezultati primerjalne analize **opredelili najboljše prakse za izboljšanje ozaveščenosti malih in srednje velikih podjetij ter državljanov glede potrebe**, da obravnavajo svoje specifične izzive in zahteve glede OIV in s tem povezane zmožnosti. ENISA bi morala imeti aktivno vlogo v tem dialogu ter pri združevanju in izmenjavi najboljših praks (COM(2006) 251, 8).

*Komisija namerava ENISO zaprositi, da vzpostavi **zaupno partnerstvo z državami članicami in zainteresiranimi stranmi** za razvoj **ustreznega okvira zbiranja podatkov**, vključno s postopki in mehanizmi zbiranja in analiziranja podatkov o varnostnih incidentih in zaupanju potrošnikov iz celotne EU* (COM(2006) 251, 8).

Vzporedno bo Komisija, zaradi zelo razdrobljenega trga EU in njegove precej specifične narave, povabila države članice, zasebni sektor in raziskovalno skupnost k **vzpostavitvi strateškega partnerstva** za zagotovitev razpoložljivosti podatkov o industriji IKT v zvezi z varnostjo in o nastajajočih tržnih trendih za izdelke in storitve v EU (COM(2006) 251, 8).

> *Za izboljšanje evropske sposobnosti odzivanja na ogrožanje varnosti omrežij bo Komisija zaprosila ENISO, da preuči **izvedljivost evropskega sistema za delitev informacij in opozarjanje,** s čimer bi omogočila učinkovito odzivanje na obstoječe in porajajoče se primere ogrožanja elektronskih omrežij. Zahteva takšnega sistema bo **večjezični portal EU** za zagotovitev ustreznih informacij o grožnjah, tveganjih in opozorilih* (COM(2006) 251, 9).

Povečanje vpliva in moči posameznih skupin interesnih skupin je predpogoj za spodbujanje ozaveščenosti glede potreb v zvezi z varnostjo in tveganj za spodbujanje OIV (COM(2006) 251, 9 – 10).

1. *V ta namen Komisija **države članice** poziva, da:*
   - *proaktivno sodelujejo* v predlagani primerjalni analizi nacionalnih politik OIV;
   - v tesnem sodelovanju z ENISO spodbujajo kampanj ozaveščanja o prednostih in ugodnostih sprejema učinkovitih varnostnih tehnologij, praks in ravnanja;
   - spodbujajo storitve e-uprave za sporočanje in pospeševanje dobrih varnostnih praks, ki bi jih potem lahko razširili na druge sektorje;
   - spodbujajo razvoj programov varnosti omrežij in informacij kot del učnega načrta *visokega izobraževanja*.
2. *Komisija prav tako poziva interesne skupine **zasebnega sektorja**, da oblikujejo pobude za:*
   - Razvoj in ustrezno opredelitev odgovornosti za proizvajalce programske opreme in ponudnike internetnih storitev v povezavi z zagotavljanjem ustrezne in preverljive stopnje varnosti. Pri tem je potrebna podpora za standardizirane procese, ki bi zadostili pravilom skupno določenih varnostnih standardov in najboljših praks.
   - Pospeševanje raznolikosti, odprtosti, interoperabilnosti, uporabnosti in konkurenčnosti, ki so ključna gonila varnosti, ter spodbujanje uporabe izdelkov, procesov in storitev, ki krepijo varnost, za preprečevanje in boj proti kraji identitete ter drugim vdorom v zasebnost.
   - Razširjanje dobrih varnostnih praks za operaterje omrežij, ponudnike storitev ter mala in srednje velika podjetja kot osnovne ravni za varnost in poslovno kontinuiteto.
   - Spodbujanje programov usposabljanja v poslovnem sektorju, zlasti za mala in srednje velika podjetja, da bi zaposleni pridobili znanje in sposobnosti, potrebne za učinkovito izvajanje varnostnih praks.
   - Delovanje v smeri dostopnih varnostnih shem potrjevanja za izdelke, procese in storitve, ki bodo obravnavale potrebe, značilne za EU (zlasti glede zasebnosti).
   - Vključitev zavarovalniškega sektorja pri razvoju ustreznih orodij in metod za obvladovanje tveganja za reševanje tveganj, povezanih z IKT, in spodbujanje kulture obvladovanja tveganja v organizacijah in podjetjih (zlasti v malih in srednje velikih podjetjih).

7.3.7 Direktiva o shranjevanju podatkov 2006 (2006/24/EC)

Marca 2006 sta evropski parlament in Svet odredila Direktivo o shranjevanju procesiranih podatkov v povezavi z ukrepi javnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežjih (2006/24/EC). Direktiva je oblikovana tako, da usklajuje zakonodajo držav članic o shranjevanju telefonskih pogovorov in e-poštnih podatkov za preiskovanje, odkrivanje in izvrševanje kriminala, kot je definiran po državnem pravu posamezne države članice. Direktiva se nanaša na prometne in lokacijske podatke o pravnih ali fizičnih osebah, na povezane podatke, ki so potrebni za identifikacijo naročnika ali registriranega uporabnika. Ne nanaša se na vsebino elektronskih komunikacijskih omrežij. Države članice morajo zagotoviti, da ponudniki komunikacije obdržijo komunikacijske podatke za obdobja najmanj do pol leta in ne več kot dve leti od datuma komunikacije. Merila, ki so jih sprejeli v Angliji po terorističnem napadu na London v juliju 2005, so zahtevali od podjetij, da shranjujejo širok spekter podatkov: tudi prihodne in odhodne klice; trajanje telefonskih pogovorov; podatke, s katerimi lahko izsledimo fiksne in mobilne telefonske klice; informacije v tekstovnih sporočilih; IP naslove, ki identificirajo koordinate računalnika na internetu; čas prijave in odjave na računalniško omrežje; podatke o e-poštnem prometu – a ne dejanske vsebine komunikacij. Podrobnosti o klicih, ki so bili neodgovorjeni, ki se lahko tudi uporabljajo kot neke vrste sporočanje signalov sokrivcem ali za detonacijo bomb, so bili prav tako arhivirani, kjer so ti podatki obstajali. Neodvisne avtoritete bodo določene, da nadzorujejo uporabo podatkov, ki bodo morali biti izbrisani na koncu prej omenjenega obdobja dveh let, razen če se bodo ohranili zaradi protiterorističnih raziskovalnih namenov (Dunn in dr. 2008, 482).

Evropska komisija mora do 15. septembra 2010 predstaviti oceno aplikacije te direktive in njen vpliv na ekonomske operaterje in potrošnike, z upoštevanjem nadaljnjega razvoja elektronske in komunikacijske tehnologije in podanih statistik. Komisija pa mora ugotoviti, ali je potrebno posodobiti ukrepe te direktive, posebej na področju vrst podatkov in časovnega obdobja za njihovo shranjevanje (Dunn in dr. 2008, 482).

7.3.8 Lizbonska pogodba 2007

Lizbonska pogodba, podpisana pri vseh 27-ih državah članicah decembra 2007 v Lizboni je stopila v veljavo januarja 2009, da bi reformirala konstitutivni okvir EU, vključuje pa ukrepe za zaščito zasebnih podatkov. Pogodba zagotavlja »pravico do zaščite osebnih podatkov« (čl. 16 b Lizbonske pogodbe). Pravi tudi, da morata evropski parlament in Svet

postaviti pravila glede zaščite posameznikov z upoštevanjem zbiranja podatkov iz strani institucij EU, organov, služb, agencij in držav članic, ko izvajajo aktivnosti, ki padejo znotraj obsega prava EU, in ta pravila bi naj omogočala prost pretok takih podatkov. Spoštovanje teh pravil bo nadzorovala neodvisna avtoriteta. Členu 16 b te pogodbe o delovanju EU pravi, da kadarkoli bi lahko imela ta pravila neposredne implikacije na nacionalno varnost, se bodo ukrepi prilagodili vsakemu posebnemu elementu specifične situacije. Deklaracija o zaščiti osebnih podatkov na področju pravnega sodelovanja v kriminalnih zadevah in sodelovanje s policijo je potrebno zaradi posebne narave teh področij (Dunn, 2008, 483).

7.4 Raziskave in razvoj na področju informacijske varnosti v EU

Raziskave in razvoj, zlasti na ravni EU, bodo tudi prispevale k razvoju novega in inovativnega partnerstva za pospeševanje rasti evropske industrije IKT na splošno in zlasti evropske industrije IKT v zvezi z varnostjo. Komisija bo zato skušala zagotoviti, da se ustrezna finančna sredstva dodelijo za raziskave o OIV in zanesljivosti tehnologij v skladu s 7. okvirnim programom EU (COM(2006) 251, 7), ki bo podrobneje opisan v naslednjih odsekih.

7.4.1 Tehnologije informacijske družbe (IST) FP6 in FP7

Splošni cilj IST-a v okviru šestega okvirnega programa (FP6 – orig. Framework Program) je bil neposredni prispevek k realizaciji evropskih politik za informacijsko družbo, ki so ga določili: lizbonski evropski svet leta 2000, stockholmski evropski svet leta 2001 ter sevillski evropski svet v letu 2002, ko so pregledovali akcijski plan E-Evrope (Dunn in dr. 2008, 473).

IST- komponenta FP6, ki je bila v veljavi od 2002 do 2006, je zagotovila vodilno mesto Evrope na področju razvoja generičnih in aplikativnih tehnologij kot osnovo ekonomije znanja. Raziskave IST-a znotraj FP6 so ojačile in dopolnile cilje e-Evrope 2005. V okviru tega raziskovalnega programa EU je IST imela prioriteto pri investicijah (Informacijska družba). Strateški cilji IST FP6 so bili: globalni okvir odgovornosti za varnost, semantični sistemi znanja, omrežena gospodarstva in vlade, e-Varnost pri cestnem in letalskem prometu, e-Zdravje, kognitivni sistemi, dopolnilni sistemi, izboljšano upravljanje tveganja in e-vključitev. Fokus prejšnjega programa FP5 je bil predvsem na tehničnih vprašanjih, medtem

ko so politični vidiki (organizacijski vidiki, etična vprašanja itd.) v povezavi s CIIP bili zapostavljeni in podcenjevani v razpravi o strateških ciljih (Dunn in dr. 2008, 474).

V sklopu FP7, ki se je začel leta 2007 in bo deloval do 2013, pa želi Komisija identificirati interesna tematska območja, ki se nadaljujejo po koncu FP6, dodala pa je tudi nove teme, ki se pojavljajo, vključujoč vesolje in varnost (Informacijska družba, raziskave). EU investira v raziskave IKT že od leta 1986, FP7 pa predvideva največji delež investicij do zdaj (Informacijska družba, raziskave). To pa je zaradi zavezanosti Evrope, da obvladuje tako razvoj kot uporabo IKT, da bi lahko nadalje razvijala ekonomsko rast, ki je potrebna za podporo socialnega modela in zaščito okolja in kvalitete življenja. (ibid) Natančneje, cilj raziskav na področju IKT v sklopu evropskega FP7 je izboljšanje evropske konkurenčnosti na vseh nivojih z osredotočanjem na tri ključne vidike IKT (Cordis):

- *produktivnost in inovacije*, olajšanje kreativnosti in managementa,
- *modernizacija javnih storitev* kot je zdravje, izobraževanje in transport,
- *napredki v znanosti in tehnologiji*, s podpiranjem sodelovanja in dostopa do informacij.

CORDIS je uradni portal za sodelovanje v FP7 in z njim povezanimi razvojnimi smernicami evropske znanosti in tehnologije (glej Cordis).

Arhitektura storitev in programske opreme, infrastruktura in tehnika

V sklopu RP7 bo evropska komisija priskrbela obsežna sredstva za raziskavo arhitekture storitev in programske opreme, infrastrukture in tehnike. Ta cilj sovpada z raziskovalnimi dejavnostmi na področju storitev, programske opreme, mreže in virtualizacijskih tehnologij (Cordis. FP7). Izziv pri oblikovanju prodornega in zaupanja vrednega omrežja in infrastrukture storitev je neločljiva komunikacijska in storitvena infrastruktura, ki bo slej kot prej nadomestila internet, mobilna, stacionarna in audio-vizualna omrežja. Cilj tega raziskovalnega projekta je integracija in nadgradnja doseganjih dosežkov iz IST programa FP6. Integrirani raziskovalni pristop vodi k svetovnemu sodelovanju evropske industrije, malih in srednje velikih podjetij, univerz, raziskovalnih institutov, od naštetih pa mora vsak dodati svoje specifično znanje, ki bo prineslo uspeh na tem področju (Dunn in dr. 2008, 478).

7.4.2 Evropski varnostni raziskovalni program (ESRP – European Security Research Programme)

Cilj evropskega raziskovanja varnosti je, da se vzpostavi bolj varno okolje za državljane in poveča industrijska konkurenčnost. S sodelovanjem in uravnavanjem učinkov na evropski ravni, lahko EU v konstantno spreminjajočem se svetu bolje razume grožnje ter se na njih hitreje odziva (Evropska komisija). Za projekte na področju raziskovanja varnosti so identificirali naslednje prioritetne misije:

- *optimizacija* varnosti in zaščite omrežnih sistemov,
- *zaščita kritične infrastrukture* proti terorizmu (tudi bio-terorizmu in dogodkom, povezanih z biološkimi, kemičnimi in drugimi snovmi),
- *izboljšanje kriznega managementa* (evakuacija, iskalne in reševalne operacije, kontrola in odprava škode),
- *doseganje interoperabilnosti in integracije informacijskih in komunikacijskih sistemov*,

  iIzboljšanje znanja o dani situaciji (na primer, v kriznem managementu, anti-terorističnih aktivnostih, mejni kontroli) (Cordis).

Komisija EU je ustanovila tudi **svetovalni odbor za evropsko varnostno raziskovanje (ESRAB)** julija 2005. ESRAB deluje v sklopu Komisije in je posvetovalni organ za vprašanja, povezana z vsebino in implementacijo evropskega varnostnega raziskovalnega programa. ESRAB izvaja svoje delo s polnim zavedanjem konteksta evropske politike, posebej v raziskovanju in razvoju aktivnosti na državnem nivoju in podpori evropskih pobud raziskovalni politiki (Uradni zapisnik EU, 2005/516/EC). ESRAB je izdal končno poročilo septembra 2006 in nehal delovati decembra 2006. V tem poročilu priporoča ustanovitev **evropskega foruma za raziskovanje varnosti in inovacij** (**ESRIF** – European Security Research and Innovation Forum), ki bi omogočal dialog in skupen pogled na evropske varnostne potrebe. Ustanovitev tega foruma so razglasili na drugi evropski konferenci o raziskovanju varnosti marca 2007, forum pa je postal javni in zasebni dialog v raziskovanju varnosti že v septembru istega leta.

Glavni cilj ESRIF je razvoj združene srednje- in dolgoročne varnosti in z njo povezanih tem, ki bi povezale ugotovitve raziskovanja varnosti z varnostno politiko in njeno implementacijo. Na podlagi raziskovanja in zavedanja, da ima tako javno kot privatno partnerstvo pomembno vlogo pri zaščiti kritične infrastrukture, so cilji ESRIF-a naslednji:

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

Najbolj pa se ESRIF posveča zaščiti kritičnih informacij. ESRIF naj bi konec leta 2009 predstavil Skupno raziskovalno agendo, s tem pa zaključil svoje delovanje (Dunn in dr. 2008, 476).

7.4.3 Koordinacija raziskovanja kritične informacijske infrastrukture (CIIRCO)

EU je sestavila opravilno silo[9], da bi raziskala ukrepe, ki so bili sprejeti pri 25-ih državah članicah, in da bi se borila proti (kibernetskim) grožnjam kritični infrastrukturi. Kot del projekta CIIRCO (Critical Information Infrastructure Research Coordination), razglašenega aprila leta 2005, namerava opravilna sila sestaviti raziskovalne skupine in programe, ki se osredotočajo na informacijsko tehnološko varnost v kritičnih infrastrukturah kot so telekomunikacijska omrežja in električno omrežje. Obseg sodelovanja je širši kot EU; opravilna skupina želi vključiti tudi ZDA, Kanado, Avstralijo in Rusijo. Projekt CIIRCO je bil koordinacijska akcija in je bil soustanovljen z IST FP6. Glavni cilji CIIRCO projekta so (Infosek news):

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

[9] Evropska opravilna sila vključuje Fraunhofer Institut za varno informacijsko tehnologijo (FhG-SIT); Nemški center za zračni prostor (DLR); podjetje Industrieanlagen-Betriebsgesellschaft (IABG); italijanska nacionalna agencija za nove tehnologije, energijo in okolje (ENEA); nizozemska organizacija za aplikativne raziskave (TNO); francoska nacionalna višja šola telekomunikacij; in svetovanje firm Ernst Basler + Partner.

Raziskava komisije o dostopnosti in vzdržljivosti infrastrukture elektronskih komunikacij (ARECI)

To raziskavo je za Komisijo opravilo Lucent Technologies. Rezultat te raziskave je 10 nasvetov za ukrepe Komisije, držav članic in privatnega sektorja, s katerimi bi izboljšali zanesljivost, odpornost in vzdržljivost osnovnih infrastruktur. Ta priporočila vključujejo naslednja področja: pripravljenost na urgentno delovanje, prednost komunikacije na javnih omrežjih, formalni sporazumi pomoči, deljenje informacij o kritični infrastrukturi, soodvisnost med infrastrukturami, integriteta in zaupne operacije oskrbovalne verige, evropski standardi, testiranje interoperabilnosti, močno lastništvo in partnerstvo in neomejena izmenjava najboljše prakse. To poročilo je bilo predloženo januarja 2007 (Dunn in dr. 2008, 467).

7.4.4 Raziskava o varnostni ekonomiki in notranjem trgu EU

Evropa se vedno bolj seli na internet in tako postaja tudi informacijska varnost vedno bolj pomembna:

1. Ker so direktne in indirektne izgube informacij ekonomsko pomembne in
2. zaradi naraščajočega števila uporabnikov, ki jih skrbi informacijska varnost in tako zavirajo razvoj trgov in javnih storitev (Anderson in dr. 2008, 89).

Informacijska varnost se sicer dotika mnogih tem, od matematike do prava in psihologije, vendar po mnenju avtorjev raziskave najbolj uporabna orodja tako za političnega analitika kot za tehničnega informatika izhajajo prav iz ekonomije. Sistemi pogosto odpovejo zaradi tehničnih razlogov, ampak to je za to, ker ni pravočasnih preventivnih ukrepov (pomanjkanje pravočasnih pobud za primerne ukrepe večinoma sovpada s tehničnimi okvarami). Tako je varnostna ekonomija postala živa tema v raziskovanju zadnjih sedmih let (Andersen in dr. 2008, 89).

V tem poročilu so se avtorji odločili za analizo na osnovi varnostne ekonomije zaradi praktičnih problemov v omrežni in informacijski varnosti, s katerimi se ukvarja EU. V poročilu so neodvisni avtorji pripravili 15 predlogov za politike, ki bi naj bile dober korak k reševanju teh varnostnih problemov in upajo, da bodo osnova za konstruktivno akcijo ENISE in Evropske komisije v prihodnosti.

Preden predstavim priporočila, ki so jih pripravili avtorji omenjene raziskave, bom primerjala priporočila iz preučevanja varnostnega mehanizma celice z aplikacijo na makrosocialno raven. Ta priporočila bom primerjala z ugotovitvami, ki delujejo na ravni

celice. Hipotetično bom torej primerjala celico oz. sistem celic z državo oz. sistemom držav (Evropsko unijo), tako da moramo ves čas imeti v mislih to hipotetično analogijo.

Predstavljamo si torej države (ali NVO) kot celice, ki komunicirajo druga z drugo preko Evropske mreže. Receptorji v celicah omogočajo zaznavanje groženj že v izvencelični mreži, kar v naši analogiji pomeni omrežja zunaj EU ali pa zunaj ene države. Se pravi, da bi naj EU razvila sistem, ki bo zaznal grožnjo že ko bo vidna v sosednjih omrežjih. Ko receptor zazna grožnjo, jo pošlje v jedro, ki potem pošlje povratno informacijo, kaj se naj z grožnjo naredi. To bi naj bila funkcija tega zakona, ki bi kot receptor v celici služil preventivnim ukrepom proti grožnjam.

Če primerjamo pet glavnih priporočil, ki jih učijo celice, ugotovimo, da obstajajo nekatere podobnosti med predstavljenimi pobudami EU in priporočili avtorjev v raziskavi, pa tudi nekatere podobnosti (in tudi pomembne razlike), ki so konsistentne z varnostnim mehanizmom v celicah:

- *Brezhibna integracija komunikacije in varnostne funkcionalnosti.* Varnostna funkcionalnost je zelo integrirana v celične mehanizme in tako bi naj bilo tudi pri EU. To pomeni, da varnost ni ločena od komunikacijskega mehanizma, ampak je integralni del sistema samega. Za informacijsko varnost se torej naj skrbi na vsakem omrežju, kjer poteka komunikacija posebej, od domače uporabe, do uporabe v organizacijah. V celici sicer ne najdemo posebnega organela, ki bi bil specializiran posebej za varnost. Gre torej za varnost, do katere imajo različni mehanizmi in organeli v celici direktno vgrajeno deljeno odgovornost. Pri EU sicer imamo ENISO, ki je deluje kot centralni upravljavec varnostno-informacijskega mehanizma in je kot specializirani organel. Vseeno pa je dejstvo, da si tudi vsaka država članica deli odgovornost za varno uporabo IKT. Primerno pa bi bilo, da bi imele le prav vse institucije in države imeti v mislih informacijsko varnost celotne EU ter implementirati ukrepe, da se ne kompromitira določen del, ki potem lahko vodi do ogrožanja celotnega omrežja v EU.
- *Proaktivni pristop do membranske obrambe in prehajanja delcev*. Celice imajo proaktiven pristop do prehajanja delcev skozi zunanjo celično membrano. Če bi denimo EU imela na svojih omrežjih še dodatno zaščitno plast pred grožnjami od zunaj, bi evropska omrežja bila bolj varna pred izvenevropskimi grožnjami, poleg tega pa bi se povečala tudi varnost za izvenevropska omrežja, saj v primeru, da ima grožnja izvor v EU, bi tudi težje prešla na zunanja omrežja. S tem se bi tudi izognili hitremu širjenju neželenih groženj. Tako kot imamo na domačem omrežju požarni zid, tako bi morala tudi vsa podjetja, organizacije, pa tudi države članice in EU v celoti ustvariti

dodatno zaščitno plast bodisi s požarnimi zidovi dodatno plast zaščite in kontrole internetnega prometa. V pobudi i2010 je prav tako omenjeno proaktivno oblikovanje politik za OIV.

- *Visoka stopnja specializacije komunikacijskih metod.* Celice imajo široko izbiro visokospecializiranih mehanizmov za prenašanje molekul preko zunanje celične membrane. Za vsako molekulo, ki jo celica potrebuje, obstaja poseben, po meri narejen mehanizem za komunikacijo in prehod te molekule skozi membrano. Tako tudi skrb za OIV v EU poteka na različnih ravneh: s sodelovanjem industrije IKT (razvoj novejših in boljših aplikacij za omrežno varnost), politični ukrepi, ustanovljeni raziskovalni forumi in portali za obveščanje, vsi ti dejavniki pa prispevajo svoj pomemben delež pri OIV.
- ***Standardizirana*** *uporaba notranjih membran, ki varujejo najbolj pomembne organele v celici.* V analogiji so to varnostni ISO standardi, ki varujejo »notranje organele« oz. pomembne oddelke EU, institucije, organizacije, države znotraj EU. Implementiral bi se torej naj skupni varnostni standard, ki bi dodatno varoval posamezne organizacije znotraj EU. Celice imajo liberalno uporabo notranjih membran in tako bi naj bilo tudi v EU, saj bi zaradi standardizacije bila tudi lažja in varnejša komunikacija znotraj EU, kar bi zagotovo vplivalo ugodno na vse vrste e-poslovanja, e-volitev itd. Pomembnejši celični organeli (mitohondrij, vakuole in jedro) imajo vsi svojo lastno membrano (ali celo več membran), ki jim poleg zunanje celične membrane nudijo dodatno zaščito. Bolj pomembno funkcijo izvaja organel, bolj robustna je njegova interna membrana. Tako bi najpomembnejše elemente kritične infrastrukture EU in njene najpomembnejše institucije še posebej varovali z dodatnimi varnostnimi ukrepi.
- *Na splošno lahko rečemo, da je varnost v celici integrirana, navzoča povsod in kontinuirana.* Tak nasvet gre tudi EU, saj drugače se ne morejo vzdrževati visoki varnostni standardi. Glede na to, koliko različnih inherentnih varnostnih mehanizmov ima celica, lahko rečemo, da je vzdržuje visoke varnostne standarde. Obrambni ukrepi so prisotni v zunanji membrani, znotraj celičnih organelov, med notranjim usmerjanjem molekul in na sploh skozi celotno celico in tako bi naj tudi bili prvi obrambni ukrepi najprej v vseh omrežjih EU v celoti, na nivoju NVO, držav, podjetij, in posameznikov, obramba mora biti organizirana tudi pri notranji komunikaciji. Varnostni mehanizmi v celici so tudi neprekinjeno, kontinuirano aktivni, kar mora biti tako pri mikro- kot makrosocioloških enotah. V celici je torej varnost del vsega,

varnost je prisotna povsod in varnostni mehanizmi vedno funkcionirajo, torej je tudi varnost vedno na visoki stopnji, kar pa si seveda želimo tudi za EU.

Priporočila Andersena, Böhma, Claytona in Moora (2008) za izboljšanje informacijske varnosti v EU:

1. *EU naj uvede razumljiv zakon za obveščanje o luknjah varnosti* (Andersen in dr. 2008, 26). Celice imajo receptorje, ki kemijsko obveščajo jedro celice o škodljivih molekulah, v EU pa bi to funkcijo naj izvajal forum za ovbeščanje o dobrih praksah OIV.
2. *Komisija (ali evropska centralna banka) naj regulira in zagotavlja publikacijo, ki bi vsebovala statistike izgube dobička na račun elektronskega kriminala* (Andersen in dr. 2008, 45).
3. *ENISA nas zbira in objavlja podatke o kvantiteti spama in ostalega slabega prometa, ki je zaznan na evropskih ponudnikih internetnih storitev (v nadaljevanju ISP)* (Andersen in dr. 2008, 46).
4. *EU naj uvede zakonito lestvico škode na ISP-jih, ki se ne odzivajo redno na prošnje za odstranitev ogroženih naprav, in ISP-je zaveže k spoštovanju uporabnikove pravice, da nepovezane naprave spet poveže* (Andersen in dr. 2008, 54).
5. *EU naj razvije in **uveljavi standarde** za opremo, ki je povezana v omrežja, da bo ta oprema varna* (Andersen in dr. 2008, 60). Tudi celice imajo visoko stopnjo standardiziranosti pri uporabi membran, ki imajo funkcijo obrambe, kot bi to naj imeli varnostni ukrepi za varovanje omrežij.
6. *EU naj sprejme kombinacijo hitrega odzivanja na odkrite grožnje in ranljivosti ter hkrati zaveže prodajalce programske opreme, da pospešijo popravljanje nepopravljene programske opreme in tako pospešijo tudi cikel razvoja posodobitev programske opreme* (Andersen in dr. 2008, 64). Tudi varnostni mehanizmi v celici so neprekinjeni, kontinuirano aktivni in instantno odzivni in se neprenehoma »posodabljajo«. Na nivoju EU opravlja to nalogo CIWIN.
7. *Varnostni popravki morajo biti neplačljivi in ločeni od drugih posodobitev programske opreme* (Andersen in dr. 2008, 65).
8. *EU naj uravna postopke za razrešitev sporov med strankami in ponudniki plačilnih storitev preko elektronskih transakcij* (Andersen in dr. 2008, 66). V celicah ni vprašanja, kaj je prav in kaj ne, natančno se ve, katere molekule so v celici dovoljene in katere ne, zato takih ukrepov sploh ne potrebuje.

9. *Evropska komisija naj pripravi predlog za direktivo o ustanovitvi **koherentnega režima** primernih in učinkovitih sankcij proti prodajnim prevaram na spletu,* (Andersen in dr. 2008, 68), kar prinaša okvirni sklep Sveta EU o napadih na informacijske sisteme iz leta 2005. V celici ne obstajajo etično sporni elementi, zato je na tem mestu analogija neprimerna.
10. *ENISA naj izvede raziskavo, ki bi bila koordinirana z Evropsko komisijo in ostalimi vpletenimi, z namenom, da se preučijo spremembe, ki so potrebne v Zakonu za zaščito potrošnikov, zaradi vedno večje selitve trgovine na splet* (Andersen in dr. 2008, 70). Celica namreč deluje samo za interese samoohranitve in nadaljevanje življenja, nima pa, kot sem že v prejšnjih točkah nakazala, etično spornih elementov.
11. *ENISA naj svetuje avtoritetam za konkurenco, ko ima raznolikost varnostne implikacije* (Andersen in dr. 2008, 73).
12. ENISA naj vlaga v raziskovanje učinkov odpovedovanja IXP (IXP – orig. Internet Exchange Point ali točka internetne izmenjave[10]). Prav tako priporočajo sodelovanje z regulatorji telekomunikacijskih storitev, da bi ugotovili optimalno prakso za večjo in varnejšo prehodnost prometa preko IXP (Andersen in dr. 2008, 77). Takšne točke, kjer se lahko nekako nadzira internetni promet so že bližje primeru podrobne celične varnosti.
13. *Evropska komisija naj apelira na tistih 15 držav članic, ki še niso ratificirale Konvencije o kibernetskem kriminalu.* Slovenija je konvencijo podpisala 24. 7. 2002, ratificirala 8. 9. 2004 , v veljavo pa je stopila komaj 1. 1. 2005 (Konvencija o kibernetskem kriminalu).
14. *Ustanovitev vseevropskega organa, ki bi skrbel za lažjo mednarodno sodelovanje v boju proti kibernetskem kriminalu, pri čemer bi naj Nato služil kot model za ustanovitev* (Andersen in dr. 2008, 81). Po tem, kar nas učijo celice, je to nepotrebno, glede na to, da je varnost vgrajena v vsak organel, torej bi lahko rekli, da bi naj vsaka država, NVO, podjetje ali organizacija poskrbela tudi sama za varnost. Vendar je vseeno potrebna standardizacija, ki pa jo lahko v primeru mednarodnega sistema izvede le direktiva iz EU.

[10] IXP ali točka internetne izmenjave je fizična infrastruktura, ki omogoča ponudnikom internetnih storitev, da izmenjajo internetni promet med njunimi omrežji (avtonomno omrežje) s pomočjo vzajemnih dogovorov, ki dovolijo, da se promet izmenja brez stroškov. IXP zmanjša delež prometa, ki ga mora internetni ponudnik dostaviti preko glavnih tranzitnih ponudnikov in tako zmanjša povprečno ceno storitve za bit prenesenih podatkov. Večje število poti potovanja podatkov pa tudi izboljša učinkovitost usmerjevanja in večjo toleranco do napak (Wikipedia 2009c).

15. *ENISA naj zagovarja interese sektorja za informacijsko varnost pred Komisijo, saj mora zagotoviti, da ne bodo nove predlagane regulacije namenjene drugim sektorjem pomotoma škodile raziskavam varnosti in podjetjem, ki se ukvarjajo z informacijsko varnostjo* (Andersen in dr. 2008, 88).

Kot sem ugotovila so celice v prednosti, ker nimajo parlamenta in politik, ki bi dovoljevala drugačna mnenja, delujejo enotno, kar pa seveda v družbenem okolju ni mogoče, če želimo živeti v svobodnem, demokratičnem svetu. Tako da v celoti aplikacija ni mogoča, lahko pa služi kot model za prihodnjo oblikovanje politik OIV EU.

8 ZAKLJUČEK

Operacionalizacija sodobnega obravnavanja varnosti je nedvomno ključen instrument za preučevanje tistih družbenih posledic uporabe IKT, ki se nanašajo na (informacijsko) varnost, torej zagotavljanje uravnoteženega duhovnega in duševnega ter gmotnega razvoja in obstoja tako posameznika kot družbenih nedržavnih in državnih varnostnih objektov. Tako sem tudi jaz svojo analizo informacijske varnosti začela s konstruktivistično teoretično paradigmo, nadaljevala pa sem s koncepti, ki so se nanašali na referenčne objekte informacijske varnosti ter mehanizme, ki jo zagotavljajo. V teoretičnem delu sem predvsem želela pokazati, kako IKT vpliva na dojemanje stvarnosti in občutka varnosti.

Vse preučevane referenčne objekte informacijske varnosti (IKT, uporabnik in EU) sem obravnavala s konstruktivizmom, saj lahko dovolj univerzalno pojasni nastanek globalne družbe, globalnih vrednot, kar še posebej nakazuje kulturalizem. Menim, da že enake osnovne značilnosti različnih verstev govorijo v prid konsenzu človeštva o tem, kar je etično in kar ne. Torej kultura kot delno pogojena z religijo torej ne bi smela biti ovira pri oblikovanju globalnih vrednot in norm. Navsezadnje so človekove pravice in prizadevanje za njihovo spoštovanje v mednarodnem okolju dokaz za ta skupen konsenz. Kultura pa je seveda svojevrsten način, kako si posamezne družbene skupine ali narodi razlagajo te osnovne človekove vrednote, med katere zagotovo spada varnost. Varnost pa je po mojem mnenju ravno najbolj ogrožena zaradi različnih človekovih interesov in nasprotujočih si identitet, oz. kulturno specifičnih razlag osnovnih vrednot človeštva, ne pa zaradi tehnologije. Torej sama menim, da se bo stanje izboljšalo, ko se bodo nepristransko varovale osrednje človekove vrednote in pravica do informiranosti. To pomeni, da države in mednarodne organizacije ne smejo povečevati nadzora pod pretvezo zagotavljanja varnosti, ampak morajo ščititi svobodo do informiranosti. Z izobraževanjem in premišljeno rabo IKT lahko vsi skupaj prispevamo k

večji informacijski varnosti. Interesi poštenih se tako ne bi križali, ampak bi bili usmerjeni v mirno, z okoljem in tehnologijo integrirano življenje. To pa bo verjetno tudi takrat, ko bodo velike korporacije in vladajoči politiki finančna sredstva začeli vlagati v kulturo in okolje – upamo, da pravočasno.

Med pisanjem diplomske naloge sem ugotovila, da ima celica kljub temu, da ima jedro, funkcije anarhično razdeljene med različne celične organele. Prav tako ima anarhično oblikovan varnostni mehanizem, ki je vgrajen v celične strukture. Ni torej enega organela, ki bi določal ostalim organelom funkcije, ampak te funkcije same sebe med seboj dopolnjujejo. Torej anarhičnost še ne pomeni kaosa, če so vse funkcije vsake enote jasno razložene. Celica ne prepušča *neznanih* molekul in molekul, ki so identificirane kot grožnje, prav tako se ljudje bojimo, česar ne poznamo (tuje kulture) in je naša percepcija varnosti zaradi tega nižje stopnje, zato je potrebno čim bolj postaviti v ospredje pojem izobraževanja in medkulturnega sprejemanja, za zmanjšanje polja nepoznanosti in povečanje lastnega občutka varnosti. Evropska unija je dokaz, da je različna kulturna okolja mogoče združiti za skupen cilj ter povečati vsaj percepcijo varnosti zaradi boljšega poznavanja družbenih / naravnih pojavov.

Mednarodni sistem je anarhičen, a vseeno se je v njem oblikovala struktura, ki ji lahko rečemo tudi EU sicer ima nehierarhično strukturo in deljene funkcije. Torej bi se dalo tudi tukaj potegniti nekatere vzporednice s celico, kar je bilo na začetku postavljeno raziskovalno vprašanje. Menim, da bi EU tudi morala svoje varnostne mehanizme prilagoditi novim družbenim in tehnološkim izzivom. Kot sem pokazala v diplomski nalogi, je možno celični varnostni mehanizem (ki je anarhičen), aplicirati tako na računalniška omrežja, kot na delovanje EU vsaj do neke mere, a s pomembno razliko, da celica nima moralnih ovir, človek pa. Potrebno je upoštevati kulturno / etično komponento vloge interesov in identitet, ki jih razlaga konstruktivizem. Celice imajo pa tudi na mikroravni molekul podlegajo zakonom kvantne fizike, ki pa tudi upošteva naključnost rezultatov reakcij med molekulami in zato le z določeno mero verjetnosti napoveduje izid reakcije. Na makrosocialni ravni pa so ravno interesi, kultura in etika tisti deli, ki odločajo izid interakcije. Iz teh analogij je tako možno črpati ideje za izboljšanje informacijske varnosti tudi na družbeni ravni.

9 Literatura

Alamgir, Jalal. 2008. *India's Open-Economy Policy: Globalism, Rivalry, Continuity.* London: Routledge.

Andersen, Peter Bøgh. 1990. *A theory of computer semiotics. Semiotic Approaches to Construction and Assessment of Computer Systems*. Cambridge: Cambridge University Press. Dostopno prek: http://euphrates.wpunj.edu/faculty/yildizm/sp/b_abstract/theory_of_ computer_semiotics.htm (2. marec 2006).

--- 1991. *Computer semiotics*. *Semiotics as a basis for a humanistic computer science.* Aahrus: Department of Information and Media Science, University of Aarhus. Dostopno prek: imv.au.dk/~pba/Homepagematerial/publicationfolder/ Computersemiotics.pdf (18. junij 2009).

Anderson, R., Rainer Böhme, Richard Clayton in Tyler Moore. 2008. *Seacurity Economics and the internal market*. Dostopno prek: www.enisa.europa.eu/doc/pdf/report_sec_econ_&_ int_mark_20080131.pdf (18. junij 2009).

Avižienis, Algirdas, Jean-Claude Laprie in Brian Randell. 2000. *Fundamental Concepts of Dependability.* Los Angeles: UCLA, Toulouse: LAAS – CNRS, Newcastle: University of Newcastle. Dostopno prek: http://www.cert.org/research/isw/isw2000/papers/56.pdf (18. maj 2008).

Brown, C. 2005. *Understanding International Relations*. Basingstoke: Palgrave Publishing.

Burton, John. 1965. *Internacional relations: A General Theory.* Cambridge: Cambridge University Press.

Cole, Eric in Sandra Ring. 2006. *The Insider Threat*. London: Syngress publishing.

Commission of the European Communities. 2005. *Green Paper on a European Programme for Critical Infrastructure Protection (COM(2005) 576).* Brussels. Dostopno prek: http://www.libertysecurity.org/IMG/pdf/EC_-_Green_Paper_on_CI_-_17.11.2005.pdf (7. julij 2009).

Cordis. Dostopno prek: http://cordis.europa.eu/ (22. maj 2009).

Deutsch, Karl. W. 1966. *The Nerves of Government: Models of political Communication and Control.* New York: Free Press.

Dunn, Miriam. 2004. *Information Age Securuty: A Qualitative Analysis of Critical Information Infrastructure Protection (CIIP)* PhD Thesis. Zurich: Center for Security Studies, ETH Zurich.

Dunn, Myriam. 2005. *A comparative analysis of cybersecurity initiatives worldwide*. Dostopno prek: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_ Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf (12. junij 2009).

Dunn Cavelty, Myriam, Victor Mauer in Andreas Wenger. 2008. *International CIIP Handbook 2008 / 2009. An inventory of 25 national and 7 international critical information infrastructure protection policies*. Zürich: Center for Security Studies, ETH.

Evropska komisija. Dostopno prek: http://ec.europa.eu/ (3. april 2009).

--- 2005. *Biometrics at the Frontiers: Assessing the Impact on Society (EUR 21585 EN).* Dostopno prek: http://ec.europa.eu/justice_home/doc_centre/freetravel/doc/ biometrics_eur21585_en.pdf (20. marec 2009).

ExportGOV. Dostopno prek: http://www.export.gov/safeharbor/ (4. junij 2009).

Figge, U. L. 1991. Computersemiotik. *Zeitschrift für Semiotik* 13(3/4): 321.

Generalni sekretariat Sveta Evrope in inštitut za varnostne študije. 2009. *Kibervarnost: vloga v skuponi zunanji in varnostni politiki (IESUE/SEM(09)04)*. Dostopno prek: http://www.iss.europa.eu/fileadmin/fichiers/pdf/seminars/2009/Report_cyber_security.pdf (3. julij 2009).

GOVCERT.NL. 2006. *Setting up a CSIRT*. Dostopno prek: http://www.first.org/resources/guides/cert-in-a-box/content/68.html, (9. julij 2009).

Grizold, Anton. 1999. *Evropska varnost.* Ljubljana: Fakulteta za družbene vede.

Infosek News. 2005. *EU task force to study IT critical infrastructure.* Dostopno prek: http://www.attrition.org/pipermail/isn/2005-April/001454.html (3. april 2009).

Jelušič, Ljubica. 1997. *Legitimnost sodobnega vojaštva*. Ljubljana: Fakulteta za družbene vede.

Kodelja, Marjan in Zoran Banovič. 2005. Biometrija v Evropi: »Evropski veliki brat«. *Moj Micro* (maj): 34.

Svet Evropske unije. 2001. *Konvencija o kibernetskem kriminalu* (ETS 185). Budimpešta. Dostopno prek: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM= &DF=&CL=EN*G* (17. junij 2009).

Kovačič, Matej. 2003. *Zasebnost na internetu*. Ljubljana: Mirovni inštitut.

--- 2006. *Nadzor in zasebnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.

Lavrenčič, Jernej. 2007. »Biometrija: Varuh ali sovražnik zasebnosti?« *Varnostni forum*, (2): 18–24.

Lyon, David. 2006. Surveillance, Power and Everyday Life. V *Oxford Handbook of Information and Communication*, ur. Robin Mansell, Chrisanthi Avgerou in Danny Quah. Dostopno prek: http://www.queensu.ca/sociology/Surveillance/files/oxford_handbook.pdf (11. april 2007).

M. B. / STA. 2005. Biometrija – kmalu še ena stalnica? *Delo*, 2. april. Dostopno prek: http://www.delo.si/index.php?sv_path=43,50&src=mm (25. marec 2007).

Mihai, Nadin. 2001. One cannot not interact. *Knowledge-based Systems* 14(8): 5. Dostopno prek:http://www.code.uniwuppertal.de/uk/computational_design/who/nadin/publications/articles_in_journals/One%20cannot%20NOT%20Interact.htm (29. junij 2009).

Miko, Klavdija. 2004. Zaradi računalniške napake se lahko znajdete tudi v zaporu. *Ona*, 1. junij. Dostopno prek: http://www.delo.si/index.php?sv_path=43,50&src=mm (10. april 2007).

Piano, Brane. 2004. Veliki brat bo še malo počakal. *Nedelo*, 25. april. Dostopno prek: http://www.delo.si/index.php?sv_path=43,50&src=mm (25. marec 2007).

Raskin, Jonathan D. 2002. »Constructivism in Psycology: Personal Construct Psycology, Radical Constructivism, and Social Constructionism«. *American Communication Journal* 5 (3):1–25.

Reich, Kersten, Lucia Sehnbruch in Rüdiger Wild. 2005. *Medien und Konstruktivismus*. Berlin: Waxmann.

Saussure, Ferdinand de. 1966. *Course in General Linguistics.* New York: McGraw-Hill.

Schneier, Bruce. 2000. *Secrets and Lies: Security in a networked world*. New York: John Wiley.

--- 2008. *The Psychology of Security*. Dostopno prek: http://www.schneier.com /paper-psychology-of-security.html (4. oktober 2008).

Slo-Tech.com. 2002. *Falus pa biometrija*, 20 maj. Dostopno prek: http://www.slotech.com/ script/forum/izpisitemo.php?threadID=136729#neprebrano (1. april 2007).

Slo-Tech.com. 2004. *Biometrija na letališču*, 30 junij. Dostopno prek: http://www.slo-tech.com/script/forum/izpisitemo.php?threadID=129790#neprebrano (1. april 2007).

Sporočilo evropske Komisije, Svetu, Evropskemu parlamentu, Evropskemu ekonomskemu in socialnemu odboru in odboru regij. Strategija za varno informacijsko družbo – „Dialog, partnerstvo ter povečanje vpliva in moči.“ (COM(2006) 251). Bruselj. Dostopno prek: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:SL:PDF (4. julij 2009).

Sušnik, Dragica. 2004. Varnostni ukrepi na letališčih se bodo v prihodnje le še zaostrovali. *Nedelo*. Dostopno prek http://www.delo.si/index.php?sv_path=43,50&src=mm (25. marec 2007).

Svete, Uroš. 2005. *Varnost v informacijski družbi.* Ljubljana: FDV.

Šilc, Edvard. 2007. Bistvo pravice do zasebnosti, v *Varnostni forum*, 1(januar): 29–30. Šempeter pri Gorici: Palsit d.o.o.

T.S. 2003. Inteligentna hiša, kot jo ima Bill Gates. *Delo*, 7. oktober. Dostopno prek: http://www.delo.si/index.php?sv_path=43,50&src=mm (25. marec 2007).

Tipton, Harold F. in Micki Krause, CISSP. 2008. *Information security management handbook*. Taylor & Francis Group, LLC. Auerbach publications.

Triglav, Joc. 2004. EVI – tehnologija za šoferje na vrvici. *Življenje in tehnika* (3): 65-66.

Vukadinović, Radovan. 1978. *Teorije o međunarodnim odnosima.* Beograd: Naklada Cdd.

Wendt, Aleksander. 1999. *Social Theory of International Politics.* Cabridge: Cambridge University Press.

--- 1992. *International Organization*. Cambridge: Cambridge University Press.

West-Brown, Moira J., Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle in Mark Zajicek. 2003. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Pittsburgh: Carnegie Mellon software engineering institute.

Wiener, Norbert. 1950. *Human Use of Human Being, Cybernetics and Society.* Boston: Da Capo Press.

Wikipedia. 2009a. *Vpliv konstruktivizma na računalniško znanost*. Dostopno prek: http://en.wikipedia.org/wiki/Constructivism_(learning_theory) (8. maj 2009).

--- 2009b. *Ergonomija.* Dostopno prek: http://sl.wikipedia.org/wiki/Ergonomija (28. junij 2009).

--- 2009c. *IXP*. Dostopno prek: http://en.wikipedia.org/wiki/IXP (17. junij 2009).

10 Prilogi

V prilogi želim pokazati konkretne rezultate in predvsem uporabljene indikatorje, ki so jih uporabili avtorji raziskave *Security Economics and the internal market*. Ti indikatorji so po mojem mnenju uporabni za prihodnje raziskovanje informacijske varnosti.

Priloga A: Indikatorji informacijske družbe (varnostni problemi posameznikov)

Tabela A.1: Indikatorji informacijske družbe: varnostni problemi posameznikov. V tabeli vidimo odstotke posameznikov, ki so uporabljali internet v zadnjem letu in so doživeli naslednje varnostne probleme:

	Goljufija pri plačilu s kartico (kreditno ali debetno)			Zloraba osebnih informacij, poslanih preko interneta			Računalniški virus, ki je povzročil izgubo informacij ali časa		
	2003	2004	2005	2003	2004	2005	2003	2004	2005
Anglija	1,7	2,4	3,3	3,2	3,3	3,1	26,6	29,8	37,4
Avstrija	0,9	1,0	1,4	2,2	2,1	1,6	15,2	29,8	26,8
Bolgarija	-	0,3	-	-	3,0	-	-	37,8	-
Ciper	-	0,9	0,5	-	4,0	8,9	-	27,0	24,5
Češka	0,1	0,1	-	0,1	0,2	-	15,3	13,9	14,0
Danska	0,8	1,1	1,2	0,4	1,1	1,5	27,6	30,1	35,0
Estonija	-	0,1	-	-	-	-	-	19,6	10,0
Finska	0,2	0,0	-	3,6	4,5	2,8	13,1	26,6	31,0
Grčija	0,1	0,1	0,4	1,2	0,8	0,5	14,7	12,0	17,9
Irska	0,7	1,1	0,6	2,4	1,8	1,3	11,6	24,8	16,6
Italija	-	-	0,7	-	-	4,0	-	-	41,3
Latvija	-	0,4	0,2	-	1,2	0,3	-	28,7	17,1
Litva	-	0,2	0,6	-	0,8	0,7	-	39,8	39,5
Luksemburg	1,5	0,6	1,4	4,1	9,8	6,3	24,9	49,8	46,0
Madžarska	-	0,4	0,3	-	1,8	2,4	-	34,1	29,6
Nemčija	-	-	-	4,3	2,7	2,0	13,1	35,0	33,3
Nizozemska	-	-	0,9	-	-	2,3	-	-	30,7
Poljska	-	0,3	0,9	-	2,2	2,0	-	29,5	31,6
Portugalska	-	-	-	4,2	1,4	2,0	14,0	17,5	23,4
Romunija	-	0,1	-	-	0,4	-	-	5,2	-
Slovaška	-	0,3	0,2	-	2,8	1,0	-	29,2	25,9
Slovenija	**-**	**0,7**	**-**	-	**1,4**	-	**-**	**33,9**	**39,8**
Španija	-	0,8	1,7	-	18,5	15,4	-	50,8	47,8
Švedska	1,1	1,2	0,9	8,6	7,3	4,0	16,7	24,7	24,4
EU 15	-	1,0	1,4	-	5,3	4,1	-	33,8	35,5
EU 27	-	0,9	1,3	-	4,6	3,8	-	32,3	34,4

Vir: *Eurostat.* Ni podatkov za Belgijo, Francijo in Malto.

Priloga B: Indikatorji informacijske družbe (varnostni problemi podjetij)

Tabela B.1: Indikatorji informacijske družbe: varnostni problemi podjetij. V tabeli so prikazani odstotki podjetij, ki so med uporabo interneta doživela naslednje varnostne probleme

	Neavtoriziran dostop			Izsiljevanje in grožnje			Računalniški virus, ki je povzročil izgubo informacij ali časa		
	2003	2004	2005	2003	2004	2005	2003	2004	2005
Anglija	-	-	3	-	-	0	-	-	29
Avstrija	4	2	1	0	0	0	30	37	31
Belgija	5	3	3	1	0	1	40	39	29
Bolgarija	-	2	2	-	1	0	-	30	27
Ciper	-	0	0	-	0	0	-	36	30
Češka	-	5	4	-	4	-	-	36	31
Danska	7	-	5	1	-	-	49	46	36
Estonija	-	5	2	-	4	2	-	46	35
Finska	7	4	4	-	-	-	48	63	63
Grčija	3	3	3	2	1	1	54	34	25
Irska	-	7	2	-	1	1	-	55	52
Italija	5	3	5	0	1	1	66	41	63
Latvija	-	2	-	-	-	-	-	30	39
Litva	-	1	3	-	1	1	-	61	60
Luksemburg	3	7	3	0	0	0	30	32	12
Madžarska	-	3	10	-	0	4	-	44	81
Malta	2	-	0	0	-	0	39	-	26
Nemčija	-	3	2	-	0	0	-	41	33
Nizozemska	7	5	2	1	1	0	41	60	29
Poljska	-	1	2	-	0	0	-	48	41
Portugalska	4	5	2	1	2	1	41	44	22
Romunija	-	3	-	-	0	-	-	44	-
Slovaška	-	1	1	-	0	0	-	22	26
Slovenija	**-**	**3**	**2**	**-**	**1**	**0**	**-**	**51**	**45**
Španija	-	3	3	-	0	0	-	48	37
Švedska	5	5	3	1	0	0	43	55	44
EU 15	-	3	3	-	0	0	-	44	36
EU 27	-	3	3	-	1	1	-	43	37

Vir: Eurostat. Ni podatkov za Francijo. Opomba: ni vključen finančni sektor in gre za podjetja, ki imajo več kot 250 zaposlenih.