UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Teja Palko

Kibernetska moč držav članic Evropske unije

Magistrsko delo

Ljubljana, 2013

UNIVERZA V LJUBLJANI
FAKULTETA ZA DRUŽBENE VEDE

Teja Palko

Mentor: doc. dr. Uroš Svete

Kibernetska moč držav članic Evropske unije

Magistrsko delo

Ljubljana, 2013

POVZETEK

Kibernetska moč držav članic Evropske unije

Kibernetski prostor postaja vedno pomembnejši in vedno bolj vpet v vse sfere našega življenja. Vedno več ključnih storitev je povezanih z informacijsko-komunikacijskim sektorjem, kar pomeni, da so finančni, prometni, zdravstveni sistemi ter sistemi za preskrbo z vodo in hrano, razna industrija ter energetika med seboj povezani in soodvisni. Ta ključna infrastruktura je v večini povezana s svetovnim spletom, deluje avtomatizirano in ima možnost spreminjanja ter kontroliranja na daljavo. Vse to omogoča vdore v najpomembnejše sisteme, ki so nujno potrebni za naša življenja. Vedno pomembnejše postaja vprašanje, kako se zavarovati pred namernimi in nenamernimi grožnjami v prostoru, kjer prevladuje decentraliziranost, brezmejnost ter anonimnost. Ali napredek na kibernetskem področju prinaša več ali manj varnosti, sem proučevala skozi magistrsko nalogo s proučevanjem kibernetske moči držav članic Evropske unije (EU), pri čemer je kibernetska moč države definirana kot vse sposobnosti in resursi, ki jih le-ta lahko uporabi za podporo lastnih političnih ciljev ter interesov za vplivanje na kibernetski in nekibernetski prostor. Kibernetska moč je dvorezen meč, saj je na eni strani ključ do napredka, na drugi pa zaradi odvisnosti povzroča nove ranljivosti in tveganja. Kako kibernetska moč vpliva na varnost, ali imajo države z bolj razvito informacijsko-komunikacijsko infrastrukturo bolj razvite varnostne mehanizme za njeno zaščito ter ali je kibernetska moč lažje dosegljiva tudi manjšim državam in je alternativa, da lahko manjše po moči konkurirajo večjim, je bil osrednji cilj proučevanja dela.

Ključne besede: kibernetska moč, EU, varnost.

SUMMARY

Cyber power of the European Union Member States

Cyberspace is becoming increasingly more important and integrated in all spheres of our lives. More and more critical services are related to information and communication sector, which means that financial, transportational, health care systems and systems for support for water and food, various industries and energy are interrelated and interdependent. This critical infrastructure is most associated with the World Wide Web, automated functions and the ability to modify and control remotely. All this can allow intruders in most systems that are essential to our lives. More importantly, the question is, how to protect ourselfs against intentional and unintentional threats to the area dominated by decentralized, without clear borders and anonymity. What effect does progress in the cyber area have on security I studied through the master's thesis by examining cyber power of the Member States of the European Union (EU). Where the cyber power of the state is defined as all the skills and resources that can be used to support their own political goals and interests to influence the cyber and none cyberspace. Cyber power is a double-edged sword because on the one hand this is the key to progress and on the other hand due to their dependence creates new vulnerabilities and risks. How cyber power affects safety, do countries with more developed information and communication infrastructure develope more security mechanisms to protect itself and whether is the cyber power more easily accessible also to smaller countries and can be an alternative so that smaller countries can compete for power with larger ones is the central objective of this work.

Key words: Cyber power, EU, security.

KAZALO

KAZALO TABEL

KAZALO SLIK

SEZNAM KRATIC

ANSSI	Agence Nationale de la Sécurité des Systèmes d‟Information (Francoska omrežna in informacijsko varnostna agencija)
ARNES	Akademska raziskovalna mreža Slovenije
BBK	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Nemški zvezni urad za civilno zaščito in reševanje)
BKA	Das Bundeskriminalamt (Nemški zvezni urad kriminalne policije)
BSI	Bundesamtes für Sicherheit in der Informationstechnik (Nemški zvezni urad za informacijsko varnost)
BSI	Department for Business Innovation and Skills (Ministrstvo za gospodarstvo, inovacije in usposabljanje Združenega kraljestva)
CERT	Computer Emergency Response Team (Računalniška skupina za urgentno odzivanje)
CESG	Communications-Electronics Securiry Group (Komunikacijsko-elektronsko varnostna skupina Združenega kraljestva)
COSSI	Centre opérationnel pour les systèmes et sécurité de l‟information (Francoski operativni center za informacijsko sistemsko varnost – kibernetsko obrambni center)
CPNI	Centre for the Protection of the National Infrastructure (Center za zaščito nacionalne infrastrukture Združenega kraljestva)
CSOC	Cyber Security Operations Centre (Nacionalni kibernetsko varnostni center Združenega kraljestva)
ENISA	European Network and Information Security Agency (Evropska agencija za varnost omrežij in informacij)
EASY WAY	Projekt EU za harmonizacijo inteligentnih transportnih sistemov v EU
EU	Evropska unija

EUROSTAT	Evropski statistični urad
GLONASS	Globalnaya navigatisionnaya sputnikovaya sistema (Ruski Globalni navigacijski satelitski sistem)
GPS	Global Positioning System (Ameriški Globalni navigacijski sistem)
IKT	Informacijsko-komunikacijska tehnologija
LABEL	Projekt delno financiran s strani Evropske komisije za vzpostavitev in spodbujanje sistema certificiranja za tovorna parkirna mesta v Evropi
LIDA	Latvijska investicijsko razvojna agencija
IRRIS	Irish Reporting and Information Security Service (Irski urad za poročanje in informacijsko varnost)
ITU	International Telecommunication Union (Mednarodna telekomunikacijska zveza)
NATO CCDCOE	The North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence (NATO center odličnosti za kibernetsko obrambo)
NCAZ	Nationale Cyber Abwehrzentrum (Nemški kibernetsko obrambni center)
NCKB	Narodni centrum kyberneticke bezpečnosti (Češki nacionalno kibernetsko varnostni center)
NCSC	Nationaal Cyber Security Centrum (Nizozemski nacionalni kibernetsko varnostni center)
NITA	Danska nacionalna agencija za informacijsko tehnologijo in telekomunikacije
OECD	Organisation for Economic Co-operation and Development (Organizacija za gospodarsko sodelovanje in razvoj)
OCISA	Office of Cyber Security and Information Assurance (Urad za kibernetsko varnost in zagotavljanje informacij Združenega kraljestva)

OCS	United Knigdom The office of Cyber Security (Urad za kibernetsko varnost Združenega kraljestva)
PPP	Public-Private Partnership (javno-zasebno partnerstvo)
SAMFI	Švedska kooperacijska skupina za informacijsko varnost
SCADA	Supervisory Control And Data Acquisition (Sistem za popolno vodenje in zajem podatkov)
SETPOS	Secure European Truck Parking Operational Service (Operativna storitev za varno parkiranje tovornih vozil v Evropi)
SOCA	Serious Organized Crime Agency (Policijska centralna e-kriminalna enota)
UNCTAD	United Nations Conference on Trade and Development (Konferenca Združenih narodov o trgovini in razvoju)
UNESCO	United Nations Educational, Scientific and Cultural Organization (Organizacija Združenih narodov za izobraževanje, znanost in kulturo).

1 UVOD

Kibernetski prostor postaja vedno pomembnejši in vedno bolj vpleten v vse sfere našega življenja. Širijo se telekomunikacijska, računalniška ter elektronska področja, ki so vedno bolj vpeta v naš vsakdanjik. Pri omembi kibernetskega prostora mislim na fizično in nefizično področje, kamor spadajo računalniki, računalniški sistemi, omrežja in programi, računalniški in prometni podatki, podatki o vsebini in uporabniki (International Telecomunication Union). Da internet postaja vedno pomembnejše področje, prikazuje tudi vedno večje število uporabnikov interneta, ki je v letu 2012 znašalo okoli 2,4 milijarde uporabnikov (Internet World Stats). Ker je kibernetski prostor decentraliziran, lahko sklepamo z veliko verjetnostjo, da bodo kibernetske grožnje postale varnostni in družbeni problem (Svete 2012, 40). Potrebno se je torej zavedati, da imajo spremembe v kibernetskem prostoru relevanten vpliv na družbene, ekonomske in kulturne zadeve (Kramer, Starr in Wentz 2009, 46) in da lahko ima večji kibernetski vdor enake posledice in povzroči isto škodo, kot lahko to stori vojna z tradicionalnim orožjem (Qiao in Wang v Betz in Stevens 2011, 76). Bodoče vojne bodo usmerjene delno ali v celoti v kibernetski prostor (Clarke in Knake 2010, 13), zato je pomembno, da se ukvarjamo tudi s kibernetsko močjo, ki kot mehka moč pridobiva na pomembnosti. Kibernetski prostor je nova domena bojevanja, ki se je pridružila tradicionalnim zemlji, morju, zraku in vesolju. Najdemo lahko več primerov, med njimi tudi napad ZDA na Irak zaradi invazije na Kuvajt leta 1991. Desert Storm je prva informacijska vojna, v kateri so bila uporabljena »pametna orožja« (precizno vodena streliva) in računalniška in druga visoka tehnologija, ki je omogočila zmago v hitrejšem času in proti četrti največji vojski na svetu v tem času (Clarke in Knake 2010, 47−49). Primer uporabe kibernetskih zmogljivosti v okviru vojaških zmogljivosti je tudi napad Izraela na Sirijo v letu 2006, pri čemer so ob napadu na sirijsko zgradbo, ki naj bi bila del jedrskega programa, motili zračne obrambne sisteme in neopazno prečkali sirijski zračni prostor (Clarke in Knake 2010, 30). Znan je tudi primer skupne uporabe kibernetskih zmogljivosti z vojaškimi v Gruziji leta 2008, pri čemer je Rusija skupaj z vojsko uporabila tudi tako imenovane kibernetske bojevnike, ki so istočasno z vojaškim izvedli tudi kibernetski napad. Z napadom je bilo Gruziji onemogočeno komuniciranje izven lastne države ob hkratnem nedelovanju vladne domene in drugih spletnih strani, s čimer so bili izolirani od preostalega sveta (Clarke in Knake 2010, 17−21). Kljub temu da kibernetski prostor in kibernetska moč spreminjata načine bojevanja (Betz in Stevens 2011, 126), se je potrebno zavedati, da nista omejena le na vojaško raven.

Občutljiva mesta ključne infrastrukture so danes prepletena z brezžičnimi omrežji in satelitskimi komunikacijami, kar omogoča vdor v njihov sistem (Geers 2009, 5). V začetku razvoja interneta niso predvidevali odvisnost ključne infrastrukture od interneta ali soodvisnosti različnih mrež, ki med seboj povezujejo življenjsko pomembne sisteme. Danes so z informacijsko-komunikacijskim sektorjem povezani vsi ostali sektorji, ki jih vključujemo v ključno infrastrukturo. Sem spadajo: energetika (proizvodnja in distribucija nafte, plina, električne energije), promet (cestni, železniški, zračni, vodni), sistemi za preskrbo z vodo, hrano, finančni ter zdravstveni sistemi, kemična ter jedrska industrija (Prezelj 2009, 470−471). Najbolj znan primer napada na ključno infrastrukturo je Stuxnet, ki je oblika škodljive programske opreme, ki napade SCADA (ang. Supervisory Control And Data Acquisition – Sistem za popolno vodenje in zajem podatkov) sisteme. Z njim je bil izveden napad na zaščiten iranski objekt za bogatenje urana Natanz, oziroma na njegove centrifuge, kar je povzročilo nazadovanje iranskega jedrskega programa. Zaradi povezanosti ključne infrastrukture s kibernetskim prostorom pa je le vprašanje časa, kdaj se bo podoben napad pojavil drugje (Blackman in drugi 2012, 33). Da pa kibernetski napadi na ključno infrastrukturo niso prisotni le izven Evropske unije, je primer kibernetskega napada na Estonijo v letu 2007, ki je onemogočil uporabo redno dostopnih strani zaradi sesutja strežnikov. Onemogočen je bil dostop do spletnega bančništva, časopisov, vladnih in drugih spletnih strani (Clarke in Knake 2010, 12−13). Vedno bolj se kaže vpliv kibernetskih bojevnikov, ki lahko dostopajo do omrežij in jih sesujejo. Lahko prevzamejo nadzor in s tem lahko pride do kraje informacij, nadzora nad omrežji, ki prenašajo denar, nafto, plin, električno energijo, povzročijo kaos v kopenskem, zračnem in drugem prometu ter dostopajo do orožij (Clarke in Knake 2010, 70).

Vedno pomembnejše postaja vprašanje, kako se zavarovati pred namernimi in nenamernimi napadi, grožnjami in naravnim silam, saj IKT ni povzročil le napredka v civilni in vojaški sferi ter povečal kvaliteto življenja, ampak ustvaril tudi nove ranljivosti. Število kibernetskih groženj s strani različnih akterjev (korporacije, kibernetski kriminalci, zaposleni, haktivisti, države in teroristi) se je povečalo v mobilnem računalništvu in družbeni tehnologiji, kamor so uvrščeni predvsem socialna omrežja ter razne aplikacije, kjer prihaja do kraj identitete, osebnih podatkov in informacij, okužb z virusi in črvi. Pomembno področje, kjer se je povečalo število posrednih kibernetskih napadov, je tudi ključna infrastruktura. Prihaja do povečanih groženj podatkov, shranjenih v virtualnem prostoru, ter do kraje večjih količin podatkov, ki vplivajo na zasebnost (ENISA 2012a).

Zaradi vseh navedenih groženj je razvidno, da je uporaba informacijsko-komunikacijske tehnologije povzročila spremembe v dojemanju in zaznavanju (varnostnega) okolja (Svete 2005, 116). Bolj kot je država odvisna od IKT-ja in so različni sektorji med seboj povezani tudi preko interneta, večja bi morala biti skrb glede možnosti napada (Geers 2009, 6). Današnja odvisnost od informacijsko-komunikacijske tehnologije povzroča ranljivosti in tveganja, saj lahko njeno nedelovanje povzroči večjo ekonomsko, finančno in fizično škodo. Vsaka tehnologija je lahko uporabljena v dobre ali slabe namene in zato je tudi IKT izpostavljen zaradi svoje odprtosti, hitrih sprememb, več funkcionalnosti in transnacionalnosti (Esterle, Ranck in Schmitt 2005, 7), a lahko to ranljivost zmanjšamo s povečanjem kibernetske moči.

2 METODOLOŠKO-HIPOTETIČNI OKVIR

2.1 OPREDELITEV PREDMETA IN CILJI RAZISKOVANJA

Cilji magistrskega dela so:

- predstaviti relevantnost in kompleksnost kibernetske moči in njen vpliv na varnost,
- izpeljati definicijo kibernetske moči na podlagi že sprejetih definicij in teorij mednarodnih odnosov realizma, liberalizma in konstruktivizma,
- izoblikovati kategorije in podkategorije, ki določajo kibernetsko moč,
- na podlagi izbranih kriterijev določiti kibernetsko moč posameznih držav članic Evropske unije,
- analizirati dobljene podatke in potrditi ali zavrniti prvotno raziskovalno vprašanje in hipotezi.

2.2 HIPOTEZE

Raziskovalno vprašanje: Kako kibernetska moč države vpliva na varnost?

H1: Bolj kot ima država razvito informacijsko-komunikacijsko infrastrukturo, bolj ima razvite varnostne mehanizme za njeno zaščito.

H2: Kibernetska moč je lažje dosegljiva tudi manjšim državam in je alternativa, da lahko manjše po moči konkurirajo večjim.

2.3 UPORABLJENA METODOLOGIJA

Pri pisanju magistrskega dela bom uporabila metodo analize in interpretacije primarnih in sekundarnih virov, deskriptivno metodo, primerjalno metodo in analizo statistik. Primarni viri bodo nacionalno-varnostne strategije, načrti, zakoni, pogodbe, resolucije in dokumenti posameznih držav članic Evropske unije, ki se tičejo kibernetskega prostora. Sekundarni viri, ki jih bom uporabila, bodo knjige, članki v znanstvenih in strokovnih revijah, članki v tiskanih občilih in članki, dostopni preko spleta, ter različna raziskovalna poročila mednarodnih organizacij. Opisno metodo bom uporabila pri pojasnjevanju temeljnih pojmov in pomembnosti posameznih segmentov v strukturi magistrskega dela, še posebej pri pojasnjevanju teoretičnega dela in kot podlago za primerjalno metodo. S primerjalno metodo bom med seboj primerjala in iskala razlike med različnimi pravnimi ureditvami, pristopi, razvoji kibernetskih zmogljivosti, skratka vse podkategorije, ki bodo določale kibernetsko moč med državami članicami EU. S kvantitativno metodo analizo statistik bom poiskala statistične podatke, ki bodo uvrščeni v kategorije, ki vplivajo na kibernetsko moč iz državnih uradnih statistik in drugih statističnih uradov.

Vzorec proučevanja bodo države EU, ki imajo strateške dokumente dostopne v angleškem, nemškem ali španskem jeziku, in za katere bo mogoče pridobiti vse potrebne podatke, ki sem jih določila kot relevantni faktor pri določanju kibernetske moči, pri čemer moram poudariti, da sem ob vstopu Hrvaške v EU 1. julija letošnjega leta že imela zbrano in obdelano večino podatkov in zato najnovejše članice v magistrski nalogi nisem obravnavala. Proučevala sem 24 držav članic, saj sem Luksemburg, Finsko ter Slovaško izločila, saj niso imele preko spleta dostopnih vseh potrebnih dokumentov in podatkov v meni razumljivih jezikih. Države proučevanja so bile: Avstrija, Belgija, Bolgarija, Češka, Ciper, Danska, Estonija, Francija, Grčija, Irska, Italija, Latvija, Litva, Madžarska, Malta, Nemčija, Nizozemska, Poljska, Portugalska, Romunija, Slovenija, Španija, Švedska in Združeno kraljestvo. Glavne kategorije bodo zajete v pravnem okvirju, ekonomskemu in socialnemu kontekstu, tehnološki infrastrukturi in vplivu v industriji (Economist Intelligence Unit 2011, 21).

Pri kategorijah kibernetske moči bom uporabila tako opisne kvalitativne kot številčne kvantitativne spremenljivke. Kvalitativne metode bom uporabljala pri opisnih nominalnih spremenljivkah, predvsem v kategoriji pravnega vidika, ki zahtevajo poglobljeno preučevanje. Preostale tri kategorije pa bodo predstavljale v večini številčne spremenljivke. Po zbranih podatkih, ki bodo sestavljali kategorije in podkategorije kibernetske moči, bom le-te rangirala

po posamezni kategoriji in s tem določila, katera država je najboljša v posameznem kontekstu, in s tem določila kibernetsko moč držav članic Evropske unije. Kibernetsko moč bom državam določila na podlagi vseh znanih numeričnih kategorij, pri čemer bom od najmanjše do najvišje vrednosti v podkategorijah državam pripisala vrednosti od 1 do 24, pri čemer ena točka pripada državi v posamezni podkategoriji z najmanjšo vrednostjo in 24. državi z najvišjo vrednostjo. V primeru, kjer sta dve ali več držav zasedli isto mesto, sem obema pripisala isto število točk, naslednja država pa je imela število točk kot če dve ali več držav ne bi zasedali istega mesta. Nekatere podkategorije, ki bodo rangirane drugače, bodo imele ob tem tudi razlago.

Prav tako bom uporabila deskriptivno oziroma opisno statistično analizo, s katero bom izoblikovala grafične in tabelarne prikaze, določila minimalne in maksimalne vrednosti ter povprečje posameznih kategorij za celovitejšo sliko. Prav tako bom glede na spremenljivke podkategorijam pri grafih in tabelah določila modus, ki je število, ki se največkrat pojavi, ter mediano, od katere je polovica vrednosti manjša ali enaka ter polovica vrednosti večja ali enaka mediani. Pri nominalnih podatkih lahko določimo le modus, ordinalnim modus in mediano ter intervalnim podatkom modus, mediano in aritmetično sredino. Po univariatni analizi bom v zaključku uporabila bivariatno analizo, s katero bom poskušala dokazati morebitno povezanost različnih podkategorij oziroma spremenljivk med seboj, pogledala bom, ali obstaja statistično značilna povezanost med naključnimi podkategorijami. Bivaratne analize bodo odvisne od lastnosti spremenljivk, oziroma od njihovega tipa (nominalne, ordinalne, intervalne ali razmernostne). Povezanost numeričnih spremenljivk sem prikazala z grafično tehniko Scatter plots, pri čemer je lahko povezanost negativna ali pozitivna. To dokaže tudi Pearsonov korelacijski koeficient, ki prikazuje stopnjo linearne povezanosti dveh spremenljivk, ki ga lahko uporabimo pri številčnih spremenljivkah. Njegov rang je od -1 do +1, pri čemer pozitivna vrednost kaže na pozitivno korelacijo in negativna na negativno oziroma obratno povezanost. O močni povezanosti spremenljivk lahko govorimo v primeru, ko je Pearsonov koeficient korelacije večji od 0,7 ali manjši od -0,7, pri šibki povezanosti lahko govorimo, ko je njegova vrednost manjša od 0,7 ali večja od -0,7, pri vrednosti, manjših od 0,3 in večjih od -0,3, povezanosti med spremenljivkami ni.

2.4 STRUKTURA DELA

Magistrska naloga je sestavljena iz teoretičnega in empiričnega dela. V teoretičnem sklopu je predstavljena izpeljava definicije kibernetske moči v povezavi s teorijami v mednarodnih odnosih realizma, liberalizma in konstruktivizma ter definicijami in različnimi pristopi

varnosti. Sledi opredelitev kategorij, ki so relevantne pri določanju kibernetske moči posamezne države, ki so razdeljene na štiri glavne kategorije: pravni okvir, socialni in ekonomski kontekst, tehnološka infrastruktura ter uporaba informacijsko komunikacijske tehnologije v industriji. V empiričnem sklopu pa so prikazani podatki za proučevane države po prej omenjenih kategorijah in njenih podkategorijah. Sledi določitev kibernetske moči po proučevanih državah, sklep in verifikacija hipotez ter raziskovalnega vprašanja.

2.5 OPREDELITEV TEMELJNIH POJMOV IN KONCEPTOV

2.5.1 Varnost

Definicije varnosti so se skozi čas spreminjale in so bile vezane na različne vire ogrožanja. V času svetovnih vojn se je v ospredje postavljala država in državna oziroma nacionalna varnost, ki je sčasoma prešla na širšo kolektivno varnost in bolj kooperativno obliko sodelovanja za zagotavljanje varnosti. Razvijali so se različni koncept, ki se med seboj dopolnjujejo in razlikujejo, kar je prikazano tudi v nadaljevanju. Pomembno vlogo so dobile mednarodne organizacije in nenazadnje posameznik. Iz vojaškega področja se je o varnosti začelo govoriti tudi v drugih nevojaških sektorjih. Grožnje in tveganja, ki definirajo varnostno okolje, združujejo vojaške, politične, družbene, ekonomske, okoljske in posameznikove aspekte.

Varnost je temeljna prvina obstoja in razvoja človeka od davne preteklosti do danes. Pojem varnosti zajema tako ohranitev posameznika kot fizičnega, duhovnega, kulturnega in družbenega bitja kot tudi zagotovitev kakovosti njegovega bivanja v družbenem in naravnem okolju (Bučar, Grizold 2011, 829). Sodobna razprava o varnosti je usmerjena predvsem na njene referenčne objekte (na koga se varnost nanaša), na grožnje varnosti (kdo ali kaj to varnost ogroža) in na varnostne mehanizme (kakšna oz. katera so sredstva za doseganje varnosti) (Liotta v Svete 2005, 55). Varnostna paradigma se lahko obravnava v obliki različnih temeljnih konceptualnih okvirov, pri čemer sem se odločila za vključitev nacionalne, družbene, človekove, informacijske ter omrežne varnosti.

Pri vseh vidikih proučevanja varnosti tako tradicionalnih kot netradicionalnih je potrebno upoštevati, da stoodstotne varnosti ni mogoče doseči. Danes je bistveno več nevojaških kot vojaških pojavov, ki predstavljajo grožnje. Grožnje so lahko naravni ali družbeni pojavi (Prezelj 2007, 7, 22). Grožnje varnosti so subjektivne, kar pomeni, da lahko o stopnji ogrožanja varnosti razpravljamo na podlagi zaznanih groženj. Stopnja ogrožanja

varnosti je splošna ocena, ki temelji na različnih indikatorjih, ki pa pomenijo poenostavljanje kompleksne stvarnosti (Prezelj 2007, 14−15).

Tradicionalno poimenovanje varnosti, ki je bilo v ospredju do konca hladne vojne, je osredotočeno na vojaško obrambo, politične vidike in fokusirano predvsem na nacionalno ter mednarodno varnost. Nacionalna varnost je varnost države in nacije. Zajema varnost državnega ozemlja, varnost življenja ljudi in njihove lastnine, ohranjanje in vzdrževanje nacionalne suverenosti in uresničevanje temeljnih funkcij države. Prisotne so predvsem zunanje grožnje, operjene proti nacionalni suverenosti in teritorialni integriteti (Dunne in drugi 2007). Grožnje nacionalni varnosti so vsi tisti dogodki ali sekvence dogodkov, ki grozijo, da bodo v kratkem času drastično zožili izbiro možnih političnih reakcij, ki so na voljo državi in zasebnim nevladnim subjektom (posameznikom, skupinam ter korporacijam) znotraj države (Ullman v Prezelj 2002, 623).

Po netradicionalističnem pojmovanju, ki se je razvilo po koncu hladne vojne, je ogrožanje varnosti kakršnokoli stanje, v katerem ni zagotovljen obstoj in uravnotežen razvoj določenega referenčnega objekta (Prezelj v Prezelj 2002). Konec hladne vojne je prinesel radikalne strateške, politične, ekonomske in kulturne spremembe v mednarodnem okolju. Te se na področju varnosti kažejo kot kompleksno ogrožanje, ki presega okvire posameznih držav (Bučar, Grizold 2011, 828). Kopenhagenska šola je definirala čezsektorski pristop k varnosti. Glavni sektorji so med seboj povezani in imajo drug na drugega vpliv, a so za lažje razumevanja razdeljeni na politični, vojaški, okoljski, ekonomski in družbeni sektor. Varnostni problemi iz enega sektorja vplivajo na varnostne probleme v drugih sektorjih. Za zagotovitev varnosti morajo biti varnostni problemi odpravljeni na vseh področjih, saj so sektorji soodvisni in povezani (Buzan, Waever in Wilde 1998).

Kot vmesni člen med nacionalno in individualno varnost lahko uvrstimo družbeno varnost, katere koncept se je izoblikoval po koncu hladne vojne, ko so poudarili razlikovanje med državo in družbo. Definicija družbene varnosti se sama po sebi ne povezuje z narodom, ampak s skupnostmi, temelječimi na identitetah, pa naj bodo nacionalne, etnične ali verske (Svete 2005, 74−75). Ta koncept je eden najpomembnejših nedržavocentričnih varnostnih konceptov, ki kot referenčne objekte, na katere se varnost nanaša, izpostavlja družbene, interesne, politične skupine in celo posameznika (Svete 2005, 76−78). Ogrožene so vrednote, kot so kultura, jezik, pisava oziroma identitete. Države uporabljajo različne mehanizme za zavarovanje lastnih skupnosti, kot so zaščita z različnimi sredstvi z ohranjanjem lastnih norm, načel, kulture, nekatere bolj nedemokratične gredo v smeri izolacije z raznimi cenzurami (Svete 2005, 78−79). Koncept družbene varnosti sem vključila, ker IKT in globalizacijo

dojema kot grožnjo varnosti, ki pa ni edina grožnja. Z vedno bolj povezanim svetom se izgubljajo kulturne in druge razlike med prebivalstvom in se začne oblikovati neka mednarodna skupna zavest, ki izpodriva identitete skupnosti.

V vedno bolj individualiziranem svetu je pomemben koncept človekove varnosti, ki se je razvil po hladni vojni. Poročilo o človekovi varnosti Razvojnega programa Združenih narodov je človekovo varnost definiralo kot osvobojenost od strahu in osvobojenost od potreb, odsotnost nasilja in vojne ter groženj, kot so lakota in bolezen. Človekova varnosti ščiti vrednote, kot so varnost, dobrobit in dostojanstvo. Navaja grožnje ekonomski varnosti, prehranjevanju, zdravstvu, okolju, skupnosti ter politični varnosti (United Nations Development Programme 1994, 22–25). Človekova varnost se nanaša na (Kantij v Bučar, Prezelj in Vogrin 2008, 12) zaščito osebne varnosti in svobode pred neposrednim in posrednim nasiljem. Kot sredstvo za zaščito varnosti navaja pospeševanje človekovega razvoja in dobro vladanje, norme na različnih področjih človekove varnosti, po potrebi tudi uporabo kolektivnih sankcij ali sile. Potrebno je sodelovanje držav, mednarodnih in nevladnih organizacij in drugih skupin civilne družbe. Vsi pristopi k človekovi varnosti se strinjajo o primarnosti posameznika kot referenčnega objekta varnosti, razlikujejo pa se glede obsega zaščite (oziroma obsega groženj posamezniku) in primernih mehanizmih za njegovo zaščito. Glavna cilja sta osebna varnost in svoboda. Grožnje človekove varnosti so tradicionalne in netradicionalne. Človekova varnost se zagotavlja s preventivo (država, nedržavni akterji), kurativo (sredstva mirnega reševanja sporov, humanitarna pomoč, usmerjene sankcije, kolektivna uporabe sile, mirovne operacije) ter neprisilnimi ukrepi za zmanjšanje ranljivosti s trajnostnim razvojem. Poleg zaščite je ključna tudi usposobljenost (Bučar, Prezelj in Vogrin 2008, 34). Grožnje človekovi varnosti so predvsem nevojaške, saj vključujejo pomanjkanje ekonomskega, socialnega, političnega in okoljskega razvoja ter tudi tradicionalne, kamor uvrščamo oborožene spopade (Bučar, Grizold 2011, 836−842). Pomembno se je zavedati, da je število groženj človekovi varnosti neskončno (Oberleitner v Bučar, Prezelj in Vogrin 2008, 27).

V sodobnem vedno bolj globaliziranem svetu so posamezne grožnje varnosti vse bolj transnacionalnega značaja. Za njih je značilno skoraj nezadržno širjenje preko meja, pretežno nevojaški značaj in nedržavni značaj nosilcev ogrožanja. Med takšne transnacionalne grožnje spadajo tudi informacijske motnje, kamor spadajo ogrožanje informacijske infrastrukture ter kibernetski kriminal (Prezelj 2007, 10). Danes se nobena država ne more sama upreti transnacionalnim grožnjam varnosti, saj je za to potrebno mednarodno sodelovanje (Prezelj 2002, 633−634).

Zaradi vedno večjega pomena IKT v sodobnih družbah so omrežja sama in IKT postali referenčni objekt, na katerega se varnost nanaša. Pojavil se je koncept omrežne in širše informacijske varnosti. Slednja se nanaša na uravnotežen in stabilen razvoj ter delovanje. Koncept informacijske varnosti za cilj ogrožanja postavi v ospredje celotno IKT, tudi njene zmogljivosti zbiranja podatkov in delovanje strojne opreme nasploh. Oblike ogrožanja informacijske varnosti so višja sila (naravne in druge nesreče), pomanjkljivosti strojne in programske opreme (izpad sistema in druge napake), človeški dejavnik, ki vključuje namerna in nenamerna dejanja. Vse večji del družbe je odvisen od omrežne informacijske infrastrukture, zato je omrežna varnost usmerjena v zavarovanje omrežja samega pred razpadom sistema, izgubo, krajo, uničenjem podatkov ter prekinitvijo informacijskih tokov. Omrežna varnost ima dve dimenziji. Prva se nanaša na zanesljivo delovanje informacijske infrastrukture, torej na notranjo omrežno varnost. Druga pa se nanaša na varovanje informacijskega toka med ponudniki in uporabniki, ki zajema razne elektronske oblike storitev, kot so e-javna uprava, e-volitve, elektronsko bančništvo in zavarovalništvo (Svete 2005, 105−108). Kibernetski prostor ni varen. Fizična infrastruktura, operacijska programska in strojna oprema, informacije in ljudje so izpostavljeni varnostnemu izpadu, bodisi skozi napade, infiltracijo ali nesrečo. Informacijska varnost obsega fizični nadzor dostopa do podatkov in zagotavljanje pravilne uporabe podatkov, onemogoča nepooblaščenim dostop do informacij; varuje pred naključnimi spremembami, uničenjem, razkritjem, izgubo ali dostopom do avtomatiziranih ali ročnih evidenc ter datotek, kot tudi pred izgubo, škodo ali zlorabo informacijskih sredstev. Za zmanjšanje ranljivosti in minimaliziranjem ogrožanja informacijske varnosti je potrebna uvedba politik in pravil, ki lahko vključuje fizično zaščito ustanov in opreme, ki procesirajo in delajo z informacijami in podatki, vzdrževanje aplikacij, integriteta podatkov, zagotovila, da avtomatski ali ročni informacijski sistemi delujejo pravilno in pod nadzorom, zaščita pred nepooblaščenim dostopom, zagotovitev kontinuitete delovanja in zanesljivost. Za zagotavljanje informacijske varnosti je pomembna zaščita programov, izobraževanje, treningi zaposlenih ter varnostno ozaveščanje (Peltier 2011, 266−267).

Grožnje kibernetski varnosti, ki je širša in vključuje tako omrežno kot informacijsko varnost, vključujejo državne in nedržavne akterje, pri čemer so države še vedno dojete kot največji potencialni sovražnik, saj lahko s svojimi resursi izvedejo popolno »kibernetsko vojno« in nevtralizirajo ključno infrastrukturo drugih držav. Kljub temu pa je posebna pozornost namenjena tudi nedržavnim akterjem, ki imajo zmožnosti, priložnosti, tehnologijo in namen povzročati škodo, kamor spadajo državno sponzorirani zunanji in izvendržavni

akterji, teroristi, zaposleni ter hekerji. Pravzaprav je lahko tako tarča kot napadalec vsakdo, ki uporablja računalnik (Eriksson in Giacomello 2004, 9−10).

V naslednji tabeli 2.1 je prikazana primerjava obravnavanih konceptov varnosti glede na referenčne objekte, grožnje referenčnemu objektu, ogrožene vrednote ter varnostne mehanizme za zagotavljanje varnosti.

Tabela 2.1: Primerjava poimenovanj varnosti

	Nacionalna varnost	**Družbena varnost**	**Človekova varnost**	**Omrežna varnost**	**Informacijska varnost**
Referenčni objekt (na koga se varnost nanaša)	Država	Skupnosti (nacionalne, etnične, verske, interesne, politične)	Posameznik	Omrežja	IKT
Grožnje	Vojaške grožnje, nasilje in moč drugih držav	Globalizacija, grožnje v identitetnem smislu, IKT	Vojaške, pomanjkanje ekonomskega, socialnega, političnega, okoljskega razvoja	Razpad sistema, izguba, kraja, uničenje podatkov, prekinitev informacijskih tokov	Višja sila, pomanjkljivosti strojne in programske opreme, človeška namerna in nenamerna dejanja
Ogrožene vrednote	Nacionalna suverenost, ozemeljska celovitost	Identiteta, kultura, jezik, pisava, vse kar identificira določeno skupnost	Osebna varnost in svoboda	Varnost omrežij	Uravnotežen, stabilen razvoj in delovanje IKT
Varnostni mehanizmi	Vojaška moč in sila, samopomoč brez državnega sodelovanja	Zaščita, izolacija skupin, interesov, ohranjanje lastnih običajev, norm, kulture	Preventiva, neprisilna sredstva za zmanjšanje ranljivosti, kurativa	Tehnična sredstva: požarne pregrade, protivirusna programska oprema, CERT in druge institucije	Preventiva, odpravljanje varnostnih pomanjkljivosti

Za namen proučevanja sem vključila tri teorije, in sicer realizem, liberalizem in konstruktivizem, ki so glavne teorije moči v mednarodnih odnosih. Za te tri teorije sem se odločila, saj vsaka iz lastnega zornega kota tvori širši pogled, ki ga moramo upoštevati pri

proučevanju kibernetske moči, kjer so pomembni različni akterji od države, mednarodnih organizacij do posameznikov in prikazujejo celostno obravnavanje varnosti. Osredotočila se bom torej na tradicionalne in netradicionalne teoretične perspektive, ki se povezujejo z zgoraj omenjenimi koncepti proučevanja varnosti.

2.5.2 Realizem

Realizem kot glavnega akterja v mednarodnih odnosih v ospredje postavlja suvereno državo. Države so po realizmu v anarhičnem svetu, kjer vlada nenehen konflikt za moč, motivirane z močjo, s katero dosegajo nacionalni interes in s katero lahko spremenijo vedenje drugih držav (Pettiford in Steans 2001, 25−30). Najpomembnejše sredstvo za zagotavljanje varnosti je moč države, ki se kaže v oboroženih silah (Bučar in Grizold 2011, 829−830). Država določa zakone in izvaja vrhovno oblast, kar pomeni, da državljanom ni potrebno skrbeti za lastno varnost, saj jo zagotavlja država preko pravnega sistema in represivnih organov (Dunne in drugi 2007, 221). Več vojaške moči pomeni tudi višjo stopnjo varnosti. Države naj bi povečevale vojaško moč, da bi dosegle ravnotežje moči kot temelj in garant stabilnosti, zavarovale svojo ozemeljsko in institucionalno integriteto (Morgentau v Svete 2005, 35). V državni skupnosti ni vrhovne oblasti, saj so države v anarhični skupnosti ter tekmujejo za varnost, ki jo je mogoče doseči zgolj na račun varnosti drugih držav. Za preživetje države je samopomoč nujno načelo. Primarni cilj je vzdrževanje in zagotavljanje nacionalne varnosti. Obstaja nezaupanje v dolgoročna sodelovanja in zavezništva. Vsi izidi pa so odvisni od relativne moči vpletenih akterjev in tisti, ki imajo večjo moč, determinirajo izide glede na lastne interese. Pojavljajo se varnostne dileme, termin, ki ga je razvil John Herz (Jennifer Sterling-Folker 2006, 13−17), in so vidne tudi na kibernetskem področju, saj ni transparentnosti pri gradnji kibernetski sil posamezne države, prav tako ne obstajajo mednarodno sprejeti dokumenti, resolucije in s tem omejitve, pri čemer države v strahu pred zaostankom in možnostjo kibernetskega napada gradijo kibernetske zmogljivosti na različnih področjih.

Kot je zapisal Nye (2010, 15), je zagotavljanje varnosti klasična naloga držav, vedno večja nevarnost bo pripeljala do povečane vloge držav v kibernetskem prostoru. Država je imela v začetni fazi ključno vlogo pri razvoju in je tehnologijo predvidela za potrebe zagotavljanja nacionalne varnosti, vendar pa se je s komercializacijo IKT njen vpliv zmanjšal. Države poskušajo omejiti in nadzirati internetno sfero z neposrednim nadzorom komuniciranja in prometa, posredno z vplivom na razvijalce programske in strojne opreme, z oblikovanjem multilateralnih sporazumov in konvencij, ki določajo načine uporabe IKT ter

predvidevajo sankcioniranje njene zlorabe (Svete 2005, 208). Gledano s stališča realizma, kjer ima vojaška moč najpomembnejšo vlogo, je za države že od nekdaj pomembno elektronsko bojevanje, ki se mu je z informacijsko dobo pridružilo še informacijsko bojevanje. Države so zaradi velikih resursov še danes dojete kot največji potencialni sovražnik za povzročitev večjega kibernetskega napada in uničenja ključne infrastrukture drugih držav (Eriksson in Giacomello 2004, 9−20).

Vloga države se danes kaže v sprejemanju zakonov in norm, ki oblikujejo mehanizme za zagotavljanje varnosti. Kot predvideva realizem, se države borijo za kibernetsko premoč, kar je vidno na področju razvoja ofenzivnih in defenzivnih kibernetskih sposobnosti, pri čemer želijo prevladati nad drugimi. Države uporabljajo IKT za izpolnjevanje nacionalnih interesov. Varnost je predstavljena kot skupna dobrina, ki pa jo zagotavlja država s svojimi nacionalno varnostnimi organi. Uporaba realizma in pomembna vloga države je razvidna skozi celotno magistrsko nalogo, saj sem proučevala državne organe, ki se ukvarjajo posredno ali neposredno z zagotavljanjem varnosti na kibernetskem področju. Države igrajo pomembno vlogo, saj ustvarjajo zakone in pravno podlago, sodelujejo na mednarodnem področju s sporazumi in raznimi konvencijami in s tem omejujejo dejanja v virtualni sferi, ozaveščajo prebivalstvo preko državnih institucij in organov, kar vse vpliva na različne koncepte varnosti. Ker pa je za celovito zagotavljanje varnosti pomembno sodelovanje držav, nedržavnih in državnih organizacij, strokovnjakov in laične javnosti, oziroma državnih in nedržavnih akterjev, je naslednja teorija proučevanja liberalizem.

2.5.3 Liberalizem

Začetke teorije najdemo že v dobi razsvetljenstva. Liberalizem definira moč kot zmožnost doseči želene cilje. Koncept moči temelji na sodelovanju držav za dosego skupnih dolgoročnih ciljev.

Liberalizem je tako kot vse teorije sestavljen iz različnih pristopov, njihove osnovne predpostavke pa so pluralnost mednarodnih akterjev, pomembnost domačih političnih faktorjev, ki določajo vedenje držav, pomembna je vloga mednarodnih institucij z uvedbo norm in pravil obnašanja ter širši pristop k proučevanju kompleksnega mednarodnega okolja. Pomembno vlogo poleg države igrajo nedržavni akterji, kot so transnacionalne korporacije, družbena gibanja, lobiji, politične stranke, migranti, teroristi in druge posamezne skupine in posamezniki (Eriksson in Giacomello 2004, 20−21). Vse perspektive znotraj liberalizma poudarjajo sodelovanje, ki preprečuje vojne, a se razlikujejo na način, kako to doseči.

Obstajajo ekonomske, demokratične, sociološke in institucionalne usmeritve (Svete 2005, 37−38).

Današnjim kompleksnim grožnjam, ki presegajo meje držav zaradi same narave kibernetskega prostora, ki je neomejen, se je mogoče zoperstaviti le s sodelovanjem na mednarodni ravni.

Varnost je dojeta širše kot pri konceptu realizma, saj vključuje poleg vojaških tudi nevojaške grožnje. Pri dojemanju varnosti so vključeni tudi nedržavni akterji. Pomembna je mehka moč, tudi ekonomska moč, ki naj bi nadomestila vojaško. Liberalna teorija vključuje tudi trditev, da pričakovano vedenje posamezne države ne odraža zgolj njenih, ampak tudi preference drugih držav, ki so z njo povezane preko medsebojne odvisnosti (Moravcsik 1997, 523). Liberalizem torej predpostavlja veliko medsebojno prepletenost držav in nedržavnih akterjev, zaradi česar je možnost za spore manjši, če pa se že pojavijo, jih lahko rešimo preko mednarodnih institucij. Sodelovanje v liberalizmu temelji na ekonomski prepletenosti, demokratičnosti držav in mednarodnih organizacijah.

Informacije in komunikacija igrajo pomembno vlogo v premagovanju ovir za kolektivne akcije, ki omogočajo realizacijo kolektivnih interesov. Sodelovanje in deljenje informacij gradi zaupanje in zato pomembno vlogo igrajo mednarodne organizacije, preko katerih potekajo interakcije. Državne preference so primarni kriterij vedenja držav. Obstaja pluralnost v državnih ukrepih, saj so odvisne od ekonomskega, vladnega sistema in kulture. Sodelovanje med državami ni omejeno le na politiko in varnost. Pri sodelovanju je mogoče doseči absolutno zmago in s tem doseči mir (Jennifer Sterling-Folker 2006, 55–61). Pluralnost družbenih akterjev je vidna s hitrim širjenjem IKT, ki spodkopava moč države in preusmerja pozornost z vojaške varnosti v smeri zagotavljanja ekonomske in socialne blaginje. Globalne družbe so omrežene v splet gospodarskih in socialnih povezav, stroški prekinitve teh povezav pa preprečujejo unilateralne poteze držav, zlasti pa uporabo sile (Walt v Svete 2005, 39).

Državi so pridruženi tudi drugi akterji, med njimi tudi posamezniki, ki pridobivajo na moči preko različne IKT, s katero lahko nadzorujejo in vplivajo na državo in njene procese. Individualnost je posebnost današnjega sveta, kjer lahko z malo truda in vložki preko spleta in druge IKT na različne načine posameznik doseže spremembe v realnem svetu. Vedno več je akterjev, ki postajajo močnejši, saj so z globalnim spletom meje držav zamegljene, kar ima pozitivne in negative učinke na varnost na splošno in varovanje zasebnih podatkov, integracijo, sodelovanje, transnacionalni kriminal, kibernetski kriminal in druge. Vidi se spremenjena vloga države z izgubljanjem monopola nad različnimi področji, kot sta izobraževanje in širjenje informacij. Globalna povezanost je s seboj prinesla tudi nove

grožnje, ki so povezane s spletom, pri čemer je zaradi anonimnosti težja ali onemogočena izsleditev storilcev kaznivih dejanj. V primeru informacijske varnosti in varnosti posameznika država ni zmožna zagotoviti popolne varnosti, saj je veliko odvisno od vsakega posameznika, njegovega vedenja in ravnanja na spletu. Liberalizem sem v nalogi uporabila, saj poleg države igrajo pomembno vlogo tudi nedržavni akterji z večino ključne infrastrukture ter posamezniki. Vloga posameznikov je razvidna iz proučevanja ekonomskega in družbenega konteksta, ki je sestavni del kibernetske moči in temelji predvsem na človeških sposobnostih ter ozaveščenosti posameznikov. Za zagotavljanje varnosti je pomembno sodelovanje med vsemi akterji, predvsem pa med državnimi organi ter akterji, v rokah katerih je večina ključne infrastrukture. Prav tako se kaže pomembnost drugih akterjev, kot so mednarodne organizacije s sprejemanjem različnih resolucij tudi na kibernetskem področju, pomembna je Evropska komisija s sprejemanjem zakonov ter priporočili in velika usmerjevalna vloga ENISE.

2.5.4 Konstruktivizem

Nekatere države so že spoznale pomen kibernetskih zmogljivosti tako ofenzivnih kot defenzivnih, saj so v okviru vojsk in drugih institucij začele razvijati enote za kibernetsko bojevanje ali obrambo. Razlaga, zakaj jih niso razvile vse države, gre verjetno v smeri, da vsaka država dojema grožnje različno in da so tudi grožnje, ki izhajajo iz kibernetskega prostora, kot vse ostale subjektivno zaznane ter družbeno pogojene.

To lahko pojasnimo s konstruktivizmom, ki predpostavlja, da je vse znanje na svetu skonstruirano, je refleksija naših predsodkov, idej, predpostavk in ni objektivna družbena realnost (Elias in Sutch 2007, 125). Poleg dejanskih virov ogrožanja je na spremembe v dojemanju varnosti v enaki meri vplivala tudi njihova zaznava, kajti zaznavni vidik varnosti je izredno pomemben (Svete 2005, 33). Z idejami konstruktivisti mislijo na cilje, grožnje, identitete ter druge elemente, ki vplivajo na zaznavo realnosti, ter na državne in nedržavne akterje v mednarodnem sistemu. Prav ideje in norme so tiste, ki skozi čas oblikujejo in spreminjajo zunanjo politiko in ne varnost, kot trdijo realisti. Konstruktivizem, ki je kot teoretski pristop nastal v 80. letih prejšnjega stoletja, upošteva ideje, kulturo, ideologijo, socializacijo in zgodovinske okoliščine, ki oblikujejo mednarodno politiko. Razvil se je po koncu hladne vojne, ko večina teorij ni predvidela njenega konca, s čimer se je odprla pot teoriji, v kateri je mogoče priti do radikalnih sprememb v kratkem času (Jennifer Sterling-Folker 2006, 115−122). Naše identitete in interesi so odvisni od socialnega okolja in so družbeno skonstruirani ter dajejo smisel materialnemu svetu. Te družbeno skonstruirane ideje,

ki nam dajo vedeti, kaj je prav ali narobe, možno in kaj ne, oblikujejo naše obnašanje, ki je v večini skladno s kolektivni razumevanjem in odobravanjem. Družbeni svet ustvarjajo ljudje, ki niso neodvisni od tega sveta (Sterling-Folker 2006, 115−122). Ljudje ustvarjajo pravila in družbo ter pravila in družba oblikujejo in vplivajo na ljudi (Kowert, Kubalkova in Onuf 1998, 64). Da lahko skonstruirana resničnost postane objektivna resničnost, je potreben pristanek ljudi. Primer za to je država (Barnett v Baylis in Smith 2007, 333).

Akterji razvijajo svoje odnose z drugimi skozi prizmo razumevanja drugih preko medijev, norm in praks. Norme pa določajo identitete. Za razlaganje, zakaj določeni akterji delujejo tako, kot delujejo, moramo v obzir vzeti njihove kulture, norme, institucije, procedure, pravila in družbene prakse, ki konstruirajo akterje in vplivajo na njihovo ravnanje. Prav tako pa so le-te spremenljive in temeljijo na zgodovinskem, političnem ter družbenem kontekstu. Na podlagi konstruktivizma varnost ni objektivno stanje, kajti grožnje varnosti niso preprosto zgolj stvar korektnega zaznamovanja medsebojnega razmerja sil, prav tako pa objekti varnosti niso niti stabilni niti nespremenljivi. Konstruktivizem želi razložiti proces oblikovanja zaznav, kaj določa konkretne stvari kot grožnje in kakšni so mehanizmi za zaščito pred njimi. Moč je v idejah in v družbeni praksi (Hopf 1998, 171–177). Konstruktivizem lahko razumemo kot gledanje sveta skozi umetne leče, katerih obstoja se niti ne zavedamo (Kowert, Kubalkova in Onuf 1998, 39). Koncept poudarja zlorabo moči nad mnenji (Carr v Kowert, Kubalkova in Onuf 1998, 52), kar pojasnjuje tudi delno konstruktivistični pristop, znan kot Kopenhagenska šola, in njena teorija o sekuritizaciji, ki razloži, zakaj so nekatere stvari opredeljene kot varnostni problem in druge ne. Delno zato ker je poudarek na lingvistično ustvarjeni realnosti in ne tudi preko prakse in simbolov ter dejanj, kot predpostavlja konstruktivizem. Sekuritizacija je ekstremna politizacija, kjer v seriji govorov tisti, ki imajo moč, običajen problem okarakterizirajo kot varnostni problem. Ta opredelitev problema ni objektiven proces, je socialno skonstruiran in mora biti sprejet s strani ljudstva, s čimer postane varnostni problem, ki lahko zahteva tudi večje posege v pravice in ustvari krizne razmere. Opredelitve so pomembne, saj vplivajo naprej na naše odzive ali neodzive (Buzan, Waever in Wilde 1998). Ustvarjanje simbolov in identitet je vidno tudi na kibernetskem področju, kjer se pojavlja za možne večje grožnje v kibernetskem prostoru izraz »elektronski Pearl Harbor«, kar daje kibernetskim napadom identiteto.

Konstruktivizem bo v magistrski nalogi uporabljen za razumevanje, zakaj nekatere države razvijajo nekatere norme in pravila na kibernetskem področju, mehanizme za zaščito ključne infrastrukture in organe v kibernetski sferi in nekatere ne. S konstruktivizmom lahko dejanja držav pojasnimo z njihovo identiteto, ki vpliva na razvoj kibernetske moči. Različne

identitete držav so razvidne tudi iz strateških dokumentov tudi na kibernetskem področju, saj na primer Nemčija in Francija, ki sta del razvitejših držav v EU, drugače gledata na razvoj kibernetskih sposobnosti kot druge manj razvite evropske države. Poudarek na vodilnih vlogah in lastnemu dojemanju kot vodilnih sil je razviden tudi iz strategij in državnih strateških dokumentov. S pristopom se da torej pojasniti razvoj različnih konceptov glede zagotavljanja varnosti in odzivov na kibernetske grožnje. Razvidni so različni koncepti, kot so koncept neomejenega informacijskega bojevanja, informacijske operacije, zaščita ključne infrastrukture, razvoj omrežnih oboroženih sil in drugi. Poudarek v konstruktivizmu ni na individualizmu ampak na idejah. Da v primeru groženj v kibernetskem prostoru ne obstajajo mednarodno sprejete definicije in zavezujoči dokumenti na mednarodni ravni, lahko pripišemo temu, da se premalo ljudi zaveda tveganj ali da družbeni konstrukt o informacijski ogroženosti ni dosegel kritične mase.

Pri širjenju idej in zaznav stvarnosti igra pomembno vlogo IKT (Svete 2005, 69−71), saj je omogočila in pospešila komunikacijo kot nujen pogoj oblikovanja kolektivnih identitet oz. predstav varnosti med različna geografska področja in države. Informacijski viri, množični mediji, internet in druga IKT so osnovni instrument oblikovanja zaznav družbene stvarnosti, zato ima njihova uporaba velik vpliv na oblikovanje kolektivnih predstav, kakor tudi na odločanje ter izpostavljanje določenih družbenih problemov.

Internet in svetovni splet sta videna kot nepogrešljiv del sedanjosti kot tudi prihodnost, kljub temu da se porajajo utemeljeni dvomi, da lahko v prihodnosti storita več škode kot koristi, saj so ključna področja medsebojno prepletena in povezana s spletom. Posledično se vedno več ljudi zanaša na delovanje teh sistemov in glede na trend digitalizacije lahko pride do ogrožanja ključnih sfer in varnosti ob njihovem nedelovanju.

2.5.5 Kibernetska moč

Prav tako kot je v glavnih teorijah mednarodnih odnosov moč različno definirana in razporejena, obstaja tudi na področju kibernetske moči več definicij. Do sedaj njena enotna definicija na mednarodni ravni ne obstaja. Posamezniki, države in nekatere organizacije, ki se ukvarjajo s kibernetskim prostorom in kibernetsko varnostjo, definicije o tem, kaj je kibernetska moč, niti nimajo izpeljane. Definicije se med seboj razlikujejo po tem, da so postavljene v širšem ali ožjem kontekstu. Ene so osredotočene na splošno druge bolj specifično na ekonomski, vojaški, politični, tehnološki, komunikacijski ali informacijski aspekt. V Evropi se države v večini ukvarjajo s kibernetsko ali omrežno varnostjo, ki sta le

del kibernetske moči. Države stare celine so osredotočene predvsem na preprečevanje kibernetskega kriminala in napadov.

Podlaga za raziskovanje te teme mi je bila Economist Intelligence Unit, ki je kibernetsko moč definirala kot sposobnost izogniti se kibernetskemu napadu in uvedbe potrebne digitalne infrastrukture za produktivno in varno gospodarstvo (Economist Intelligence Unit 2011, 2).

Klimburg (2012, 43) meni, da je kibernetska moč posamezne države sestavljena iz treh dimenzij: koordinacije in delovanja politik med vladnimi strukturami, koherentnostjo politike v mednarodnih zavezništvih/organizacijah in legalni okvir ter sodelovanje z nedržavnimi kibernetskimi akterji.

Naslednja definicija kibernetske moči (Kramer, Starr, Wentz 2009, 38−39) je definirana kot sposobnost uporabe kibernetskega prostora v svojo prednost in možnost vplivanja na dogodke v vseh operativnih okoljih in preko instrumentov moči. Instrumenti moči so ekonomsko, politično, vojaško, diplomatsko in informacijsko področje.

Kibernetska moč države ne pomeni le števila treniranih hekerjev, ampak vsoto vseh resursov in zmožnosti, kamor spadajo tudi koncepti za zaščito kritične infrastrukture in upravljanje interneta. Velika večina državnih zmožnosti ni pod državnim nadzorom, zato je potrebno uporabiti širši pogled (European parliament 2011, 15).

Betz in Stevens (2011, 44) sta prišla do ugotovitve, da je posamezna kibernetska moč sestavljena iz več različnih moči v kibernetskem prostoru. Ni nujno, da so vedno vse istočasno prisotne. Kibernetska moč ni nekaj novega, ampak se jo da povezati z že obstoječimi definicijami moči. Vse »moči« pa naj bi spadale v štiri skupine: obvezna/prisilna kibernetska moč, institucionalna, strukturna in produktivna. Prva oblika kibernetske moči je oblika direktne prisile s strani enega akterja v poskusu spremeniti vedenje, pogoje ali obstoj drugega z materialnimi ali nematerialnimi sredstvi. Prepričamo drugega, da se ravna po naši volji. Druga oblika je institucionalna kibernetska moč, ki izhaja iz posredne moči akterja s posredovanjem formalnih in neformalnih institucij (mediji). Tretja oblika je strukturna kibernetska moč, ki ohranja in vzdržuje strukture, v katerih se nahajajo akterji. Dovoljuje ali onemogoča določena dejanja v kibernetskem prostoru omrežne družbe. Sem so vključene prednosti in slabosti delovanja v kibernetskem prostoru, ki omogočajo posameznikom moč, ki je v nefizičnem prostoru nimajo. Produktivna kibernetska moč je temelj vseh ostalih kibernetskih moči, saj brez družbenih akterjev ni družbenih odnosov, skozi katere se manifestira moč. Produktivna moč se izraža v mehki moči, ki jo lahko dosežemo s pomočjo kibernetskega prostora (osvojitev glav in src). Promoviranje določenih idej, pogledov,

ideologij, mišljenj, opredelitev, ki lahko omejujejo ali olajšajo družbene dejavnosti (Betz, Stevens, 2011, 42−53).

Kibernetska moč je sposobnost doseči želene rezultate z uporabo med seboj povezanih informacijskih virov v elektronski obliki na področju kibernetike. Lahko se uporablja za dosego želenih izidov znotraj kibernetskega prostora in na drugih področjih izven njega (zrak, morje, kopno). Kibernetska moč je odvisna od infrastrukture, omrežja, programske opreme, znanja in usposobljenosti ljudi (Nye 2010).

Države lahko kibernetsko moč izvajajo na različne načine: skupaj z vojaškimi operacijami, skrito brez možne povezave z napadalcem, kot del kompleksnih vojaško-diplomatskih zaostrenj, ali posredno za dokazovanje vpliva in doseganje nacionalnih ciljev. Prevladujejo napadalne operacije in zaščita je možna le z zmanjševanjem ranljivosti (Hunker 2010, 4).

Kibernetska moč in kibernetska tehnologija sta na eni strani ključ do napredka, širjenja kolektivnega in individualnega bogastva, na drugi strani pa Ahilova peta zaradi vedno večje odvisnosti, ki nas dela ranljive (Fuerth v Kramer, Starr in Wentz 2009, 558). Kibernetska moč je lahko definirana enako, kot sta Clarke in Knake (2010, 148−149) definirala skupno vojaško kibernetsko moč, ki je skupek kibernetskih napadalnih in obrambnih zmogljivosti ter kibernetske odvisnosti, pri čemer moramo pri kibernetski odvisnosti vedeti, da gre za obseg, v katerem je ključna infrastruktura odvisna od omrežnih sistemov.

Kaj pomeni kibernetska moč, je torej še vedno stvar debate v mednarodnem okolju in tudi med posamezniki, ki se s tem področjem ukvarjajo. Kibernetska moč je razpršena med različne akterje, težko jo je ohranjati in nadzorovati. Za izoblikovanje kategorij in podkategorij, ki določajo kibernetsko moč, bom izhajala iz definicije, da je pod kibernetsko moč države možno šteti vse sposobnosti in resurse države, ki jih lahko le-ta uporabi za podporo lastnih političnih ciljev in interesov za vplivanje na kibernetski in nekibernetski prostor, pri čemer je potrebno poudariti, da kibernetske zmožnosti niso le v rokah države in pod njenim direktnim nadzorom in da je potrebno upoštevati tudi nedržavne akterje. Koncept kibernetske moči vsebuje tako možnost kibernetskega bojevanja kot kibernetsko zaščito.

3 KIBERNETSKA MOČ DRŽAV ČLANIC EU

Proučevanje kibernetske moči posamezne države lahko razdelimo na štiri glavne kategorije, ki so:

1. uporaba IKT v industriji

2. ekonomski in družbeni kontekst
3. tehnološka infrastruktura
4. pravni okvir (Economist Inteligence Unit 2011)

3.1 UPORABA IKT V DRŽAVAH ČLANICAH EU

Zadnja kategorija obravnava uporabo IKT v industriji, kamor so uvrščene podkategorije:

1. pametna omrežja
2. e-zdravje
3. naročila podjetij preko interneta
4. internetna naročila posameznikov
5. individualna uporaba internetnega bančništva
6. e-uprava in
7. inteligentni promet (Prirejeno po: Economist Inteligence Unit 2011)

3.1.1 Pametna omrežja

Pametna omrežja so po Evropski delovni skupini za pametna omrežja definirana kot elektroenergetska omrežja, ki lahko učinkovito integrirajo vedenje in ravnanja vseh porabnikov, ki so nanj priklopljeni – generatorji in potrošniki, da se zagotovi ekonomska učinkovitost in trajnostni sistem napajanja z nizkimi izgubami in visoko stopnjo kakovosti in varnosti oskrbe (European Commission). Razlika med današnjimi omrežji in pametnimi omrežji je, da slednje omogočajo bolj učinkovito porabo energije, zmanjšujejo stroške, zagotavljajo večjo zanesljivost, dostopnost, zmanjšujejo ranljivosti in vplive na okolje. Pametna omrežja temeljijo na dvosmerni komunikaciji (uporabnik-proizvajalec), ki vključuje nadzor, komunikacijo, avtomatizacijo, nove tehnologije in opremo (obnovljivi viri energije), ki omogočajo hitrejše odzivanje na zahteve po energiji in aktualne podatke o njeni porabi.

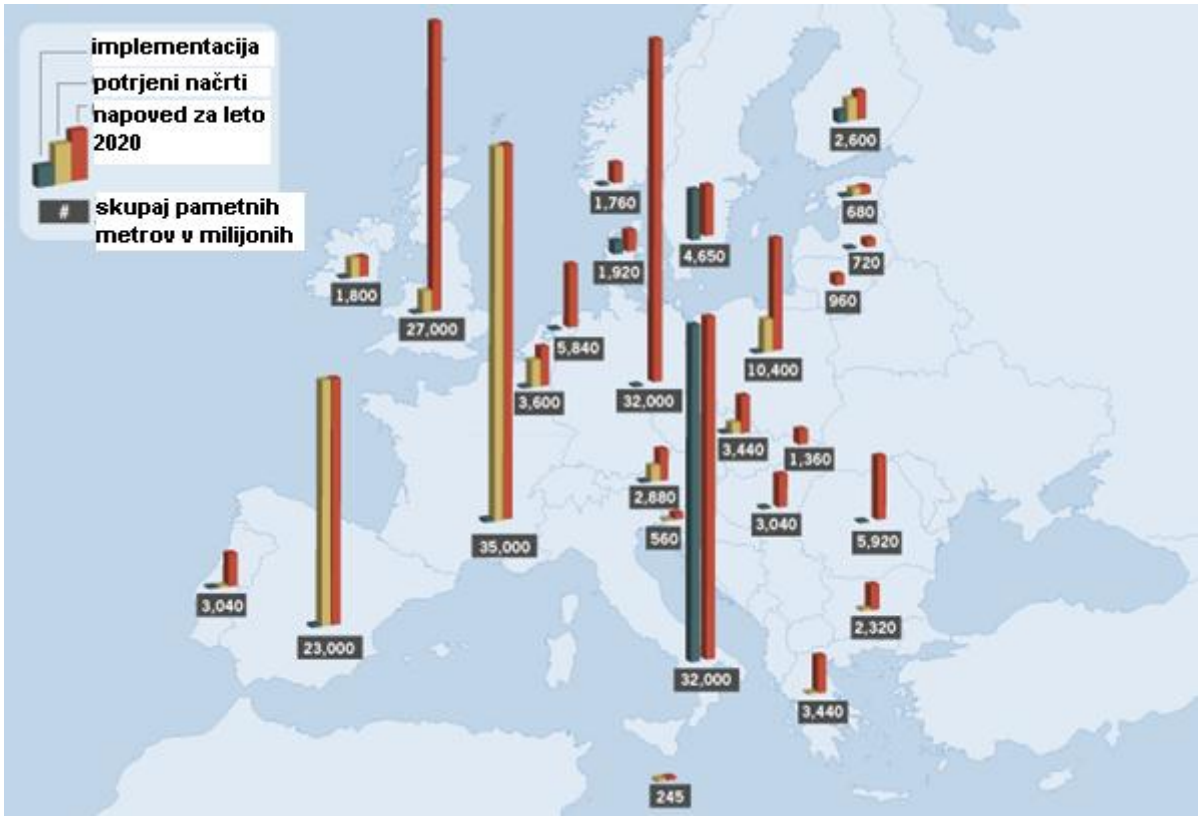
V Evropi je viden neenakomeren razvoj pametnih omrežij. Za razvoj pametnih omrežij EU daje okoli 184 milijonov evrov, večji znesek za razvoj pametnih omrežij v svetu najdemo v Južni Koreji, Avstraliji, Braziliji in na Japonskem (European Commission, Instute for Energy in Joint Research Center 2011).

Za kriterij, katera država ima najbolj razvita pametna omrežja, sem izbrala obstoj števila pametnih števcev v posamezni proučevani državi, ki zagotavljajo tekoče podatke z dvosmerno komunikacijo o uporabi energije v gospodinjstvih in lahko privedejo do zmanjšanja energijske porabe, ki je tudi cilj EU. Takšni števci lahko merijo porabo elektrike, vode ali plina in omogočajo trajnost s fleksibilnostjo vključevanja različnih virov energije.

Uporabniki imajo aktualne podatke o uporabi, prav tako pa lahko nadzirajo in prilagajajo porabo energije z nadzornimi programi, ki so povezani s pametnimi števci.

EU si je zadala cilj, da bo do leta 2020 80 % domov uporabljajo pametne števce. Večji porast v bližnji prihodnosti bo viden v državah, v katerih do zdaj ne najdemo večjega števila pametnih števcev, kot so Nemčija, Francija, Velika Britanija, Poljska in Španija. Število pametnih števcev v letu 2011 je na celotni ravni EU znašalo 45 milijonov. Število pametnih števcev je daleč najvišje v Italiji in na Švedskem (Geerth-Jan 2011).

Slika 3.1: Implementacija, načrti in napovedi števila pametnih števcev



Vir: Geerth-Jan (2011).

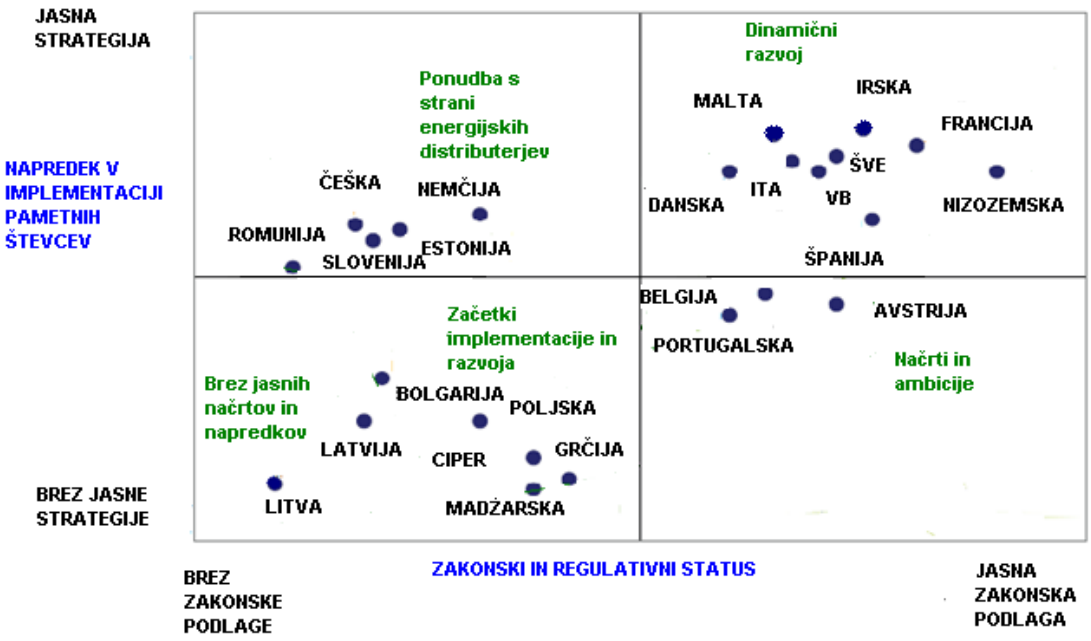
Dinamični razvoj tudi s pilotnimi projekti je viden na Danskem, v Franciji, Irski, Italiji, na Nizozemskem, Malti, v Veliki Britaniji, Španiji in na Švedskem. Brez zakonske podlage namestitve pametnih števcev s strani ponudnikov električne in druge industrije najdemo v Nemčiji, Estoniji, Češki, Sloveniji in Romuniji. Zakonski okvir je delno ustvarjen v Avstriji, Belgiji in na Portugalskem, ampak se zaradi nejasnosti pametni števci uvajajo le s strani ponudnikov energije. Bolgarija, Ciper, Grčija, Madžarska in Poljska spadajo v skupino, ki imajo interes za uvedbo pametnih števcev, ampak so priprave šele v začetnih fazah. Izmed proučevanih držav le v Litvi pametni števci niso stvar debate, v vseh ostalih, tudi če jih še ne

nameščajo, imajo vsaj poskusne pilotne projekte in načrte za vpeljavo v prihodnost (Intelligent Energy Europe 2011).

Odvisnost pametnih omrežij od IKT komponent, kot so računalniška omrežja, pametne naprave, nadzorni in distribucijski sistemi, operacijski sistemi in internet, vodi do družbenih ranljivosti zaradi možnosti zlonamernih napadov in motenjem dobave energije (ENISA 2012b). Polemike pri pametnih števcih se pojavljajo zaradi možnih napadov in vdorov glede na to, da pametni števci z distribucijskimi sistemi delujejo preko brezžičnih naprav, v katere je možno vdreti. Druga izpostavljena negativna stran pametnih števcev je tudi, da glede na to, da se meri trenutna poraba energije in so le-ti nameščeni izven hiš, lahko kriminalci vidijo po porabi energije, ali so ljudje v gospodinjstvih doma ali so odsotni, kar bi lahko vodilo do večjega števila vlomov.

Proučevane države se med seboj razlikujejo po načrtnih, pilotnih projektih, že uvedenemu številu pametnih števcev, kar pomeni, da je implementacija in zakonska podlaga kljub direktivi EU o uvedbi pametnih števcev še vedno različna.

Slika 3.2: Razvrstitev držav glede na implementacijo in zakonsko podlago pametnih števcev



Vir: prirejeno po Intelligent Energy Europe (2011, 10).

3.1.2 E-zdravje

Podkategorija e-zdravje proučuje obstoj ali neobstoj elektronskih zdravstvenih zapisov in podatkov o pacientih, shranjenih v računalniški obliki, ki omogočajo dostop do podatkov iz

različnih lokacij, hitrejše iskanje, izvajanje raziskav in obdelavo večjih količin informacij. Takšen sistem ima tudi pomanjkljivosti, saj je potrebno za uporabo zdravstvenih informacijskih sistemov ljudi izobraziti; izpostavljenost kibernetskega prostora in groženj, ki mu pretijo, ter stroški, potrebni za vzpostavitev zdravstvene informacijske elektronske infrastrukture. Podatki so za leto 2010 in možno je, da so države že izboljšale opisane razmere.

Razlike med proučevanimi državami so zelo velike, od tistih, ki so le pri načrtih in strategijah, do redkih izjem, ki imajo delujoči elektronski zdravstveni sistem. Posebne zakone glede e-zdravstva izmed proučevanih držav imajo Danska, Velika Britanija, Estonija, Francija in Švedska. Vse države pa imajo zakonsko poudarjene nujnosti in obligacije glede zagotavljanja varnosti in varovanja zasebnih podatkov. Večina držav torej nima sprejete legalne podlage za elektronske storitve v zdravstvu (EPSOS).

Danska strategija, ki je nastala prva izmed proučevanih držav, je iz leta 1996. Država ima elektronsko zdravstveno infrastrukturo najbolje izpeljano, saj ima elektronske zdravstvene zapise za vse prebivalce. Država izvaja e-recepte (elektronski recepti), kar pomeni, da se med zdravniki in lekarnami recepti prenašajo v elektronski obliki in da lahko pacienti prevzamejo zdravila v katerikoli lekarni ali celo pooblastijo druge osebe, da jih prevzamejo namesto njih samih. Izdaja e-receptov obstaja še v Estoniji in na Švedskem. Nizozemska, Italija, Španija in Portugalska jih uporabljajo le v določenih regijah držav, prav tako so v Veliki Britaniji v uporabi le v Angliji. Na zemljevidu, prikazanim nižje, je označena tudi Grčija, katere e-zdravstvo je pod evropskim povprečjem in v večini omejeno le na elektronsko shranjevanje zdravstvenih podatkov (European Commission 2011a in EPSOS).

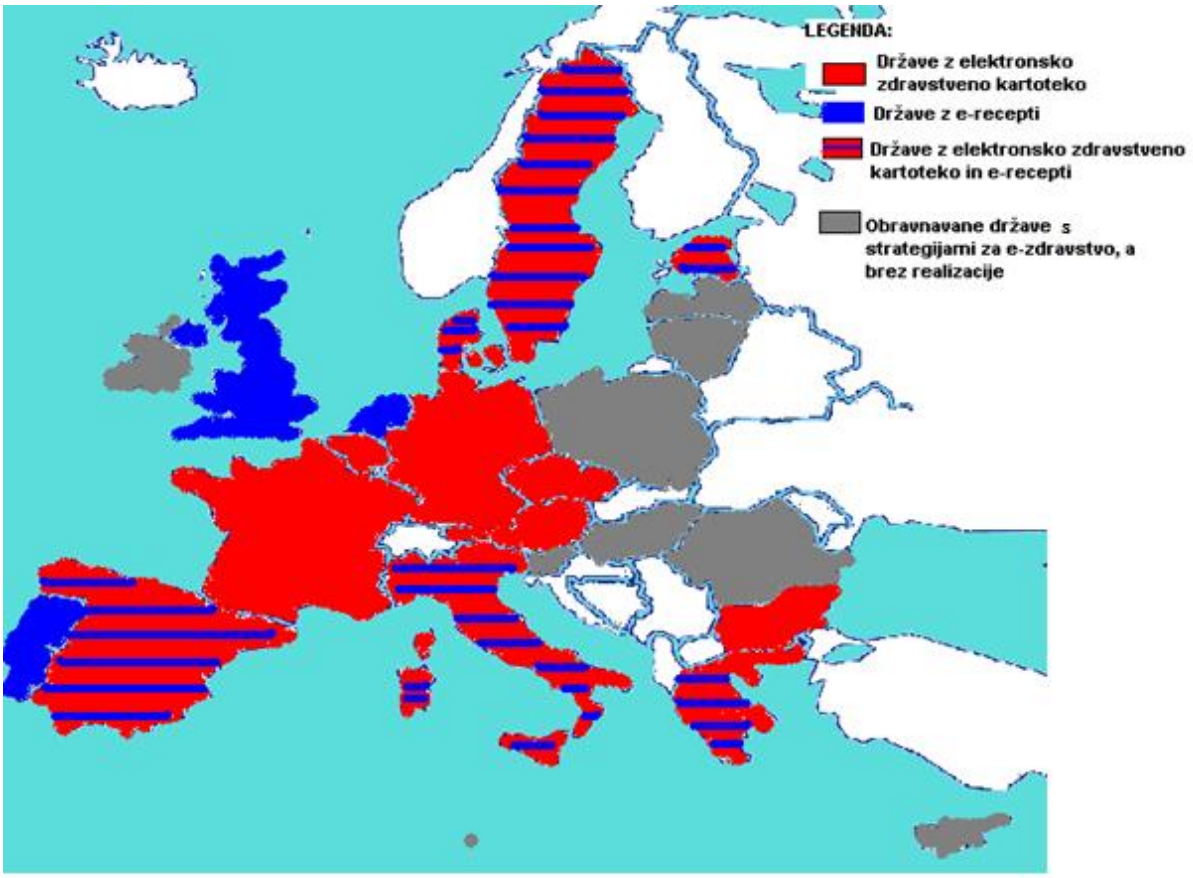
Elektronski zdravstveni zapisi pacientov so na ravni celotne države izpeljani le na Danskem, na Češkem je v elektronski obliki le del zdravstvenih podatkov, in sicer le za okoli 20 % prebivalstva. V Bolgariji, Franciji in na Nizozemskem je sistem v izdelavi in ne vključuje vseh podatkov prebivalstva. V nekaterih državah, kot so Španija, Estonija, Nemčija, Belgija, Francija in Italija morajo pacienti oddati pisno ali ustno soglasje, da se strinjajo z uvedbo osebne elektronske zdravstvene kartoteke. Shranjevanje teh podatkov je različno, po nekod centralizirano (Češka), decentralizirano (Nizozemska, Belgija, Španija) ali po individualni izbiri, kot je to v Franciji, kjer se lahko pacienti sami odločajo, pri katerem ponudniku bodo shranjeni njihovi osebni elektronski zapisi. Mobilno zdravstvo je v Evropi izjema in ne splošno pravilo, pri katerem lahko pacienti s kroničnimi boleznimi preko telefona dobijo recept. Poskusni sistem je v delovanju v Veliki Britaniji, na Švedskem in Danskem. V več državah pa implementacija ni mogoča zaradi zakonskih uredb, ki predvidevajo predhoden

pregled pri zdravniku, na primer v Avstriji, na Cipru in Madžarskem, pri čemer pa ne morem trditi, da mobilno zdravstvo ne obstaja zaradi neenotnosti zakonov, saj v Belgiji, Češki, Grčiji, Italiji in na Nizozemskem le-teh ni, prav tako pa ne obstajajo posebne regulacije za izvedbo telefonskega zdravstva (European Commission 2011a in EPSOS). V Sloveniji je e-zdravje slabo razvito, predvsem zaradi slabega informacijskega in dokumentacijskega sistema (RIS). Situacija je podobna na Cipru, kjer ne obstajata zakonska podlaga, zdravstveni informacijski sistem za uvedbo e-zdravstvenih kartotek ter e-receptov (Angelidis in drugi 2010), na Irskem zaradi premajhnega vlaganja in nezadostnega števila strokovnjakov za vzpostavitev zdravstvenega sistema (Artmann in drugi 2010c), v Romuniji (Artmann, in drugi 2010a), Litvi (Dumortier in drugi 2010) in Latviji (Artman in drugi 2010d). V Bolgariji e-recepti obstajajo le med določenimi zdravstvenimi ustanovami, prav tako obstaja telefonsko zdravstvo, a v zelo omejeni obliki, v državi pa še ni med seboj povezanega sistema, ki bi omogočal elektronske kartoteke pacientov (Artmann in drugi 2010b). Pri elektronski zlorabi zdravstvenih podatkov je le-ta lažje odkrita zaradi elektronskega odtisa, kot pa če nekdo gleda v tvojo zdravstveno kartoteko v papirni obliki.

Danes so preko telefonov in raznih mobilnih aplikacij možna različna merjenja zdravstvenih stanj, od krvnega tlaka do višine sladkorja od doma in nato posredovana zdravnikom, s čimer je možno trenutno spremljanje zdravstvenih razmer pacientov in lažje vodenje evidenc, prav tako se s tem zmanjšata delo in čakalne vrste v ambulantah.

Iz slike 3.3 je razvidno, da v 9 državah kljub načrtom ali strategijam elektronsko zdravstvo zaenkrat še ni v razvoju in ne obstaja, v šestih državah obstajajo elektronske zdravstvene kartoteke, v 3 državah se poslužujejo e-receptov ter v 6 državah obstaja tako elektronska zdravstvena kartoteka kot elektronski recepti. Elektronsko zdravstvo je v začetku razvoja na Irskem, v Romuniji, Sloveniji, Poljski, Malti, Madžarski, Litvi, Latviji ter na Cipru. Države z elektronsko zdravstveno kartoteko so Belgija, Francija, Nemčija, Avstrija, Češka in Bolgarija. Elektronski recepti obstajajo na Nizozemskem, Portugalskem in v Veliki Britaniji. Države z elektronsko zdravstveno kartoteko in e-recepti so Danska, Švedska, Italija, Grčija, Španija ter Estonija, pri čemer moram poudariti, da v Grčiji, Španiji in Italiji storitve elektronskih receptov obstajajo le v določenih predelih države in ne na celotnem ozemlju.

Slika 3.3: Elektronske kartoteke in e-recepti

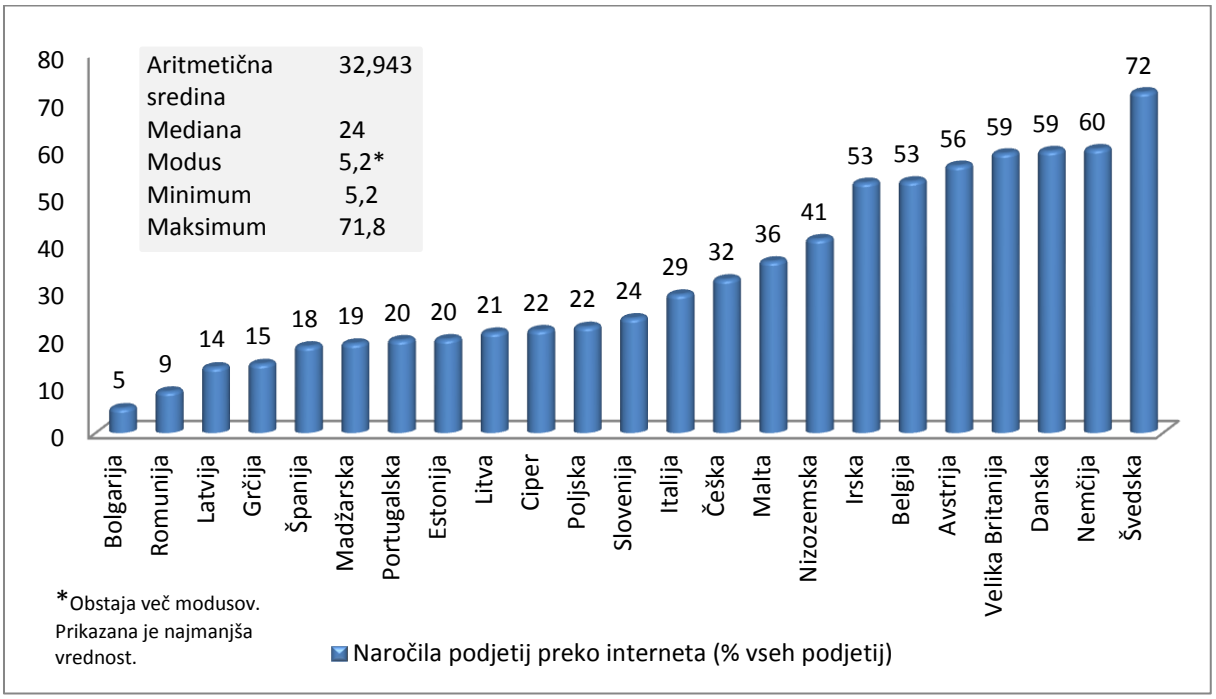


* Grčija, Španija in Italija imajo storitev e-receptov le v posameznih regijah in ne po celotni državi.

3.1.3 E-trgovina

E-trgovanje oziroma e-trgovina je prikazana s podatki o naročilih podjetij in posameznikov preko interneta ter uporabo spletnega bančništva. Slika 3.4 prikazuje odstotek podjetij v državi, ki so v določenem letu oddajala naročila preko spleta. Aktualnih podatkov v bazi ni bilo, zato sem uporabila podatke za leto 2007, razen za Francijo, za katero ni podatkov za nobeno leto. Podjetja na Švedskem, v Nemčiji, na Danskem, v Veliki Britaniji in Avstriji največ uporabljajo naročila preko spleta, saj je v vseh omenjenih državah več kot polovica podjetij v državah naročevala preko spleta. Najmanjši odstotek podjetij, ki naročajo preko spleta, najdemo v Bolgariji, Romuniji, Latviji, Grčiji in Španiji. Morebiti se je situacija že spremenila, saj za tekočo leto podatki niso bili dostopni (UNCTAD).

Slika 3.4: % vseh podjetij v državah, ki naročajo preko interneta

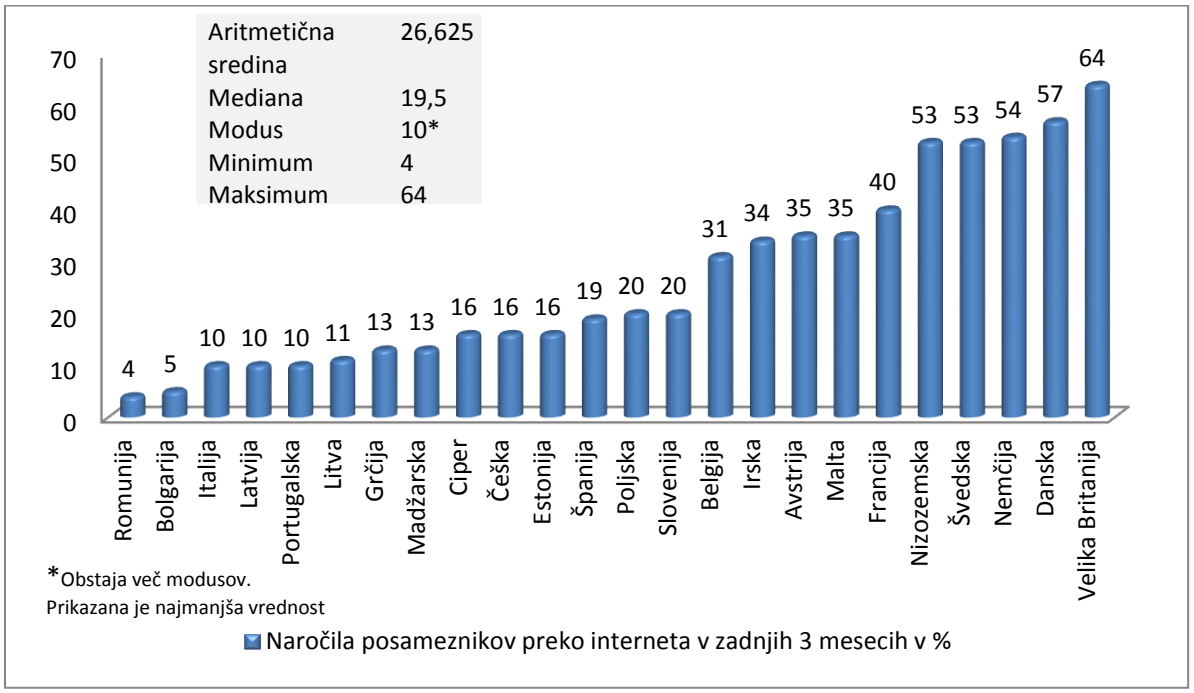


Vir: prirejeno po UNCTAD.

Naslednja tabela prikazuje naročila posameznikov preko spleta v zadnjih treh mesecih za leto 2011. Največ individualnih naročil v letu 2011 je bilo v Veliki Britaniji, kjer je kar 64 % posameznikov v zadnjih treh mesecih naročalo preko spleta, v peterici najvišjih odstotkov po individualnih internetnih naročilih so še Danska, Nemčija, Nizozemska in Švedska, kjer več kot polovica posameznikov naroča preko spleta. Najmanj internetnih naročil je bilo v Romuniji, Bolgariji, Latviji, Portugalski in Italiji, kjer odstotek ne znaša več kot 10 % (EUROSTAT).

Polovica prebivalcev EU kupujejo storitve in stvari na spletu (53 %) in okoli 20 % jih prodaja stvari in storitve. 29 % ljudi v EU nimajo zaupanja v spletne nakupe in spletno bančništvo. 69 % jih je dokaj zadovoljnih in v spletne nakupe tudi zaupa (European Commission 2012, 4).

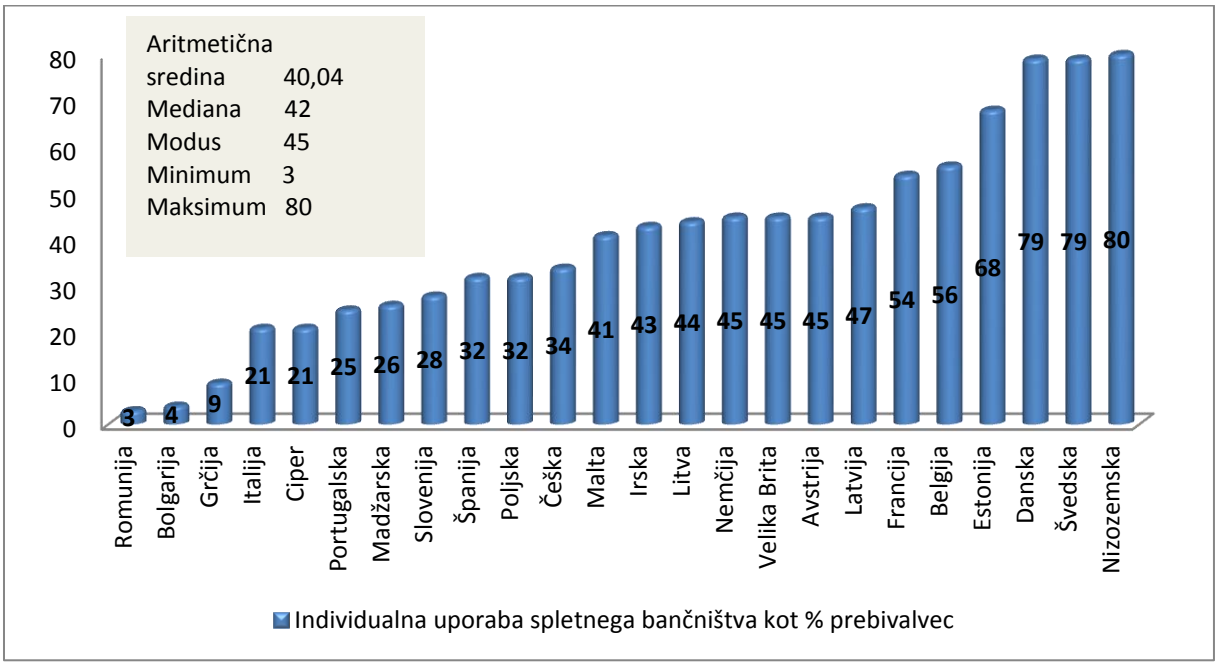
Slika 3.5: Internetna naročila posameznikov



Vir: EUROSTAT.

Individualna uporaba internetnega bančništva je prikazana kot odstotek prebivalstva v posamezni državi, ki uporablja spletno bančništvo. Podatki so za leto 2012, razen za Veliko Britanijo, za katero so podatki za leto 2010. Največ posameznikov se spletnega bančništva poslužuje na Nizozemskem, Danskem, Švedskem, v Estoniji in Belgiji. V teh državah od 80 do 56 % ljudi uporablja spletno bančništvo. Situacija je ravno obratna v Romuniji, Bolgariji, Grčiji, Cipru in Italiji, kjer se teh možnosti poslužuje le majhen odstotek prebivalcev (EUROSTAT).

Slika 3.6: Individualna uporaba spletnega bančništva



Vir: EUROSTAT.

Pomembno je tudi zaupanje, ki ga imajo ljudi v informacijsko komunikacijsko tehnologijo. Percepcija varnosti v EU na podlagi raziskave Eurobarometra kaže, da le 12 % uporabnikov interneta v EU meni, da so internetne transakcije popolnoma varne, 46 % pa da so varne, kar 42 % pa nima zaupanja v njih. Eden izmed desetih internetnih uporabnikov v EU verjame, da internetne transakcije niso varne in 43 % jih ne izvaja finančnih transakcij (Eurobarometer 2009). Pri uporabi spletnega bančništva in spletnih nakupov se pri ljudeh EU pojavljata predvsem skrb glede zlorabe osebnih podatkov ter varnosti spletnih transakcij (38 %) (European Commission 2012, 4).

3.1.4 E-uprava

E-uprava oziroma elektronska uprava je definirana kot uporaba interneta in svetovnega spleta za zagotavljanje upravnih informacij in storitev za državljane. Podkategorija meri kvaliteto, obseg in novosti upravnih spletnih storitev. Podatek 0 v tabeli predstavlja nizko stopnjo spletnih storitev in 1 visoko stopnjo upravnih spletnih storitev. Najboljše spletne storitve, pomoč, obrazce, participacijo državljanov, večjo transparentnost, razne baze, zakone, poročila, novosti in drugo imajo na Nizozemskem, v Veliki Britaniji, Danski, Franciji in na Švedskem. Najnižje upravne spletne storitve so v Romuniji, Bolgariji, Poljski, Češki in na Cipru. E-uprave so vseh državah skupek več portalov in ne enega samega, gredo pa v smeri

prenosa na računalništvo v oblaku, s čimer bi se zmanjšali stroški javne administracije. Vendar se še vedno porajajo dvomi glede varnosti, zasebnosti in regulacije (United Nations 2012 in United Nations Department of Economic and Social Affairs). E-uprava je pomembna ne samo zaradi obveščanja in storitev, ampak tudi povečuje odgovornost, produktivnost in transparentnost javnega sektorja (Economist Intelligence Unit 2011, 20).

Tabela 3.1: E-uprava

Države	E-uprava
Romunija	,6060
Bolgarija	,6132
Poljska	,6441
Češka	,6491
Ciper	,6508
Latvija	,6604
Grčija	,6872
Malta	,7131
Irska	,7149
Portugalska	,7165
Italija	,7190
Madžarska	,7201
Litva	,7333
Slovenija	,7492
Belgija	,7718
Španija	,7770
Avstrija	,7840
Estonija	,7987
Nemčija	,8079
Švedska	,8599
Francija	,8687
Danska	,8889
Velika Britanija	,8960
Nizozemska	,9283

Aritmetična sredina	0,748254
Mediana	0,7267
Modus	0,606*
Minimum	0,606
Maksimum	0,9283

*Obstaja več modusov

Vir: United Nations Department of Economic and Social Affairs.

3.1.5 Inteligentni transportni sistemi

Inteligentni transportni sistemi so napredne aplikacije, ki so – čeprav ne predstavljajo inteligence kot take – namenjene zagotavljanju inovativnih storitev na področju različnih vrst prevoza in upravljanja prometa, omogočajo boljšo obveščenost različnim uporabnikom ter bolj usklajeno in »pametnejšo« uporabo prometnih omrežij (Direktiva 2010/40/EU Evropskega parlamenta in Sveta, 3. člen). Pod inteligentnimi transportnimi sistemi se razume uporaba IKT na področju prometa. So sistemi, aplikacije in storitve v prometu, ki imajo velik potencial, da naredijo promet varnejši, učinkovitejši, bolj konkurenčen in trajnosten (Ministrstvo za promet 2010, 5).

Njegova vpeljava je pomembna zaradi števila žrtev v prometu, ki je v EU leta 2009 znašalo kar 34.826 žrtev samo v cestnem prometu; boljše načrtovanje in informiranje bi zmanjšalo zastoje v prometu za 20 % in število prometnih nesreč za 30 %; zaradi emisij, ki onesnažujejo okolje (v EU največ emisij CO2 v cestnem prometu – 70 % od vsega transporta) ter zaradi preobremenjenosti cestnega omrežja, ki povzroča večje stroške (European Commission 2011b).

Direktiva EU iz leta 2010 je pomemben inštrument za razvoj inovacij v inteligentnih transportnih sistemih v Evropi, katere cilj je usklajenost IT sistemov, pri čemer se lahko države same odločajo, v katere sisteme bodo vlagale. Prioritete so prometne in potovalne

informacije (javni prevozi in tarife) v realnem času, s čimer bo dosežena boljša informiranost, e-klic ter zagotavljanje storitev obveščanja glede varovanih parkirišč za tovornjake in komercialna vozila ter s tem povezane aplikacije, ki bodo omogočale informacije v realnem času, usklajenost in čezmejno povezanost. Primarni cilj inteligentnih transportnih sistemov je varnost. Glede na prioritetne omenjene cilje, ki jih direktiva izpostavlja, sem preverila, do katere mere so razviti inteligentni transportni sistemi v štiriindvajsetih proučevanih državah.

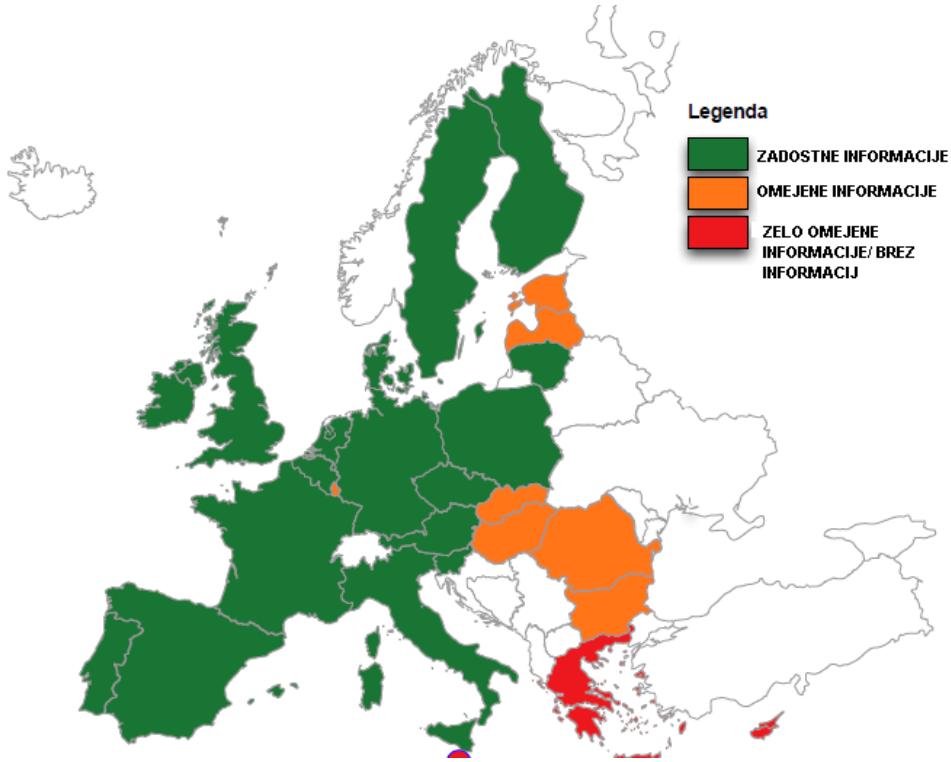
Tekoče potovalne informacije so informacije, ki jih lahko vozniki in potniki pridobijo in vsebujejo pomembne informacije, ki so vezane na varnost potovanja. Proučevanje obstoja tekočih potovalnih informacij zavzema dostopnost informacij na avtocestah ter sekundarnih cestah, podatke glede nevarnih vozišč, zmanjšani vidljivosti, ljudeh, živali in drugih ovirah na cestiščih, nezavarovana prizorišča nesreč, vremenske razmere, označbe kratkotrajnih del na vozišč ter mestna opozorila (European Commission 2013).

Proučevane države so uvrščene v tri skupine. V prvi največji skupini so tiste, kjer so prometne informacije v večini dostopne na pomembnejših in bolj prometnih cestah, v drugi skupini so države z omejenimi ali nejasnimi informacijami ter v zadnji skupini so države, kjer potovalne informacije ne obstajajo ali pa so zelo omejene. V skupini z omejenimi potovalnimi informacijami je Bolgarija, kjer ni znan način zbiranja informacij, le-te pa so posredovane voznikom preko zasebnih podjetij. V državi so podrobne informacije dostopne le v glavnem mestu Sofiji. V to skupino so uvrščene še Romunija, Estonija, Litva ter Madžarska. V teh državah je neznano ali obstajajo radio prenosi na nacionalni ravni glede potovalnih informacij ali pa so omejeni le na določene regije v državi. V nekaterih državah so različni sistemi v začetni uporabi oziroma v testni fazi. V zadnjo skupino so uvrščene Malta, Ciper ter Grčija. Na Cipru in Malti ne obstaja ne zasebni ne javni organ, ki bi zbiral potovalne informacije in jih nato preverjal ter nazadnje posredoval uporabnikom. V Grčiji je zbiranje podatkov v zasebnih rokah, storitve končnim uporabnikom pa ponujajo le zasebna podjetja. V prvo skupino spada ostalih 16 proučevanih držav, kjer imajo zasebne in javne institucije ter organe, ki zbirajo podatke in jih preko zasebnih ali javnih agencij (radio) posredujejo naprej uporabnikom. V večini držav obstaja vzporedno preverjanje potovalnih informacij, ki zagotavlja popolnejšo sliko realnih ter tekočih prometnih podatkov. V Litvi in Latviji ni bilo definiranega ponudnika, ki ponuja storitve končnim uporabnikom. V večini so podatki o potovalnih informacijah dostopni brez dodatnega plačila, preko radia, spleta, aplikacij ter navigacijskih sistemov (European Commission 2013).

Dinamično upravljanje prometa temelji na aktualnih cestnih podatkih, vozilih, z mobilnimi napravami, navigacijskimi sistemi, ki omogočajo bolj sproščeno in varnejšo

vožnjo. Za 90 % prometnih nesreč je odgovoren človek in ta delež se z IKT tehnologijo lahko zmanjša. Za ta kriterij sem pogledala, ali v državi obstajajo prometni nadzorni centri, ki prejemajo razne informacije iz raznih virov (tv, radio, internet, klicni centri, nadzor cestnih kamer) in jih nato posredujejo uporabnikom preko spremenljivih cestnih znakov. Nadzorni center glede potovalnih informacij obstaja v sedmih državah, in sicer na Danskem, Portugalskem, Nizozemskem, v Estoniji, Italiji ter v Sloveniji. V Litvi obstaja center, ampak so podatki posredovani le preko spleta. Kljub temu pa obstoj nadzornega centra, ki zbira vse informacije preko različnih virov, ni nujno edini dober način obveščanja in sporočanja uporabnikom aktualnih informacij in podatkov, saj na primer na Švedskem in v Nemčiji obstaja dobro obveščanje voznikov, kljub temu da takšen center ne obstaja. Informacije se v Nemčiji zbirajo na lokalnih ravneh v okviru zveznih dežel. Potovalne informacije so posredovane preko radia, telefonov (sms-i, aplikacijami), navigacijskimi sistemi, označbah na cestiščih, ki imajo vsaka svoje prednosti in slabosti (European Commission 2013).

Slika 3.7: Dostopnost potovalnih informacij, povezanih z varnostjo v prometu v Evropi



Vir: European Commission (2013, 16).

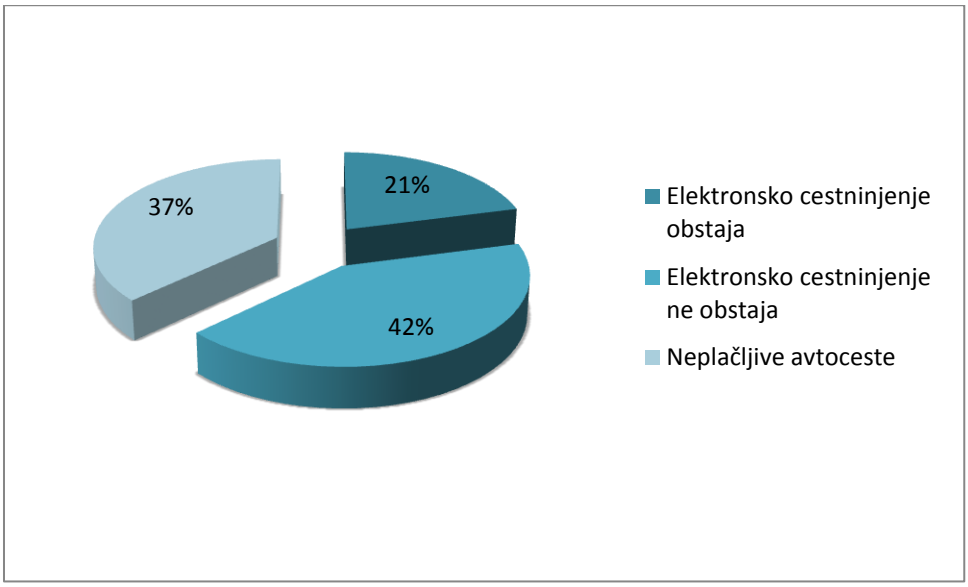
Elektronsko parkiranje temelji na eni zmed prioritet Evropske komisije glede razvoja inteligentnih transportnih sistemov, ki zagotavlja informacije o varnih parkiriščih, njihove kapacitete in zasedenost ter možnost rezervacij. Na ravni EU potekajo različni projekti, kot so EasyWay, LABEL in SETPOS, ki so v manjši ali večji meri financirani s strani EU. V okviru

projekta EasyWay so po državah članicah ustanovili dinamične informacijske centre glede parkiranja tovornjakov in komercialnih vozil. Ti centri nudijo informacije o zasedenosti varnih parkirišč, ki so v večini nastali v Italiji, Nemčiji in Franciji, kjer je zasedenost parkirnih mest ob prometnejših cestah tudi največja. Naslednji projekt je SETPOS, ki ga v 50 % financira EU, katerega cilj je gradnja novih varnih parkirišč. In nenazadnje projekt LABEL, ki ustvarja sheme za certifikat o varnih parkiriščih. Elektronsko parkiranje je v EU še v razvoju in je pomembno za zvišanje varnosti voznikov, ki se morajo zakonsko ustaviti po določenem času zaradi prenatrpanosti parkirišč ter ustavljanja izven parkirnih mest in s tem povezanim kriminalom (European Commission 2011c). Evropski center za študije o varnosti in analizah tveganja je prišel do sklepa, da lahko 44 izgub življenj in 1.430 poškodb na leto pripišemo parkiranju na nevarovanih območjih. Prav tako pa se s tem povzroča ekonomska škoda (European Commission 2011c, 8). Proučevane države v EU zaenkrat še nimajo povezanih sistemov glede elektronskega parkiranja tovornjakov in komercialnih vozil, kljub temu pa so v nekaterih državah vidni napredki v smeri razvoja centrov, gradnja novih varnih parkirišč in podeljevanje certifikatov o varnih parkiriščih (European Commission 2011c).

Elektronsko cestninjenje povečuje pretok prometa, ki mora temeljiti na interoperabilnosti preko nacionalnih meja. Za zmanjševanje onesnaževanja je predlagano, da plačana pristojbina temelji na vrsti vozila in njegovi emisiji. Elektronsko cestninjenje najdemo v Avstriji, Bolgariji, Češki, Romuniji in Sloveniji. V Belgiji, na Danskem, v Estoniji, Irski, Latviji, Nizozemskem, Švedski, Malti uporabo avtocest ni potrebno plačevati, V Litvi za osebne avtomobile uporaba avtocest ni plačljiva, pri uporabi kombijev in avtobusov, torej tovornih vozil, pa velja vinjetno cestninjenje. Prav tako v Nemčiji cestnine za osebna vozila ni, za tovorna pa obstaja glede na tip vozila. Na Poljskem se cestnina za avtoceste plačuje le na določenih avtocestah, obstaja elektronski sistem za tovorna vozila nad 3,5 ton na vseh hitrih cestah in avtocestah ob vnaprejšnji registraciji s pridobljeno napravo, ki omogoča elektronsko cestninjenje. Na Portugalskem se cestninjenje razlikuje, saj imajo tako elektronsko kot plačljivo z gotovino in kartico, odvisno od krakov avtocest. Različni sistemi obstajajo tudi v Španiji in Veliki Britaniji. Z gotovino ali kartico je potrebno plačevati v Franciji, prav tako imajo elektronsko cestninjenje s posebno kartico, na katero se ne nalaga dobroimetje, ampak dobimo račun za cestnino po pošti. V Grčiji ni elektronskega cestninjenja, prav tako v Italiji turisti in tujci ne morejo kupiti kartice TELEPASS, ki omogoča elektronsko cestninjenje in je zato potrebno plačevanje z gotovino ali kartico. Na Madžarskem imajo vinjete, ampak ne v obliki nalepk, in sicer v obliki potrdila, ki ga lahko kupimo tudi preko telefona (AMZS).

Iz slike 3.8 je razvidno, da v večini proučevanih držav elektronsko cestninjenje ne obstaja, pri čemer je potrebno vzeti v obzir, da med državami, ki so spodaj prikazane, kot da nimajo razvitega elektronskega cestninjenja, imajo le-tega razvitega na določenih predelih in regijah v državi, a ni operativen na celotnem ozemlju. Prav tako je sem šteta Italija, ki ima možnost elektronskega cestninjenja, a le za državljane. V kar 37 % proučevanih držav uporabo avtocest ni potrebno plačevati, pri čemer v večini ne plačljiva uporaba, velja le za zasebne avtomobile in ne za tovorne.

Slika 3.8: Obstoj/neobstoj elektronskega cestninjenja v proučevanih državah EU



Razvoj inteligentnih transportnih sistemov je viden tudi v naprednem sledenju in spremljanju različnih tovorov, kot je na primer sledenje nevarnih snovi in živih živali. Takšni sistemi so v EU razviti na lokalnih ravneh, kot v Španiji, vendar v nobeni državi na celotnem ozemlju ne obstaja delujoči sistem o opozarjanju oziroma sledenju nevarnega tovora. V Nemčiji podoben sistem glede transporta nevarnih snovi deluje v alpski regiji. Sistem naprednega sledenja in opozarjanja naj bi v prihodnosti temeljil na globalnem satelitsko navigacijskem sistemu Galilejo, ki ga gradita EU in Evropska vesoljska agencija in naj bi bil s svojimi 30 sateliti operativen do leta 2019. Z lastnim navigacijskim sistemom EU ne bi bila več odvisna od sistemov drugih držav, kot je ruski GLONASS, ameriški GPS in kitajski Kompas, ki so lahko onemogočeni v času konfliktov ali vojn.

Evropska komisija v okviru direktive 2010/40/EU o razvoju inteligentnih transportnih sistemov poudarja tudi prednosti razvoja e-klica, ki je avtomatski ali ročni klic reševalnim službam v primeru večjih nesreč, ki odda lokacijo nesreče in s tem zmanjša odzivni čas

nujnim službam do prihoda do nesreče, kar naj bi po izračunih vodilo do zmanjšanja števila žrtev za 5-10 %, kar pomeni okoli 25.000 življenj letno. E-klic omogoča prednosti voznikom v tujini in na domačih cestah, ki so jim neznane in ne poznajo natančno lastne lokacije nesreče, prav tako z e-klicem izginejo jezikovne ovire. Takšen klic bi v primeru nesreče poslal sporočilo o prometni nezgodi na enotno evropsko reševalno številko 112, ki nato omogoči prikaz lokacije javni varnostni točki, ki sprejema nujne klice. Hkrati bo operator imel možnost slišati, kaj se v avto dogaja in morebiti celo govoriti z voznikom in potniki, nato se bodo lahko na podlagi tega odločili, katere nujne službe so potrebne, ter sporočili cestno prometnim centrom o pripetljaju. Na podlagi prostovoljne uvedbe e-klica temelji tudi memorandum glede uvedbe e-klica v vozila (European parliament 2012). Memorandum je podpisalo 22 držav članic EU, in sicer med proučevanimi državami leta 2005 Grčija, Italija, Ciper, Litva, Slovenija, Švedska, v letu 2007 Avstrija, Nizozemska, Češka, Nemčija, Portugalska in Španija, v letu 2009 Estonija, v letu 2010 Malta, Danska, Romunija ter Belgija, v letu 2011 Madžarska in Latvija. Pismo o podpori sta izdali Bolgarija in Irska leta 2012 (Europe's Information Society Thematic Portal). Izmed proučevanih držav je 19 držav podpisnic, kar pomeni, da okoli 79 % proučevanih držav je podpisnic, 2 sta izrazili podporo, 3 pa niso podpisnice memoranduma o e-klicu. Nepodpisnice so Francija, Velika Britanija in Poljska.

3.2 EKONOMSKI IN DRUŽBENI KONTEKST DRŽAV ČLANIC EU

Za zagotavljanje kibernetske varnosti in s tem povečanje kibernetske moči potrebujemo kontinuirane investicije v znanje, izobrazbo ter v raziskave in razvoj. Prav tako so posamezniki dominantni akterji v kibernetskem prostoru, ki izvajajo, raziskujejo in špekulirajo kibernetske napade. Pri ekonomskem in družbenem kontekstu so podkategorije osredotočene na prebivalce in druge nedržavne subjekte, ki vplivajo na samo kibernetsko moč posamezne države, jo večajo ali manjšajo.

Podkategorije ekonomskega in družbenega konteksta so:

1. pričakovana doba šolanja
2. terciaren študentski vpis
3. raziskovalci v raziskavah in razvoju
4. število diplom iz znanosti in tehnologije
5. ozaveščenost prebivalstva
6. izvoz informacijsko-komunikacijske tehnologije
7. uvoz informacijsko-komunikacijske tehnologije

8. izdatki za raziskave in razvoj
9. vložitve domačih patentov (Prirejeno po: Economic Inteligence Unit 2011)

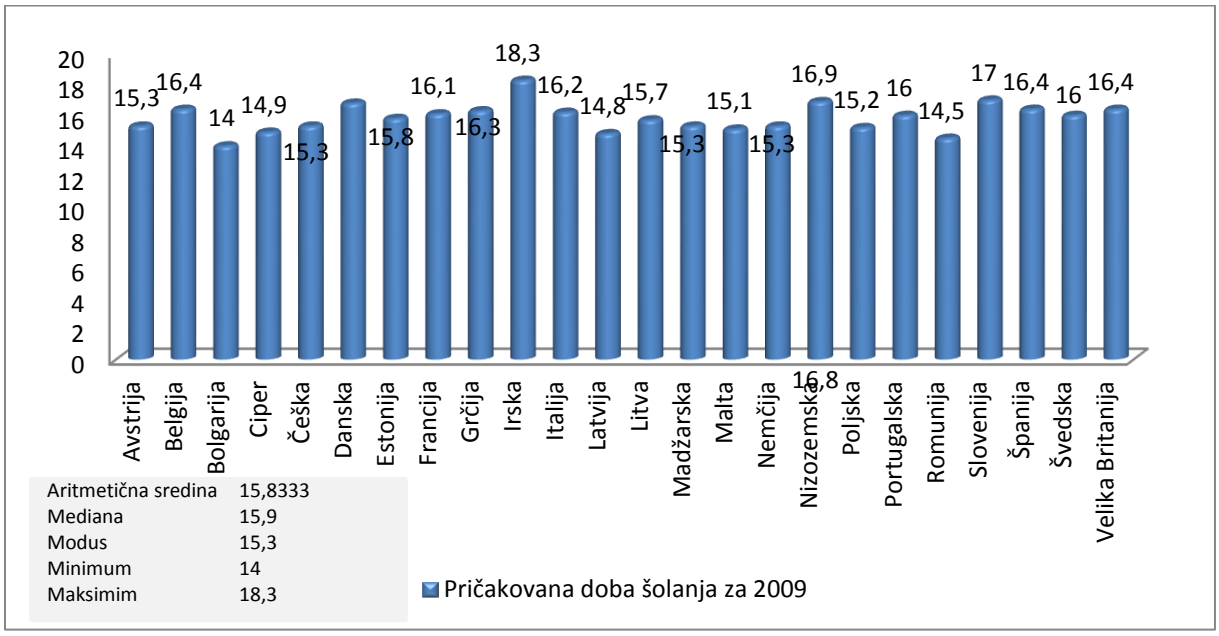
Pomembno vlogo igra tudi politični sistem, od katerega je odvisna stopnja internetne cenzure, ki je v totalitarnih in avtokratičnih državah večja. Ker bom obravnavala le nekatere države Evropske unije, kjer se politični sistem ne bo spreminjal, ga zato nisem uvrstila med podkategorije kibernetske moči, ki pa bi se moral upoštevati ob drugačni izbiri in primerjavi držav z različnim političnim sistemom. Treba pa se je zavedati, da cenzura obstaja tudi v proučevanih državah, na primer v Nemčiji in Avstriji zaradi nacizma. V ostalih državah pa lahko vidimo sovražni govor, ki se ga preganja na različne načine. O popolnoma svobodnem internetu in necenzuriranju torej ne moremo govoriti.

3.2.1 Izobrazba

Poleg investicij v nove tehnologije in njeno varnost so ravno ljudje s svojim znanjem, sposobnostmi in možnostmi za implementacijo determinanta uspeha ali neuspeha teh tehnologij. Pomembni so strokovnjaki na kibernetskem prostoru tako v javnem kot zasebnem sektorju. Zato pomembno vlogo igra izobrazba in usposabljanje posameznikov (Evans in Reeder 2010, 8). Terciarna izobrazba sledi sekundarni srednješolski izobrazbi. Zagotavljajo jo univerze in druge izobraževalne institucije. Višja izobrazba igra pomembno vlogo v družbi, saj ustvarja nova znanja, prenaša znanje in podpira inovativnost (EUROSTAT).

Izobrazba je prikazana s pričakovano dobo šolanja in število prebivalcev, vključenih v terciarno izobraževanje. Namen podkategorij je prikaz splošne ravni razvoja izobraževalnega sistema glede na povprečno število let šolanja. Pričakovana doba šolanja v članicah EU se giblje od 14 do 18,3 let, pri čemer je povprečna pričakovana doba šolanja 15,8 let. Najvišja pričakovana doba šolanja je na Irskem, v Sloveniji, na Nizozemskem, Danski in v Belgiji. Najnižjo pa najdemo v Bolgariji, Romuniji, Latviji na Cipru in Malti (UNESCO).

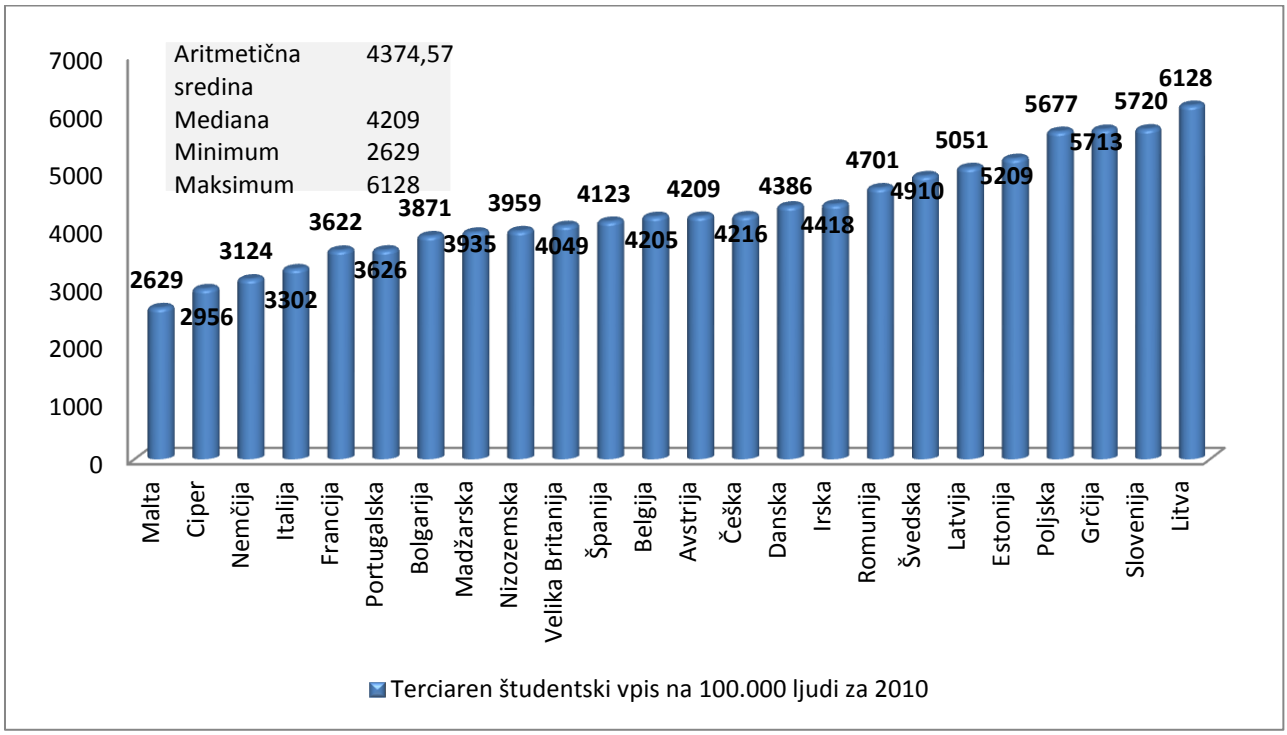
Slika 3.9: Pričakovana doba šolanja za leto 2009



Vir: prirejeno po Encyclopedia of the Nations, EUROSTAT, The World Bank in UNESCO.

Poleg pričakovane dobe šolanja je pomembno tudi, koliko prebivalcev je vključenih v terciarno izobraževanje. V samem vrhu po številu terciarnih študentskih vpisov na 100.000 ljudi so Litva, Slovenija, Grčija, Poljska in Estonija ter na dnu Malta, Ciper, Italija, Francija in Portugalska. Najmanjše število znaša 2629 ter največje 6128. Povprečje pa se giblje okoli 437,57 študentov na 100.000 prebivalcev (Encyclopedia of the Nations, EUROSTAT in UNESCO).

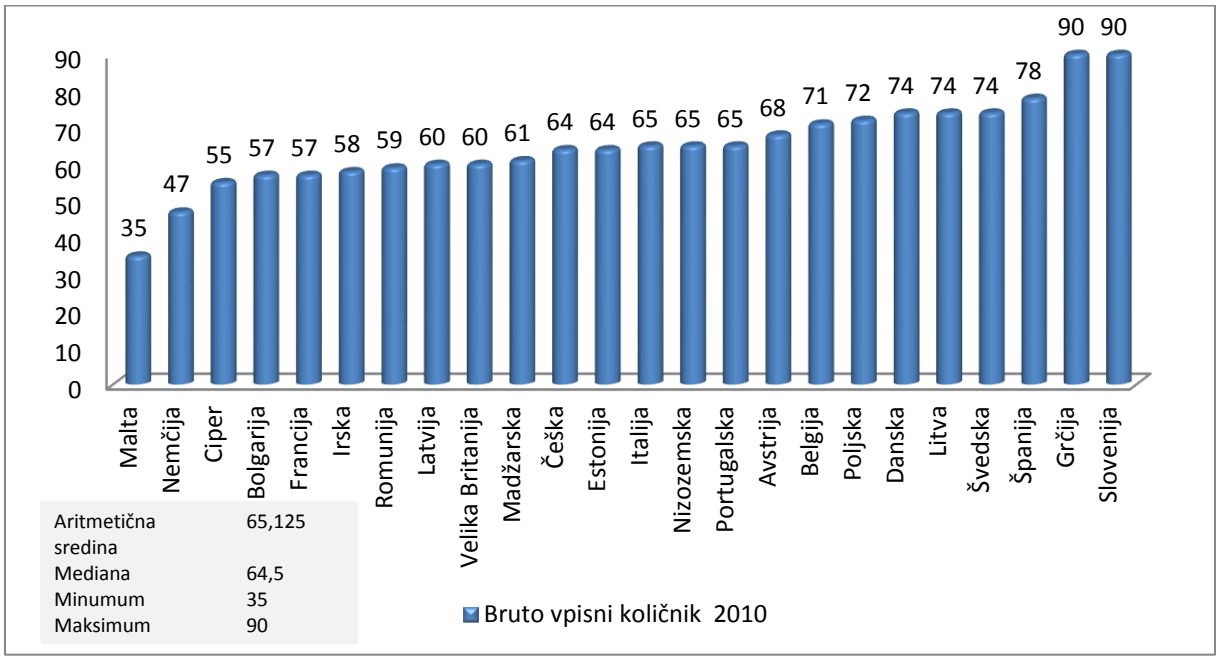
Slika 3.10: Terciaren študentski vpis na 100.000 prebivalcev za leto 2010



Vir: prirejeno po Encyclopedia of the Nations, EUROSTAT, The World Bank in UNESCO.

Za lažjo primerjavo in predstavo sem dodala še bruto vpisni količnik, ki prikazuje vse prebivalce, vpisane v terciarno izobraževanje, ne glede na starost, ki je izražen v odstotku celotnega prebivalstva petletne starostne skupine, ki zapušča sekundarno izobraževanje oziroma srednje šole. Najmanj srednješolcev se je po končani sekundarni stopnji vpisalo na terciarno na Malti, v Nemčiji, na Cipru, v Bolgariji in Franciji. Odstotki znašajo od 35 do 57, pri čemer je potrebno poudariti, da je podatek za Nemčijo neaktualen, saj je iz leta 1997, ker novejših podatkov nisem zasledila. Največ jih je izobraževanje nadaljevalo v Grčiji, Sloveniji, Španiji, na Danskem in Švedskem, pri teh je odstotek višji od 70 (Encyclopedia of the Nations, EUROSTAT in UNESCO). Pri naslednjem grafu moram dodati, da podatkov glede bruto vpisnega količnika za leto 2010 ni bilo mogoče dobiti za Dansko, podatki so iz leta 2009, za Grčijo, podatki so za leto 2007, za Irsko, podatki so za leto 2008 ter za Nemčijo, podatki so za leto 1997.

Slika 3.11: Bruto vpisni količnik v proučevanih državah EU za leto 2010



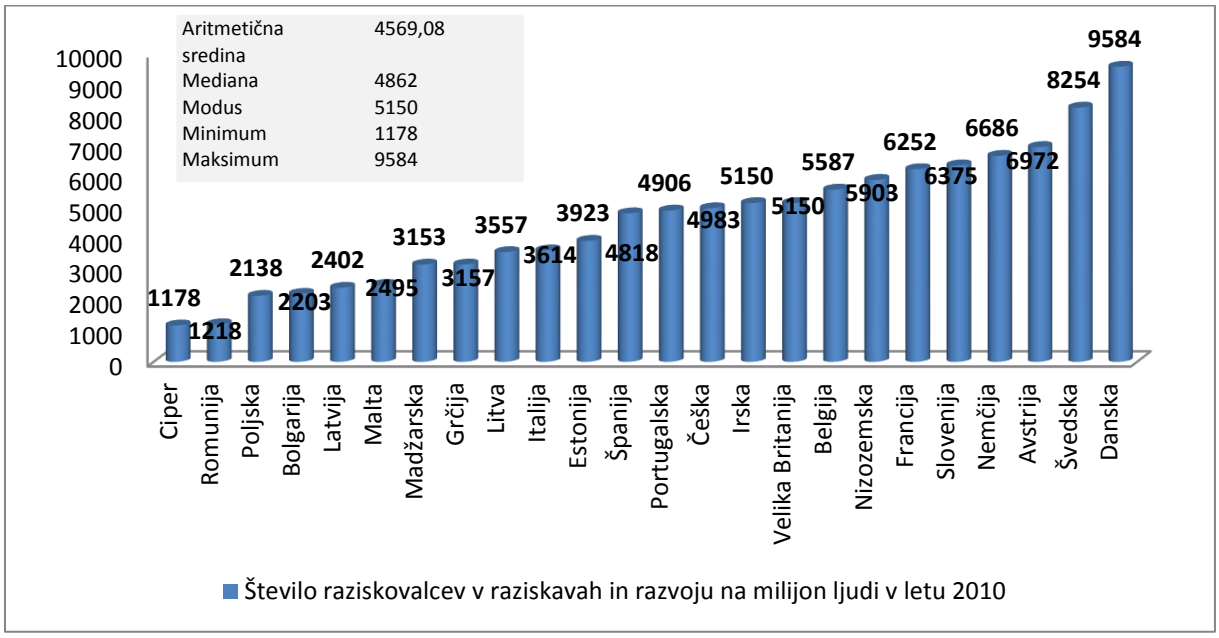
Vir: prirejeno po Encyclopedia of the Nations, EUROSTAT, The World Bank in UNESCO.

3.2.2 Tehnične kompetence prebivalcev

Tehnične kompetence prebivalcev posameznih držav se kažejo v številu raziskovalcev v raziskavah in razvoju ter številu podeljenih diplom iz znanosti. Število raziskovalcev in podeljenih diplom iz znanosti je izredno pomembno za zagotavljanje kibernetske varnosti s pomočjo usposobljenih ljudi s tehničnimi znanji za oblikovanje varnih sistemov, kodiranje, vzdrževanje sistemov in odzivanje na kibernetske grožnje (Evans in Reeder 2010).

Število raziskovalcev v raziskavah in razvoju je od države do države različno. V letu 2010 je bilo najvišje na Danskem, Švedskem, v Avstriji, Nemčiji ter Sloveniji. Najvišje število znaša 9584 ter najnižje 1178 raziskovalcev na milijon ljudi. Najmanj raziskovalcev najdemo na Cipru, v Romuniji, Poljski, Bolgariji in Latviji. Zaradi ne dostopnosti podatkov za vse države iz leta 2010 so podatki za Grčijo iz leta 2007 in za Francijo iz leta 2009 (UNESCO).

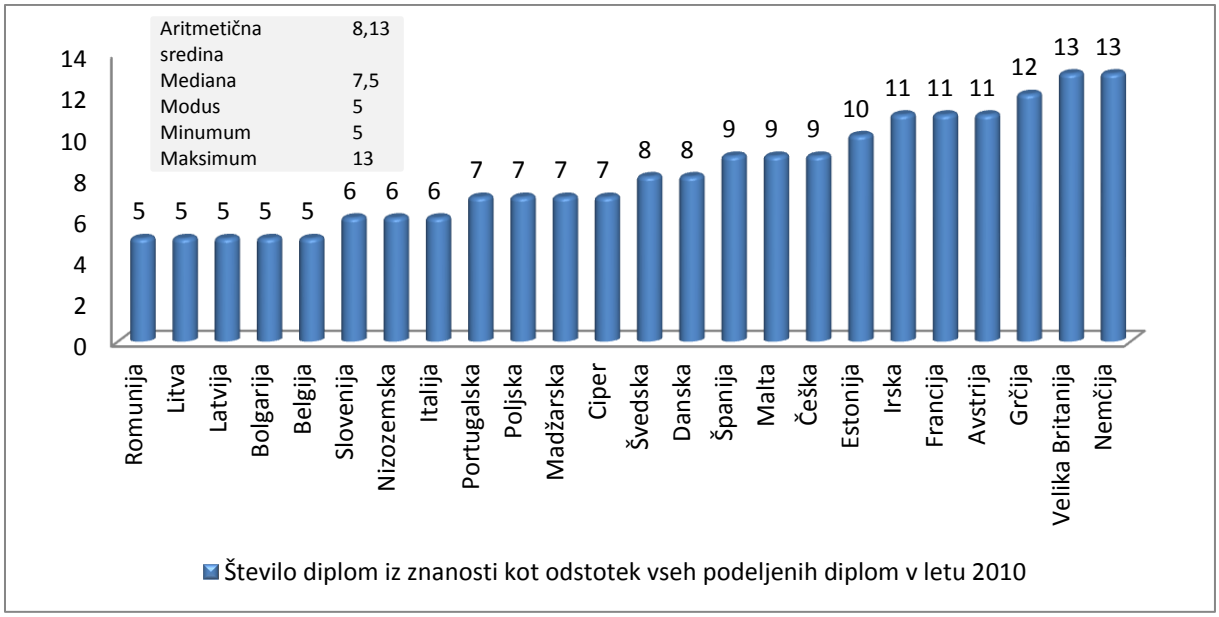
Slika 3.12: Število raziskovalcev v raziskavah in razvoju na milijon ljudi za leto 2010



Vir: prirejeno po OECD in UNESCO.

Največ podeljenih diplom iz znanosti v letu 2010 je bilo v Nemčiji, Veliki Britaniji, Grčiji, Franciji in Avstriji. Najmanj pa v Romuniji, Bolgariji, Litvi, Latviji in Belgiji. Podatki za Italijo so iz leta 2006 ter za Francijo iz leta 2009 (UNESCO).

Slika 3.13: Število diplom iz znanosti in tehnologije kot % vseh podeljenih diplom v letu 2010



Vir: prirejeno po OECD in UNESCO.

Tehnične kompetence so pri proučevanju drugih držav v državah v razvoju višje od evropskih, saj je v teh državah več diplom kot % vseh diplom na področju znanosti in tehnologije. Prav tako se zahod zaveda, da so ti strokovnjaki ključni za zasnovo varnih sistemov (Economist Intelligence Unit 2011, 13).

3.2.3 Ozaveščenost prebivalstva o kibernetskih grožnjah

Ozaveščenost prebivalstva o kibernetskih grožnjah in dojemljivost oziroma zaznavanje kibernetskih groženj je pomemben dejavnik, ki vpliva na individualno vedenje na svetovnem spletu, ki je pomemben dejavnik pri zagotavljanju kibernetske varnosti, saj je potrebno začeti pri posamezniku, ki se mora zavedati, kako ohranjati varnost tudi v virtualnem prostoru, ki lahko ima posledice tudi v realnem svetu. Za zagotavljanje kibernetske varnosti je pomembna družbena osveščenost o kibernetskem prostoru in grožnjah, ki jim pretijo, saj lahko bistveno zmanjšajo možnosti za kibernetski napad (Esterle, Ranck in Schmit 2005, 11).

Internetni uporabniki so po raziskavi Eurobarometra dobro seznanjeni s tipičnimi grožnjami, ki jim pretijo v kibernetskem prostoru, največ jih je seznanjenih z računalniški virusi, saj je delež v vseh proučevanih državah višji od 90 %. Kraje elektronskih gesel, uporabniških imen in kreditnih kartic se najbolj zavedajo v Nemčiji in Veliki Britaniji ter najmanj v Bolgariji, Romuniji in Belgiji. Nezaželeno pošto na Cipru, v Belgiji in Romuniji največ prebivalcev ne dojema kot varnostni problem. Distribuiranega internetnega napada se ljudje najmanj zavedajo v Bolgariji ter najbolj na Švedskem. V vseh državah se zavedajo možnosti zlorabe osebnih podatkov, saj povprečje znaša 90 % na ravni celotne EU. Velika večina jih zaradi tega uporablja varnostne ukrepe, kamor spadajo protivirusna programska oprema, filtri in požarni zidovi. 75 % jih verjame, da so sami osebno odgovorni za zagotavljanje lastne varnosti v kibernetskem prostoru. Spodnja tabela 3.2 v odstotkih prikazuje, koliko ljudi se zaveda določenih varnostnih problemov, ter odstotek ljudi, ki uporabljajo programsko zaščitno opremo (Eurobarometer 2009).

Tabela 3.2: Dojemljivost in zavedanje prebivalcev glede kibernetskih groženj

Države	Računalniški virusi kot varnostni problem	Zloraba osebnih podatkov kot varnosti problem	Nezaželena pošta kot varnostni problem	Distribuiran internetni napad kot varnostni problem	Uporaba zaščitne programske opreme
Avstrija	97,8	90	97,8	70	96,6
Belgija	92,6	73	91,2	67,8	94,8
Bolgarija	93,2	73	70,6	60,2	89,4

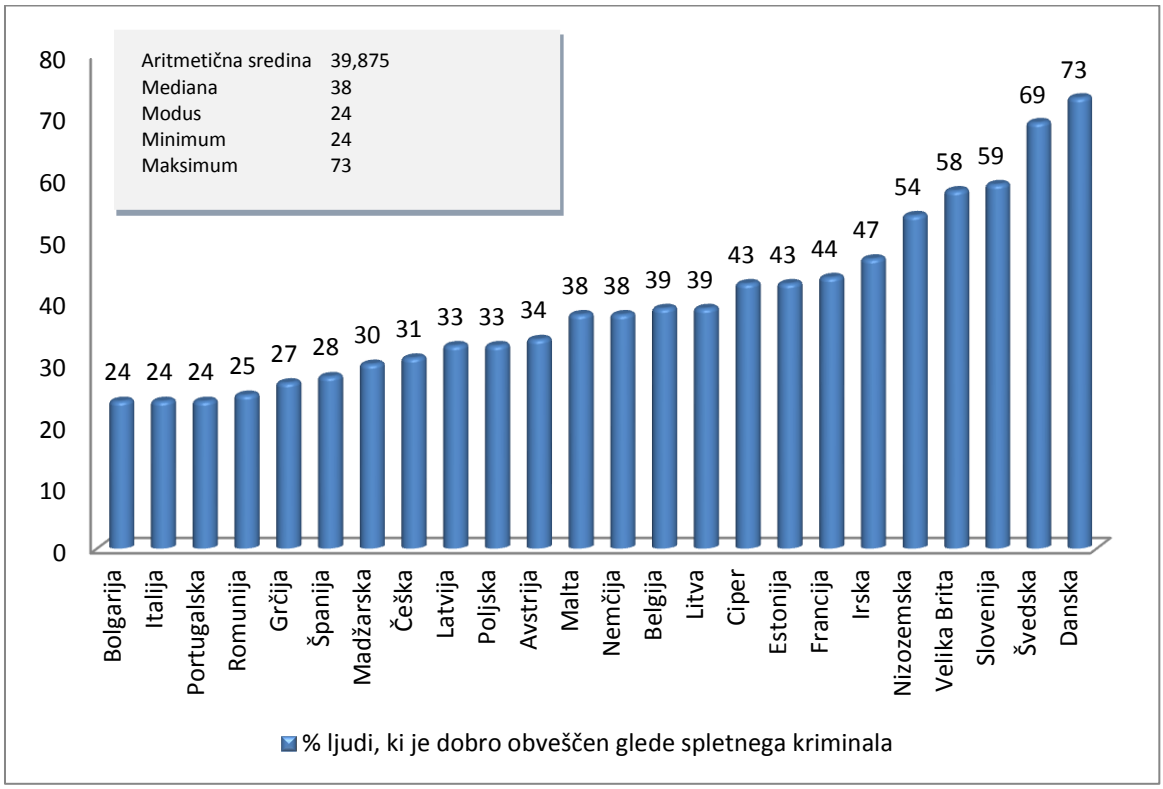
Ciper	91,2	89	67,2	77,6	82
Češka	98,6	78	89,6	77,1	95
Danska	94,2	81	93,4	78,4	94,4
Estonija	97	88	93,4	83	92,4
Francija	97	85	94,6	86,5	98,2
Grčija	95,8	89	76,8	73,5	93
Irska	89,6	85	90,6	76	92,6
Italija	98,8	92	91,6	74,1	96,2
Latvija	98,8	85	87,3	75,6	91,7
Litva	96,4	87	84,6	74,6	93
Madžarska	99,4	91	93	74,1	93,2
Malta	99,6	91	97,2	87,7	96,8
Nemčija	98,4	93	98,2	85	95,4
Nizozemska	96	88	96,8	82,5	97,2
Poljska	95,2	93	92,5	81,6	90,9
Portugalska	97,6	96	97,8	93,1	98,4
Romunija	91,6	69	73,6	66,6	85,4
Slovenija	98,2	92	95,8	83,6	95,2
Španija	93,6	92	92	79,1	95,4
Švedska	97,8	92	97,2	88,6	94,4
Velika Britanija	98,2	97	98,8	80,8	97,4

Vir: prirejeno po Eurobarometer (2009).

Seveda pa percepcije varnosti in dojemljivost groženj še ne odraža dejanskega stanja, zato je potrebno pregledati tudi tehnološko infrastrukturo in njeno uporabo v posameznih državah.

Iz spodnjega prikaza slike 3.13 je razvidno mnenje prebivalcev proučevanih držav EU o tem, ali menijo, da so dobro obveščeni glede spletnega kriminala. V povprečju 39 % prebivalcev meni, da je o tej temi dobro ozaveščena, več kot polovica, da je o spletnem kriminalu premalo obveščena. Ljudje so s to temo najbolj seznanjeni na Danskem, Švedskem, v Sloveniji in Veliki Britaniji. Najmanj o tej temi po lastnih mnenjih o tem vedo v Bolgariji, Italiji, na Portugalskem, v Romuniji in Grčiji.

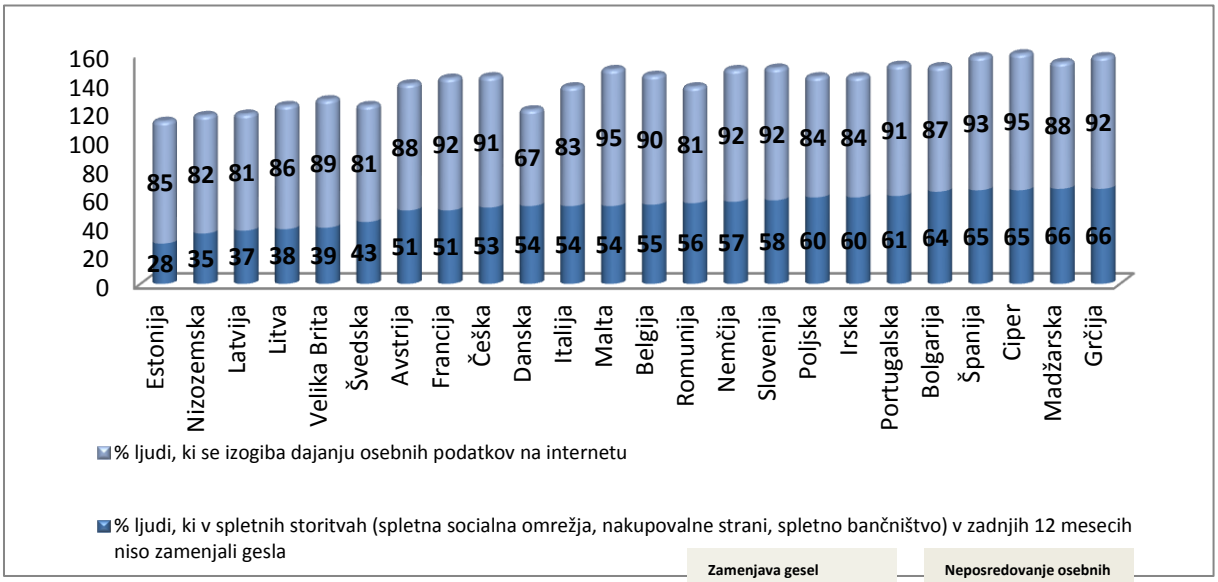
Slika 3.14: Obveščenost prebivalcev glede spletnega kriminala



Vir: prirejeno po European Commission (2012).

Individualno vedenje na spletu pomembno vpliva na posameznikovo varnost, predvsem na varstvo njegovih podatkov, zato sem dodala tudi naslednji prikaz, ki kaže, v kolikšni meri se ljudje izogibajo dajanju osebnih podatkov na internetu, ter ali so zamenjali gesla v spletnih storitvah v zadnjih 12 mesecih.

Slika 3.15: Individualno vedenje na internetu



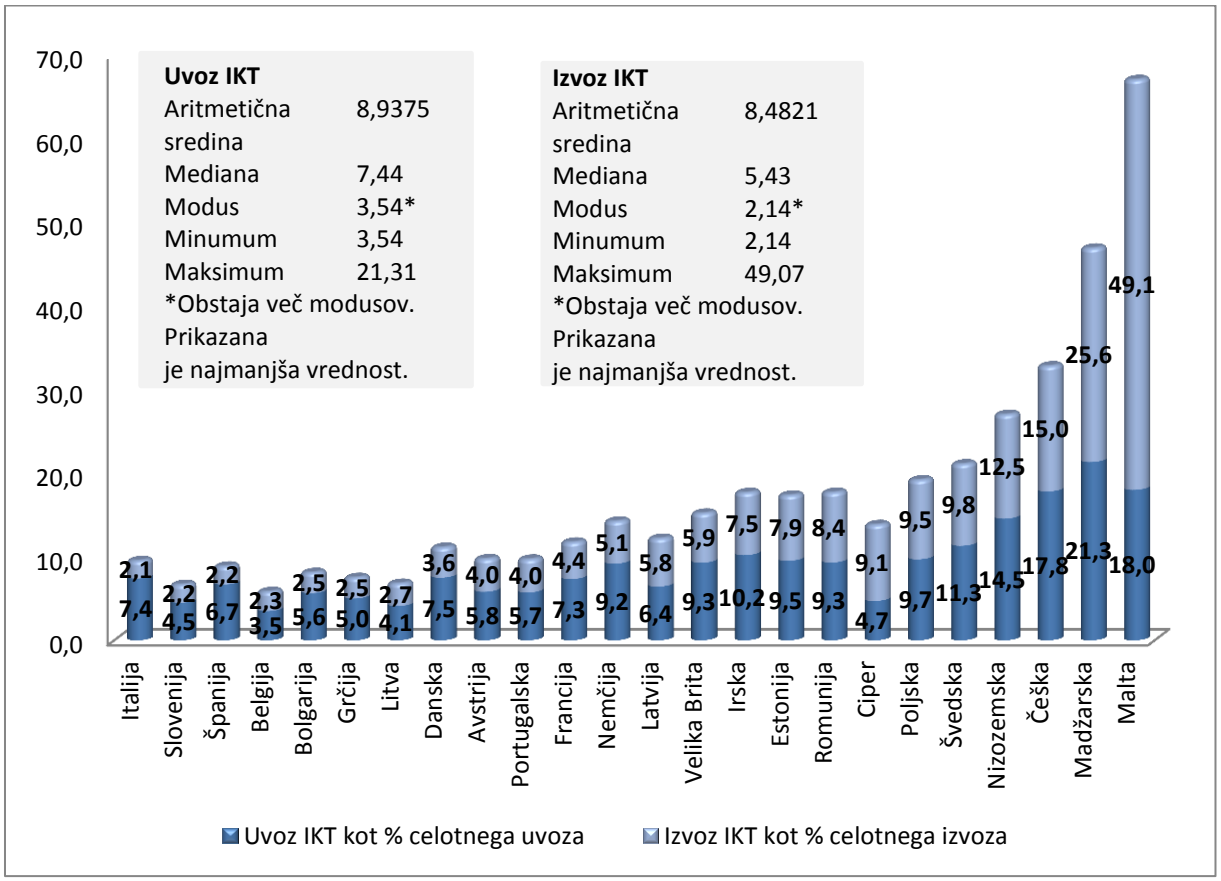
Vir: prirejeno po European Commission (2012).

3.2.4 Trgovanje

Naslednja podkategorija, ki določa področje trgovanja, je izražena z izvozom in uvozom IKT tehnologije. Prikazani podatki za izvoz in uvoz informacijsko-komunikacijske tehnologije so za leto 2010. Izraženi pa so kot odstotek celotnega izvoza in uvoza posameznih držav. V uvoz in izvoz je všteto blago za obdelavo informacij in komunikacij z elektronskimi sredstvi, avdio, video in računalniška oprema ter elektronske komponente. Podatki ne vključujejo programske opreme (UNCTAD).

Največ IKT tehnologije izvozijo Malta, Madžarska, Češka, Nizozemska in Švedska. Že med petimi največjimi izvoznicami je velika razlika, saj na Malti IKT izvoz znaša kar 49 % celotnega izvoza in na Švedskem okoli 9 %. Najmanj IKT izvozijo v Italiji, Sloveniji, Španiji, Belgiji in Bolgariji, pri čemer je najmanjši odstotek v Italiji in znaša 2,14 %. Pri uvozu IKT so največje uvoznice iste države kot pri izvoz, pri čemer je zamenjan le vrstni red, saj je na prvem mestu Madžarska, sledijo ji Malta, Češka, Nizozemska in Švedska. Situacija je podobna tudi pri državah, ki uvozijo najmanj IKT, pri čemer med petimi najmanjšimi deleži uvoza IKT ni Italije. Vrstni red od najmanjšega do največjega deleža pa je Belgija, Litva, Slovenija, Ciper in Grčija (UNCTAD).

Slika 3.16: Izvoz/uvoz IKT držav članic EU kot % celotnega izvoza/uvoza



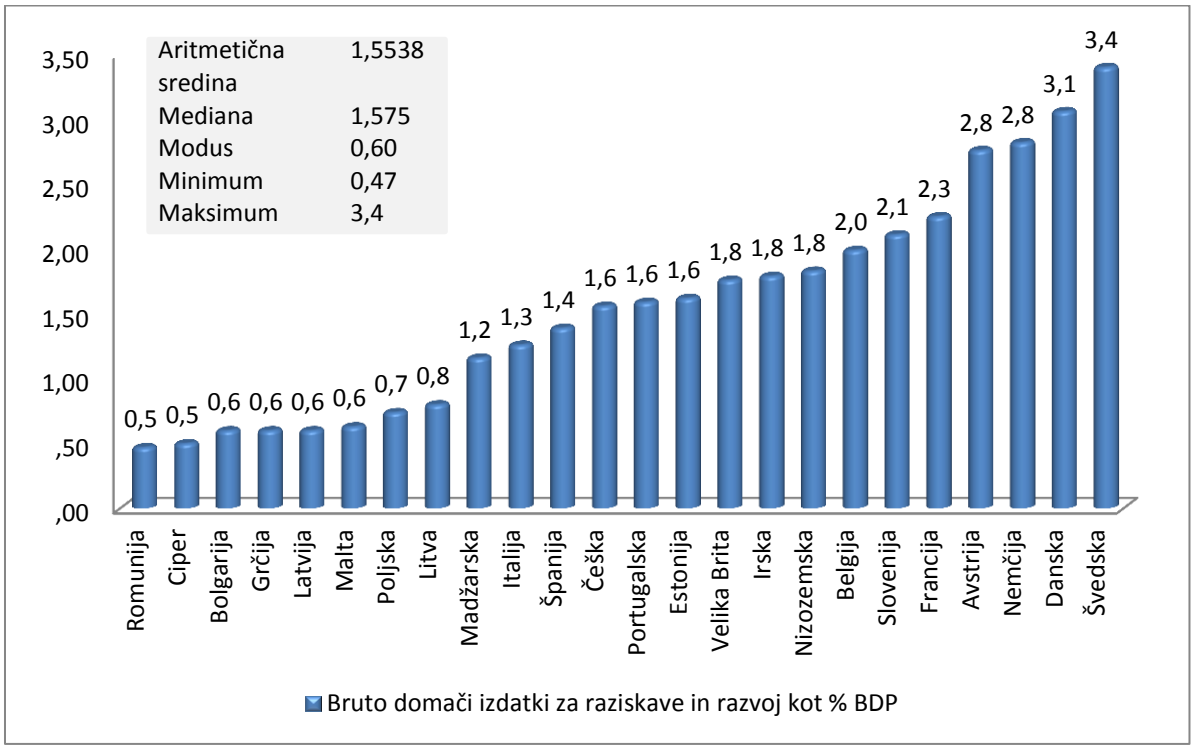
Vir: prirejeno po UNCTAD.

3.2.5 Inovacije

Inovacijsko ozračje v državah je izraženo s podatki o izdatkih za raziskave in razvoj, ki so prikazani z bruto domačimi izdatki za raziskave in razvoj kot odstotek BDP. Podatki so za leto 2009 za vse države razen za Grčijo, za katero so podatki iz leta 2007 (UNESCO).

Največ za raziskave in razvoj namenjajo na Švedskem, Danskem, v Nemčiji, Avstriji in Franciji. Najvišji odstotek BDP, namenjen za raziskave, je znašal 3,4 ter najmanjši 0,6 %, povprečje pa znaša 1,5 %. Najmanj denarja za to področje gre v Romuniji, na Cipru, v Bolgariji, Latviji in Grčiji, kar je prikazano na naslednjem točkovnem grafu.

Tabela 3.3: Bruto domači izdatki za raziskave in razvoj kot odstotek BDP



Vir: prirejeno po UNESCO.

Intelektualna lastnina, še zlasti patenti, zagotavljajo povezavo med inovacijami, izumi in trgom. Zahtevek za patent pomeni, da bo izum dostopen javnosti ob hkratnem nudenju njegove zaščite. Število vloženih patentov je eno izmed meril inovativne dejavnosti posamezne države in pokaže sposobnost izkoriščanja znanja, kar privede do možne gospodarske rasti (EUROSTAT). Patent je izključna pravica fizične ali pravne osebe za izum, ki je nov, na inventivni ravni in je industrijsko uporabljiv (Urad Republike Slovenije za intelektualno lastnino). Število domačih vloženih patentov sem prikazala na podlagi povprečja vloženih domačih patentov od leta 1997 do 2011. Največje povprečno število vloženih patentov 57.422 je v Nemčiji, sledijo ji Velika Britanija, Francija, Nizozemska in Italija. Najnižje pa 31 na Malti, ki ji sledijo druge države z najmanjšim številom vloženih domačih patentov Ciper, Estonija, Litva in Latvija (World Intellectual Property Organization).

Tabela 3.4: Povprečno število domačih vloženih patentov od 1997. do 2011. leta

Države	Povprečno število vloženih domačih patentov od 1997 do 2011 leta
Malta	31
Ciper	33
Estonija	44
Litva	89
Latvija	158
Bolgarija	276
Portugalska	282
Grčija	292
Slovenija	357
Češka	720
Madžarska	796
Irska	1110
Romunija	1135
Belgija	1763
Poljska	2459
Avstrija	2504
Danska	2632
Španija	3654
Švedska	5337
Italija	7286
Nizozemska	7663
Francija	17584
Velika Britanija	23240
Nemčija	57422

Aritmetična sredina	5702,78
Mediana	1122,83
Modus	31*
Minimum	31
Maksimum	57422

*Obstaja več modusov.
Prikazana je najmanjša vrednost.

Vir: prirejeno po World Intellectual Property Organization.

3.3 TEHNOLOŠKA INFRASTRUKTURA ČLANIC EU

Tretja kategorija je tehnološka infrastruktura, brez katere kibernetski prostor ne bi obstajal, in vsebuje naslednje podkategorije:

1. internetna razširjenost
2. razširjenost mobilne telefonije
3. brezžične dostopne točke
4. razširjenost spletnih družabnih medijev
5. naročniki širokopasovnih linij
6. cena mobilne telefonije
7. cena širokopasovnega interneta
8. izdatek za informacijsko tehnologijo
9. varnost strežnikov
10. število kibernetskih vdorov (Prirejeno po: Economist Inteligence Unit 2011)

V primerjavi z ekonomskim in družbenim kontekstom je kategorija tehnološke infrastrukture veliko bolj spremenljiva, saj se nenehno pojavljajo inovacije na vseh tehnoloških področjih, ki so nujno potrebne za boj proti nenehno spreminjajočim se kibernetskim grožnjam. Hitre spremembe so vidne tudi pri naraščanju številu prebivalstva, ki je v letu 1995 zajemalo le 0,4 % svetovnega prebivalstva, v letu 2012 pa okoli 34 % (Internet World Stats).

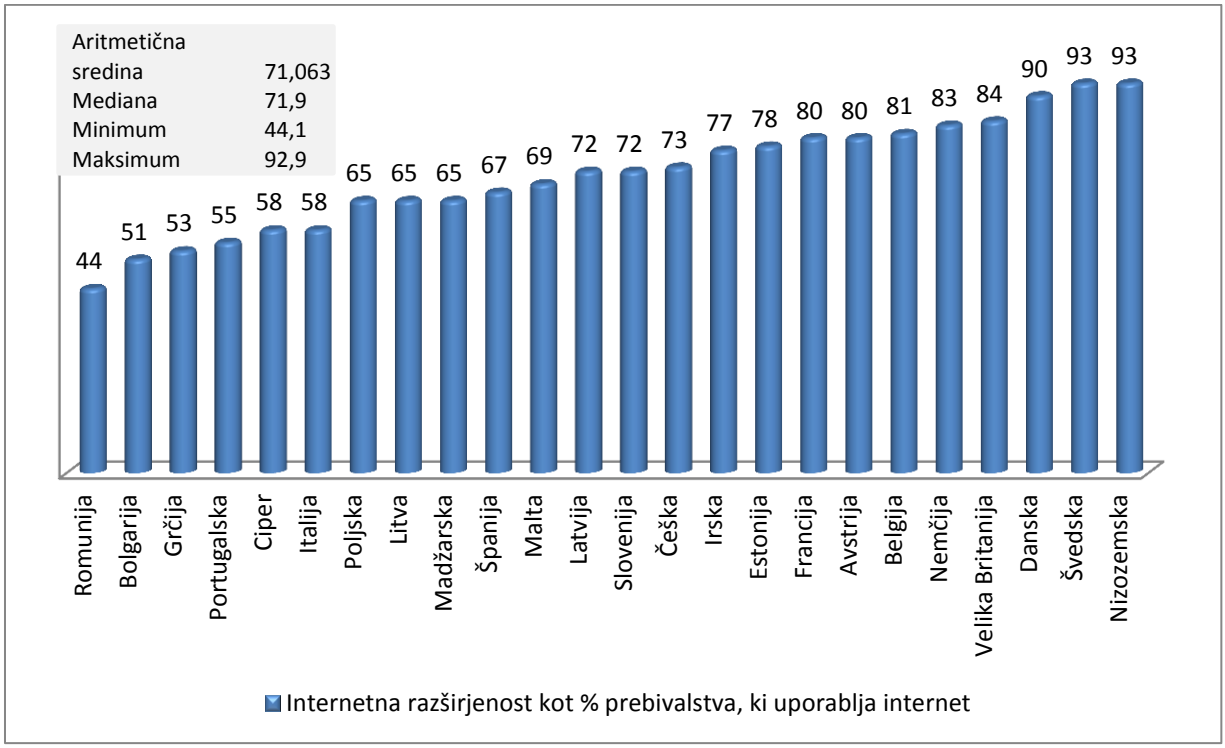
3.3.1 Dostopnost tehnologije

Dostop do tehnologije je prikazan s kategorijami: internetna ter mobilna razširjenost, število vročih točk, razširjenost družbenih medijev ter mesečne cene internetne ter mobilne telefonije.

Število internetnih uporabnikov je v letu 2012 znašalo okoli 2,4 milijarde. V Evropi je v letu 2012 internet uporabljalo 63 % vseh prebivalcev, večji odstotek najdemo na svetu le še v Severni Ameriki in Avstraliji. V Evropski uniji in 27 njenih članicah je odstotek še višji in znaša 73 %. Je pa naš kontinent nad svetovni povprečjem, ki znaša dobrih 34 %. Internetna razširjenost v proučevanih državah je merjena v odstotkih prebivalcev, ki uporabljajo internet. Internet je najbolj razširjen glede na odstotek prebivalcev na Nizozemskem, Švedskem, Danskem, v Veliki Britaniji in Nemčiji. Najmanj pa v Romuniji, Bolgariji, Grčiji, na Portugalskem in Cipru. Najvišji odstotek prebivalcev, ki uporabljajo internet, je 92,9 %, najnižji pa 44,1 % (Internet World Stats).

Več kot polovica prebivalcev EU dostopa do interneta najmanj enkrat na dan (53 %), manjšina (29 %) interneta ne uporablja. Vsi uporabniki dostopajo do svetovnega spleta doma (95 %), 39 % iz službe, 16 % med gibanjem ter 11 % v šolah in univerzah. Večina jih uporablja stacionarni računalnik ali prenosni računalnik, 24 % jih dostopa do interneta s pametnimi telefoni in 6 % preko tabličnih računalnikov (European Commission 2012, 4).

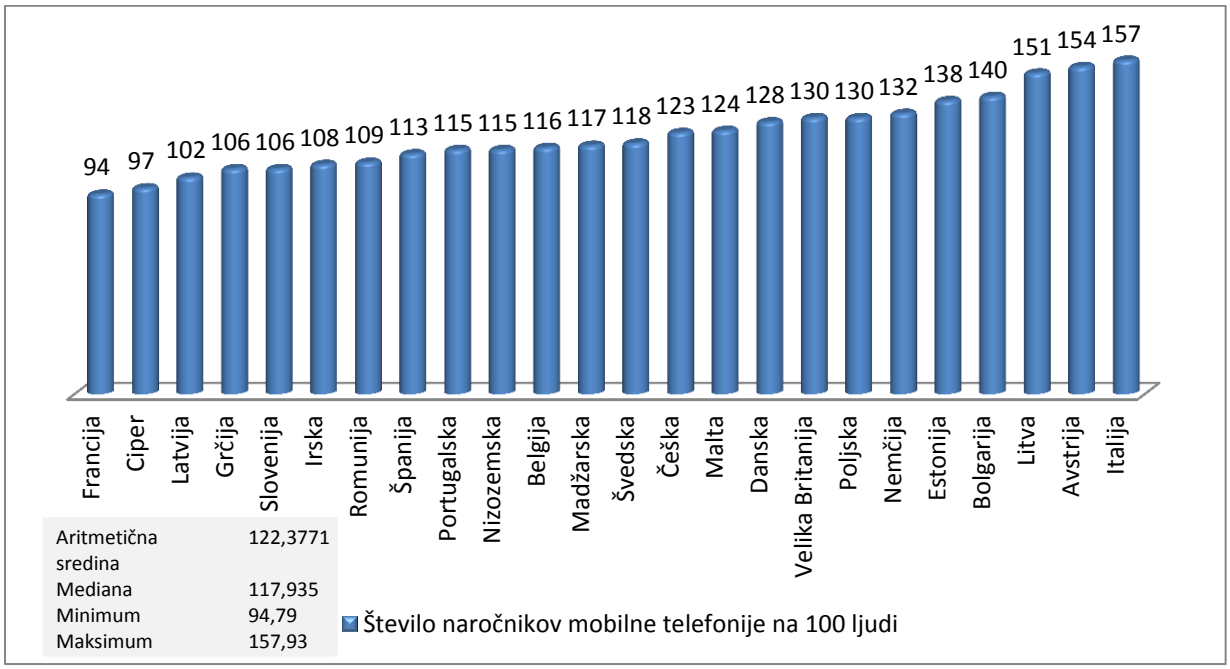
Slika 3.17: Internetna razširjenost



Vir: prirejeno po International Telecommunication Union in Internet World Stats.

Razširjenost mobilne telefonije je predstavljena kot število naročnikov mobilne telefonije na 100 ljudi za leto 2011. Na koncu istega leta je število naročnin na svetovni ravni doseglo skoraj 6 milijard. V 105 državah na svetu je število naročnin večje od števila prebivalcev, a je viden trend svetovnega zmanjševanja. V proučevanih državah je najmanjše število naročnikov mobilne telefonije v Franciji, Cipru, Latviji, Grčiji in Sloveniji, pri čemer je potrebno poudariti, da število naročnin že pri tretji državi z najmanjšim številom mobilnih naročnin na 100 ljudi kaže, da je na 100 ljudi več kot 100 naročnin. Največ naročnikov je v Italiji, Avstriji, Litvi, Bolgariji in Estoniji (International Telecommunication Union). V državah OECD je trend prevladovanja mobilnih naprav, kot so pametni telefoni in druge naprave s 3G omrežjem v primerjavi z namiznimi računalniki, kar je še posebej pomembno za sodelovanje v digitalni ekonomiji manj razvitih držav, v katerih nimajo dobro razvite informacijsko komunikacijske infrastrukture (The Economist Intelligence Unit 2011, 16).

Slika 3.18: Razširjenost mobilne telefonije



Vir: prirejeno po International Telecommunication Union in Internet World Stats.

Brezžične dostopne točke sem poiskala s pomočjo JiWire baze, ki ima lokacije brezplačnih in plačljivih brezžičnih točk v 145 državah (JiWire). Iz tabele 3.5 je razvidno, da je največ brezžičnih dostopnih točk v Veliki Britaniji, Franciji, Nemčiji in na Švedskem ter najmanj v Estoniji, Litvi, Bolgariji in na Malti. Brezžične dostopne točke se od države zelo razlikujejo, saj v Veliki Britaniji, ki je na prvem mestu, število znaša 182.629 in v Estoniji, kjer jih je najmanj 7.

Tabela 3.5: Število brezžičnih točk

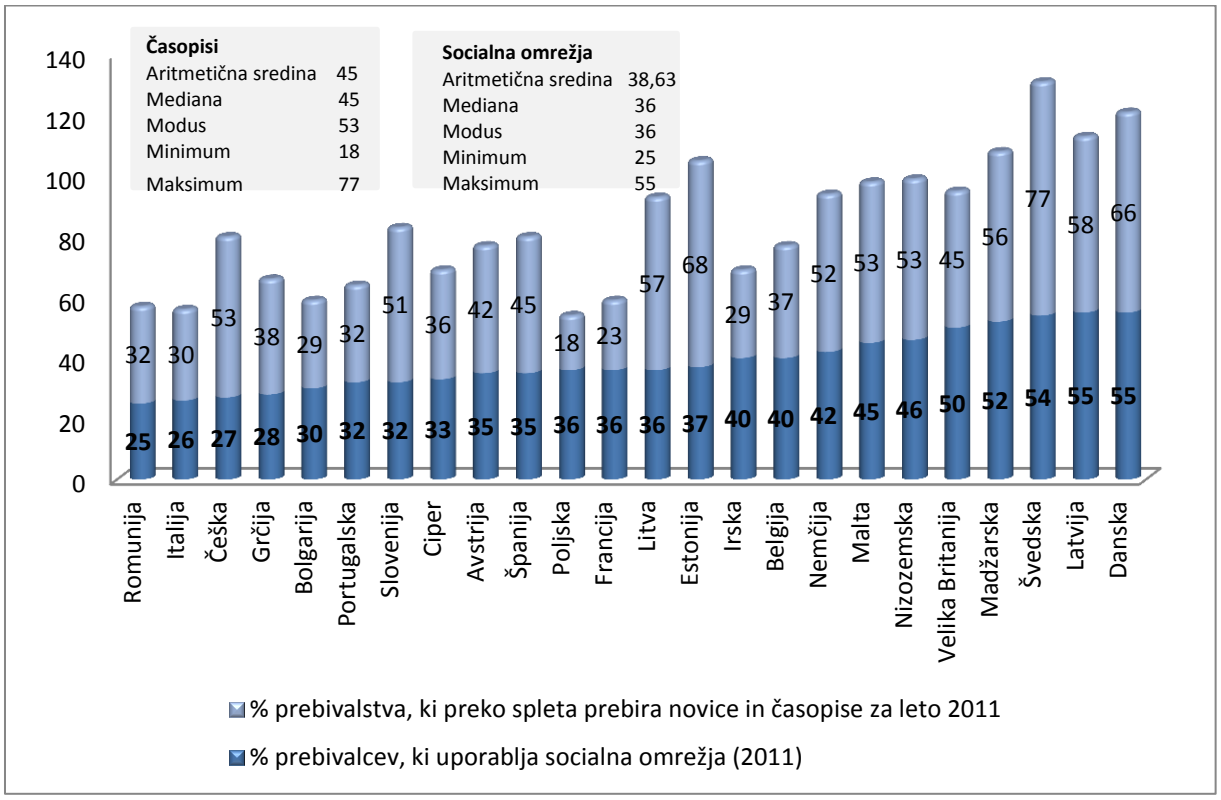
Države	Število brezžičnih točk
Estonija	7
Litva	17
Bolgarija	33
Malta	33
Slovenija	76
Ciper	121
Latvija	235
Češka	414
Romunija	448
Poljska	467
Grčija	535
Madžarska	879
Avstrija	962
Danska	1494
Irska	2514
Belgija	2539
Portugalska	3127
Nizozemska	3570
Španija	5177
Italija	5279
Švedska	9546
Nemčija	15092
Francija	35431
Velika Britanija	182629

Aritmetična sredina	11276,04
Mediana	920,5
Modus	33
Minimum	7
Maksimum	182629

Vir: JiWire.

Družbeni mediji igrajo pomembno vlogo tudi v kibernetskem prostoru, ki se je pokazala tudi v tako imenovani arabski pomladi. Z družbenimi mediji lahko ljudje z majhnimi vložki širijo svoje ideje in opisujejo dogodke mimo uradnih državnih institucij, prav tako pa omogočajo komuniciranje po vsem svetu ter lažjo dostopnost do informacij, s čimer je svet postal tako imenovana »globalna vas«. Razširjenost socialnih omrežij je prikazana kot odstotek prebivalcev, ki uporabljajo družbene medije, kot so Facebook in Twiter. V letu 2011 je več kot 50 % prebivalcev na Danskem, v Latviji, na Švedskem, Madžarskem in v Veliki Britaniji uporabljalo socialna omrežja. Najmanjšo uporabo najdemo v Romuniji, Italiji, na Češkem, v Grčiji in Bolgariji, kjer manj kot 30 % prebivalstva uporablja socialna omrežja. V več kot polovici proučevanih državah polovica prebivalcev bere novice in časopise kar preko spleta, ki ponekod nadomeščajo tradicionalne medije, kot so časopisi (EUROSTAT).

Slika 3.19: Razširjenost socialnih omrežij in prebiranje novic in časopisov preko spleta

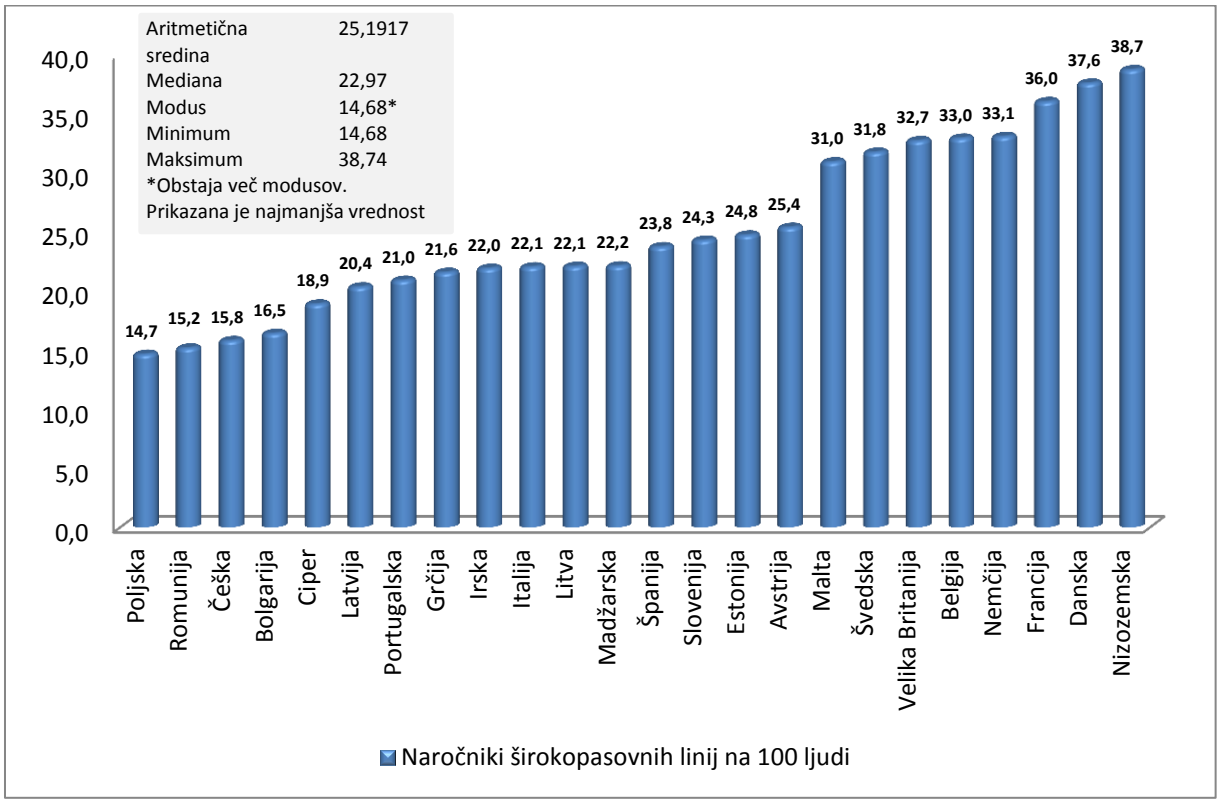


Vir: EUROSTAT.

Največ naročnikov širokopasovnih linij na 100 prebivalcev v letu 2011 je bilo na Nizozemskem, Danskem, v Franciji, Nemčiji in Belgiji. Najmanj pa na Poljskem, v Romuniji, na Češkem, Bolgariji in na Cipru, kjer je od 100 prebivalcev le od 14 do 18 ljudi imelo širokopasovne linije (International Telecommunication Union). Pojem naročniki širokopasovnih linij se nanaša na naročnine visokih hitrosti dostopa do javnega spleta, ki ni manjša od 256 kbit/s in vključuje kabelski modem, DSL (ang. Digital subscriber line) in druge fiksne širokopasovne naročnine. Ne vključuje pa naročnin drugih naprav, ki imajo dostop do podatkovnih komunikacij preko mobilnih omrežij (International Telecommunication Union in The World Bank 2012, 235). 256 kbit/s je 32kB/s, pri čemer pri prenosu enostavne spletne strani, velike 1 MB, kar je enako 1024 kB, potrebujemo 32 sekund. Pri tej hitrosti bi za prenos filma, v velikosti 20 MB, kar je enako 20480 kB, potrebovali 640 sekund, ter za prenos glasbe, v velikosti 5 MB, kar je enako 5129 kB, 160 sekund[1].

[1] Za boljšo predstavo naj povem, da je prenos oziroma naročnina izražena v količini prenesenih podatkov na sekundo, pri čemer je bit najmanjša enota informacije, ki jo računalnik uporablja in je lahko izražena z dvema informacijama, kot sta da ali ne. En bajt je enko 8 bitov. Naslednji enoti sta kilobajt, ki je 1024 bajtov, ter megabajt, ki je 1000 kilobajtov.

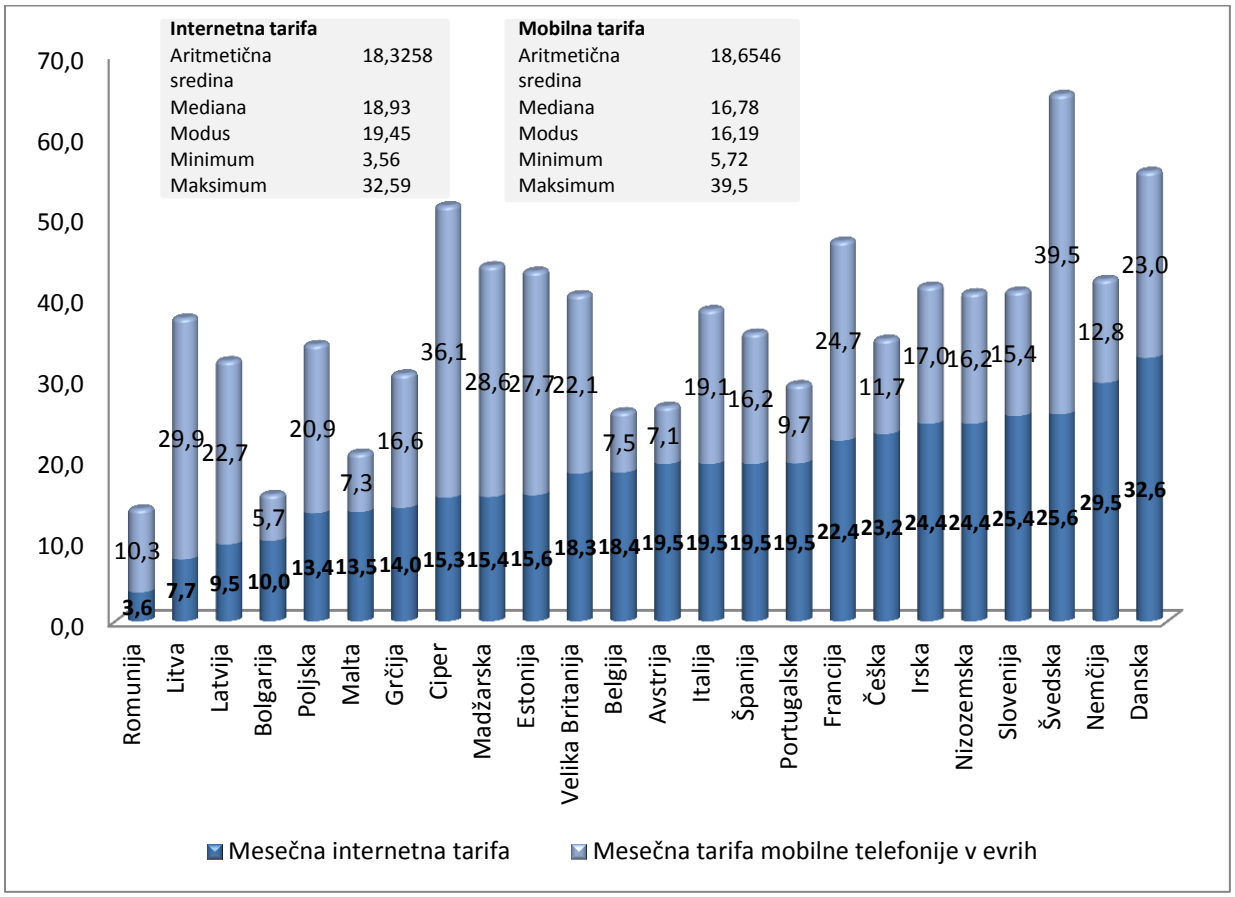
Slika 3.20: Naročniki širokopasovnih linij



Vir: prirejeno po International Telecommunication Union.

S cenami mobilne telefonije in širokopasovnega interneta v paketih za leto 2010 je prikazana njuna cenovna dostopnost. Iz dolarjev sem zaradi boljše predstave valuto spremenila v evre. Za mobilne pakete je upoštevan standardni mobilni paket za mesečno porabo 30 klicev in 100 sms-ov. Po zbranih podatkih je cena mobilne telefonije oziroma mesečni naročniški paket najmanj stal na Cipru, v Litvi, Danskem, Latviji in v Nemčiji, kjer so bile cene v letu 2010 od 5,72 do 9,73 evrov. Najdražji pa so bili v Španiji, Franciji, Belgiji, Grčiji in na Irskem, kjer je najdražji paket stal 39,50 evra. Najvišje mesečne naročnine za internet so na Danskem, v Nemčiji, na Švedskem, v Sloveniji in na Nizozemskem. Najvišja cena je okoli 32 evra ter najnižja okoli 4 evre. Najnižje mesečne naročnine so v Romuniji, Litvi, Latviji, Bolgariji in Poljski (International Telecommunication Union in The World Bank 2012).

Slika 3.21: Mesečne internetne in mobilne tarife v evrih



Vir: prirejeno po International Telecommunication Union in The World Bank (2012).

3.3.2 Izdatki za IKT

Izdatki za informacijsko tehnologijo se od države do države razlikujejo. V statističnem uradu EUROSTAT ni bilo podatkov za Ciper in Malto. Izdatki za informacijsko tehnologijo so prikazani kot % BDP za leto 2010. Največ za informacijsko tehnologijo namenijo v Veliki Britaniji – 3,8 % BDP, na Danskem, Švedskem, v Nizozemski in Irski. Najmanj, in sicer 1,1 % BDP, pa na Irskem, v Romuniji, Latviji, Grčiji in Estoniji (EUROSTAT).

Tabela 3.6: Izdatki za informacijsko tehnologijo

Države	Izdatki za informacijsko tehnologijo kot % BDP leta 2010
Latvija	1,1
Grčija	1,2
Litva	1,2
Romunija	1,2
Estonija	1,4
Italija	1,6
Bolgarija	1,7
Poljska	1,7
Madžarska	1,8
Španija	1,8
Avstrija	2,0
Slovenija	2,0
Portugalska	2,1
Češka	2,2
Belgija	2,4
Francija	2,6
Nemčija	2,6
Irska	2,8
Nizozemska	2,8

Danska	2,9
Švedska	2,9
Velika	3,8

Britanija	
Ciper	Ni podatka
Malta	Ni podatka

Aritmetična sredina	2,082
Mediana	2
Modus	1,2
Minimum	1,1
Maksimum	3,8

Vir: prirejeno po EUROSTAT.

3.3.3 Varnost strežnikov

Varnost strežnikov je izražena s številom varnih strežnikov na milijon ljudi za leto 2010. Varni strežniki so tisti, ki uporabljajo šifrirano tehnologijo za internetne transakcije in so pomembni za varnost v kibernetskem prostoru. Najvišje število varnih strežnikov je na Nizozemskem, Danskem, Malti, v Veliki Britaniji in na Švedskem. Najmanjše pa v Romuniji, Bolgariji, Grčiji, Italiji in Latviji (International Telecomunication Union in The World Bank 2012).

Tabela 3.7: Število varnih strežnikov

Države	Število varnih strežnikov na milijon ljudi
Romunija	53,7
Bolgarija	139,0
Grčija	154,0
Italija	191,5
Latvija	205,0
Madžarska	219,8
Portugalska	223,8
Litva	237,0

Poljska	270,0
Španija	284,2
Francija	355,6
Češka	387,3
Slovenija	433,2
Estonija	533,6
Belgija	604,4
Avstrija	995,6
Nemčija	1025,6
Ciper	1121,3
Irska	1145,0
Švedska	1455,3

Velika Britanija	1594,3
Malta	1669,1
Danska	2184,6
Nizozemska	2756,6

Aritmetična sredina	759,9792
Mediana	410,25
Minimum	53,7
Maksimum	2756.6

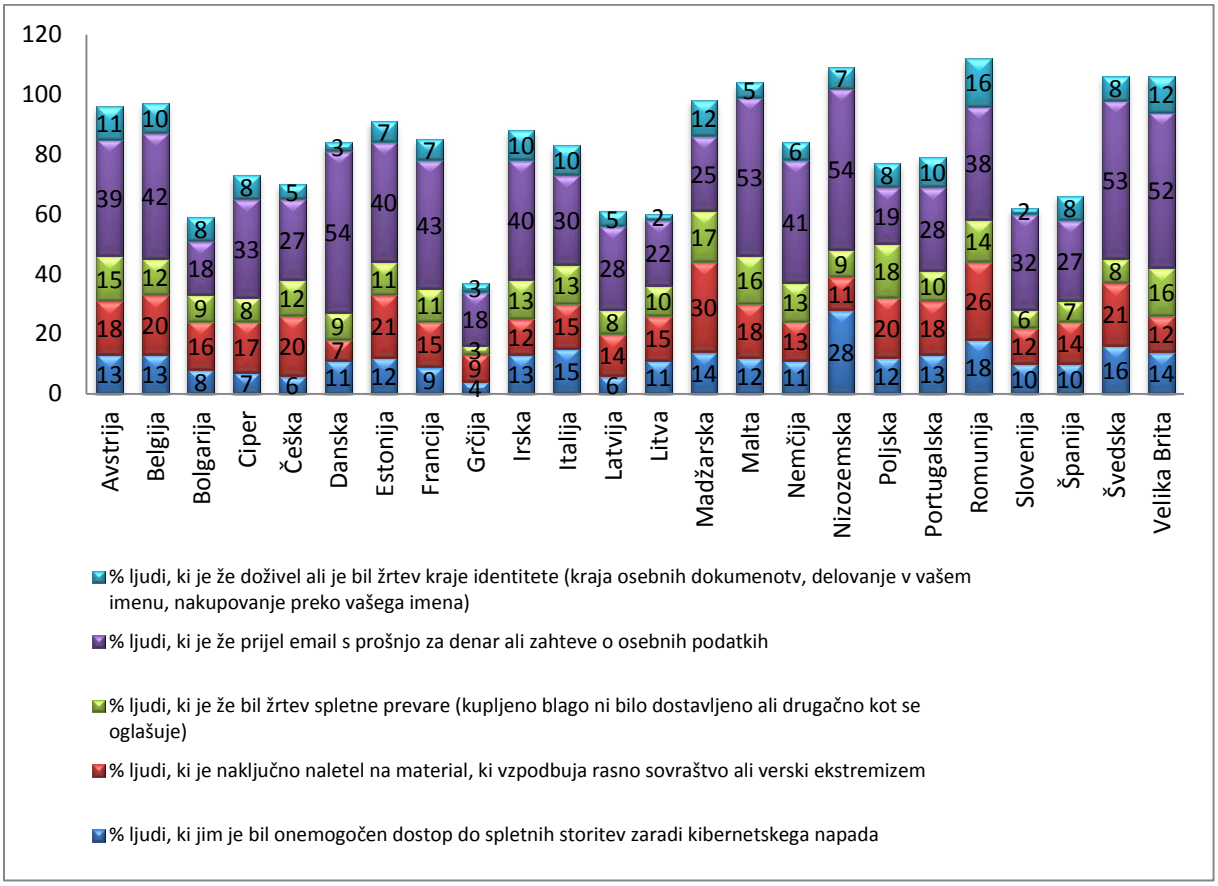
Vir: prirejeno po International Telecommunication Union in The World Bank (2012).

3.3.4 Število kibernetskih vdorov

Zadnja podkategorija v kategoriji tehnološka infrastruktura je število kibernetskih vdorov v posameznih državah, ki je težko merljiva. Bi pa lahko pomenila dober indikator za kibernetsko moč posamezne države, če bi jo gledali skupaj z odzivom na kibernetske grožnje. Po svetu je vsak dan milijon ljudi žrtev kibernetskega kriminala (European Commission 2012, 2). 12 % uporabnikov interneta v EU je že doživelo spletno prevaro, 8 % jih je bilo soočenih s krajo identitete in 13 % jih ni moglo dostopati do spletnih storitev zaradi kibernetskega napada. Več kot tretjina (38 %) je že prijelo nezaželeno elektronsko pošto, 10 % se to dogaja konstantno. 89 % prebivalcev se izogiba razkritju osebnih podatkov na spletu, 74 % se jih

strinja, da se je kibernetski kriminal povečal, 72 % je izrazilo skrb glede varnosti osebnih podatkov na spletu, kar 66 % jih skrbi, da njihovi podatki na spletu v rokah javnih institucij niso varni.

Slika 3.22: Žrtve kibernetskega kriminala



Vir: prirejeno po European Commission (2012).

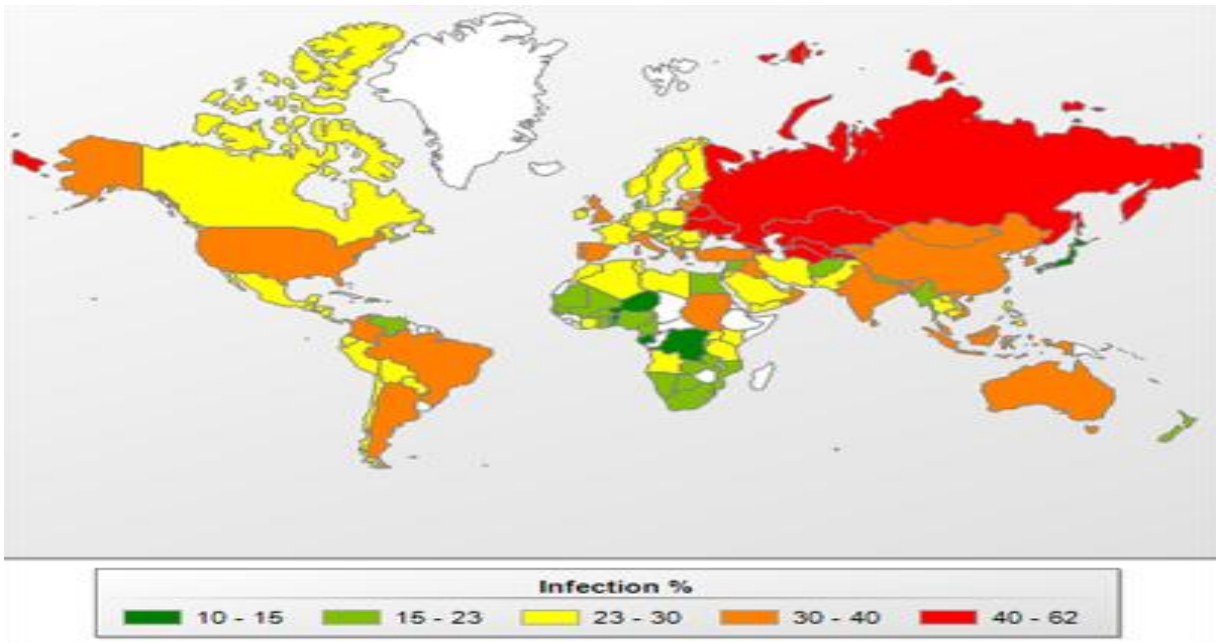
Število kibernetski vdorov ter določitev kibernetskega kriminala je težko tudi zaradi neporočanja posameznikov, podjetij pristojnim avtoritetam, neobstoj avtoritet, ki bi po zakonu bile dolžne izbirati podatke in katerim bi moralo ljudstvo poročati, nezadostni razvoj kibernetskih zakonov, tehnična zapletenost preverjanja in kaznovanja, težko vidne posledice in izvajalci, ki lahko presegajo meje države. Težko je dobiti podatke o številu kibernetskih napadov zaradi klasifikacije ali zaradi nesodelovanja podjetij za razkritje informacij, ki lahko škodujejo njihovemu trgu ali zaradi potencialne izgube zaupanja potrošnikov (Svete 2012, 40).

ENISA je izdala poročilo o kibernetskih vdorih, zbranih iz različnih virov brez geografske opredelitve, ampak le katere grožnje se v kibernetskem prostoru povečujejo in katere zmanjšujejo. Leta 2012 je ENISA prvič objavila letno poročilo o kibernetskih napadih,

ki ima zakonsko podlago z zakonom s področja telekomunikacij iz leta 2009, ki v nekaterih državah še ni popolnoma v veljavi. Zavezuje pa ponudnike javnih komunikacijskih omrežij, da poročajo o incidentih državnim organom, ki o tem letno poročajo ENISI. V tem poročilu za leto 2011 je le 11 držav poročalo o 51 večjih kibernetskih incidentih, 9 jih je poročalo o incidentih brez večjega pomena, ampak verjetno zato, ker so nekatere članice implementirale zakon leta 2011, zato bodo podatki jeseni leta 2013 dali jasnejšo sliko (ENISA 2012a).

Zanimiv je prikaz spodnje slike s stopnjami tveganja spletne okužbe, ki je merjena na podlagi zaznanih izdanih protivirusnih opozoril računalnikov v posamezni državi. Stopnja tveganja spletne okužbe je v proučevanih državah različna. Stopnje tveganja so razvrščene v štiri skupine: maksimalna stopnja tveganja od 42 do 60 %, visoka stopnja tveganja od 34 do 42 %, zmerna stopnja tveganja od 29 do 34 % in nizka stopnja tveganja okužbe od 12 do 29 %. V zmerno tveganje z okužbo spadajo Latvija, Litva, Grčija, Španija, Portugalska, Velika Britanija in Italija s 30−40 % tveganja. V nizko stopnjo tveganja spadajo vse ostale države razen Malte in Slovenije, za kateri podatki niso dostopni. Poudariti je potrebno, da je najvarnejša država Danska, katere stopnja tveganja znaša najmanj izmed proučevanih držav, in sicer 17 %. V nizko stopnjo tveganja so torej uvrščene Francija, Nemčija, Avstrija, Ciper, Belgija, Estonija, Češka, Nizozemska, Bolgarija, Romunija, Švedska, Irska in Madžarska (Namestnikov 2012a).

Slika 3.23: Stopnje tveganja spletnih okužb na svetu



Vir: Namestnikov (2012a).

3.4 PRAVNI OKVIR DRŽAV ČLANIC EU

Prva kategorija je pomembna, saj na področju kibernetskega prostora in pri zagotavljanju kibernetske varnosti igrajo države in mednarodne organizacije pomembno vlogo. V njihovem okviru se razvijajo zakoni, norme, varnostni mehanizmi in pravne ureditve, ki nekatera dejanja prepovejo, kaznujejo in posredno dovoljujejo. Kibernetske grožnje so še vedno nerešene v zakonskem smislu ter tudi v mednarodnem pravu. Rešujejo se v okviru zagotavljanja varnosti ključne infrastrukture, ki je povezana z informacijsko-komunikacijsko infrastrukturo. Regulacija poteka predvsem na področju kibernetske kriminalne dejavnosti, vohunjenja, terorizma, prevar in informacijskega bojevanja (Svete 2012, 39).

Med podkategorije pravnega okvira so vključeni:

1. državna kibernetska strategija
2. centralno kibernetsko izvršilni organ
3. kibernetsko varnostni zakoni
4. odgovor na kibernetsko kriminalno dejavnost
5. sodelovanje javno-zasebnega partnerstva
6. kibernetsko varnostne obligacije na ravni Evropske unije
7. politična učinkovitost (Prirejeno po: Economic Inteligence Unit 2011)

Med podkategorije pravnega okvira spada tudi zaščita intelektualne lastnine, saj so pravice intelektualne lastnine iz ekonomskega vidika izredno pomembne, ker vplivajo na povečanje konkurenčnosti subjektov na trgu, njihov dolgoročni razvoj, na raziskave, razvoj, investicije, na vzpostavljanje novih in širjenje že obstoječih vej gospodarstva, na odpiranje novih delovnih mest in nenazadnje tudi na povečanje prihodkov države iz naslova davkov (Urad za intelektualno lastnino). Zaščito intelektualne lastnine nisem vključila, saj ima vsaka država svoje zakone, ki spadajo pod različne kategorije avtorskih, sorodnih ter industrijskih pravic. Zaščita programske in strojne opreme na področju IKT ter vsebin v virtualnem prostoru je v začetnem razvoju in nima skupne točke s katero bi lahko obravnavala njeno zaščito in določila, katera država ima boljše zakone ter ukrepe in katera slabše za zaščito intelektualne lastnine. Na ravni Evropske unije obstajajo določene direktive za to področje, ampak njihovo obravnavanje za namen magistrske naloge ni smiselno, saj so le splošne usmeritve.

3.4.1 Državne kibernetske strategije

Državne kibernetske strategije so pomemben usmerjevalni in strateški dokument za delovanje na kibernetskem področju. V letu 2011 je v Evropski uniji 11 držav članic imelo razvite

državne kibernetske strategije, ki so usmerjevalni in strateški dokument za zagotavljanje varnosti v kibernetskem prostoru. Prva strategija v Evropi je bila izdana leta 2008 s strani Estonije, ki so ji sledile strategije Nemčije, Francije, Nizozemske, Avstrije, Velike Britanije, Slovaške, Luksemburga, Češke, Litve ter Finske. Zaradi nedostopnosti strategij Finske in Luksemburga v razumljivem jeziku, sem državi izločila iz nadaljnjega proučevanja, prav tako nisem vključila Slovaške, ki po podatkih ENSIE nacionalno kibernetsko strategijo ima, a le-ta ni dostopna preko spleta. Od 24 proučevanih držav jih 8 ima, 16 pa nima razvitih nacionalnih kibernetskih strategij. Pri čemer je 6 strategij bilo razvitih v letu 2011, ena 2008 in ena leta 2012 (ENISA).

Kibernetske strategije imajo več skupnih točk, saj kot strateški dokument določajo vladni okvir za zagotavljanje kibernetske varnosti, določajo mehanizme, opredeljujejo glavne grožnje ter glavne akterje, določajo smernice delovanja, v večini poudarjajo nujnost vključevanja nedržavnih akterjev, ki so odgovorni za zagotavljanje delovanja ključne infrastrukture, poudarki so tudi na sodelovanju znotraj in zunaj držav in razvoju boljših operativnih zmogljivosti. Poudariti je treba, da se med seboj bistveno razlikujejo, saj ni veliko mednarodno sprejetih definicij na področju kibernetskega prostora (ENISA).

Tabela 3.8: Države z in brez državne kibernetske strategije

Obstoj kibernetske strategije/ leto nastanka	Neobstoj kibernetske strategije
Avstrija/ 2012	Belgija
Češka/ 2011	Bolgarija
Estonija/ 2008	Ciper
Francija/ 2011	Danska
Litva/ 2011	Grčija
Nemčija/ 2011	Irska
Nizozemska/ 2011	Italija
Velika Britanija/ 2011	Latvija
	Madžarska
	Malta
	Poljska
	Portugalska
	Romunija
	Slovenija
	Španija
	Švedska

Viri: ANSSI (2011), Austrian Federal Chancellery (2012), Czech Republic (2011), Dutch Ministry of Security and Justice (2011), ENISA (2011), Estonias Ministry of Defence (2008), German Federal Ministry of Interior (2011), Government of the Republic of Lithuania (2011), United Kingdom Cabinet Office (2011).

3.4.2 Centralno kibernetsko izvršilni organ

V tej podkategoriji pravnega okvira sem preučila, ali v državah EU obstaja centralni organ oziroma center, ki prevzema centralno in vodilno vlogo na področju kibernetskega prostora, preko katerega potekajo različne naloge in deluje kot povezovalni organ med različnimi državnimi ter nedržavnimi institucijami in organi. Za boljšo kibernetsko varnost bi morali v državi obstajati izvršilni organi, ki bi med seboj povezovali javni in zasebni sektor, torej razne agencije, organizacije, znanstvenike in strokovnjake, ministrstva ter podjetja.

Iz tabele 3.9 je razvidno, da jih izmed štiriindvajset proučevanih držav ima 5 centralno koordinacijsko izvršilni organ, ki povezuje ključne organe, ki se ukvarjajo s kibernetsko varnostjo in tudi privatno sfero, v rokah katerih je večina ključne infrastrukture, kar prikazuje tudi spodnja tabela. Države, ki imajo centralno kibernetski organ, so v nadaljevanju podrobneje opisane, prav tako so predstavljene nekatere države, v katerih obstaja povezovalni organ, a ne povezuje vseh glavnih akterjev. V nekaterih proučevanih državah so razvili

posebne nacionalne kibernetsko varnostne svete ter nacionalne kibernetsko odzivne centre. Ti organi izpolnjujejo in uresničujejo kibernetske varnostne strategije in druge akcijske načrte v posamezni državi.

Centralno kibernetsko izvršilne organe najdemo v Nemčiji, Veliki Britaniji, Franciji, na Češkem in Nizozemskem.

V Nemčiji so leta 2011 pod okriljem notranjega ministrstva ustanovili Kibernetsko obrambni center NCAZ – Nationale Cyber Abwehrzehntrum kot odgovor na naraščajoče grožnje iz kibernetskega prostora. Združuje resurse vladnih agencij, federalne policije, zveznega urada za civilno zaščito in reševanje, tuje obveščevalne agencije ter tudi industrijo in znanost. V okviru centra sodelujejo vsi pomembnejši državni organi in akterji, ki nadzorujejo ključno infrastrukturo, njegove glavne naloge pa so prenos in izmenjava informacij, izmenjava podatkov o obliki napadov, profili storilcev, ki jih usklajuje skupaj z kibernetsko varnostnim svetom. Prav tako obstaja izmenjava informacij in sodelovanje med različnimi CERT-i preko nacionalnega CERT-Bund-a, ki spada pod okrilje Zveznega urada za informacijsko varnost BSI, kateremu poroča tudi Kibernetsko obrambni center NCAZ. Obstaja hierarhična ureditev, kjer pod notranje ministrstvo spada BSI, Zvezni urad kriminalne policije BKA in Zvezni urad za civilno zaščito in reševanje BBK. Prvi organ se ukvarja s telekomunikacijami in informacijsko tehnološkim sektorjem, z načrti glede zaščite ključne infrastrukture, drugi pa z analiziranjem in statističnimi podatki glede informacijsko-komunikacijskega kriminala, preventive proti kibernetskemu kriminalu in drugimi kibernetskim temami. Sodelovanje med akterji, ki so v državi odgovorni za kibernetsko varnost je veliko, prav tako je dobro urejeno sodelovanje z akademskim in gospodarskim področjem (German Federal Ministry of the Interior 2011, 8−10, ENISA 2011h).

Velika Britanija je naslednja država, kjer tako kot v Nemčiji obstaja centralno kibernetski izvršilni organ. V letu 2009 sta nastala Urad za kibernetsko varnost OCS (The office of Cyber Security) in nacionalni kibernetsko varnostni center CSOC (Cyber Security Operations Cetre). Oba organa ščitita ključno infrastrukturo v državi. CSOC povezuje med seboj privatno in javno sfero ter državne organe, ki so pred njegovim nastankom delovali decentralizirano in nepovezano. Povezuje večja komunikacijska podjetja, električne dobavitelje in druge akterje (Internet1). Center je ustanovljen v obrambne namene a ima tudi napadalne zmogljivosti (Espiner 2009a). OCS na drugi strani povezuje vse državne organe, ki delujejo na kibernetskem področju od ministrstev, policije, do obveščevalnih služb, pri svojem načrtovanju pa upoštevajo tudi industrijo in privatno sfero. Center povezuje urad za kibernetsko varnost in zagotavljanje informacij OCSIA (Office of Cyber Security and

Information Assurane), Center za zaščito nacionalne infrastrukture CPNI (Centre for the Protection of the National Infrastructure), Ministrstvo za gospodarstvo, inovacije in usposabljanje BSI (Department for Business Innovation and Skills), Komunikacijsko – elektronsko varnostno skupino CESG (Communications-Elecrtonics Security Group), CSOC, Policijsko centralno e-kriminalno enoto SOCA (Serious Organized Crime Agency) ter vladni CERT (Espiner 2009b). Obstaja tudi neformalni forum, ki povezuje 25 CERT-ov iz različnih področij (ENISA 2011z, 20).

V Franciji je centralni izvršilni organ od leta 2009 naprej Francoska omrežna in informacijsko varnostna agencija ANSSI, ki povezuje javno in zasebno sfero. Agencija zagotavlja nasvete ter podporo vladnim in gospodarskim subjektom. V okviru agencije je tudi Francoski kibernetsko obrambni center COSSI, v okviru katerega je vladni CERT in CFSSI (Centre of Education and Training in Information Security), ki nudi izobraževanje in usposabljanje različnim informacijsko tehnološkim javnim akterjem, v njegovem okviru poteka tudi izmenjava na področju izobraževanja z univerzami in drugimi centri (French Network and Information Security Agency).

V Nizozemski kibernetski strategiji je omenjen načrtovan razvoj Kibernetsko varnostnega sveta in Nacionalnega kibernetsko varnostnega centra NCSC (National Cyber Security Centre), v katerem bodo zastopani tako javni kot zasebni akterji, ki bodo usklajevali dejavnosti na področju kibernetske varnosti. S sodelovanjem akterjev preko centra bi dobili vpogled v razvoj, grožnje, trende ter podporo za odzivanje na incidente. Center je postal operativen januarja 2012 in se bo v naslednjih letih še razvijal, trenutno poteka razvoj preko vladnega CERT-a (Neaderlands National Cyber Security Centre).

Na Češkem je v strategiji omenjena pomembnost nastanka koordinacijskega in centralnega organa na kibernetskem področju (Czech Republic 2011). V letu 2011 je nastala nacionalna varnostna agencija kot avtoriteta za kibernetsko varnost, v okviru katere sta se razvila Koordinacijski svet za kibernetsko varnost in Nacionalni kibernetsko varnosti center NCKB (Narodni centrum kyberneticke bezpečnosti). Nacionalni kibernetsko varnostni center je koordinacijski organ na nacionalni in mednarodni ravni za področje kibernetske varnosti. Center povezuje razne CERT-e nacionalni in mednarodni ravni, razvija varnostne standarde in raziskuje področje kibernetske varnosti (Narodni cetrum kyberneticke bezpečnosti). V okviru centra sta vladni CERT in Koordinacijski svet za kibernetsko varnost, ki sta v pristojnosti ministrstva za notranje zadeve ter združujeta policijo, ministrstvo za obrambo, za zunanje zadeve, za finance, za industrijo in trgovino, za promet, češko narodno banko, urad za zunanje zadeve in informatiko, varnostne informacijske službe, obveščevalne službe in druge. Njegov

cilj je usklajevalna vloga na področju kibernetske varnosti, ki zahteva sodelovanje državnih institucij (ENISA 2011č). Povezuje torej 5 CERT-ov, ki obstajajo v državi, nikjer pa ni nobenega poročila glede sodelovanja z industrijo in znanstveniki izven CERT-ov.

Estonija je svoje kibernetsko varnostne zmogljivosti v polni meri začela razvijati po kibernetskem napadu leta 2007, ko se je pokazalo, da je odziv na kibernetski napad omejen, saj vlade in države nimajo nadzora nad svetovnim spletom. Kljub temu da država nima lastnega centralnega izvršilnega organa, poteka prenos informacij z drugimi državami preko NATO CCDCOE Cooperative Cyber Defence Centre of Excellence, ki je lociran v Talinu, katerega pobudnica za ustanovitev je tudi Estonija. Poleg Estonije lahko njegove zmogljivosti, po določitvi Usmerjevalnega odbora, izobraževanja, raziskav, razvoja, lekcij, konzultacij koristijo tudi druge sponzorske države, ki so Nemčija, Italija, Latvija, Litva, Slovaška in Španija, ki tudi krijejo stroške delovanja. Center je eden izmed najbolj naprednih kibernetsko obrambnih in raziskovalnih centrov na svetu, preko katerega potekajo izmenjave informacij, ozaveščanje, treningi, raziskave in razvoj, analiziranje in svetovanje (CCDCOE – NATO Cooperative Cyber Defence Centre of Excellence).

V Avstriji centralno kibernetskega izvršnega organa ni, njegove bistvene naloge se izvajajo preko CERT-a, federalnih provinc, mest in občin, ki operirajo s tem področjem, kljub temu pa poudarjajo pomembnost in vzpostavitev tako imenovanega kibernetsko situacijskega centra. V večini v državi obstajajo dobre kibernetske strukture znotraj zasebnih podjetij. Avstrijski akterji delujejo v večini ločeno in neodvisno med seboj. Procedure na kibernetskem področju so decentralizirane in ukrepi pri kibernetski incidentih temeljijo na odzivih na lokalnih ravneh (Austrian Federal Chancellery 2012).

V Belgiji ne obstaja vladni organ, ki bi bil v funkciji kot Varnostne agencije, prav tako ni centralnega organa, ki bi bil odgovoren za razvoj nacionalne informacijske varnostne politike. Vendar kljub temu v državi od leta 2011 naprej obstaja Belgijski center za kibernetski kriminal, ki povezuje znanja zasebnih in javnih akterjev, akademsko, vladno in industrijsko sfero. Center se ukvarja z usposabljanjem sodnikov in policistov, izvaja vaje, treninge ter raziskave o kriptografiji in nudi svoje strokovno znanje. Sodelovanje različnih akterjev poteka na podlagi različnih iniciativ, ki so po navadi usmerjana v sodelovanje ožjega kroga akterjev (ENISA 2011b).

Na Danskem centralnega izvršilnega organa ni, obstaja pa sodelovanje preko različnih državni akterjev s privatno sfero. Varnostni svet, ustanovljen s strani Ministrstva za znanost, tehnologijo in inovacije, povezuje člane iz privatne sfere, ki predstavljajo javni sektor, zaposlene ter ljudi iz raziskovalnega in izobraževalnega področja. Sodelovanje med zasebnimi

in javnimi akterji je vidno preko raznih iniciativ, med njimi tudi iniciative za varno obnašanje na spletu (ENISA 2011e).

Decentralizirano delovanje na področju zagotavljanja kibernetske varnosti najdemo v Bolgariji, Cipru, Danski, Litvi, Latviji, Sloveniji, Španiji. V teh državah obstajajo državni organi; različna ministrstva, ki so odgovorna za izvajanje politike na področju kibernetskega prostora, ločeno od njih obstajajo gospodarska združenja in sodelovanja s posameznimi akterji, kot so razni IKT in energijski ponudniki. Ne obstaja pa en izvršni organ, ki bi med seboj povezal ministrstva, akterje ključne infrastrukture, akademsko sfero, CERT-e in druge državne organe in organizacije ter izvendržavne akterje, ki so pomembni za izvajanje dejanj, ki vodijo do boljše kibernetske varnosti. Sodelovanje poteka preko raznih projektov, iniciativ ter pobud preko različnih državnih organov (ENISA 2011a-z).

Švedska nima enega samega organa, ki bi bil centralno izvršni organ na kibernetskem področju. Različne institucije se ukvarjajo z informacijsko varnostjo, kot so Švedska agencija za pošto in telekomunikacije, kazensko in preiskovalne službe, obveščevalne ter civilno zaščitne službe, Švedski podatkovni inšpekcijski svet, policija ter druge. Tako kot v večini proučevanih držav so za nacionalno informacijsko strategijo, zakonodajo, raziskave ter strategije odgovorna pristojna ministrstva. Kljub temu da v državi ne obstaja organ, ki bi povezoval zasebno in javno sfero, obstaja SAMFI – kooperacijska skupina za informacijsko varnost, ki združuje ter povezuje državne organe, ki zagotavljajo kibernetsko varnost. Sodelovanje med javno in zasebno sfero je vidno predvsem v okviru iniciativ in kampanj za varnejši internet, v katerih sodelujejo relevantni državni organi in industrija. Kot je že izpostavljeno v nacionalni strategiji, je eden izmed najpomembnejši dejanj ozaveščanje prebivalstva, ki poteka preko švedskega medijskega sveta, v okviru katerega se izvajajo pobude za ozaveščanje zasebnih akterjev in državljanov (ENISA 2011v).

Tabela 3.9: Nastanek centralno izvršilnih organov

Države	Centralno izvršilni organ	Leto nastanka
Ciper	/	/
Romunija	/	/
Poljska	/	/
Bolgarija	/	/
Latvija	/	/
Malta	/	/
Madžarska	/	/
Grčija	/	/
Litva	/	/

Italija	/	/
Estonija	/	/
Španija	/	/
Portugalska	/	/
Češka	Narodni centrum kyberneticke bezpečnosti	2011
Irska	/	/
Velika Britanija	Cyber Security Operations Centre (CSOC)	2009
Belgija	/	/
Nizozemska	National Cyber Security Centre (NCSC)	2012
Francija	Agence nationale de la securite des systems d'information	2009
Slovenija	/	/
Nemčija	Nationales Cyber-Abwehrzentrum	2011
Avstrija	/	/
Švedska	/	/
Danska	/	/

Viri: Austrian Federal Chancellery (2012), Czech Republic (2011), French Network and Information Security Agency (2013), ENISA 2011a-z in Neaderlands National Cyber Security Centre.

3.4.3 Kibernetsko-varnostni zakoni

Proučevala sem obstoj kibernetsko varnostnih zakonov v državah članicah EU, pri čemer lahko podkategorijo razdelimo na: obstoj zakonov o kibernetski kriminaliteti, o zaščiti ključne infrastrukture in na obstoj zakonov o zaščiti informacijskih in omrežnih sistemov. Zaradi nedostopnosti zakonov nekaterih držav sem proučevanje varnostnih zakonov zožila na proučevanje zakonov o kibernetski kriminaliteti.

Za povečanja kibernetske kriminalitete je pomembno, da imajo države zakone, ki kibernetski kriminal opredeljujejo kot kazniva dejanja, in da imajo le-ta tudi predvidene kazni. Za obstoj zakonov o kibernetskem kriminalu sem štela omembo kaznivih dejanj v kibernetskem prostoru v kazenskih zakonikih ali konkretnih kibernetskih zakonih.

V proučevanih državah ima največ držav področje kibernetskega kriminala urejeno v kazenskem zakoniku. Posebne zakone o kibernetskem kriminalu najdemo v devetih državah:

Belgija, Francija, Irska, Malta, Nizozemska, Portugalska, Romunija, Velika Britanija, Ciper. Na drugi strani imajo Avstrija, Bolgarija, Češka, Danska, Grčija, Italija, Latvija, Litva, Madžarska, Poljska, Estonija, Češka, Slovenija, Španija, Švedska posamezne člene v kazenskem zakoniku, ki se navezujejo na omenjeno temo (ENISA 2011a-2011z).

Kazenski zakoniki in zakoni, ki so lahko razdrobljeni, opredeljujejo različna dejanja, kot so nedovoljen dostop do informacij, podatkov in procesov, neavtorizirana sprememba informacij ter podatkov, okužbe in virusi, ogrožanje sistemov, vdori, otroška pornografija, kraja identitete, nezaželena pošta in drugi. Organi pregona so v večini policijske enote, ki imajo v nekaterih držav izoblikovane posebne enote za posebne kibernetske zločine ter sodišča. Sodelujejo tudi internetni in drugi ponudniki IKT ter posamezni strokovnjaki.

Natančno določene kazni za kibernetski kriminal so predvidene v vseh proučevanih državah, le da vsaka različno opredeljuje, kaj je kaznivo in kaj ne. Kazni se razlikujejo, ampak vse države predvidevajo kazenske sankcije, ki so odvisne od kibernetski dejanj in prekrškov. Zaporne kazni se gibajo od 6 mesecev pa vse do 10 let, razvidne pa so v tabeli 3.2 (ENISA 2011a-2011z, Rand Europe in Lawfort 2005). Za Romunijo uradnega podatka ni bilo, najvišja kazen za kibernetski kriminal pa naj bi bila kar 20 let, vendar je v realnosti večina obsojenih na 4 leta (Constantin 2011). Za nadaljnje proučevanje bi bilo zanimivo pogledati statistiko obtoženih za kibernetski kriminal in spoštovanje ter uresničevanje zakonov.

Tabela 3.10: Zakonska podlaga kibernetskega kriminala

Države	Zakoni o kibernetskem kriminalu	Predvidena zaporna kazen
Ciper	Poseben zakon	do 5 let
Romunija	Poseben zakon	do 20 let
Poljska	V kazenskem zakoniku	do 8 let
Bolgarija	V kazenskem zakoniku	do 8 let
Latvija	V kazenskem zakoniku	do 10 let
Malta	Poseben zakon	do 2 leti
Madžarska	V kazenskem zakoniku	do 5 let
Grčija	V kazenskem zakoniku	do 10 let
Litva	V kazenskem zakoniku	do 3 leta
Italija	V kazenskem zakoniku	do 8 let
Estonija	V kazenskem zakoniku	do 5 let
Španija	V kazenskem zakoniku	do 7 let
Portugalska	Poseben zakon	do 10 let
Češka	V kazenskem zakoniku	do 6 let
Irska	Poseben zakon	do 10 let
Velika Britanija	Poseben zakon	do 5 let

Belgija	Poseben zakon	do 5 let
Nizozemska	Poseben zakon	do 4 leta
Francija	Poseben zakon	do 5 let
Slovenija	V kazenskem zakoniku	do 5 let
Nemčija	V kazenskem zakoniku	do 5 let
Avstrija	V kazenskem zakoniku	do 6 mesecev
Švedska	V kazenskem zakoniku	do 4 leta
Danska	V kazenskem zakoniku	do 8 let

Viri: Constantin (2005), ENISA (2011a−2011z), Rand Europe in Lawfort (2005).

Internet nima meja, ampak se kibernetski kriminal pojavlja na specifičnih »geografskih« lokacijah v kibernetskem prostoru. Ključni faktorji za določitev tarč napada so ekonomska razvitost, število internetnih uporabnikov in internetna razširjenost. Kjer je dostopnost do interneta možna v šolah, javnih institucijah, doma in v službi, večja uporaba tablic, pametnih telefonov ob nizkih in dostopnih cenah, dostopanje preko interneta do javnih storitev in bančnih računov, je možnost kibernetskega kriminala večja (Namestnikov 2012b).

3.4.4 Odgovor na kibernetski kriminal

Za odgovor na kibernetski kriminal je pomembno, da imajo države poleg zakonov, ki opredeljujejo, kaj je kaznivo, tudi organ, ki bo zagotavljal njegovo spoštovanje in izvajal naloge za večjo varnost v kibernetskem prostoru. Poleg policijskih enot imajo države ustanovljene računalniške skupine za urgentno reševanje kibernetskih groženj s kratico CERT (ang. computer emergency response team). So temeljnega pomena pri zaščiti ključne informacijske infrastrukture, ki sestavlja pomemben del nacionalne ekonomije in družbe, saj se le-ti odzivajo na informacijsko varnostne incidente. Med seboj povezujejo različne državne organe ter prebivalce in sodelujejo tudi z drugimi državami. Njihove naloge variirajo od države do države, v glavnem pa izvajajo preventivo, izobražujejo, analizirajo, povezujejo, zaznavajo napade in v primerih napadov ukrepajo (ENISA).

Prvi CERT je nastala leta 1988 v Združenih državah Amerike v okviru današnjega obrambnega ministrstva kot odgovor na prvi večji incident. Nastanek CERT-ov po državah v Evropski uniji se razlikuje. Letnica nastanka državnih in vladnih CERT-ov sega v leto 1994, pri čemer do danes v Italiji, na Cipru in v Sloveniji le-ti ne obstajajo. Nekatere države imajo ločena CERT-a, enega za delovanje na vladni, drugega na državni ravni, druge pa imajo CERT, ki združuje oba področja. Pred razvojem državnih in vladnih CERT so se ti razvijali v okviru različnih panog in glavnih sektorjev, kot so izobraževalni/akademski, energijski, finančni ter industrijski. Ravno zaradi razdrobljenosti je CERT na državni ravni še toliko bolj

pomemben, saj povezuje in deluje kot usmerjevalni organ, v katerem se izmenjujejo informacije.

Večina proučevanih članic EU ima državne CERT-e, ampak se bistveno razlikujejo po širini nalog, ki jih opravljajo. Države imajo tudi po več CERT-ov v različnih panogah. Skupine so ustanovljene za zbiranje, analiziranje informacij, obveščanje, sodelovanje, povezovanje različnih državnih organov, za odzivanje na grožnje ter njihovo odkrivanje, ozaveščanje in opozarjanje na ranljivosti. Štiri države: Belgija, Bolgarija, Latvija in Estonija izven državne in vladne ravni v drugih sektorjih nimajo nobenega CERT-a. Najvišje skupno število teh skupin za odzivanje na incidente je v Nemčiji in Veliki Britaniji, kjer je 20 in 18 skupin brez državnih in vladnih razdeljenih med različne ključne sektorje v družbi (ENISA).

CERT-i so omenjeni v šestih nacionalnih kibernetskih strategijah, in sicer v Avstriji, Litvi, Estoniji, Nemčiji, Češki in na Nizozemskem. V Franciji in Veliki Britaniji jih v strategiji ni zaslediti, prav tako pa tudi tiste države, ki jih imajo v strateškemu dokumentu omenjene, nimajo v njih opredeljenih nalog in mandatov. Izmed osmih držav, ki imajo razvite nacionalne kibernetske strategije, so CERT-i omenjeni v 6 strategijah, pri čemer so v nekaterih omenjena konkretna imena in drugod le poudarek o njihovi pomembnosti (ANSSI (2011), Austrian Federal Chancellery (2012), Czech Republic (2011), Dutch Ministry of Security and Justice (2011), ENISA (2011a), Estonias Ministry of Defence (2008), German Federal Ministry of Interior (2011), Government of the Republic of Lithuania (2011), United Kingdom Cabinet Office (2011)).

Število zaposlenih naj bi znašalo po podatkih ENISE najmanj od 6 do 8 članov. V državah pa najdemo tudi manjše število ter na drugem koncu tudi do trikrat višje (ENISA 2012a, 10, 51). Zaradi nedostopnosti števila zaposlenih za več držav podatka nisem uvrstila v nalogo. Glede na to, da 90 % CERT v Evropski uniji in članic organizacije EFTA sodeluje pri svetovanju in nastanku nacionalnih strategij in drugih zakonov, zaradi visokega odstotka nisem preverjala, kateri državni CERT-i pri tem ne sodelujejo. Nekatere države razvijajo in imajo razvite tudi kibernetsko varnostne centre, ki so odgovorni za implementacijo kibernetskih strategij in za skupno delovanje različnih CERT-ov v državi (ENISA 2012a, 9).

Spletne strani CERT-ov proučevanih držav imajo opisane ključne naloge, nikjer pa nimajo omenjeno, ali v državi obstaja zakon, ki opredeljuje njihov mandat ali ne. Razlog je verjetno v naštetih pomanjkljivostih pri določanju mandata: nejasnost ali ne podpira vseh nalog, ki jih CERT-i izvajajo, zaprtost javnosti, premalo promoviranja, neobstoj strategij, ki bi določale naloge ali nepromoviranje njihove pomembnosti ter omejena avtoriteta v primeru incidentov (ENISA 2012a, 39).

Kljub temu da večina baz in zbirk o incidentih ni javno dostopna preko uradnih strani, se mi zdi pomanjkljivo, da poročanje vladnim/državnim CERT-om v nekaterih državah ni obvezno, ampak prostovoljno. Nekatere imajo prostovoljno poročanje, druge pa zakonsko nujno poročanje, vendar podatki niso jasni za vse proučevane države. Pri nekaterih državah je kljub prostovoljnemu poročanju o kibernetskih incidentih zakonsko obvezno poročati o tistih incidentih, ki so v kazenskih zakonikih ali drugih zakonih opredeljeni kot kriminalno dejanje. V Estoniji so na podlagi posebnega zakona Emergency act vsi ponudniki vitalnih storitev oziroma ključne infrastrukture zakonsko obvezani pripraviti ocene tveganja ter načrt za neprekinjeno delovanje, nikjer pa ni omembe o obveznem poročanju glede kibernetskih incidentov (ENISA 2011f, 15). Irski ponudniki poročajo o varnostnih incidentih od primera do primera posamezno. Obstaja formular za poročanje, kljub temu pa ni nikjer omenjeno, da je to poročanje (zakonsko) obvezno. Vladni CERT nima dostopne niti spletne strani, ampak obstaja poseben CERT – IRISS CERT – Irish Reporting and Infromation Security Service samo za poročanje o incidentih (IRISS in ENISA 2011k). Danska ima posebno agencijo – NITA (National Information Tehnology and Telecom Agency), v okviru katere deluje tudi vladni CERT, ki sprejema obvezna poročila o incidentih (ENISA 2011e). V Nemčiji je poročanje o incidentih nemških zveznih organov obvezno. Organizacija za obvezno poročajo je BSI (Bundesamt für Sicherheit in der Informations technik) – Zvezni urad za informacijsko varnost, pod okrilje katerega spada tudi nacionalni CERT (BSI 2010). Nizozemska v svojih dokumentih nima omenjenega ne obveznega ne prostovoljnega poročanja CERT-u. Kljub temu pa ima dobro razvito sodelovanje med državnimi in nedržavnimi akterji preko vladnega CERT-a, saj potekajo vaje in izmenjave informacij med ključnimi akterji v državi (ENISA 2011p). Podatki za ostale države so razvidni v tabeli 3.11.

Zaradi omejenosti proračunov so nacionalne kibernetsko varnostne vaje in druge kampanje za večanje ozaveščenosti prebivalstva omejene (ENISA 2012a, 10). Iz tabele 3.11 je razvidno, da sem proučevala vladne CERT-e glede na njihovo omembo v nacionalnih kibernetskih strategijah, na leto nastanka, število drugih CERT izven vladne/državne ravni ter glede obveznosti poročanja o incidentih.

Tabela 3.11: Primerjava CERT-ov

Države	CERT v kibernetskih strategijah	Leto nastanka nacionalnega/ vladnega CERT	Število drugih CERT v državi	Poročanje o incidentih
Ciper	Brez strategije	Brez vladnega CERT	1	/

Romunija	Brez strategije	2008	1	Prostovoljno
Poljska	Brez strategije	2006	3	Prostovoljno
Bolgarija	Brez strategije	2008	0	Obvezno
Latvija	Brez strategije	2006	0	Obvezno
Malta	Brez strategije	2002	0	Informacija ni dostopna
Madžarska	Brez strategije	2005	2	Prostovoljno
Grčija	Brez strategije	2009	3	Prostovoljno
Litva	Omenjen	2006	3	Obvezno
Italija	Brez strategije	Brez vladnega CERT	7	/
Estonija	Omenjen	2006	0	Informacija ni dostopna
Španija	Brez strategije	2006	10	Prostovoljno
Portugalska	Brez strategije	2002	4	Informacija ni dostopna
Češka	Omenjen	2008	4	Prostovoljno
Irska	Brez strategije	Letnica ni določena	4	Prostovoljno
Velika Britanija	Ni omenjen	2007	18	Obvezno
Belgija	Brez strategije	2004	0	Prostovoljno
Nizozemska	Omenjen	2002	13	Informacija ni dostopna
Francija	Ni omenjen	1999	9	Informacija ni dostopna
Slovenija	Brez strategije	Brez vladnega CERT	1	/
Nemčija	Omenjen	2001	20	Obvezno
Avstrija	Omenjen	2008	2	Prostovoljno
Švedska	Brez strategije	2005	6	Informacija ni dostopna
Danska	Brez strategije	2009	5	Obvezno

Viri: ANSSI (2011), Austrian Federal Chancellery (2012), Czech Republic (2011), Dutch Ministry of Security and Justice (2011), ENISA CERT enventory, ENISA (2011a−2011ž), Estonias Ministry of Defence (2008), German Federal Ministry of Interior (2011), Government of the Republic of Lithuania (2011), United Kingdom Cabinet Office (2011), GovCERT Austria, CERT Bulgaria, CSIST Czech Republic, CERT Hungary, CERT Estonia, CERT Slovenia, Spanish Governmental CERT, IRISS CERT, BSI German, BSI (2010), GovCertUK.

Pri podatkih glede obstoja državnih in vladnih CERT-ov po posameznih državah v bazah ENISA sem našla odstopanja, saj je v Sloveniji Sl-CERT opredeljen kot vladni/državni, a temu ni tako. Res je, da je ustanovljen preko javnega zavoda Arnes (Akademska in

raziskovalna mreža Slovenije), ampak ni državni niti vladni CERT. Njegove naloge pa so omejene na izobraževalno ter raziskovalno sfero.

V medijih lahko že dlje časa beremo o predlogi direktive Evropske unije in uvedbe obveznega poročanja podjetij in organizacij nacionalnim avtoritetam glede kibernetskih incidentov. Države naj bi ustanovile posebno organizacijo ali organ, ki bi zbiral prijave o incidentih in o njih po njihovi presoji tudi poročal javnosti ali organizacije v primeru površnosti tudi kaznoval. Te nacionalne avtoritete bi nato naprej poročale nadnacionalnim organom. Predvideva se tudi obvezna uvedba državnega CERT-a, ki pa v večini proučevanih državah že obstaja. Obvezno poročanje bi imelo velik vpliv na podjetja in bo v prihodnosti še stvar debate (Buckenham 2013). Kot je razvidno iz prejšnje tabele, CERT-i na državni/vladni ravni ne obstajajo na Cipru, v Italiji in Sloveniji. Na Cipru obstaja CERT, ustanovljen v raziskovalne namene, ter v Italiji več CERT-ov na vojaškem, energijskem in na področju raziskovanja. V proučevanih državah so se ti CERT-i najprej razvili na raznih izvendržavnih področjih, kot je akademska sfera za raziskovalne namene ter raznih gospodarskih združenjih v okviru industrije. V vseh ostalih državah obstajajo državni/vladni CERT-i, ki so nastajali od leta 1994 naprej (ENISA 2011d in ENISA 2011l).

3.4.5 Javno-zasebno partnerstvo

Zaščita ključne infrastrukture je pomemben del nacionalne varnosti. Ker je velik del ključnih sektorjev v zasebnih rokah in pod okvirom različnih industrij, je pomembno sodelovanje med vladnimi in zasebnimi akterji. Pomembno je torej, ali v državi obstaja organizirano sodelovanje med javno in zasebno sfero. Enotne definicije, kaj pomeni javno-zasebno partnerstvo, ni, saj se razlikuje zaradi različnih kultur, okolja in zakonskih podlag. ENISA (2011ž, 10) ga je opredelila kot organiziran odnos med javnimi in zasebnimi organizacijami, ki vzpostavlja skupen obseg, cilje, namene, določa vloge in metodologijo za doseganje skupnih ciljev.

Do sodelovanja pride pri pojavu različnih groženj, kot so terorizem, kibernetski kriminal, naravne grožnje, odpoved sistema, za katere je potrebno širše sodelovanje in pri čemer varnosti ne morejo zagotoviti le državni akterji, ter pri izvajanju preventive. Cilje v državnih strategijah je mogoče doseči le s sodelovanjem zasebnega sektorja, saj lahko le z njegovo pomočjo države ščitijo ključno infrastrukturo. Vključenost akterjev je odvisna od grožnje, ki je postavljena kot prioriteta. Delujejo lahko na različnih ravneh: lokalni, znotraj posameznega sektorja ključne infrastrukture, medsektorsko, tematsko na podlagi skupnega interesa, na evropski ali globalni ravni. Sodelovanje lahko poteka med različnimi javno-

zasebnimi partnerstvi, lahko imajo centralni organ, ki vse regulira, vladno telo ali preko CERT-a.

V podkategoriji sem preverjala, ali imajo države zakonsko podlago za javno-zasebno sodelovanje. Zakonsko obvezno sodelovanje z akterji ključne infrastrukture ni uveljavljeno v proučevanih državah, vendar države regulirajo odnos javno-zasebno z različnimi pristopi, kot so zakoni o javnem naročanju in drugimi zakoni, ki regulirajo odnos z določenimi shemami sodelovanja. Potrebno se je zavedati, da prevelike omejitve s strani države preko zakonov negativno vplivajo na zainteresiranost privatnega sektorja, zato prevelike omejitve in zakonski okvir lahko pomenijo tudi potencialno izgubo zasebnih akterjev, pripravljenih sodelovati v tako imenovanem partnerstvu.

V letu 2009 v Avstriji in Bolgariji ni obstajala specifična zakonodaja na področju javno-zasebnega partnerstva, projekti so se izvajali v obliki koncesij v skladu z zakonodajo o javnih naročilih. Podobno kot v Bolgariji so na Cipru želeli uvesti posebno formo za sodelovanje med javnim in zasebnim sektorjem, a poseben zakon na tem področju ne obstaja. Situacija je enaka na Danskem, kjer kljub prizadevanju parlamenta za uvedbo shem za sodelovanje na tem področju posebna zakonodaja ne obstaja (European Public Private Partnership Expertise Centre 2009, 29−39). V Litvi ne obstaja zakon na tem področju, prav tako ni začrtane PPP strategije. Podobna je situacija na Malti ter Romuniji (European Public Private Partnership Expertise Centre 2009, 68−88). Na Švedskem ne obstaja posebna zakonodaja, prav tako je ena izmed redkih proučevanih držav, katerih vladna politika ne favorizira javno-zasebnega partnerstva in mu ni naklonjena. Kar se kaže tudi v podatku, da v letu 2009 na državni ravni ni bil izveden noben PPP projekt ter le dva na lokalni ravni. Na Nizozemskem so uvedeni EU zakoni glede javnih naročil, v letu 2009 so predlagali tudi nov zakon. V državi so določeni sektorji bolj regulirani z ustanavljanjem organov za PPP, kot je na primer obrambno, izobraževalno in transportno področje. Poseben zakon na področju javno-zasebno partnerstvo ne obstaja (European Public Private Partnership Expertise Centre 2009, 75−107). V Estoniji ne obstaja enoten in specifičen zakon glede javno-zasebnega partnerstva, to področje je regulirano z zakonom o javnih naročilih. Poleg usmeritev v zvezi z javnim naročanjem v državi ne obstajajo uradne smernice in pravni okvirji za sodelovanje, prav tako ne obstaja PPP organ, ki bi se s tem področjem ukvarjal (Gide 2011, 7).

Na drugi strani so države, kot je Češka, kjer kljub njegovim določenim nepopolnostim obstaja zakon na področju javno-zasebnega partnerstva. V skupino z zakonom na tem področju spada tudi Francija, ki je zakon sprejela leta 2008, v državi je v letu 2009 obstajalo več kot 200 projektov, v katerih sta sodelovala javni in zasebni sektor. V Nemčiji obstaja

zakonodaja na tem področju, prav tako pa ima država razvite regionalne organe in organe – pristojne centre za javno-zasebno partnerstvo, na ravni zveznih državah od leta 2009, ki pomagajo pri načrtovanju sodelovanja, svetovanju in s praksami. V Grčiji od leta 2005 obstaja posebna zakonodaja, prav tako pa imajo ustanovljena posebna organa, ki se ukvarjata z javno-zasebnimi projekti, in sicer medresorski odbor in poseben sekretariat za javno-zasebna partnerstva. Njihova oblika organiziranja javno-zasebnega partnerstva naj bi bila zgled tudi drugim državam. Na Madžarskem je od leta 2003 poseben zakon na tem področju doživel že več amandmajev. Prihodnost sodelovanja javno-zasebno ni videti v najboljši luči. V Italiji obstaja zakon, ki ureja proceduro sodelovanja med javnim in zasebnim sektorjem (European Public Private Partnership Expertise Centre 2009, 37−65). V Latviji zakon obstaja od leta 2000, prav tako obstaja register vseh javno-zasebnih partnerstev, investicijska razvojna agencija - LIDA, ki je odgovorna za implementacijo PPP projektov, izvajanje osnutkov, promocijo in nudenjem informacij, PPP posvetovalni odbor. Zakoni obstajajo na Irskem, na Poljskem, v Sloveniji, Španiji. Portugalska je ena izmed najbolj aktivnih držav na PPP trgu in ima zakon na PPP področju iz leta 2008, čas, v katerem so sistematizirali in združili različna pravila v raznih statutih (European Public Private Partnership Expertise Centre 2009, 83−104). Podatki niso bili dosegljivi za Veliko Britanijo in Belgijo.

Tabela 3.12: Obstoj in neobstoj zakonov na področju javno-zasebnega partnerstva

PPP zakon obstaja	PPP zakon ne obstaja
13	10
Češka	Avstrija
Francija	Bolgarija
Nemčija	Ciper
Grčija	Danska
Madžarska	Litva
Italija	Malta
Latvija	Nizozemska
Portugalska	Romunija
Poljska	Švedska
Irska	Estonija
Slovenija	
Španija	
Češka	

Vir: European Public Private Partnership Expertise Centre (2009) in Gide (2011).

3.4.6 Kibernetsko varnostne obligacije

Kibernetsko varnostne obligacije na ravni EU sem merila z »Budimpeštsko« konvencijo o kibernetskem kriminalu, ki je edini mednarodni zavezujoči dokument na področju kriminala, storjenega preko interneta in drugih računalniških omrežij.

Po podatkih iz poročila Norton o kibernetski kriminaliteti iz leta 2011 so stroški svetovne kibernetske kriminalitete letno znašali 114 milijard dolarjev. Temu strošku so prišteli še čas, ki so ga uporabniki izgubili zaradi kibernetskega kriminala, pri čemer je bila izguba še nadaljnjih 274 milijard dolarjev. Predvideni stroški so znašali 388 milijard dolarjev letno. Po njihovih podatkih je dve tretjini odraslih že bilo žrtev spletnega kriminala. Vsako sekundo naj bi bilo 14 odraslih žrtev spletnega kriminala (Symantec).

Konvencija je bila sprejeta leta 2001 s strani Sveta Evrope. Služi kot usmeritev za dopolnjevanje nacionalne zakonodaje v preprečevanju kibernetskega kriminala in kot okvir za sodelovanje med državami podpisnicami s harmonizacijo nacionalnih zakonov. Obsega področja kršitev avtorskih pravic, povezanih z računalniškimi goljufijami, otroško pornografijo ter kršitve varnosti omrežij. Ilegalni dostop, ilegalno prestrezanje, motenje podatkov in sistemov, zloraba naprav, računalniško povezane prevare in ponarejanja, otroška pornografija in kršitve glede avtorskih pravic so opredeljeni kot kriminalno dejanje. Za preprečevanje omenjenih kriminalnih dejanj so predvideni ukrepi, med njimi je tudi takojšnje zavarovanje shranjenih podatkov o prometu, iskanje in prestrezanje podatkov o vsebini, zaseg računalniških podatkov, omogočeno spremljanje s strani internetnih ponudnikov o uporabi spleta v realnem času ter vedno dostopna mreža med podpisnicami za zagotavljanje medsebojne pomoči. Države podpisnice morajo z inkriminacijo omenjenih kaznivih dejanj uvesti spremembe v kazenskem in materialnem pravu ter spremeniti predpise, ki urejajo telekomunikacije. Konvencija je v veljavi v 19 državah, 5 držav jo je podpisalo, a ne ratificiralo. Med proučevanimi državami so vse podpisnice omenjene konvencije (Svet Evrope in Svet Evrope 2001).

Tabela 3.13: Varnostne obligacije s Konvencijo o kibernetskem kriminalu

Nepodpisnice	Podpis, brez ratifikacije (leto)	V veljavi (od leta)
0	5	19
	Češka (2005)	Avstrija (2012)
	Grčija (2001)	Belgija (2012)
	Irska (2002)	Bolgarija (2005)
	Poljska (2001)	Ciper (2005)

	Švedska (2001)	Danska (2005)
		Estonija (2004)
		Francija (2006)
		Nemčija (2009)
		Madžarska (2004)
		Italija (2008)
		Latvija (2007)
		Litva (2004)
		Malta (2012)
		Nizozemska (2007)
		Portugalska (2010)
		Romunija (2004)
		Slovenija (2005)
		Španija (2010)
		Velika Britanija (2011)

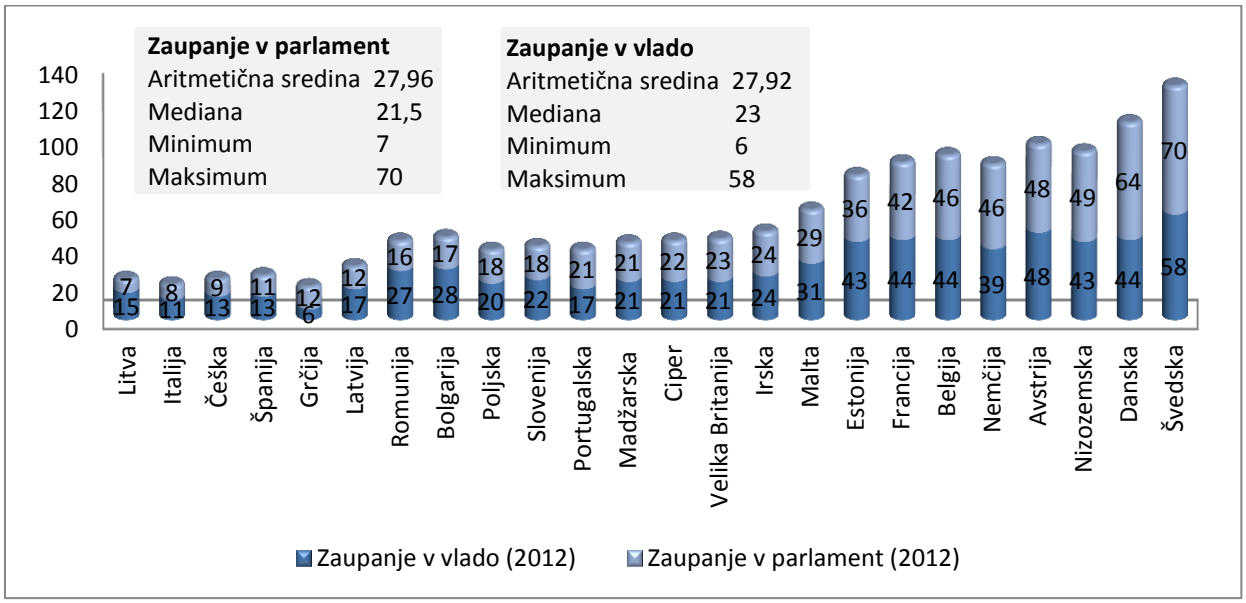
Vir: Svet Evrope.

3.4.7 Politična učinkovitost

Politično učinkovitost lahko merimo po uspešnih izvedenih politikah, jaz pa jo bom določila na podlagi dojemanja korupcije in anket o zaupanju v politične institucije, in sicer v vlado in parlament.

Javni instituciji nimata večinske podpore v kar 22 državah, za kar lahko iščemo vzroke tudi v ekonomski krizi. Več kot polovica prebivalstva zaupa parlamentu in vladi le na Švedskem, kjer vladi zaupa 58 %, parlamentu pa 70 % ljudi. Večje zaupanje v proučevanih državah najdemo na Danskem, Nizozemskem, v Avstriji, Nemčiji, Belgiji in Franciji, kjer malenkost manj kot polovica prebivalcev zaupa v javne institucije. Najmanjše zaupanje najdemo v Litvi, Italiji, na Češkem, v Grčiji, Latviji in Romuniji, kjer je zaupanje nižje od 20 % v obe državni instituciji (Eurobarometer 2012).

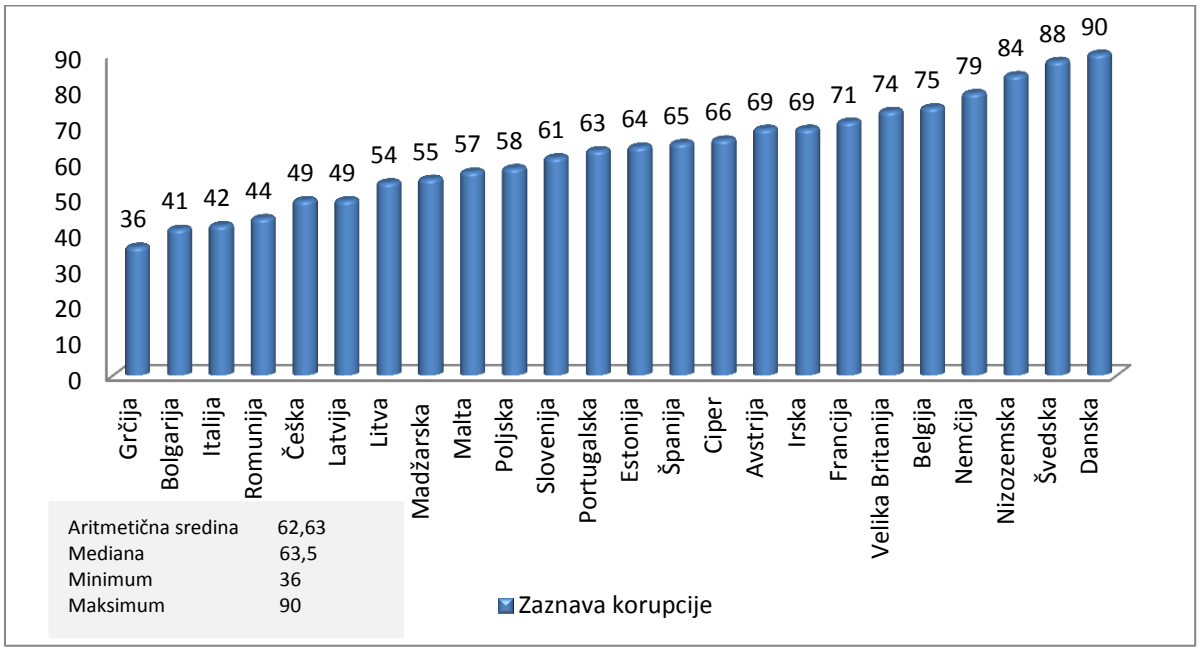
Slika 3.24: Zaupanje v javne nacionalne institucije



Vir: prirejeno po Eurobarometer (2012).

Transparency International razvršča države glede na zaznavnost korupcije, pri čemer vsaka država zasede določeno vrednost od 0 do 100, kjer je 100 najboljši rezultat in pomeni, da v državi ni korupcije, ter 0, da je korupcija razširjena po celotni državi in predstavlja velik problem. Korupcija je najmanjša na Danskem, ki je na prvem mestu tudi pri razvrstitvi vseh držav sveta. Korupcija je prisotna na Švedskem, v Nemčiji, Veliki Britaniji, Franciji, Avstriji in na Cipru, a ne predstavlja perečega problema, saj so vse države med 29 državami z najmanjšo korupcijo. V Grčiji je korupcija največji problem izmed proučevanih držav, na svetovnem mestu je izmed 174 držav uvrščena na 94. mesto in spada v tretjo skupino držav z najbolj razširjeno korupcijo. Zaznava korupcije je velika tudi v Bolgariji, Italiji, Romuniji, na Češkem in v Latviji (Transperancy International 2012).

Slika 3.25: Zaznava korupcije



Vir: Transparency International (2012).

3.5 RAZVRSTITEV DRŽAV GLEDE NA KIBERNETSKO MOČ

Kibernetsko moč sem državam določila na podlagi vseh znanih numeričnih kategorij, pri čemer sem od najmanjše do najvišje vrednosti v podkategorijah državam pripisala vrednosti od 1 do 24, pri čemer ena točka pripada državi v posamezni podkategoriji z najmanjšo vrednostjo in 24 državi z najvišjo vrednostjo. V primeru, kjer sta dve ali več držav zasedli isto mesto, sem obema pripisala isto število točk, naslednja država pa je imela število točk, kot če dve ali več držav ne bi zasedali istega mesta. Nekatere podkategorije, ki so sestavljene iz različnih kriterijev, sem točkovala enako kot ostale podkategorije in jih nato seštela, zato imajo tudi vrednosti večje od 24. Število vseh doseženih točk prikazuje kibernetsko moč držav, pri čemer ima država z večjim številom točk večjo kibernetsko moč. Tabele s pripisom točk najdemo v prilogah.

Za lažjo interpretacijo določitve kibernetske moči v uporabi IKT v industriji naj navedem, kako sem kategorizirala države v enotnih ter sestavljenih podkategorijah. Pri razvrstitvi držav neštevilčnih podkategorij, kot je e-zdravje, sem državam pripisala številke od ena do tri (odvisno, koliko je podobnosti med državami), pri čemer sem z vrednostjo ena označila države, ki nimajo razvitega elektronskega zdravstva, tiste z vrednostjo dva imajo delno razvito elektronsko zdravstvo, z elektronskimi kartotekami ali elektronskimi recepti,

tiste z vrednostjo tri pa imajo razvite elektronske kartoteke in elektronske recepte na ravni celotne države in ne le v določenih regijah kot države, ki imajo pripisano vrednost dva. Prav tako je podkategorija inteligentni promet sestavljena iz dveh dimenzij, in sicer iz dostopnosti potovalnih informacij in obstoja elektronskega cestninjenja. Pri potovalnih informacijah sem državam pripisala vrednosti od ena do tri, pri čemer države z vrednostjo ena nimajo dostopnih ali imajo zelo omejene potovalne informacije, države z vrednostjo dva imajo omejene informacije in države z vrednostjo tri imajo dostopne potovalne informacije. Pri elektronskem cestninjenju pri državah z vrednostjo ena elektronsko cestninjenje ne obstaja, z vrednostjo dva imajo brezplačno uporabo avtocest, države z vrednostjo tri imajo različne sisteme cestninjenja za tujce in domačine ali v državi obstaja na določenih predelih elektronske cestninjenje na nekaterih pa ne, države z vrednostjo 4 pa imajo elektronsko cestninjenje na celotnem območju države na avtocestah. Vrednosti v prilogi pod inteligentnimi transportnimi sistemi prikazujejo seštevek vrednosti iz potovalnih informacij, obstoja/neobstoja elektronskega cestninjenja ter pristopa ali nepristopa k memorandumu o elektronskem klicu. V tej kategoriji je sestavljena podkategorija še inteligentni promet. Države sem razvrstila glede na implementacijo, načrte ter napovedi števila pametnih števcev ter glede na zakonsko podlago za njihov razvoj.

Tabela 3.14: Razvrstitev držav na podlagi uporabe IKT v industriji

Razvrstitev držav na podlagi uporabe IKT v industriji	
1. Nizozemska	13. Estonija
2. Švedska	14. Češka
3. Velika Britanija	15. Slovenija
4. Francija	16. Poljska
5. Danska	17. Portugalska
6. Nemčija	18. Madžarska
7. Avstrija	19. Litva
8. Belgija	20. Grčija
9. Irska	21. Latvija
10. Španija	22. Ciper
11. Italija	23. Romunija
12. Malta	24. Bolgarija

Iz tabele 3.14 lahko vidimo, da imajo Nizozemska, Švedska, Velika Britanija, Danska in Francija v povprečju najbolj razvita pametna omrežja, elektronsko zdravstvo, inteligentni promet, elektronsko upravo ter največ ljudi in podjetij, ki naročajo preko spleta ter uporabljajo spletno bančništvo. Najmanj razvito uporabo IKT v industriji pa najdemo v Bolgariji, Romuniji, na Cipru in v Latviji. Z vedno novimi zahtevami v okviru napredka in večanju produktivnosti se vidi konstanten napredek v vseh držav članicah EU na vseh proučevanih

področjih. Pojavljajo se nove iniciative za razvoj pametnih omrežij tako na ravni posameznih držav kot tudi na ravni EU, vedno več je govora in razvijanja elektronskega zdravstva in prenašanje podatkov v računalniške oblake in v elektronske oblike, čeprav se vidi tudi manjši denarni vložek v razvoj zaradi globalne krize. Kljub temu pa se vidijo razlike med državami članicami, saj še vedno obstaja vidna razdelitev na razviti zahod in manj razviti vzhod.

V naslednji kategoriji ekonomski in družbeni kontekst tabela 3.15 prikazuje, da Švedska, Velika Britanija, Nizozemska, Francija in Nemčija v povprečju vodijo v podkategorijah pričakovane dobe šolanja, terciarnemu študentskemu vpisu, številu diplom iz znanosti in tehnologije, številu raziskovalcev v raziskavah in razvoju, v izvozu in uvozu IKT, izdatkih za raziskave in razvoj, številu vloženih domačih patentov ter ozaveščenosti prebivalstva. Situacija je podobna kot pri kategoriji uporabi IKT v industriji, saj so na prvih petih mestih zahodnoevropske, medtem ko zadnja mesta v večini zasedajo vzhodnoevropske države. Na zadnjih petih mestih so uvrščene Romunija, Belgija, Litva, Ciper ter Bolgarija. Podkategorije so pomembne za zagotavljanje kibernetske varnosti preko človeškega kapitala s tehničnimi kompetencami in usposobljenostjo. Kljub vodstvu Švedske je le-ta na prvem mestu le v podkategoriji izdatki, namenjeni za raziskave in razvoj, prav tako pa je uvrščena v večini ostalih podkategorijah v sam vrh.

Tabela 3.15: Razvrstitev držav na podlagi ekonomskega in družbenega konteksta

Razvrstitev držav na podlagi ekonomskega in družbenega konteksta	
1. Švedska	13. Irska
2. Velika Britanija	14. Češka
3. Nizozemska	15. Poljska
4. Francija	16. Italija
5. Nemčija	17. Portugalska
6. Slovenija	18. Estonija
7. Madžarska	19. Latvija
8. Avstrija	20. Romunija
9. Danska	21. Belgija
10. Grčija	22. Litva
11. Malta	23. Ciper
12. Španija	24. Bolgarija

Razlike v podkategoriji izobrazba med proučevanimi državami niso velike. V podkategorijah izvoz in uvoz IKT, ki prikazujeta trgovanje posameznih držav, so nepričakovano na prvem mestu Malta, Madžarska in Češka, ki vodijo v izvozu in uvozu IKT kot % celotnega uvoza in izvoza. Zanimivo je tudi, da so v vseh proučevani državah ljudje

dobro seznanjeni s pomembnejšimi grožnjami, ki jim pretijo iz kibernetskega prostora, ter v vseh državah več kot 90 % ljudi uporablja razne zaščitne programske opreme, kar zmanjšuje grožnje in tveganja, ki so značilna za virtualni prostor.

Naslednja kategorija je tehnološka infrastruktura, ki je hitro spremenljiva kategorija, saj je v letu 2012 v EU internet uporabljalo že 73 % prebivalstva. Ob predpostavki, da so vse podkategorije v kategoriji tehnološka infrastruktura enakovredne, Danska dosega najboljše rezultate, sledijo ji Švedska, Velika Britanija, Nizozemska ter Nemčija. V teh državah je odstotek prebivalcev, ki uporabljajo internet, višji od 81. So v večini nad povprečjem glede razširjenosti mobilne telefonije. Velika Britanija, Nemčija in Švedska so uvrščene med štiri države z najvišjim številom brezžičnih dostopnih točk. V državah najdemo tudi nadpovprečno uporabo socialnih omrežij, dostopanje do novic preko spleta, pri čemer je Danska na prvem mestu tudi pri številu naročnikov širokopasovnih linij in varnih strežnikov ter večjih izdatkih, namenjenih za informacijsko tehnologijo. Za hitrejši internet pa je v teh državah predvidena tudi višja mesečna tarifa. Grčija, Romunija, Bolgarija in Ciper imajo najslabše razvito tehnološko infrastrukturo. Kljub temu je Ciper v podkategorijah dostopnost do mobilne telefonije in interneta, ki sem jo izrazila z mesečnimi tarifami, dosegel visoke vrednosti, saj bolj kot je cena nižja, večja je dostopnost.

Tabela 3.16: Razvrstitev držav na podlagi razvitosti tehnološke infrastrukture

Razvrstitev držav na podlagi razvitosti tehnološke infrastrukture	
1. Danska	13. Latvija
2. Švedska	14. Irska
3. Velika Britanija	15. Slovenija
4. Nizozemska	16. Češka
5. Nemčija	17. Španija
6. Avstrija	18. Portugalska
7. Belgija	19. Poljska
8. Malta	20. Italija
9. Estonija	21. Ciper
10. Litva	22. Bolgarija
11. Madžarska	23. Romunija
12. Francija	24. Grčija

V zadnji kategoriji pravni okvir sem zaradi opisnih podkategorij uporabila različno točkovanje od ostalih podkategorij, pri čemer sem, kjer je podkategorija prisotna, dodala številko 1 in ob odsotnosti državi dodala 0, saj so v večini podkategorij nominalne spremenljivke, pri katerih je možno videti le razlikovanje med njimi, torej odsotnost ali

prisotnost določenega akterja oziroma organa ali prisotnost in odsotnost zakonske podlage pri podkategoriji javno-zasebno partnerstvo. Podkategorija obstoj kibernetskih zakonov mi ni dala vpogleda, katera država ima boljšo in katera slabšo zakonsko podlago, saj imajo vse države določene zakone in predvidene kazni za posamezna kibernetska kriminalna dejanja, pri katerih pa ni mogoče določiti, kaj je boljša in kaj slabša ureditev. Za nadaljnjo proučevanje bi bilo potrebno pogledati tudi izvajanje v praksi. Prav tako imajo vse države razen Cipra, Slovenije in Italije razvit državni/vladni CERT, pri čemer sem z 0 točkovala te države, z 1 tiste, ki državni CERT imajo, a nimajo obveznega poročanja o kibernetskih incidentih, ter z 2 tiste, ki imajo državni CERT z obveznim poročanjem o kibernetskih incidentih.

Tabela 3.17: Razvrstitev držav na podlagi pravnega okvira

Razvrstitev držav na podlagi pravnega okvira	
1. Danska	13. Slovenija
2. Švedska	14. Madžarska
3. Nizozemska	15. Portugalska
4. Nemčija	16. Poljska
5. Belgija	17. Romunija
6. Avstrija	18. Bolgarija
7. Francija	19. Španija
8. Estonija	20. Latvija
9. Velika Britanija	21. Litva
10. Irska	22. Češka
11. Malta	23. Italija
12. Ciper	24. Grčija

V pravnem okviru, kjer sem proučevala obstoj ali neobstoj državne kibernetske strategije, centralno kibernetsko izvršilnega organa, javno-zasebnega partnerstva, kibernetsko varnostnih zakonov, mednarodnih varnostnih obligacij na kibernetskem področju ter politične učinkovitosti so na prvih mestih Danska, Švedska, Nizozemska ter Nemčija. Na zadnja mesta pa so uvrščene Grčija, Italija, Češka ter Litva. Kljub pomembnosti kibernetskega prostora večina držav nima razvitih strateških dokumentov, kot je nacionalna kibernetska strategija. Izmed 24 držav jih 16 nima razvitega usmerjevalnega dokumenta. EU spodbuja razvoj državnih CERT-ov, ki za enkrat ne obstajajo le v treh proučevanih državah. V večini držav poročanje o kibernetskih incidentih ni obvezno ali obveznost in na drugi strani prostovoljnost ni jasno določena, kar predstavlja pomanjkljivosti pri zagotavljanju varnosti, saj ne poznamo realnega stanja vdorov in se posledično na probleme ne odzivamo primerno. Le v petih proučevanih državah obstaja centralno kibernetsko izvršilni organ, ki koordinira delo in

informacije med različnimi akterji, katerih sodelovanje je nujno potrebno za učinkovito delovanje v smeri zaščite, preventive in odpravljanje posledic vdorov. V vseh državah imajo določene kazni za določena kazniva dejanja v kibernetskem prostoru, pri čemer ne morem reči, da so ene kazni, zakoni in členi v zakonikih boljše in boljši od drugih. Za celovitejšo sliko bi morali pogledati tudi dejansko stanje upoštevanja zakonov in predpisovanja kazni. V večini držav se vidi tudi sodelovanje med javnim in zasebnim sektorjem. Prav tako so vse proučevane države podpisnice Budimpeštske konvencije, v petih še ni prišlo do ratifikacije. Zaupanje v javne institucije je v večini držav zelo nizko, saj le na Danskem in Švedskem več kot 50 % prebivalstva zaupa v parlament in le na Švedskem več kot 50 % v vlado. Rezultati so v določeni meri pogojeni z gospodarskim nazadovanje in trenutno gospodarsko ter ekonomsko krizo. Zaznava korupcije je največji problem v južnih in vzhodnih proučevanih državah ter najmanjši v zahodnih. Danska in Švedska sta na prvem mestu predvsem zaradi politične učinkovitosti, kljub temu da nimata zakona na področju javno-zasebnega partnerstva, državne kibernetske strategije ter prav tako ne centralno kibernetsko izvršilnega organa. Švedska, ki zaseda drugo mesto, ni niti ratificirala Budimpeštske konvencije. Medtem ko imajo Nizozemska, Nemčija, Francija, Velika Britanija v večini razvite celovite nacionalne kibernetske načrte, vendar zaradi manjše politične učinkovitosti niso na prvih mestih, ampak kljub temu v samem vrhu.

Tabela 3.18 prikazuje razvrstitev vseh štiriindvajset proučevanih držav članic EU glede na kibernetsko moč. Prvo mesto zasedajo Švedska, Velika Britanija, Nizozemska, Danska, Nemčija ter Francija. Najmanjšo kibernetsko moč pa imajo države Bolgarija, Romunija, Ciper, Litva in Grčija. Države na prvih mestih imajo več resursov in zmogljivosti, ki jih lahko uporabijo za vplivanje na kibernetski in nekibernetski prostor za podporo lastnih političnih ciljev in interesov. Na kibernetsko moč torej vplivajo uporaba IKT v industriji, tehnološka infrastruktura, ekonomsko-socialni kontekst ter pravna podlaga.

Tabela 3.18: Razvrstitev držav na podlagi vseh kategorij

Razvrstitev držav glede na kibernetsko moč	
1. Švedska	9. Irska
2. Velika Britanija	10. Estonija
3. Nizozemska	11. Belgija
4. Danska	12. Španija
5. Nemčija	13. Madžarska
6. Francija	14. Slovenija
7. Avstrija	15. Poljska
8. Malta	16. Italija

17. Češka	21. Litva
18. Portugalska	22. Ciper
19. Latvija	23. Romunija
20. Grčija	24. Bolgarija

IKT sektor je pomembni dejavnik za nadaljnji razvoj, vendar se z rastjo kibernetske odvisnosti večajo tudi varnostna tveganja. Za ohranjanje ravnovesja morajo države razvijati tudi varnostne mehanizme, koherentne in celostne politike. V vedno bolj povezanem in soodvisnem svetu je potrebno razumeti, kaj kibernetska moč prinaša posameznim državam, organizacijam, nedržavnim akterjem ter posameznikom. S širjenjem kibernetsko tehnološke infrastrukture ter vedno večjo uporabo IKT v industriji postaja vprašanje kibernetske in na splošno varnosti v digitaliziranem svetu pomembno vprašanje.

4 SKLEP IN VERIFIKACIJA HIPOTEZ

Danes je vse povezano z IKT sektorjem in se tako ali drugače navezuje na kibernetski prostor. Rast kibernetske moči s seboj prinaša tudi »nove« ranljivosti ter grožnje. Skozi empirični del se da razbrati, da na vse vidike varnosti bodisi, da je to nacionalna, družbena, posameznikova, omrežna ali informacijska, vplivajo stopnja uporabe IKT v industriji, ekonomsko-socialni kontekst, tehnološka infrastruktura ter pravni okvir. V kibernetskem prostoru se pojavljajo različne grožnje, napadi, nedelovanja, motnje, napake, kraje ter spremembe podatkov v virtualnem svetu, ki so bodisi namerni bodisi nenamerni, a vsi vplivajo na zmanjševanje varnosti. Vidi se porast uporabe IKT v vseh panogah, prav tako je govora o kibernetski vojnah in napadih, ki se marsikomu zaradi premajhnega poznavanja področja zdijo dokaj neverjetne, a lahko najdemo primere v sedanjosti in nedavni zgodovini. Ljudje se premalo zavedamo, da je vsa ključna infrastruktura povezana s svetovnim spletom, se jo da upravljati na daljavo in je vanjo možno tudi vdreti, kar lahko povzroči njeno nedelovanje in z njim ogroža tudi izvenkibernetska področja ter posameznike. Motnje, spremembe, nedelovanja v kibernetskem prostoru lahko povzročijo materialno, gmotno, finančno, gospodarsko in človeško škodo v realnem svetu. Večji vpliv imajo torej posredni učinki kibernetskega napada in ne neposredni. Ravno zaradi novih ranljivosti z razvojem kibernetske moči se je prvotno raziskovalno vprašanje glasilo, kako kibernetska moč vpliva na varnost. Kibernetska moč vpliva na vse akterje, bodisi so to države, družbene skupine, mednarodne organizacije, posamezniki, IKT in omrežja. Kibernetska moč je v večini uporabljena skupno z drugimi aspekti moči, saj je celota resursov države, ki jih lahko le-ta uporabi za uresničevanje lastnih interesov, ki obsegajo tako

državne kot nedržavne akterje. Kot vemo, je varnost težko meriti in s posameznimi indikatorji, ki določajo stopnjo varnosti, poenostavljamo kompleksno stvarnost. Popolne varnosti seveda ni mogoče doseči, prav tako je le-ta subjektivno zaznana. Sklep glede povezave med varnostjo in kibernetsko močjo je, da večja kibernetska moč ne pomeni nujno večje ali manjše varnosti. Večja odvisnost od IKT in povezanost ključne infrastrukture vodi do večje ranljivosti, saj v primeru napada ali nedelovanja prekinemo tok vsakodnevnih nujnih in manj nujnih storitev. Družbam in državam, ki so omrežno bolj prepletene, predstavlja nedelovanje omrežij večjo grožnjo kot tistim, ki imajo slabše razvito tehnološko infrastrukturo in s tem tudi manj uporabe IKT v industriji in v vsakdanjem življenju z dostopanjem do spletnih storitev, kot so e-uprava, e-volitve in drugih. Na drugi strani pa tudi ne morem trditi, da kibernetska moč zmanjšuje varnost, saj lahko ranljivosti in grožnje varnosti zmanjšamo z oblikovanjem zakonov, strategij, splošnih načel in norm, ki naj se v virtualnem svetu upoštevajo, organov za preiskovanje, odkrivanje, obnovo in preprečevanje, z obveščanjem in ozaveščanjem o oblikah ogrožanja varnosti. Kibernetska moč na eni strani pomeni več ranljivosti in izpostavljenosti za možne napade v primeru njene odvisnosti, ki pa jo je mogoče zmanjšati s sodelovanjem, izobrazbo, ozaveščanjem, inovacijami v strojni in programski opremi. Kibernetska moč torej ne zmanjšuje niti ne povečuje varnosti. Vse je odvisno od posamezne države ali se neomejenih groženj varnosti zaveda ter v tej smeri tudi deluje z razvojem varnostnih mehanizmov. Dejstvo je, da je za zagotavljanje varnosti potrebno sodelovanje vseh akterjev. Kljub temu da ne moremo govoriti o negativni ali pozitivni povezanosti kibernetske moči in varnosti, pa povezava med obema obstaja. Zagotavljanje varnosti v kibernetskem prostoru je težka naloga, saj ne obstaja monopol zaradi decentraliziranosti. V ostalih domenah, kot so zrak, voda, kopno igrata vlada in država s svojimi organi za zagotavljanje varnosti najpomembnejšo vlogo, kar pa v primeru kibernetskega prostora ne drži, saj imajo veliko vlogo nedržavni akterji. Države so usposobljene za zagotavljanje varnosti na vojaškem področju, kjer obstajajo različni načrti v primeru napada, ki pa v nekaterih državah za primer kibernetskega napada niti ne obstajajo. Tehnologija je postala področje ter tudi tehnika bojevanja. Kibernetska moč torej zajema tako ofenzivne kot defenzivne zmogljivosti države, pri čemer so pomembni različni akterji in ravno zaradi te kompleksnosti pridejo v poštev vse teorije od realizma, liberalizma do konstruktivizma, ki predpostavljajo različne načine zagotavljanja varnosti.

Države članice EU imajo lastne zakone, ideje, razlike in večinoma vsaka po svoje definira mehanizme za zagotavljanje kibernetske varnosti, kljub temu pa imamo na ravni EU že sprejete skupne zakone za to področje, ki pa so še v razvoju. Na kibernetskem področju je

malo skupnih definicij, dogovorov, skupnih ukrepov ob morebitnih grožnjah, nekoherentnost regulacije in nadzornih mehanizmov, kar predstavlja problem pri sklepanju skupnih resolucij in ukrepov, ki so potrebni za zagotavljanje varnosti.

V nalogi sem preučevala, ali imajo države z bolj razvito IKT infrastrukturo bolj razvite varnostne mehanizme za njeno zaščito. Za zanesljivo, trajnostno in varno uporabo je potreben enakomeren razvoj v smislu razvoja IKT infrastrukture in zmogljivosti ter zaščitnih mehanizmov. Med mehanizme za zaščito IKT infrastrukture spadajo človeški kapital z znanjem, izobrazbo, usposobljenostjo ter ozaveščenostjo prebivalstva, zakonska podlaga, obstoj organov za zaščito kibernetskega prostora, inovacije v programski in strojni opremi in tehnologiji, sodelovanje med javnim in zasebnim sektorjem za delovanje v preventivi, v primeru napadov in v času obnove.

Države z bolj razvito IKT infrastrukturo, kamor sem štela kategoriji tehnološke infrastrukture in uporabe IKT v industriji, so Švedska, Velika Britanija, Danska, Nizozemska, Nemčija, Avstrija, Belgija, Francija, Malta, Irska, Estonija in Španija. Pri čemer sem države ločila na polovico, 12 jih ima bolj razvito IKT infrastrukturo, druga polovica pa manj. V ostalih državah so pametna omrežja, e-zdravje, inteligentni promet, e-uprava, internetna ter mobilna razširjenost ter njuna dostopnost, izdatki za IKT, število varnih strežnikov ter druge podkategorije manj razviti ter manjši.

Vseh pet držav v EU, ki imajo centralno kibernetsko izvršilne organe, obstajajo v državah z bolj razvito IKT infrastrukturo. Prav tako imajo vse razvite državne CERT-e, katerim poročanje je obvezno le na Danskem, v Veliki Britaniji ter Nemčiji. V večini teh držav ne obstaja poseben zakon na področju javno-zasebnega partnerstva, kar tvori pomanjkljivosti zaradi neregulacije in manjšega sodelovanja z nedržavnimi akterji. Dve državi nista ratificirali Konvencije o kibernetskem kriminalu, ki služi kot usmerjevalni dokument za dopolnjevanje nacionalnih zakonodaj na področju kibernetskega kriminala, ki letno povzroči več kot 100 milijard dolarjev stroškov. V državah z manj razvito IKT infrastrukturo konvencije niso ratificirale tri države, prav tako v treh državah ne obstaja državni CERT, a v več državah obstaja zakon na področju javno-zasebnega partnerstva. V vseh proučevanih državah ima osem držav nacionalno kibernetsko strategijo, od tega jih je šest v državah z bolj razvito IKT infrastrukturo. Razen Malte in Irske vse države z bolj razvito IKT infrastrukturo spodbujajo inovacije, kar je vidno iz števila domačih vloženih patentov, ki je v teh državah večje. Večinoma so v teh državah ljudje tudi bolj seznanjeni ter obveščeni glede spletnega kriminala, ostalih kibernetskih groženj pa se prebivalci v EU v povprečju enako dobro zavedajo. Prav tako so vse države v zgornji polovici po številu diplom iz

znanosti kot odstotek vseh podeljenih diplom. Prav tako imajo v večini največje število raziskovalcev v raziskavah in razvoju. Imajo pa manjše število terciarnih študentskih vpisov na 100.000 prebivalcev kot države z manj razvito IKT infrastrukturo. Hipotezo, da imajo države z bolj razvito IKT infrastrukturo bolj razvite varnostne mehanizme za njeno zaščito, torej potrjujem za proučevane članice EU.

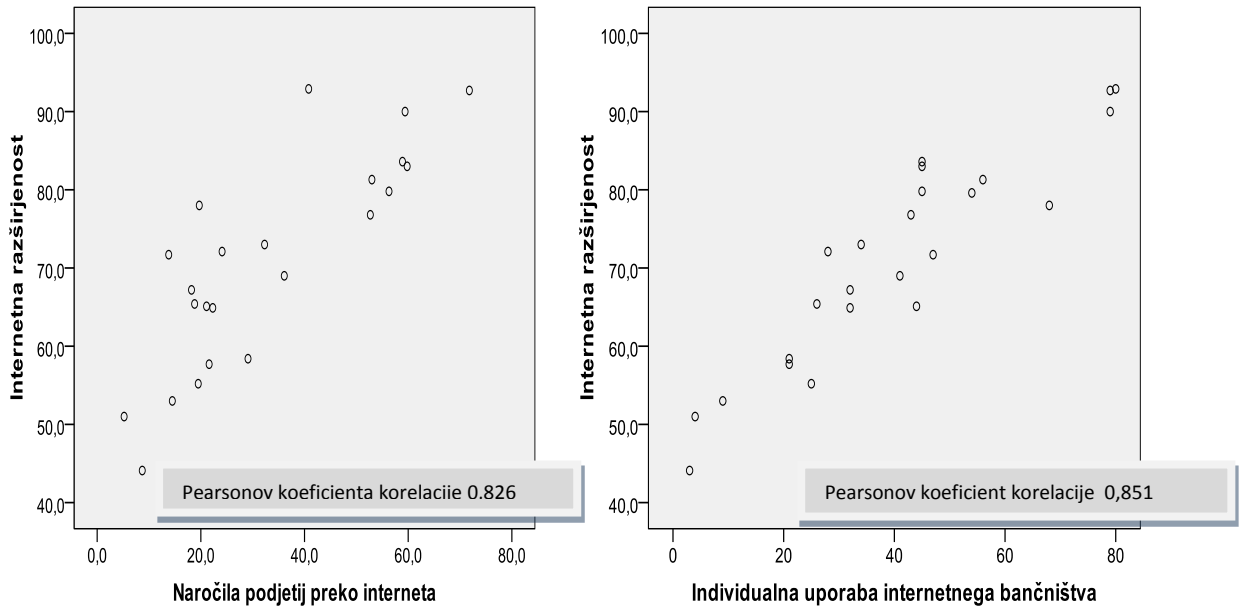
Za potrebe druge hipoteze, ki se glasi, da je kibernetska moč lažje dosegljiva tudi manjšim državam in je alternativa, da lahko po moči konkurirajo večjim, sem med manjše proučevane države uvrstila vse države, katerih prebivalstvo je manjše od petih milijonov. Manjših držav je torej sedem, in sicer so to Ciper (0,8 milijona prebivalcev), Estonija (1,3 milijona prebivalcev), Irska (4,5 milijona prebivalcev), Latvija (2,3 milijona prebivalcev), Litva (3,3 milijone prebivalcev), Malta (0,4 milijona prebivalcev) in Slovenija (2 milijona prebivalcev) (Portal EU). Vse omenjene manjše države niso na prvih sedmih mestih po kibernetski moči. Malta zaseda osmo mesto, Irska deveto, Estonija enajsto, Slovenija štirinajsto, Latvija devetnajsto, Litva enaindvajseto ter Ciper dvaindvajseto mesto. Majhne države, ki nimajo prevlade gledano na število prebivalcev in velikost države, lahko s kibernetsko močjo nadoknadijo te pomanjkljivosti, saj je kibernetska moč enakovredna drugim močem, ki so potrebne za uveljavljanje lastnih nacionalnih interesov. Manj kot polovica manjših držav, in sicer Malta, Irska, Estonija so uvrščene v prvo polovico držav z večjo kibernetsko močjo. Prav tako zadnji dve mesti zasedata večji državi. Načeloma je kibernetska moč definitivno alternativa za konkuriranje večjim državam po moči, vendar je možno situacijo na kibernetskem področju v proučevanih manjših državah članicah EU izboljšati. V podkategoriji uporabe IKT v industriji je Irska na devetem, Malta na dvanajstem, Estonija na trinajstem, Slovenija na petnajstem, Litva na devetnajstem, Latvija na enaindvajsetem, Ciper na dvaindvajsetem mestu. V ekonomskem-družbenem kontekstu Slovenija zaseda šesto mesto, Malta enajsto, Irska trinajsto, Estonija osemnajsto, Latvija devetnajsto ter Litva in Ciper dvaindvajseto ter triindvajseto mesto. Pri tehnološki infrastrukturi je Malta na osmem, Estonija na devetem, Litva desetem, Latvija trinajstem, Irska štirinajstem, Slovenija na petnajstem ter Ciper na enaindvajsetem mestu. V zadnji kategoriji pravni okvir je Estonija na osmem, Irska na desetem, Malta na enajstem, Ciper na dvanajstem, Slovenija na trinajstem, Latvija na dvajsetem ter Litva na enaindvajsetem mestu. Iz tega se vidi, da so države v posameznih podkategorijah različno razvrščene. Vse države kljub temu da so majhne, še niso izkoristile možnosti razvoja lastne kibernetske moči, saj so v večini podkategorij v sredini ali na zadnjih petih mestih. Vidi se tudi razlikovanje med vzhodnimi ter južnimi in zahodnimi državami. Hipotezo, da lahko manjše države s

kibernetsko močjo po moči konkurirajo večjim, na podlagi proučevanja kibernetske moči držav članic EU ne morem potrditi, vendar bi bilo to mogoče doseči s konstantnim napredkom na kibernetskem področju, s čimer zastavljeno hipotezo zavračam za konkreten primer proučevanja.

S pomočjo statističnega programa SPSS sem tudi preverila, ali katera naključna podkategorija vpliva na katero drugo ter ali obstaja njihova medsebojna povezanost, iskala sem statistične povezave med njimi. Pri uporabi grafične tehnike Scatter plots in Pearsonovega koeficenta korelacije, ki kaže linearno povezanost dveh številčnih spremenljivk, sem ugotovila, da v proučevanih državah EU obstaja pozitivna povezanost med internetno razširjenostjo in individualno uporabo spletnega bančništva ter med internetno razširjenostjo in naročili podjetij preko interneta. Večji kot je % prebivalcev, ki uporablja internet, več ljudi uporablja tudi spletno bančništvo ter več podjetij naročuje preko spleta. Prav tako velja obratno, saj v državah, kjer manjši % ljudi uporablja internet, ljudje tudi manjkrat uporabljajo spletno bančništvo in nakupujejo preko spleta, kar kaže tudi slika 4.1. Pearsonov koeficient korelacije pri obeh podkategorijah kaže na močno pozitivno povezanost, saj znaša več kot 0,8 in je statistično značilen s stopnjo značilnosti nižjo od 1 %. Potrebno je poudariti, da Pearsonov koeficient korelacije ne kaže vpliva ene spremenljivke na drugo, ampak le njuno povezanost.

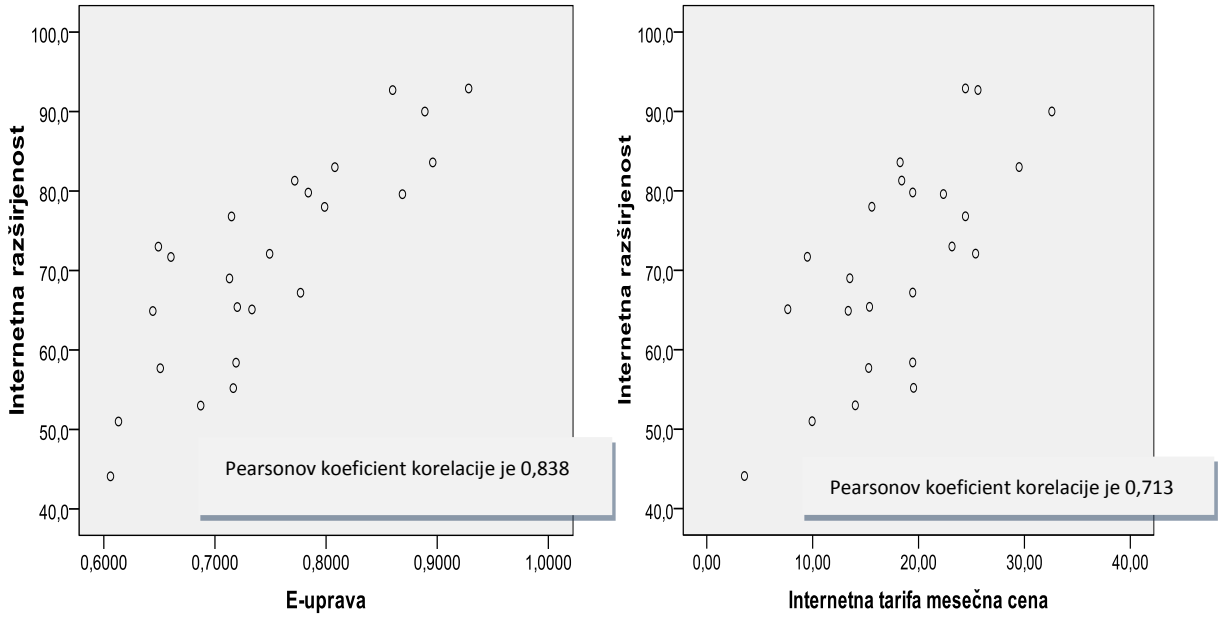
Po podatkih Evropske komisije (2012, 4) sta nakupovanje preko spleta in uporaba spletnega bančništva odvisna od stopnje samozaupanja v lastne sposobnosti ter seznanjenosti s kibernetskimi grožnjami. Kar 59 % prebivalcev EU namreč meni, da o kibernetskih grožnjah niso dobro informirani, kar lahko povežemo tudi z nizko povprečno stopnjo prebivalcev, ki nakupujejo preko spleta, ki znaša 26 % ter v povprečju okoli 40 % tistih, ki uporabljajo spletno bančništvo.

Slika 4.1: Pozitivna povezanost internetne razširjenosti s spletnimi naročili ter individualno uporabo spletnega bančništva



Več kot je uporabnikov interneta, bolj je tudi razvita e-uprava. Pearsonov koeficient korelacije znaša 0,838, kar kaže na močno pozitivno povezanost med internetno razširjenostjo in stopnjo razvoja e-uprave. Iz tega torej ne morem sklepati, da število uporabnikov interneta vpliva na stopnjo razvoja e-uprave, ampak da v proučevanih državah, kjer je več uporabnikov interneta, je bolj razvita elektronska uprava. Močna pozitivna povezanost obstaja tudi med internetno razširjenostjo in internetno mesečno tarifo, ki pokaže, da več, kot je internetnih uporabnikov, višja je internetna mesečna tarifa. Pearsonov koeficient korelacije kaže z več kot 0,7 na močno pozitivno povezanost. Države, kot so Danska, Švedska in Nemčija, imajo višje internetne mesečne tarife ter prav tako večji odstotek uporabnikov interneta, medtem ko je v državah, kot so Romunija, Litva, Latvija in Bolgarija, situacija ravno obratna. Poleg tega je potrebno upoštevati še, da v zahodnih in bolj razvitih državah obstaja večje število naročnikov linij visokih hitrosti, kar se po navadi kaže tudi v dražjih paketih, zato tudi takšna povezanost med spremenljivkama.

Slika 4.2: Pozitivna povezanost med internetno razširjenostjo in e-upravo ter internetnimi mesečnimi tarifami



Pozitivna povezanost obstaja tudi med zaznano korupcijo in zaupanjem v vlado in v parlament. Manjša kot je zaznana korupcija, večje je zaupanje v vlado in parlament. Pearsonov koeficient korelacije med zaznavo korupcije in zaupanjem v parlament je 0,844 ter med zaznavo korupcije in zaupanjem v vlado 0,732, kar kaže na močno pozitivno povezanost.

Internetna razširjenost oziroma odstotek prebivalcev, ki uporablja internet, ni povezan z % prebivalcev, ki zaznavajo kibernetske groženje, kot so distribuiran internetni napad, nezaželena pošta, kraja identitete, prav tako spremenljivka ni povezana z uporabo varnostno zaščitne programske opreme. Povezava je pozitivno šibka ali pa je sploh ni. Torej ne morem trditi, da večja ali manjša, kot je internetna razširjenost, bolj ali manj so ljudje ozaveščeni o kibernetskih grožnjah ter nujni uporabi varnostne programske opreme.

Med internetno razširjenostjo in uporabo družbenih medijev obstaja zmerna do srednja povezanost, saj Pearsonov koeficient korelacije znaša 0,676. To pomeni, da več kot je uporabnikov interneta, bolj ljudje uporabljajo družbene medije, kot sta Facebook in Twitter. Med internetno razširjenostjo in % prebivalstva, ki prebira časopise in novice preko spleta, ne obstaja statistična povezava.

Statistična povezava med številom kibernetskih vdorov, dobljenih na podlagi anket, prav tako ni statistično značilna in linearno povezana z višino predvidene kazni za kibernetski kriminal. Torej določitev višine kazni za posamezne kibernetske zločine nima vpliva na število kibernetskih vdorov.

5 LITERATURA

1. *AMZS*. Dostopno prek: http://www.amzs.si/si/425/6/Relacije.aspx (10. maj 2013).
2. Angelidis, P., J. Artmann, J. Dumortier in S. Giest. 2010. *eHelath Strategies: Country Brief Cyprus.* Dostopno prek: http://ehealth-strategies.eu/database/documents/Cyprus_CountryBrief_eHStrategies.pdf (31. januar 2013).
3. ANSSI – French Network and Information Security Agency. 2011. *Information systems and security: France's strategy*. Dostopno prek: http://www.ssi.gouv.fr/en/ (10. januar 2013).
4. Artmann, J., J. Dumortier, Jos Farcas, D. in J. Heywood. 2010a. *eHealth Strategies: Country Brief Romania*. Dostopno prek: http://ehealth-strategies.eu/database/documents/Romania_CountryBrief_eHStrategies.pdf (31. januar 2013).
5. Artmann, J., D. Dimitrova, B. Dobrev, Jos Dumortier in J. Heywood. 2010b. *eHealth Strategies: Country Brief Bulgaria*. Dostopno prek: http://ehealth-strategies.eu/database/documents/Bulgaria_CountryBrief_eHS_FinalEdit.pdf (31. januar 2013).
6. Artmann, J., J. Dumortier, S. Giest in T. Kenny. 2010c. *eHelath Strategies: Country Brief Ireland.* Dostopno prek: http://ehealth-strategies.eu/database/documents/Ireland_CountryBrief_eHStrategies.pdf (31. januar 2013).
7. Artman, J., J. Dumortier, S. Giest in M. Šitcs. 2010d. *eHelath Strategies: Country brief Latvia*. Dostopno prek: http://ehealth-strategies.eu/database/documents/Latvia_CountryBrief_eHStrategies.pdf (31. januar 2013).
8. Austrian Federal Chancellery. 2012. *Digital Austria: National ICT Security Strategy Austria.* Dostopno prek: http://www.oesterreich.gv.at/DocView.axd?CobId=48411 (15. februar 2013).
9. Baylis, John in Steve Smith. 2007. *Globalizacija svetovne politike: uvod v mednarodne odnose.* Ljubljana: FDV (323−48).
10. Betz, J. David in Tim Stevens. 2011. *Cyberspace and the state: toward a strategy for cyber power*. The International Institute for Strategic Studies: Velika Britanija.

11. Blackman, Colin, Maarten Botterman, Gwendolyn Carpenter, Emma Disley, Deidre Culley, Jermy Millard, Maryse Penny, Dimitris Potoglou, Anais Reding in Neil Robinson. 2012. *Feasibilitiy study for a European Cybercrime Centre*. Dostopno prek: http://ec.europa.eu/homeaffairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf (10. marec 2013).
12. Buckenham, Paddy. 2013. *Proposal for an EU Cyber-security Strategy*. Dostopno prek: http://www.iiea.com/blogosphere/proposal-for-an-eu-cyber-security-strategy (8. april 2013).
13. Bučar, Bojko in Anton Grizold. 2011. *Izzivi sodobne varnosti: od nacionalne in mednarodne do človekove varnosti.* Teorija in praksa 48 (4): 827−849.
14. Bučar, Bojko, Iztok Prezelj in Andreja Vogrin. 2008. *Človekova varnost v mednarodnih odnosih.* Fakulteta za družbene vede: Ljubljana.
15. Buzan, Barry; Ole Waever in Jaap de Wilde. 1998. *Security: A New Framework for Analysis.* London: Lynne Rienner.
16. *BSI – Bundesamt fur Sicherheit in der Informations technik*. 2010. Anual Report: Imrpoving IT Security. Dostopno prek: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/annualreport/BSI_annual_report_2010_pdf.pdf?__blob=publicationFile (8. april 2013).
17. *CCDCOE* – NATO Cooperative Cyber Defence Centre of Excellence. Dostopno prek: https://www.ccdcoe.org/385.html (20. marec 2013).
18. *CERT Bulgaria*. Dostopno prek: https://govcert.bg/EN/Pages/default.aspx (20. marec 2013).
19. *CERT Estonia*. Dostopno prek: https://www.ria.ee/cert-estonia/ (20. marec 2013).
20. *CERT Hungary*. Dostopno prek: http://www.cert-hungary.hu/en/node/6 (20. marec 2013).
21. *CERT Slovenia*. Dostopno prek: http://www.cert.si/ (20. marec 2013).
22. Clarke, Richard A, in Robert Knake K. 2010. *Cyber war*. Harper Collins: New York.
23. Constantin, Lucian. 2011. *Romani's anti.cybercrime efoorts lack social component.* Dostopno prek: http://www.pcworld.idg.com.au/article/402072/romania_anti-cybercrime_efforts_lack_social_component/ (27. marec 2013).
24. *CSIRT Czech Republic*. Dostopno prek: http://www.csirt.cz/page/882/about-us/ (20. marec 2013).
25. Czech Republic. 2011. *Cyber Security Strategy of the Czech Republic for 2011−2015 period*. Dostopno prek:

http://www.enisa.europa.eu/media/newsitems/CZ_Cyber_Security_Strategy_20112015.PDF (10. januar 2013).

26. *Direktiva 2010/40/EU Evropskega parlamenta in sveta*. 2010. Dostopno prek: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:207:0001:0013:EN:PDF (15. marec 2013).
27. Elias, Juanita in Peter Sutch. 2007. *International relations: the basics*. Routledge: London.
28. Espiner, Tom. 2009a. *UK cybersecurity centre starting operations in March*. Dostopno prek: http://www.zdnet.com/uk-cybersecurity-centre-starting-operations-in-march-3039877965/ (15. marec 2013).
29. --- 2009b. *UK launches dedicated cybersecurity agency*. Dostopno prek: http://www.zdnet.com/uk-launches-dedicated-cybersecurity-agency-3039667231/ (15. marec 2013).
30. Dumortier, J., S. Giest in A. Kiskiene. 2010. *eHealth Strategies: Country brief Lithuania.* Dostopno prek: http://ehealth-strategies.eu/database/documents/Lithuania_CountryBrief_eHStrategies.pdf (31. januar 2013).
31. Dunne, Tim, Milja Kukri in Steve Smith. 2007. *International relations theories*. Oxford University press: New York.
32. Dutch Ministry of Security and Justice. 2011. *The National Cyber Security (NCSS): Strength through cooperation.* Dostopno prek: http://english.nctb.nl/Images/cyber-security-strategy-uk_tcm92-379999.pdf (10. januar 2013).
33. Economist Intelligence Unit. 2011. *Cyber power index: Findings and Methodology*. Dostopno prek: http://www.cyberhub.com/CyberPowerIndex (25. oktober 2012).
34. *Encyclopeda of the Nations*. Dostopno prek: http://www.nationsencyclopedia.com/WorldStats/Edu-tertiary-gross-enrollment-rate.html (1. februar 2013).
35. ENISA. 2011a. *Austria Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Austria.pdf (10. februar 2013).
36. --- 2011b. *Belgium Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Belgium.pdf (10. februar 2013).

37. --- 2011c. *Bulgaria Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Bulgaria.pdf (10. februar 2013).
38. --- 2011č. *CzechRepublic Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/CzechRepublic.pdf (5. februar 2013).
39. --- 2011d. *Cyprus Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/country-reports (5. februar 2013).
40. --- 2011e. *Denmark Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Denmark.pdf (5. februar 2013).
41. --- 2011f. *Estonia Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Estonia.pdf (5. februar 2013).
42. --- 2011g. *France Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/France.pdf (10. februar 2013).
43. --- 2011h. *Germany Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Germany.pdf (10. februar 2013).
44. --- 2011i. *Greece Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Greece.pdf (10. februar 2013).
45. --- 2011j. *Hungary Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Hungary.pdf (10. februar 2013).
46. --- 2011k. *Ireland Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Ireland.pdf (10. februar 2013).
47. --- 2011l. *Italy Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Italy.pdf (10. februar 2013).

48. --- 2011m. *Latvia Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Latvia.pdf (10. februar 2013).
49. --- 2011n. *Lithuania Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Lithuania.pdf (5. februar 2013).
50. --- 2011o. *Malta Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Malta.pdf (6. februar 2013).
51. --- 2011p. *Netherlands Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Netherlands.pdf (6. februar 2013).
52. --- 2011r. *Poland Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Poland.pdf (6. februar 2013).
53. --- 2011s. *Portugal Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Portugal.pdf (6. februar 2013).
54. --- 2011š. *Romania Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Romania.pdf (6. februar 2013).
55. --- 2011t. *Slovenia Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Slovenia.pdf (6. februar 2013).
56. --- 2011u. *Spain Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Spain.pdf (6. februar 2013).
57. --- 2011v. *Sweden Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Sweden.pdf (10. februar 2013).
58. --- 2011z. *United Kingdom Country Report*. Dostopno prek: http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/UK.pdf (10. februar 2013).

59. --- 2011ž. *Cooperative Models for Effective Public Private Partnerships: Deskop Research Report.* Dostopno prek: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps (25. marec 2013).
60. --- Dostopno prek: http://www.enisa.europa.eu/ (7. november 2012).
61. --- 2012a. *ENISA Threat Landscape: Responding to Evolving Threat Environment.* Dostopno prek: http://www.enisa.europa.eu/ (7. januar 2013).
62. --- 2012b. *Appropriate security measures for Smart Grid.* Dostopno prek: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/appropriate-security-measures-for-smart-grids (5. februar 2013).
63. *EPSOS – European Patients Smart Open Services*. Dostopno prek: http://www.epsos.eu/?id=14 (30. januar 2013).
64. Eriksson, Johan in Giacomello Giampeiro. 2004. *International Relations Theory and Security in the Digital Age.* Conference Papers – International Studies Association. Dostopno prek: http://ehis.ebscohost.com.nukweb.nuk.uni-lj.si/ehost/pdfviewer/pdfviewer?sid=5280cbd6-535d-4fc6-a6d0 d7a3ca522597%40sessionmgr10&vid=1&hid=3 (10. maj 2013).
65. Esterle, Alain, Hano Ranck in Schmitt Burkard. 2005. *Information security: A new challenge fot the EU.* Dostopno prek: http://www.iss.europa.eu/uploads/media/cp076.pdf (5. februar 2013).
66. *Estonias Ministry of Defence.* Cyber Security Strategy. Dostopno prek: http://www.kmin.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf (10. januar 2013).
67. *Eurobarometer*. 2009. Confidence in the Information Society: Analitical Report. Dostopno prek: http://ec.europa.eu/information_society/policy/nis/docs/eurobarometre/confidence_infosoc_analytical_report_v30_4_09.pdf (1. februar 2013).
68. --- 2012. Country Reports. Dostopno prek: http://ec.europa.eu/public_opinion/archives/eb/eb77/eb77_en.htm (10. februar 2013).
69. European Commission. Dostopno prek: http://ec.europa.eu/energy/gas_electricity/smartgrids/taskforce_en.htm (10. januar 2013).

70. --- 2011a. *European countries on their journey towards national eHelath infrastructures.* Dostopno prek: http://www.ehealth-strategies.eu/report/eHealth_Strategies_Final_Report_Web.pdf (30. januar 2013).
71. --- 2011b. *Statistical pocket book: EU transport in figures*. Dostopno preko: http://ec.europa.eu/transport/facts-fundings/statistics/doc/2011/pocketbook2011.pdf (15. marec 2013).
72. --- 2011c. *Study regarding secure parking places for trucks and commercial vehicles, telematics-controlled parking and reservation systems*. Dostopno prek: http://ec.europa.eu/transport/themes/its/studies/doc/2011_08-secure-parking-places-for-trucks.pdf (10. maj 2013).
73. --- 2012. *Special Eurobarometer 390: Cyber security report*. Dostopno prek: http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf (20. maj 2013).
74. --- 2013. *Its Action Plan – Free Road Safety Traffic Information*. Dostopno prek: http://ec.europa.eu/transport/themes/its/studies/doc/final_report.pdf (10. maj 2013).
75. European Commission, Instute for Energy in Joint Research Center. 2011. *Smart Grid projects in Europe: lessons learned and curent developments.* Dostopno prek: http://ses.jrc.ec.europa.eu/sites/ses/files/documents/smart_grid_projects_in_europe_lessons_learned_and_current_developments.pdf (5. februar 2013).
76. *Europe's Information Society Thematic Portal*. E-Call Memorandum of Unterstanding: Status of signatures. Dostopno prek: http://ec.europa.eu/information_society/activities/esafety/doc/library/mou/list_of_signatures.pdf (10. maj 2013).
77. *EUROSTAT.* Dostopno prek: http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home/ (10. januar 2013).
78. European parliament. 2011. *Cyber security and cyberpower: concepts, conditions and capabilities for cooperation for action within the EU.* Dostopno prek: http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf (15. december 2012).
79. --- 2012. *Report on e-call: a new 112 for citizens.* Dostopno prek: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2012-0205+0+DOC+PDF+V0//EN (10. maj 2013).
80. European Public Private Partnership Expertise Centre. *European PPP Report 2009*. Dostopno prek: http://www.eib.org/epec/resources/dla-european-ppp-report-2009.pdf (20. junij 2013).

81. Evans, Karen, in Franklin Reeder. 2010. *A Human Capital Crisis in Cybersecurity*. Dostopno prek: http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity (20. marec 2013).
82. *French Network and Information Security Agency*. Dostopno prek: http://www.ssi.gouv.fr/en/ (31. marec 2013).
83. Geers, Kenneth. 2009. *The Cyber Threat to National Critical Infrastructures: Beyond Theory.* Dostopno prek: http://www.informatik.uni-trier.de/~ley/db/journals/isjgp/isjgp18.html (5. januar 2013).
84. Geerth-Jan Van der Zanden. 2011. *The Smart Grid in Europe 2012−2016: Tehnologies, Market Forecasts and Utility Proles*. Dostopno prek: http://www.greentechmedia.com/articles/read/100-million-meters-coming-to-europe-by-2016 (5. februar 2013).
85. German Federal Ministry of Interior. 2011. *Cyber Security Strategy for Germany*. Dostopno prek: http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1 (10. januar 2013).
86. Gide, Loyrette Novel - European Bank for Reconstruction and Development. 2011. *Estonia: Assesment of the quality of the PPP legislation and effectivness of its implementation.* Dostopno prek: http://www.ebrd.com/downloads/legal/concessions/estonia.pdf (1. julij 2013).
87. *GovCERT Austria*. Dostopno prek: http://www.govcert.gv.at/home/scope/content.html (20. marec 2013).
88. *GovCertUK*. Dostopno prek: http://www.cesg.gov.uk/policyguidance/GovCertUK/Pages/index.aspx (20. marec 2013).
89. Government of the Republic of Lithuania. 2011. *On the approval of the programme for the development of electronic information security (cyber security) for 2011−2019*. Dostopno prek: http://www.ird.lt/doc/teises_aktai_en/EIS%28KS%29PP_796_2011-06-29_EN_PATAIS.pdf (10. januar 2013).
90. Hunker, Jeffrey. 2010. *Cyber war and cyber power: Issues for NATO doctrine*. Dostopno prek: http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?id=124343&lng=en (5. januar 2013).
91. Intelligent Energy Europe. 2011. *SmartRegions: European Smart Metering Landscape Report.* Dostopno prek: http://www.smartregions.net/default.asp?SivuID=26927 (5. februar 2013).

92. *International Telecommunication Union*. Dostopno prek: http://www.itu.int/cybersecurity/ (29. december 2012).
93. International Telecommunication Union in The World Bank. 2012. *The Little Data Book on Information and Communication Technology*. Dostopno prek: http://www.itu.int/ITU-D/ict/publications/material/LDB_ICT_2012.pdf (26. januar 2013).
94. Internet1. *UK Government Cyber Security Operations Centre goin glive soon.* Dostopno prek: http://www.infosecurity-magazine.com/view/8020/uk-government-cyber-security-operations-centre-going-live-soon/ (15. marec 2013).
95. *Internet World Stats*. Internet Users in the World. Dostopno prek: http://www.internetworldstats.com/stats.htm (3. januar 2013).
96. *IRISS CERT* – Irish Reporting and Information Security Service. Dostopno prek: http://www.iriss.ie/iriss/ (20. marec 2013).
97. *JiWire*. Dostopno prek: http://www.jiwire.com/ (27. januar 2013).
98. Klimburg Alexander. 2012. *Mobilizing cyber power*. Dostopno prek: http://web.clas.ufl.edu/users/zselden/coursereading2011/Klimcyber.pdf (4. november 2012).
99. Kowert Paul, Kubalkova Vendulka in Nicholas Onuf ed. 1998. *Internatonal relations in a constructed world*. M. E. Sharpe: NewYork.
100. Kramer D., Star Franklin, H. Stuart in Larry K. Wentz. 2009. *Cyber power and national security.* Center for Tehnology and National Security Policy: Združene države Amerike.
101. Ministrstvo za promet. 2010. *ITS Direktiva 2010/40/EU: poročilo o dejavnostih in projektih uvajanja inteligentnih transportnih sistemov v cestnem prometu v Republiki Sloveniji.* Dostopno prek: http://www.connekt.nl/uploads/2011/09/its-report-slovenia.pdf (15. marec 2013).
102. Moravcsik, Andrew. 1997. *Taking Preferences Seriously: A Liberal Theory of International Politics*. International organization 51 (4): 513−553.
103. Namestnikov, Yury. 2012a. *IT Threath Evolution*. Dostopno prek: http://www.securelist.com/en/analysis/204792250/IT_Threat_Evolution_Q3_2012 (9. februar 2013).
104. --- 2012b. *The geography of cybercrime: Western Europe and North America*. Dostopno prek:

http://www.securelist.com/en/analysis/204792244/The_geography_of_cybercrime_Western_Europe_and_North_America (10. februar 2013).

105. *Narodni cetrum kybernetицke bezpečnosti*. Dostopno prek: http://www.govcert.cz/en/ (31. marec 2013).
106. *Nederlands National Cyber Security Centre*. Dostopno prek: https://www.ncsc.nl/english (15. marec 2013).
107. Nye, S. Joseph. 2010. *Cyber power*. Dostopno prek: http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf (6. november 2012).
108. *OECD* – Organisation for Economic Co-operation and Development. Dostopno prek: http://www.oecd.org/ (10. januar 2013).
109. Peltier, R. Thomas. 2001. *Information Security Risk Analaysis*. CRS Press LLC: ZDA.
110. Pettiford, Lloyd in Jill Steans. 2011. *International relations: perspectives and themes.* Longman: England.
111. *Portal EU*. Dostopno prek: http://europa.eu/about-eu/countries/member-countries/index_sl.htm (25. avgust 2013).
112. Prezelj, Iztok. 2002. Konceptualizacija nacionalnih varnostnih interesov. *Teorija in praksa* 39 (4): 621−637. Dostopno prek: http://dk.fdv.uni-lj.si/tip/tip20024Prezelj.PDF (10. marec 2013).
113. --- 2007. *Model celovitega ogrožanja nacionalne varnosti Republike Slovenije*. Ministrstvo za obrambo, Direktorat za obrambne zadeve, Sektor za civilno obrambo: Ljubljana.
114. --- 2009. Nacionalna kritična infrastruktura v Republiki Sloveniji. *Teorija in praksa* 46 (4): 464−484.
115. Rand Europe in Lawfort. 2005. *Update to the Handbook of Legal Procedures of Computer and Network Misuse in EU Countries*. Dostopno prek: ftp://ftp.cordis.europa.eu/pub/ist/docs/directorate_d/trust-security/ec-csirt-d15.pdf (15. marec 2013).
116. Reveron, S. Derek. 2012. *Cyberspace and National Security: Threaths, Opportunities, and Power in a Virtual World*. Georgetown University Press: Washingotn, DC. Dostopno prek: http://ehis.ebscohost.com.nukweb.nuk.unilj.si/ehost/ebookviewer/ebook/nlebk_491171_AN?sid=8fa52b6f-b5b0-475d-a26b-c493618b2134@sessionmgr112&vid=2&hid=106&format=EB (20. avgust 2013).

117. *RIS* - raba interneta v Sloveniji. Dostopno prek: http://www.ris.org/ (31. januar 2013).
118. *Spanish Governemntal CERT*. Dostopno prek: https://www.ccn-cert.cni.es/index.php?option=com_content&view=frontpage&Itemid=1&lang=en (31. januar 2013).
119. Sterling-Folker, Jennifer. 2006. *Making sense of international relations theory*. Boulder: L. Rienner Publishers.
120. Svet Evrope. *Signature on Convention on Cybercrime*. Dostopno prek: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/10/2010&CL=ENG (13. januar 2013).
121. --- 2001. *Convention on Cybercrime*. Dostopno prek: http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (13. januar 2013).
122. Svete, Uroš. 2005. *Varnost v informacijski družbi*. Fakulteta za družbene vede: Ljubljana.
123. --- 2012. European e-readiness? Cyber dimension of national security policies. *Journal of Comparartive Politics.* 5 (1). Dostopno prek: http://www.jofcp.org/assets/jcp/JCP-January-2013.pdf (30. november 2012).
124. Symantec. *Norton Study Calculates Cost of Global Cybercrime.* Dostopno prek: http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02 (10. februar 2013).
125. Ted Hopf. 1998. *The Promise of Constructivism in International Relations Theory.* Dostopno prek: http://ehis.ebscohost.com.nukweb.nuk.uni-lj.si/ehost/pdfviewer/pdfviewer?sid=96b0dcfe-8294-4eec-8876-6e5b31aa8510%40sessionmgr104&vid=1&hid=109 (15. maj 2013).
126. *The World Bank*. Dostopno prek: http://www.worldbank.org/ (10. februar 2013).
127. *Transparency International*. 2012. Co. Dostopno prek: http://cpi.transparency.org/cpi2012/results/ (10. februar 2013).
128. *UNCTAD* – United Nations Conference on Trade and Development. Dostopno prek: http://unctadstat.unctad.org/ReportFolders/reportFolders.aspx (28. januar 2013).
129. *UNESCO*. Dostopno prek: http://www.unesco.org/new/en/ (10. januar 2013).
130. United Kingdom Cabinet Office. 2011. *The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world.* Dostopno prek: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf (10. januar 2013).
131. United Nations Development Programme. 1994. *Human Development Report 1994*. Dostopno prek: http://hdr.undp.org/en/reports/ (10. marec 2013).

132. United Nations. 2012. E-*Government Survey 2012: E-Government for the people*. Dostopno prek: http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf (29. januar 2013).
133. *United Nations Department of Economic and Social Affairs*. E-Government Development Database. Dostopno prek: http://www2.unpan.org/egovkb/datacenter/CountryView.aspx (29. januar 2013).
134. *Urad za intelektualno lastnino*. Dostopno prek: http://www.uil-sipo.si/uil/urad/o-intelektualni-lastnini/osnove-intelektualne-lastnine/ (10. februar 2013).
135. *World Intellectual Property Organization*. Statistical Country Profiles. Dostopno prek: http://www.wipo.int/ipstats/en/statistics/country_profile/ (25. januar 2013).

Priloga A: Rangiranje držav članic EU glede uporabe IKT v industriji

Države	Pametna omrežja	E-zdravje	Internetna naročila podjetij	Internetna naročila posameznikov	Individualna uporaba internetnega bančništva	Inteligentni promet	E-uprava	Skupaj točk	Mesto
Nizozemska	57	2	16	20	24	8	24	151	1
Švedska	55	3	23	20	22	8	20	151	2
Velika Britanija	55	2	20	24	15	7	23	146	3
Francija	68	2	Nni podatka	19	19	7	21	136	4
Danska	37	3	20	23	22	8	22	135	5
Nemčija	44	2	22	22	15	8	19	132	6
Avstrija	36	2	19	17	15	10	17	116	7
Belgija	37	2	17	15	20	8	15	114	8
Irska	50	1	17	16	13	7	9	113	9
Španija	55	2	5	12	9	9	16	108	10
Italija	59	2	13	3	4	9	11	101	11
Malta	39	1	15	17	12	6	8	98	12
Estonija	23	3	7	9	21	7	18	88	13
Češka	29	2	14	9	11	10	4	79	14
Slovenija	19	1	12	13	8	10	14	77	15
Poljska	31	1	10	13	9	7	3	74	16
Portugalska	33	2	7	3	6	9	10	70	17
Madžarska	22	1	6	7	7	6	12	61	18
Litva	7	1	9	6	14	7	13	57	19
Grčija	27	2	4	7	3	5	7	55	20
Latvija	12	1	3	3	18	8	6	51	21
Ciper	14	1	10	9	4	5	5	48	22

Romunija	30	1	2	1	1	9	1	45	23
Bolgarija	20	2	1	2	2	8	2	37	24

Priloga B: Rangiranje držav članic EU glede na inteligentne transportne sisteme

Države	Potovalne informacije	Elektronsko cestninjenje	E-klic	Skupaj
Bolgarija	2	4	2	8
Romunija	2	4	3	9
Latvija	3	2	3	8
Grčija	1	1	3	5
Španija	3	3	3	9
Madžarska	2	1	3	6
Portugalska	3	3	3	9
Estonija	2	2	3	7
Litva	2	2	3	7
Ciper	1	1	3	5
Poljska	3	3	1	7
Slovenija	3	4	3	10
Italija	3	3	3	9
Češka	3	4	3	10
Malta	1	2	3	6
Nizozemska	3	2	3	8
Irska	3	2	2	7
Belgija	3	2	3	8
Avstrija	3	4	3	10
Velika Britanija	3	3	1	7
Danska	3	2	3	8
Nemčija	3	2	3	8
Švedska	3	2	3	8
Francija	3	3	1	7

Priloga C: Rangiranje držav članic EU glede na podkategorijo pametna omrežja

Države	Implementacija načrti napovedi števila pametnih števcev	Zakonska podlaga pametnih števcev	Jasna strategija o pametnih števcih	Skupaj
Bolgarija	8	5	7	20
Romunija	17	2	11	30
Latvija	4	3	5	12
Grčija	12	12	3	27
Španija	19	21	15	55
Madžarska	11	10	1	22
Portugalska	10	15	8	33
Estonija	3	7	13	23
Litva	5	1	1	7

Ciper	Ni podatka	10	4	14
Poljska	18	8	5	31
Slovenija	2	5	12	19
Italija	22	17	20	59
Češka	13	3	13	29
Malta	1	15	23	39
Nizozemska	16	24	17	57
Irska	6	21	23	50
Belgija	14	13	10	37
Avstrija	9	19	8	36
Velika Britanija	20	18	17	55
Danska	7	13	17	37
Nemčija	21	8	15	44
Švedska	15	19	21	55
Francija	23	23	22	68

Priloga Č: Rangiranje držav članic EU glede na ekonomski in družbeni kontekst

Države/ Podkategorije	Pričakovana doba šolanja	Terciarni študentski vpis	Št. Diplom iz znanosti in teh.	Ozaveščenost	Št. Raziskovalcev	Izvoz IKT	Uvoz IKT	Izdatki raziskave in razvoj	Vložitve domačih patentov	Skupaj točk	Mesto
Švedska	13	18	14	98	23	20	20	24	19	249	1
Velika Britanija	18	19	24	89	16	14	15	15	23	233	2
Nizozemska	22	9	8	74	18	21	21	17	21	211	3
Francija	15	5	21	79	19	11	11	20	22	203	4
Nemčija	7	3	24	75	21	12	14	22	24	202	5
Slovenija	23	23	8	79	20	2	3	19	9	186	6
Madžarska	7	8	12	82	7	23	24	9	11	183	7
Avstrija	7	13	21	64	22	9	8	21	16	181	8
Danska	21	15	14	39	24	8	13	23	17	174	9
Grčija	17	22	22	82	8	6	5	4	8	174	10
Malta	5	1	17	88	6	24	23	6	1	171	11
Španija	18	11	17	70	12	3	10	11	18	170	12
Irska	24	16	21	28	15	15	19	16	12	166	13
Češka	7	14	17	46	14	22	22	12	10	164	14
Poljska	6	21	12	62	3	19	18	7	15	163	15
Italija	16	4	8	77	10	1	12	10	20	158	16
Portugalska	13	6	12	76	13	10	7	13	7	157	17
Estonija	12	20	18	44	11	16	17	14	3	155	18
Latvija	3	19	5	81	5	13	9	5	5	145	19
Romunija	2	17	5	39	2	17	16	1	13	112	20
Belgija	18	12	5	18	17	4	1	18	14	107	21

Litva	11	24	5	30	9	7	2	8	4	100	22
Ciper	4	2	12	36	1	18	4	2	2	81	23
Bolgarija	1	7	5	19	4	5	6	3	6	56	24

Priloga D: Rangiranje držav članic EU glede na tehnološko infrastrukturo

Države	Razširjenost interneta	Razširjenost mobilne telefonije	WI-fi	Socialna omrežja	Spletni časopis / novice	Naročniki širokopasovnih linij	Mesečne internetne tarife	Mesečne mobilne tarife	Izdatki za IKT	Varnost strežnikov	Skupaj točk	Mesto
Danska	22	16	14	23	22	23	1	22	20	23	186	1
Švedska	24	13	21	22	24	18	3	17	20	20	182	2
Velik Britanija	21	17	24	20	13	19	14	7	22	21	178	3
Nizozemska	24	10	18	19	18	24	5	6	18	24	166	4
Nemčija	20	19	22	17	15	21	2	20	16	17	169	5
Avstrija	18	23	13	9	11	16	12	19	11	16	148	6
Belgija	19	11	16	15	9	20	13	3	15	15	136	7
Malta	11	15	4	18	17	17	19	15	ni podatka	22	138	8
Estonija	16	20	1	14	23	15	15	13	5	14	136	9
Litva	8	22	2	12	20	11	23	23	2	8	131	10
Madžarska	9	12	12	21	19	12	16	11	9	6	127	11
Francija	17	1	23	11	2	22	8	2	16	11	113	12
Latvija	12	3	7	24	21	6	22	21	1	5	122	13
Irska	15	6	15	16	4	9	6	5	18	19	113	14
Slovenija	13	5	5	7	14	14	4	16	11	13	102	15
Češka	14	14	8	3	16	3	7	10	14	12	101	16
Španija	10	8	19	10	12	13	10	1	10	10	103	17
Portugalska	4	9	17	6	6	7	9	12	13	7	90	18
Poljska	7	18	10	13	1	1	20	18	7	9	104	19
Italija	6	24	20	2	5	10	11	9	6	4	97	20
Ciper	5	2	6	8	8	5	17	24	ni podatka	18	93	21
Bolgarija	2	21	3	5	3	4	21	8	7	2	76	22
Romunija	1	7	9	1	7	2	24	14	2	1	68	23
Grčija	3	4	11	4	10	8	18	4	2	3	67	24

Priloga E: Rangiranje držav članic EU glede na pravni okvir

Države	Državna	Centralno	Kibernetsk	CERT	Javno-	Kibernetsk	Politična	Skupaj točk	Mesto

	kibernetska strategija	kibernetski izvršilni organ	o varnostni zakoni		zasebno sodelovanje	o varnostne obligacije na ravni EU	učinkovitost		
Danska	0	0	1	2	0	1	69	73	1
Švedska	0	0	1	1 brez inf. o obveznem poročanju	0	0	71	71	2
Nizozemska	1	1	1	1 brez inf. o obveznem poročanju	0	1	63	64	3
Nemčija	1	1	1	2	1	1	57	64	4
Belgija	0	0	1	1	Ni podatka	1	61	64	5
Avstrija	1	0	1	1	0	1	60	61	6
Francija	1	1	1	1 brez inf. o obveznem poročanju	1	1	58	60	7
Estonija	1	0	1	1 brez inf o obveznem poročanju	0	1	49	52	8
Velik Britanija	1	1	1	2	Ni podatka	1	41	47	9
Irska	0	0	1	1	1	0	45	46	10
Malta	0	0	1	1 brez inf. o obveznem poročanju	0	1	41	42	11
Ciper	0	0	1	0	0	1	36	38	12
Slovenija	0	0	1	0	1	1	32	35	13
Madžarska	0	0	1	1	1	1	27	31	14
Portugalska	0	0	1	1 brez inf. o obveznem poročanju ni dostopna	1	1	29	31	15
Poljska	0	0	1	1	1	0	26	29	16
Romunija	0	0	1	1	0	1	25	28	17
Bolgarija	0	0	1	2	0	1	25	26	18
Španija	0	0	1	1	1	1	21	25	19
Latvija	0	0	1	2	1	1	17	22	20
Litva	1	0	1	2	0	1	13	14	21
Češka	1	1	1	1	1	0	11	12	22
Italija	0	0	1	0	1	1	7	9	23
Grčija	0	0	1	1	1	0	7	8	24

Priloga F: Rangiranje držav članic EU glede na politično učinkovitost

Države	Zaupanje v parlament	Zaupanje v vlado	Zaznava korupcije	Skupaj točk	Mesto
Švedska	24	24	23	71	1
Danska	23	22	24	69	2
Nizozemska	22	19	22	63	3
Belgija	19	22	20	61	4
Avstrija	21	23	16	60	5
Francija	18	22	18	58	6
Nemčija	19	17	21	57	7

Estonija	17	19	13	49	8
Irska	15	13	17	45	9
Velik Britanija	14	8	19	41	10
Malta	16	16	9	41	11
Ciper	13	8	15	36	12
Slovenija	9	12	11	32	13
Portugalska	11	6	12	29	14
Madžarska	11	8	8	27	15
Poljska	9	7	10	26	16
Bolgarija	8	15	2	25	17
Romunija	7	14	4	25	18
Španija	4	3	14	21	19
Latvija	5	6	6	17	20
Litva	1	5	7	13	21
Češka	3	3	5	11	22
Italija	2	2	3	7	23
Grčija	5	1	1	7	24

Priloga G: Razvrstitev držav na podlagi kibernetske moči

Države	Uporaba IKT v industriji	Ekonomski-socialni kontekst	Tehnološka infrastruktura	Pravni okvir	Skupaj točk	Mesto
Švedska	151	249	182	71	653	1
Velik Britanija	146	233	178	47	604	2
Nizozemska	151	211	166	64	592	3
Danska	135	174	186	73	568	4
Nemčija	132	202	169	64	567	5
Francija	136	203	113	60	512	6
Avstrija	116	181	148	61	506	7
Malta	98	171	138	42	449	8
Irska	113	166	113	46	438	9
Estonija	88	155	136	52	431	10
Belgija	114	107	136	64	421	11
Španija	108	170	103	25	406	12
Madžarska	61	183	127	31	402	13
Slovenija	77	186	102	35	400	14

Poljska	74	163	104	29	370	15
Italija	101	158	97	9	365	16
Češka	79	164	101	12	356	17
Portugalska	70	157	90	31	348	18
Latvija	51	145	122	22	340	19
Grčija	55	174	67	8	304	20
Litva	57	100	131	14	302	21
Ciper	48	81	93	38	260	22
Romunija	45	112	68	28	253	23
Bolgarija	37	56	76	26	195	24

Priloga H: Razvoj IKT infrastrukture (v industriji + tehnološka infrastruktura)

Države	Uporaba IKT v industriji	Tehnološka infrastruktura	Skupaj točk	Mesto
Švedska	151	182	333	1
Velik Britanija	146	178	324	2
Danska	135	186	321	3
Nizozemska	151	166	317	4
Nemčija	132	169	301	5
Avstrija	116	148	264	6
Belgija	114	136	250	7
Francija	136	113	249	8
Malta	98	138	236	9
Irska	113	113	226	10
Estonija	88	136	224	11
Španija	108	103	211	12
Italija	101	97	198	13
Madžarska	61	127	188	14
Litva	57	131	188	15
Češka	79	101	180	16
Slovenija	77	102	179	17
Poljska	74	104	178	18
Latvija	51	122	173	19
Portugalska	70	90	160	20
Ciper	48	93	141	21
Grčija	55	67	122	22
Romunija	45	68	113	23
Bolgarija	37	76	113	24

Priloga I: Prikaz kategorij in podkategorij, ki določajo kibernetsko moč

KATEGORIJE/PODKATEGORIJE	RAZLAGA KATEGORIJ IN PODKATEGORIJ
1. UPORABA IKT V INDUSTRIJI	
1.1 PAMETNA OMREŽJA	Implementacija, načrti in napovedi števila pametnih števcev v posamezni državi, ter razvrstitev držav glede na zakonsko podlago pametnih števcev
1.2 E-ZDRAVJE	Obstoj ali neobstoj elektronskih zdravstvenih zapisov in strategij, e-receptov in telefonske mobilne zdravstvene dostave
1.3 INTERNETNA NAROČILA PODJETIJ	% podjetij, ki je preko interneta izvedel internetna naročila v danem letu
1.4 INTERNETNA NAROČILA POSAMEZNIKOV	% uporabnikov interneta, ki so naročevali preko spleta v zadnjih treh mesecih
1.5 INDIVIDUALNA UPORABA INTERNETNEGA BANČNIŠTVA	% internetnih uporabnikov, ki uporabljajo spletno bančništvo
1.6 E-UPRAVA	Kvaliteta, obseg in novosti spletnih upravnih storitev
1.7 INTELIGENTNI PROMET	Uporaba IKT na področju prometa: dostopnost potovalnih informacij, elektronsko cestninjenje, e-klic
2. EKONOMSKO-DRUŽBENI KONTEKST	

2.1 PRIČAKOVANA DOBA ŠOLANJA	Povprečno število let šolanja (osnovno šolsko do terciarno)
2.2 TERCIAREN ŠTUDENTSKI VPIS	Število ljudi vpisanih v terciaren študij na 100.000 ljudi
2.3 RAZISKOVALCI V RAZISKAVAH IN RAZVOJU NA MILIJON LJUDI	Število raziskovalcev v raziskavah in razvoju na milijon ljudi
2.4 ŠTEVILO DIPLOM IZ ZNANOSTI IN TEHNOLOGIJE KOT % VSEH PODELJENIH DIPLOM	Število diplom
2.5 OZAVEŠČENOST PREBIVALSTVA	Dojemljivost ter zaznavanje kibernetskih groženj, obveščenost glede spletnega kriminala, individualno vedenje na internetu
2.6 IZVOZ IKT KOT % CELOTNEGA IZVOZA	IKT izvoz vključuje telekomunikacije, avdio in video, računalniško povezano opremo, elektronske komponente med drugimi IKT stvarmi, programska oprema je izključena
2.7 UVOZ IKT KOT % CELOTNEGA CELOTNEGA UVOZA	IKT uvoz zajema telekomunikacije, avdio in video, računalniško povezano opremo, elektronske komponente in druge IKT stvari, programska oprema je izključena
2.8 IZDATKI ZA RAZISKAVE IN RAZVOJ KOT % BDP	Med izdatke so vključeni trenutni investicijski odhodki za sistematično ustvarjalno dejavnost zalog znanja

2.9 VLOŽITVE DOMAČIH PATENTOV	Povprečno število vložitev patentov od leta 1977. do 2011.
3. TEHNOLOŠKA INFRASTRUKTURA	
3.1 INTERNETNA RAZŠIRJENOST	% prebivalstva, ki uporablja internet
3.2 RAZŠIRJENOST MOBILNE TELEFONIJE	Število naročnikov mobilnih telefonov na 100 ljudi
3.3 BREZŽIČNE DOSTOPNE TOČKE NA MILIJON LJUDI	Razširjenost brezžičnih dostopnih točk, tako brezplačnih kot plačljivih
3.4 RAZŠIRJENOST DRUŽBENIH MEDIJEV	% prebivalcev, ki uporablja socialna omrežja ter % prebivalcev, ki preko spleta prebira novice in časopise
3.5 NAROČNIKI ŠIROKOPASOVNIH LINIJ NA 100 LJUDI	Naročnine visokih hitrosti dostopa do javnega spleta, ki ni manjša od 256 kbit/s
3.6 CENA MOBILNE TELEFONIJE	Povprečni strošek mobilnih paketov, ki se uporablja kot merilo za dostopnost IKT
3.7 CENA ŠIROKOPASOVNEGA INTERNETA	Mesečno naročnina širokopasovnega interneta, ki se uporablja kot merilo za IKT dostopnost
3.8 IZDATEK ZA INFORMACIJSKO TEHNOLOGIJO KOT % BDP	Skupni izdatki za informacijsko tehnologijo na pakirano programsko ter strojno opremo, IT storitve
3.9 VARNOST STREŽNIKOV	Število strežnikov na milijon ljudi, ki uporabljajo kodirano tehnologijo za

	internetne transakcije
3.10 ŠTEVILO KIBERNETSKIH VDOROV	% ljudi, ki so že bili žrtve kibernetskega kriminala, stopnja tveganja okužbe na spletu
1. LEGALNO PRAVNI OKVIR	
1.1 DRŽAVNA KIBERNETSKA STRATEGIJA	Ali v državi obstaja kibernetska strategija, ki je okvirni dokument za izboljšanje zagotavljanja kibernetske varnosti in večjo zaščito nacionalne infrastrukture in storitev, ki nudi smernice za pristop h kibernetski varnosti
1. 3 KIBERNETSKO IZVRŠILNI ORGAN	Obstoj ali ne obstoj centralnega kibernetsko izvršilnega organa, ki med seboj povezuje različne agencije, ki skrbijo za varen kibernetski prostor
1.4 KIBERNETSKO VARNOSTNI ZAKONI	Obstoj ali ne obstoj zakonov o kibernetski kriminaliteti ali členov v kazenskih zakonikih s področja kibernetskega kriminala ter določitev kazni za kršitev določil/ zakonov
1.5 ODGOVOR NA KIBERNETSKI KRIMINAL	Ali v državi obstaja/jo CERT varnostne odgovorne enote, ki se odzivajo na kibernetski kriminal. Potrebno je preveriti ali so omenjeni v nacionalnih kibernetskih strategijah, imajo zadane naloge in področja delovanja, izvajajo vaje ter usposabljanja za zaposlene, izmenjujejo informacije na državni ravni in sodelujejo

	na mednarodni ravni z drugimi državnimi CERT-i
1.6 ZASEBNO/JAVNO PARTNERSTVO	Ali obstaja zakonska podlaga za sodelovanje
1.7 KIBERNETSKO VARNOSTNE OBLIGACIJE	Ali je država podpisnica mednarodnih prizadevanj na področju kibernetske varnosti, Konvencije o kibernetski kriminaliteti. Zanima me ali je država konvencijo podpisala, ratificirala in če je le ta vstopila v veljavo
1.8 POLITIČNA UČINKOVITOST	Zaupanje ljudi v javne institucije (vlado, parlament) in zaznava korupcije

Vir: prirejeno po Economist Intelligence Unit (2011).