Damjan Štrucl

DOI:10.33179/BSV.99.SVI.11.CMC.22.4.2

TERMINOLOŠKA ZMEDA PRI ZAGOTAVLJANJU VARNOSTI V KIBERNETSKEM PROSTORU

TERMINOLOGY CONFUSION IN ENSURING CYBERSPACE SECURITY

Povzetek Terminologija je temeljna za razumevanje in obravnavanje neke tematike, še posebej, če ta tematika vpliva na reševanje varnostnih vprašanj v sodobnem varnostnem okolju, ki ni omejeno le na fizične meje in posamične države. Svet je s kibernetskim prostorom in informacijskim okoljem postal soodvisen ter medsebojno povezan s pomočjo informacijsko-komunikacijske tehnologije, zato so se pojavili novi termini, ki jih posamezniki, strokovna javnost, države in mednarodna skupnost razumejo drugače in se posledično tudi različno odzivajo, kar vpliva na varnost vseh sodelujočih. V prispevku želimo prikazati, da urejanje varnosti v kibernetskem prostoru brez enotne in strokovne terminologije ni dovolj, še posebej, če upoštevamo definicijo kibernetske varnosti.

Ključne besede ***Terminologija, zaščita informacij, informacijska varnost, kibernetska varnost, kibernetska obramba***.

Abstract Terminology is fundamental to understanding and addressing a particular topic, especially if that topic has implications for addressing security issues in a modern security environment that is not limited to physical borders and individual countries. With the existence of cyberspace and information environment, the world has through the use of information and communication technology become interdependent and interconnected. As a result, new terms have emerged which are understood differently by individuals, the professional public, countries and the international community. Consequently, their responses differ, also affecting the security of all the involved entities. The aim of this article is to show that the regulation of security in cyberspace without uniform and professional terminology is not enough, especially if we consider the definition of cyber security.

Key words ***Terminology, information assurance, information security, cyber security, cyber defence.***

Uvod

Čas, v katerem živi današnja družba, je odvisen od informacijsko-komunikacijske tehnologije. Ta odvisnost se kaže predvsem v digitalizaciji storitev držav, dostopnosti informacij v realnem času, digitalnem poslovanju podjetij, digitalni diplomaciji itn. Te prednosti pomenijo tudi pomanjkljivosti, predvsem v smislu novih groženj in izzivov, tako za stroko kot politiko in posameznika.

Novo varnostno okolje je kompleksno, saj ne pozna teritorialnih meja, v njem sodelujejo virtualne osebe, prav tako pa omogoča številne legalne in nelegalne dejavnosti itn. Države poskušajo večinoma na politični ravni in z neenotnim pristopom ter razumevanjem novih terminov vzpostavljati koncept sistema varnosti, ki se kaže s sprejemanjem različnih pravnih aktov in ureditvijo različnih institucionalnih sestav. Za vsem tem je neusklajena terminologija. Na neenotno terminologijo so opozorili številni strokovnjaki, kot so Klimburg, Falessi in drugi (Klimburg, 2012, str. 9; Falessi, Gavrila, Klejnstrup in Moulinos, 2019, str. 1). Pri tem je Klimburg ugotovil, da je na primer termin kibernetska varnost pogosto uporabljen v političnih razpravah, vendar politična srenja skoraj nikoli ne pojasni, kaj pravzaprav pomeni (Klimburg, 2012, str. XV).

Na terminološko zmedo sem opozoril tudi v doktorski disertaciji, v kateri sem navedel ustanove (na primer Nato, EU, NIST, ISO)[1], ki različno razumejo termine s tega področja (Štrucl, 2020, str. 3). Med svojim raziskovanjem sem tudi ugotovil, da Republika Slovenija v svojih strateških in pravnih dokumentih za isti termin uporablja različne definicije, kar povzroča še dodatno zmedo v učinkovitosti nacionalnega koncepta sistema zaščite pred sodobnimi grožnjami (Štrucl, 2020, str. 3).

Enotna in strokovna terminologija je temeljna za ustrezen ter učinkovit nacionalni in mednarodni koncept sistema varnosti, v katerem ni prostora za velika odstopanja. Zato je namen prispevka skozi prizmo terminologije predstaviti terminološko zmedo glede zagotavljanja učinkovitega koncepta sistema zaščite pred sodobnimi grožnjami, ki posledično vpliva na varnost posameznika, družbe, države in mednarodnega varnostnega okolja. V prispevku sta z uporabo dedukcije in deskriptivne metode predstavljena kibernetski prostor in informacijsko okolje. V nadaljevanju izhajamo iz standardov ISO27XXX, ki so temeljni za razumevanje pogosto uporabljene in napačno razumljene terminologije.

1 TERMINOLOGIJA

Dejstvo je, da se koncept sistema zaščite v smislu zagotavljanja varnosti informacij ne zagotavlja samo z uporabo termina kibernetska varnost, temveč poznamo še druge termine in ukrepe, ki jih je treba v povezavi s tem upoštevati. Zaradi tega dejstva bomo izvedli precej razsežno terminološko obravnavo, ki bo tudi laičnemu bralcu omogočila razumevanje vsebine in predstavila kompleksnost vsebine. V našem primeru bomo na terminološki podlagi preučevali genezo varnosti v kibernetskem

[1] *NIST – National Institute of Standards and Technology; ISO – International Organization for Standardization.*

prostoru. Obravnavali bomo termine, ki so v današnjem času večkrat izrečeni in premalo natančno opredeljeni ali celo obravnavani, ter opisali terminološko zmedo, ki se kaže v večjih ali manjših odstopanjih pri opredeljevanju istega termina.

1.1 Kibernetski prostor

Kibernetski prostor ni novodoben pojav, saj ga je pred več kot 30 leti omenil že pisatelj Gibson v svoji znanstvenofantastični knjigi Nevromant. Po Gibsonu je kibernetski prostor »/…/ *skupna halucinacija, ki jo vsak dan doživljajo milijarde povsem legitimnih operaterjev povsod po svetu, celo otroci, ki se učijo matematičnih pojmov /…/ Grafična predstavitev vseh podatkov, abstrahiranih iz bank vseh računalnikov človeškega sistema*« (Gibson, 1997, str. 61).

Od prve uporabe termina kibernetski prostor se je razvilo veliko njegovih opredelitev. V splošnem se lahko strinjamo z opredelitvijo Strehovca, ki je kibernetski prostor opredelil kot »/…/ *a-geografski in fizično nedoločljiv prostor,*« ki je nastal z rastjo informacijsko-komunikacijske tehnologije (Strehovec, 1997, str. 300). Precej širše sta kibernetski prostor opredelila Schmitt in Nacionalni inštitut za standardizacijo Združenih držav Amerike (NIST): »/…/ *kibernetski prostor tvorijo fizične in nefizične komponente, katerih značilnost je uporaba računalnikov in elektromagnetnega spektra, ki omogoča shranjevanje, spreminjanje in izmenjavo podatkov z računalniškimi mrežami*«. Pri tem je NIST upošteval tudi interakcijo ljudi z informacijsko-komunikacijsko tehnologijo (Štrucl, 2020, str. 39).

Clark, Mednarodna zveza za telekomunikacije in Združeni štab Združenih držav Amerike so kibernetski prostor razdelili na sloje (slika 1), pri čemer so ti sloji različni, vendar hkrati tudi medsebojno povezani (Clark, 2019, str. 1–2; Probert, 2019, str. 69). Razdelitev kibernetskega prostora na sloje je pomembna, saj omogoča identifikacijo subjektov in objektov, ki ga sestavljajo, hkrati pa je iz slojev razvidno, katere elemente varnosti morajo države upoštevati pri vzpostavitvi koncepta sistema varnosti.

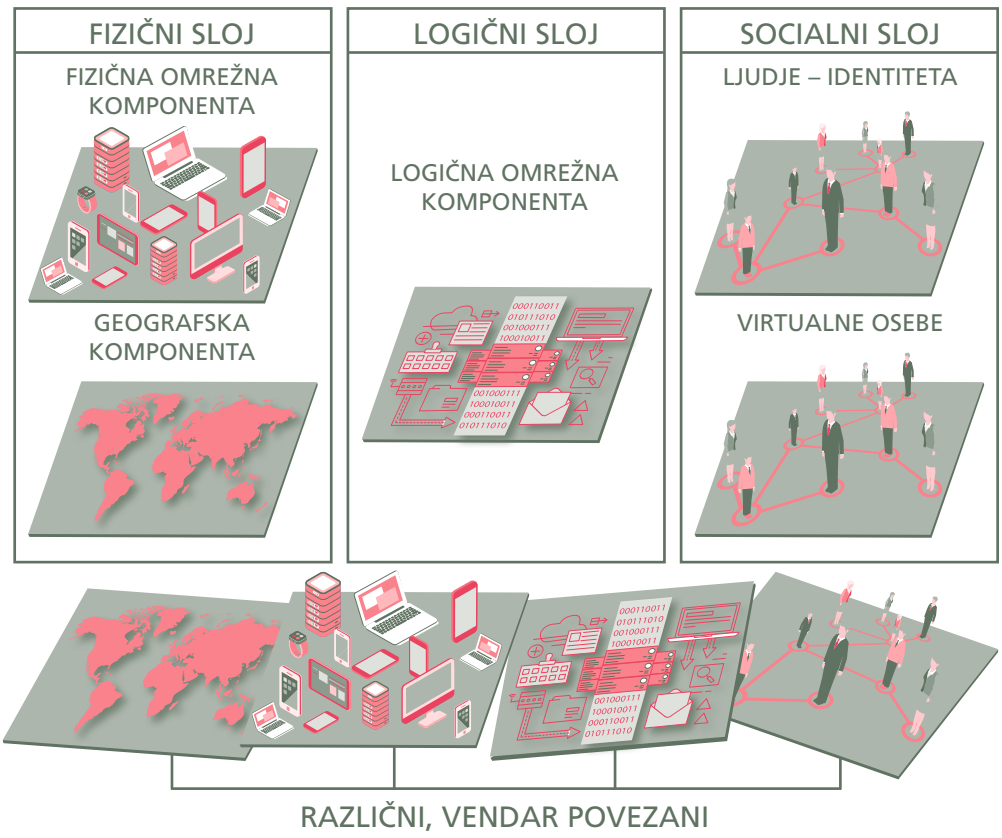
Kljub taki razdelitvi je organizacija CISCO[2] ugotovila, da nobena država oziroma organizacija ni vključila vseh bistvenih elementov kibernetskega prostora, pri čemer gre za največje odstopanje pri neupoštevanju interakcije med subjekti in objekti v kibernetskem prostoru (Cyberspace – What is it?, CISCO, 2019, e-vir).

V Republiki Sloveniji je opredelitev kibernetskega prostora zajeta v dveh dokumentih, in sicer v Zakonu o informacijski varnosti (ZInfV) in v Strategiji kibernetske varnosti, pri čemer gre za dve popolnoma različni definiciji. Definicijo kibernetskega prostora, ki izhaja iz aktov Republike Slovenije, je celo mogoče razumeti tako, da je kibernetski prostor globalno informacijsko okolje[3] oziroma globalno omrežje

[2] *CISCO – Cisco Systems, Inc. – globalno podjetje za omrežja informacijsko-komunikacijske tehnologije.*

[3] *»Kibernetski prostor je globalno informacijsko okolje, ustvarjeno s pomočjo elektronskih komunikacijskih omrežij in informacijskih sistemov« in kot takšen »/.../ omogoča nastanek, obdelavo in izmenjavo podatkov« (Uradni list RS, št. 30/18).*

informacijske tehnologije[4] (Uradni list RS, št. 30/18, Strategija kibernetske varnosti RS, 2016, str. 3), kar pa glede na predstavljene opredelitve ne drži. Obe definiciji namreč izpuščata socialni sloj in infrastrukturo ter interakcijo med subjekti in objekti.



Slika 1: Sloji kibernetskega prostora (Vir: prirejeno po Joint Chiefs of Staff, 2018, str. 1–3; Probert, 2019, str. 69)

1.2 Informacijsko okolje

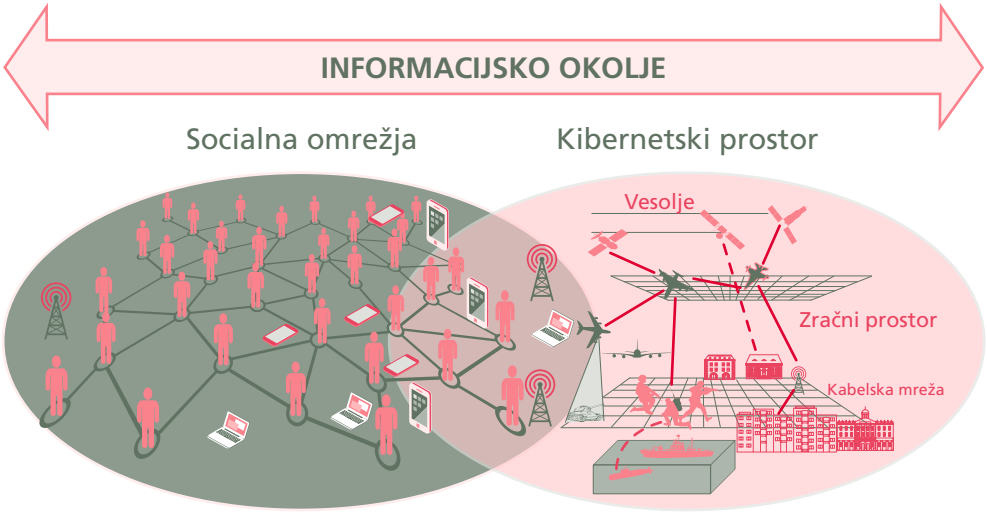
Informacijsko okolje je precej nov termin oziroma termin, ki je redko uporabljen. Tako kot pri opredeljevanju kibernetskega prostora je tudi pri opredeljevanju informacijskega okolja zmeda. Zakon o informacijski varnosti opredeljuje informacijsko okolje kot »/…/ *skupek družbenih omrežij, kibernetskega prostora, vključno z informacijami*« (Uradni list RS, št. 30/18). Škufca zavzame precej podrobnejšo opredelitev in pravi, da je informacijsko okolje »/…/ *povezano delovanje tehnologij, procesov in ljudi, ki zbirajo, obdelujejo, uporabljajo in posredujejo znanje, pridobljeno na podlagi podatkov, ki napajajo informacijsko okolje podjetja.*

[4] *»Kibernetski prostor je globalno omrežje informacijske tehnologije, telekomunikacijskih omrežij in sistemov za računalniško obdelavo« (Strategija kibernetske varnosti RS, 2016, str. 3).*

Informacijsko okolje najbolje določimo, če jasno opredelimo vlogo informatike, informacijsko arhitekturo, tehnologije in podatke« (Škufca v Štrucl, 2020, str. 41).

Precej širše informacijsko okolje opredeljujeta Obrambno ministrstvo Združenih držav Amerike in Porche III. Pri tem ugotavljata, da je informacijsko okolje sestavljeno iz socialnih omrežij (interakcije in odnosov med posamezniki, organizacijami in sistemi) in kibernetskega prostora, ki omogoča širšemu okolju tehnično izvedbo interakcij (slika 2) (Joint Concept for Operating in the Information Environment (JCOIE), United States Department od Defence, 2018, str. 2; Porche III, 2016, str. 1–2).

Slika 2: Informacijsko okolje (Vir: Porche III, 2016, str. 2)



Tako lahko sklenemo, da je informacijsko okolje precej širši pojem od kibernetskega prostora, kar v tem delu upošteva tudi Zakon o informacijski varnosti. Zato ni mogoče razumeti, da v zakonu tej opredelitvi ne sledi pojmovanje termina kibernetskega prostora.

1.3 Temeljni pojmi varovanja in zaščite informacij

Kot podlago za genezo kibernetske varnosti lahko vzamemo ISO- ali NIST-standard, pri čemer je ISO-standard mednarodno priznan, medtem ko je NIST-standard nacionalni organ za standardizacijo Združenih držav Amerike. Serija standardov ISO27XXX opredeljuje okvir za minimalno zaščito informacijsko-komunikacijske tehnologije in informacij, ne glede na obliko, zato bomo v članku sledili temu okviru.

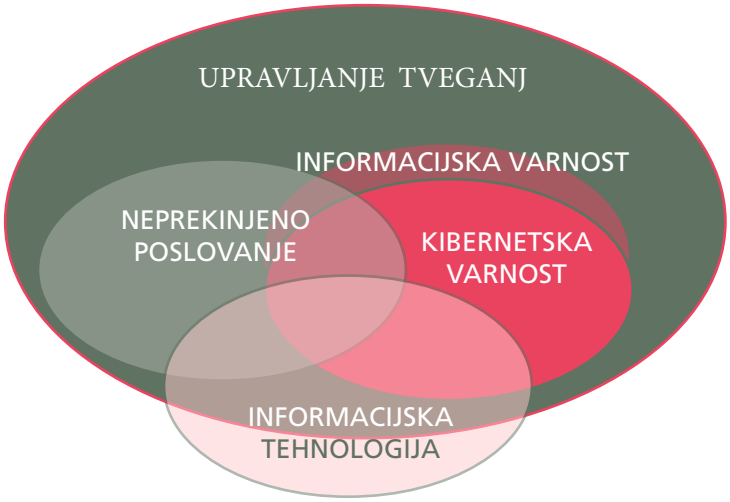
1.3.1 Zaščita informacij

Termina *zaščite informacij* (angl. Information Assurance) v standardu ISO ni mogoče jasno razbrati, prav tako pa ga ni mogoče najti v slovenskih normativnih aktih. Štrucl ugotavlja, da ISO tega termina ne navaja, temveč uporablja termin upravljanje tveganj[5]. Pri tem je pomembno, da ISO 27001 vertikalno in horizontalno ureja zaščito informacij, procesov, informacijsko-komunikacijsko tehnologijo in ljudi, kot je razvidno iz slike 3 (Štrucl, 2020, str. 23).

Ne glede na to so definicijo termina zaščite informacij opredelili v NIST-standardu, Nato, organizacija RAND in tudi Agencija EU za varnost omrežij in informacij (angl. European Network and Information Security Agency – ENISA). Vsaka izmed teh organizacij opredeljuje termin drugače:

– NIST: »/…/ *ukrepi, s katerimi se ščitijo in branijo informacije in informacijske sisteme, vključno z ukrepi zmogljivosti zaščite, odkrivanja, odzivanja in obnove, da bi se zagotovili razpoložljivost, avtentičnost, celovitost, nezatajljivost in zaupnost tako informacij kot informacijskih sistemov*« (Glossary of Key Information Security Terms, NIST IR 7298 Revision 2, NIST, 2019, str. 62).

Slika 3: ISO 27001 (Vir: The basics of ISO 22301, Advisera, 2019, e-vir)



– Nato: »/…/ *ukrepi, s katerimi se doseže določena stopnja zaupanja v zaščito komunikacijskih, informacijskih ter drugih elektronskih in neelektronskih sistemov ter informacij, ki so shranjene, obdelane ali prenesene v teh sistemih, pri*

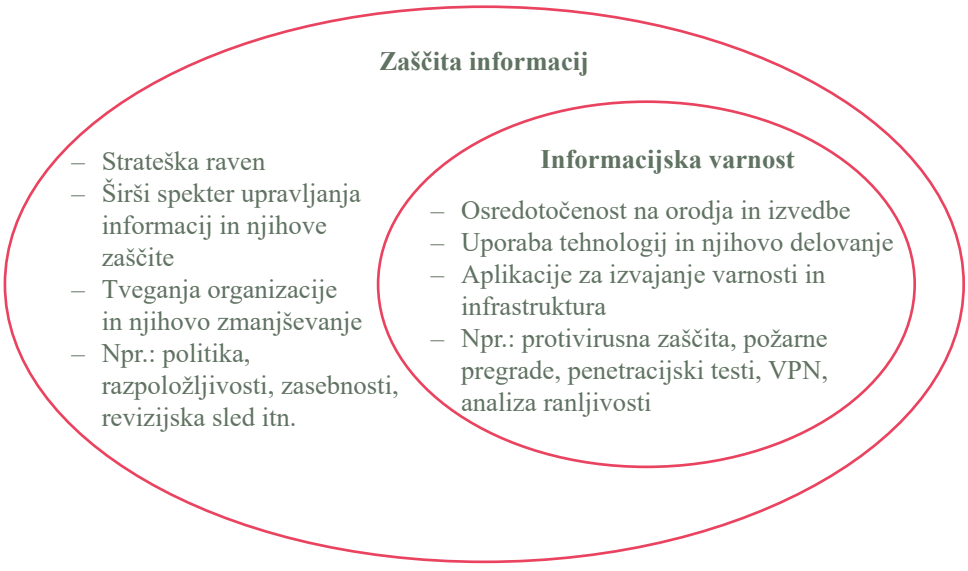
[5] *V slovenski literaturi se uporabljata dva izraza za »Risk management«: Upravljanje s tveganji in upravljanje tveganj.*

čemer se morajo zagotoviti razpoložljivost, avtentičnost, celovitost, nezatajljivost in zaupnost informacij« (Multinational Cyber Defence Education and Training Common Taxonomy, Draft: 2.05, NATO, 2016, str. 7).
- RAND: »/…/ *gotovost, da so informacije točne, zasebne, zanesljive in varne, k čemur je treba prišteti upravljanje tveganj, neprekinjeno poslovanje in upravljanje informacijske varnosti«* (Rathmell, Daman, O'Brien in Anhal, 2004, str. 11).
- ENISA: posebej ne opredeljuje zaščite informacij, temveč določa zahteve, med katere spadajo: osebna, operativna in fizična varnost, upravljanje identitete in dostopa, prenos podatkov, upravljanje sredstev in neprekinjenega poslovanja, oskrbovalna veriga, okoljski nadzor in normativne zahteve (Štrucl, 2020, str. 24–26).

Sklenemo lahko, da je zaščita informacij temeljni termin, ki ne razlikuje oblik informacij (fizična ali digitalna oblika) in ki opredeljuje zaščito elektronskih ter neelektronskih sistemov, pri čemer je treba zagotoviti razpoložljivost, avtentičnost, celovitost, nezatajljivost in zaupnost informacij ter teh sistemov. Pri tem torej ne gre za posebno tehnično znanje, temveč za strateška, politična in organizacijska vprašanja glede vrednotenja informacij ter za to, s katerimi tehničnimi in netehničnimi ukrepi bomo te informacije ter sisteme zavarovali.

1.3.2 Informacijska varnost

Informacijska varnost predstavlja poddomeno zaščite informacij. Spoznali smo, da se zaščita informacij ukvarja z vrednotenjem informacij in ukrepi za njihovo zaščito, pri čemer kader ne potrebuje posebnega tehničnega znanja (slika 4).



Slika 4: Zaščita informacij (Vir: Information Assurance versus Information Security, Novainfosec, 2011, e-vir)

Informacijska varnost je nekoliko drugačna, saj je treba imeti vsaj nekaj tehničnega znanja tako na aplikativni kot na strojni ravni, če izvajamo ukrepe varnosti digitalnih informacij. Vendar tudi informacijska varnost še ne razlikuje oblike informacij, kar je razvidno iz definicije instituta SANS in organizacije NIST[6]: »/…/ *so procesi in metodologije za zaščito katere koli oblike informacij ali podatkov in informacijskih sistemov pred nepooblaščenim dostopom, zlorabo, razkritjem, uničenjem, spreminjanjem ter motnjami, da se zagotovijo zaupnost, celovitost in razpoložljivost informacij«* (Information Security Resources, SANS, 2018, e-vir in Glossary of Key Information Security Terms, NIST IR 7298 Revision 2, NIST, 2019).

McDaniel sledi terminologiji instituta SANS in ne razlikuje oblike informacij, pri opredelitvi termina pa povzema računalniški slovar IMB, ki informacijsko varnost opredeljuje kot celoto konceptov ter tehničnih in netehničnih ukrepov, ki preprečujejo nepooblaščeno uporabo, izgubo, spremembo ali razkritje informacij ali povzročanje škode (McDaniel, 1994, str. 94).

Longly, Shain in Caelli so bolj naklonjeni definiciji NIST, pri čemer zagovarjajo, da je informacijska varnost zaščita informacij in informacijskih sistemov zaradi zagotovitve zaupnosti, celovitosti in razpoložljivosti informacij ter informacijskih sistemov. Pri tem je treba upoštevati tudi druge elemente informacijske varnosti, kot so TEMPEST ter računalniška, komunikacijska, kadrovska, operativna, fizična in industrijska varnost (Longley, Shain in Caelli, 1992, str. 268).

Nato termina informacijska varnost ne pozna, čeprav Natova varnostna direktiva ACO 70-1 uporablja kratico INFOSEC, ki jo večina zamenjuje z informacijsko varnostjo. V Natu namreč kratica INFOSEC obravnava vse vidike informacijske varnosti, vključno s fizično, kadrovsko, personalno, industrijsko, komunikacijsko, računalniško in dokumentacijsko varnostjo ter varnostjo informacij, kar pomeni, da tudi Nato ne razlikuje oblike informacij (Štrucl, 2020, str. 27–28).

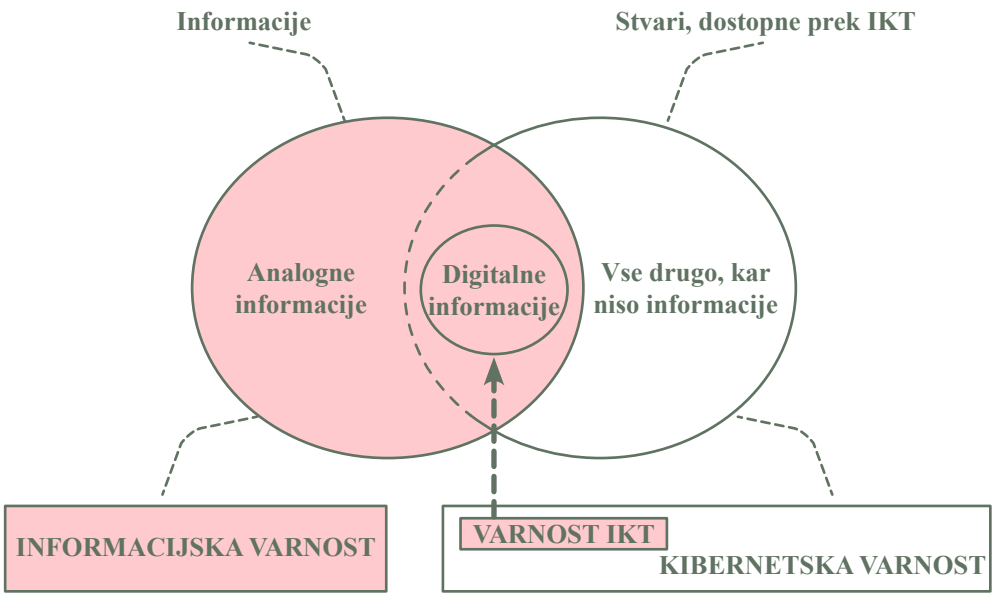
Popolnoma drugače je v zakonodaji Republike Slovenije, ki termin informacijska varnost obravnava v Zakonu o informacijski varnosti in v Uredbi o informacijski varnosti v državni upravi. Kot je bilo ugotovljeno do zdaj, tudi pri tem Slovenija ni izjema, saj tako zakon kot uredba ne zavzemata enakih opredelitev informacijske varnosti. Zakon o informacijski varnosti opredeljuje informacijsko varnost skoraj enako, kot je ta opredeljena že v NIST: »/*…/ je zaščita, varovanje in obramba informacijskega okolja pred nedovoljenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem, z namenom zagotavljanja zaupnosti, avtentičnosti, celovitosti in razpoložljivosti«*, medtem ko uredba ta termin opredeljuje drugače, kot »/…/ *zagotavljanje (ohranjanje) zaupnosti, celovitosti in razpoložljivosti informacij*« (Uradni list RS, št. 30/18; Uradni list RS, št. 29/18).

[6] *NIST eksplicitno ne določa oblike informacij, opredeljuje pa le informacijske sisteme. To pomeni, da ne opredeljuje neelektronskih sistemov (Štrucl, 2020, str. 27).*

1.3.3 Kibernetska varnost

V širši strokovni javnosti je polemika o tem, ali sta kibernetska varnost in kibernetska obramba sopomenki, kar povzroča zmedo pri uvajanju obeh terminov. Galinec in drugi ugotavljajo, da nekateri termin kibernetska varnost celo uporabljajo kot sinonim informacijski varnosti ali, kot ugotavlja Dhawan, da se v tem smislu uporablja tudi termin podatkovna varnost, kar pa povzroča še dodatno zmedo (Galinec, Dhawan in drugi v Štrucl, 2020, str. 31).

Dhawan zato na primeru številk 14041989 pojasni razlikovanje med podatkovno, informacijsko in kibernetsko varnostjo. Pri tem poudari, da je treba razlikovati med podatkom in informacijo. Podatek namreč še ni informacija, saj dobi njene lastnosti šele, ko ga lahko z nečim povežemo ali pa ga preučimo. Tako primer navedenih številk predstavlja zgolj podatek, ko pa te številke povežemo z določeno osebo in njenim rojstnim datumom, dobimo informacijo. Zato po Dhawnovem mnenju informacijska varnost predstavlja zaščito informacij ne glede na obliko in ima namen zagotoviti celovitost, razpoložljivost in zaupnost informacij, medtem ko je kibernetska varnost ožji pojem in je usmerjena v zaščito informacij v izključno digitalni obliki ter hkrati v zaščito informacijsko-komunikacijske tehnologije in ljudi (slika 5) (Dhawan, 2019, e-vir).

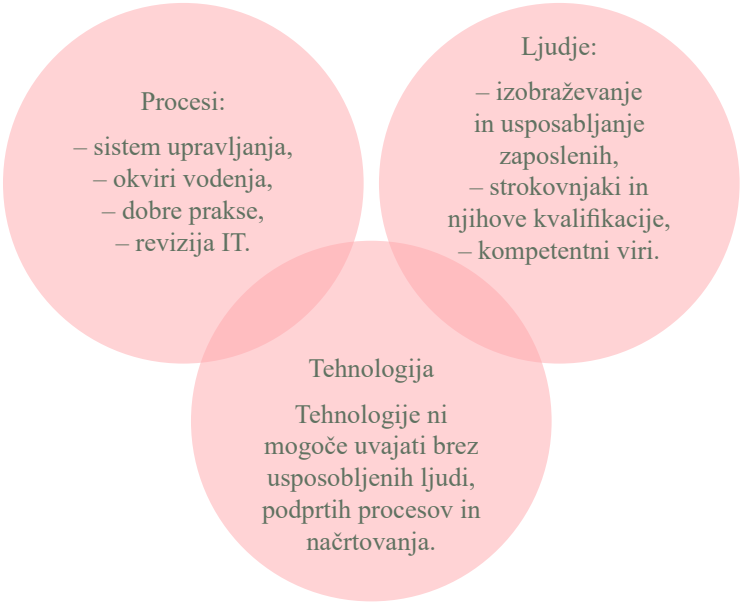


Slika 5: Razmerje med informacijsko in kibernetsko varnostjo (Vir: Košir, 2018, str. 36)

Terminološko zmedo na tem področju so ugotovili tudi na Evropskem sodišču, pri čemer je bilo zavzeto stališče, da kibernetska varnost EU ni omejena le na varnost informacij in omrežij, temveč obsega vse dejavnosti, ki so povezane z uporabo informacijsko-komunikacijske tehnologije in kibernetskega prostora (Challenges to effective EU cybersecurity policy, European Court of Auditors, 2019, str. 6). Temu stališču je sledila ENISA, ki je zavzela mnenje, da je pri zagotavljanju kibernetske varnosti treba upoštevati vse plasti kibernetskega prostora in njegovih komponent, da bi bile zagotovljene varnost, razpoložljivost, zanesljivost, celovitost, nezatajljivost, avtentičnost, robustnost, vzdržljivost in odpornost informacij ter omrežij, pri tem pa bi se upoštevali sposobnost preživetja in raven odgovornosti (ENISA overview of cybersecurity and related terminology. European Union Agency for Cybersecurity, 2017, str. 6).

Nato termina kibernetske varnosti ne pozna, temveč ga posredno obravnava v okviru pametne obrambe (angl. Smart Defense) ter v skupni taksonomiji izobraževanja in usposabljanja s področja kibernetske obrambe, pri čemer je kibernetska varnost opredeljena kot uporaba preventivnih, zaščitnih, odzivnih in obnovitvenih ukrepov za zaščito informacij, sredstev, virov in storitev v kibernetskem prostoru, da se zagotovijo njihova celovitost, razpoložljivost in zaupnost (Štrucl, 2020, str. 33).

Duttonova meni, da je tako kot pri informacijski treba tudi pri kibernetski varnosti upoštevati tri temeljne stebre upravljanja informacijske varnosti, in sicer ljudi, procese in tehnologije (slika 6). Samo vsi trije stebri skupaj zagotavljajo učinkovito izvajanje kibernetske varnosti (Dutton, 2019, e-vir).



Slika 6: Trije stebri sistema upravljanja kibernetske varnosti (Vir: Dutton, 2019, e-vir)

Kibernetska varnost je v Republiki Sloveniji opredeljena v dveh dokumentih, in sicer v Zakonu o informacijski varnosti in Strategiji kibernetske varnosti. Ponovno obravnavamo dva sicer različna dokumenta, ki pa vsak na svoj način opredeljujeta isti termin. Zakon o informacijski varnosti kot pravni akt opredeljuje kibernetsko varnost kot »/…/ *sposobnost zaščititi, varovati in braniti kibernetski prostor pred kibernetskimi grožnjami, incidenti in kibernetskimi napadi«* (Uradni list RS, št. 30/18). Po drugi strani Strategija kibernetske varnosti kot razvojno usmerjevalni dokument kibernetsko varnost opredeljuje kot »/…/ *skupek aktivnosti in drugih ukrepov, tehničnih in netehničnih, katerih namen je zaščititi računalnike, računalniška omrežja, strojno in programsko opremo ter informacije, ki jih ta vsebuje in obravnava, kar vključuje programsko opremo in podatke kot tudi druge elemente kibernetskega prostora, pred vsemi grožnjami, vključno z grožnjami nacionalni varnosti*« (Strategija kibernetske varnosti RS, 2016, str. 4).

1.3.4 Kibernetska obramba

Nekateri avtorji menijo, da je kibernetska varnost sopomenka kibernetski obrambi. Klimburg meni, da ni bistvene razlike med tema dvema terminoma, temveč je razlika samo zaradi različne uporabe terminov med vojaško in civilno sfero (Klimburg, 2012, str. 12–13).

Da Silva ugotavlja, da je terminološko nerazumevanje razlik med kibernetsko varnostjo in kibernetsko obrambo nastalo predvsem zaradi pravnih in kulturnih razumevanj funkcij države v odnosu do državljanskih in ekonomskih pravic. Izhaja iz družboslovnega razumevanja obrambno-varnostnega sistema in pravi, da je varnost precej širši pojem od obrambe, zato poenotenje kibernetske varnosti s kibernetsko obrambo ni sprejemljivo, saj država ne more uporabiti samo vojaških sil za obrambo pred kibernetskimi grožnjami in napadi (Da Silva, 2019, str. 1–2).

Tudi Galinec meni, da je treba razlikovati med kibernetsko obrambo in kibernetsko varnostjo, pri tem pa izhaja predvsem iz tehničnega vidika. Zmogljivosti kibernetske obrambe ustvarijo obrambni mehanizmi računalniškega omrežja vključno z odzivanjem, medtem ko je kibernetska varnost osredotočena na preprečevanje in odkrivanje kibernetskih groženj in napadov (Galinec, 2018, str. 16).

Podobno mnenje kot Galinec zagovarja tudi Dennigova, ki meni, da je treba kibernetsko obrambo ločevati na aktivno in pasivno, pri čemer so v pasivno vključeni tehnični in netehnični ukrepi, med katere spadajo nekateri elementi informacijske varnosti (nadzor dostopa, fizična varnost, izobraževanje in usposabljanje, kriptiranje, omrežna in fizična varnost ter vzpostavljeni procesi). Aktivna obramba je povsem drugačna, saj je usmerjena k aktivnim obrambnim ukrepom za uničenje ali zmanjšanje kibernetskih groženj in napadov. Denningova pri tem opozarja, da je treba pri aktivni kibernetski obrambi popolnoma slediti mednarodnemu pravu in upoštevati njegova splošna načela, da se zaščitijo človekove pravice in prepreči kolateralna škoda (Denning, 2013, str. 3–7).

Nato kibernetske obrambe pri njenem opredeljevanju ne ločuje na pasivno in aktivno, temveč jo opredeljuje kot proaktivne ukrepe za odkrivanje ali pridobivanje informacij o kibernetskih vdorih, grožnjah, napadih in operacijah, pri čemer so vključeni preventivni in preprečevalni ukrepi proti viru grožnje (Cyber definition, CCDCOE, 2018, e-vir).

V Republiki Sloveniji je termin kibernetska obramba vključen le v Zakon o informacijski varnosti, ki opredeljuje omenjeni termin podobno kot Nato, in sicer: »/…/ *je celota ukrepov in dejavnosti države, s katerimi se odvrača, onemogoča, preprečuje ali odbija kibernetski napad v informacijskem okolju*« (Uradni list RS, št. 30/18).

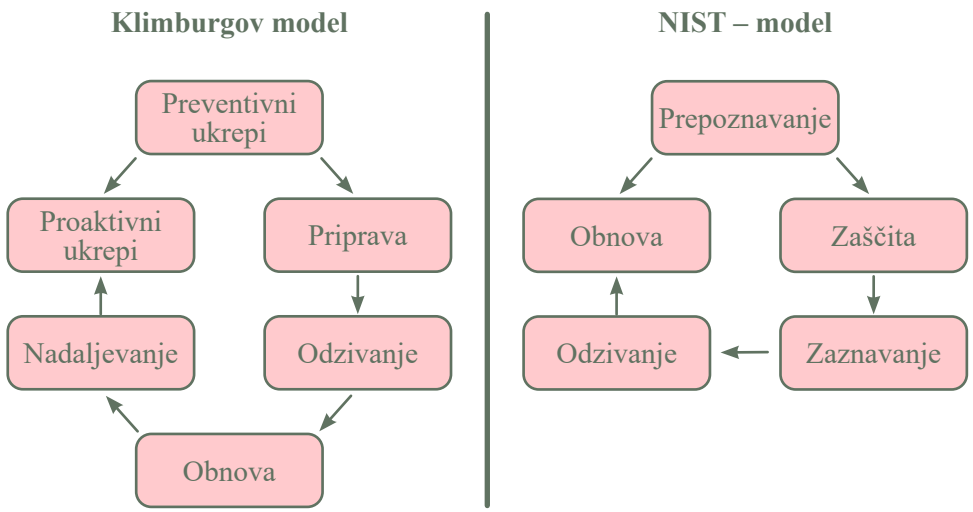
2 TERMINOLOŠKA ZMEDA V PRAKSI

Zaradi terminološke zmede se s težavami pri oblikovanju koncepta sistema zaščite srečujejo vse države in mednarodne organizacije. Kosseff je ugotovil, da bi si države morale najprej odgovoriti na pet ključnih vprašanj, če želijo pravno opredeliti kibernetsko varnost, in sicer kaj varujemo (pri tem je treba imeti v mislih ukrepe informacijske varnosti), kje in koga varujemo, kako varujemo, kdaj varujemo in zakaj varujemo (Kosseff, 2018, str. 1001–1003).

Klimburg je ugotovil, da terminološka zmeda določa tudi zmedo v nacionalnih strategijah kibernetske varnosti, saj noben politični predstavnik ne pojasni, kaj pravzaprav kibernetska varnost je, kar povzroča težave pri uresničevanju nacionalnih strategij kibernetske varnosti, terminološko razumevanje pa je prepuščeno bralcu ali predstavniku politike (Klimburg, 2012, str. 8–30).

Klimburg zato predlaga tri modele oblikovanja zmogljivosti kibernetske varnosti, ki bi omogočili njeno učinkovito izvajanje: 1. glede na razmejitev organizacijskih funkcij, zmogljivosti in odgovornosti, kibernetsko diplomacijo, vojaške kibernetske operacije, krizno upravljanje in zaščito kritične infrastrukture; 2. glede na vertikalno razdelitev po ravneh upravljanja kibernetske varnosti (politična, strateška, operativna in tehnična raven) in 3. glede na razdelitev funkcij in odgovornosti kibernetske varnosti, skladno s ciklom upravljanja incidentov (slika 7) (Klimburg, 2012, str. 109–112).

Vzpostavljena sta dva različna cikla upravljanja incidentov kibernetske varnosti, ki sta najpogosteje uporabljena: tako imenovani Klimburgov model (proaktivni ukrepi, preventivni ukrepi, priprava, odzivanje in obnova), ki je značilen za Evropo, ter NIST-model (prepoznavanje, zaščita, zaznavanje, odzivanje in obnova), ki je značilen za Združene države Amerike (Klimburg, 2012, str. 118).



Slika 7: Cikel upravljanja incidentov kibernetske varnosti (Vir: Klimburg, 2012, str. 113–114; Framework for Improving Critical Infrastructure Cybersecurity, NIST, 2019, str. 5)

Večina držav v svojih terminoloških opredelitvah ne upošteva komunikacijskih sistemov, temveč le informacijske sisteme, čeprav je v današnjem času težko ločiti komunikacijsko sredstvo od informacijskega. Oba namreč omogočata tako izmenjavo podatkov kot komunikacijo, na kar je delno že opozorilo podjetje CISCO (Cyberspace – What is it?, CISCO, 2019, e-vir).

Klump je na terminološko zmedo opozoril tudi na področju izobraževanja, pri katerem kurikulumi niso ustrezno sestavljeni. Po Klumpovem mnenju terminološka zaščita informacij spada na družboslovne fakultete, področja informacijske in kibernetske varnosti ter kibernetske varnosti pa bi morali poučevati na tehničnih fakultetah (Klump, 2019, e-vir).

S Klumpovo teorijo se ne strinjam, saj menim, da glede na serijo standardov ISO27XXX informacijska in kibernetska varnost ne obravnavata le tehničnih ukrepov, temveč tudi netehnične, za kar pa ni nujno poglobljeno znanje iz tehnične smeri, temveč zadostujejo osnove iz na primer informatike, omrežij ipd. (Štrucl, 2020, 171).

Nerazumevanje terminologije v Republiki Sloveniji se kaže v sprejetem pravnem aktu, ki je poimenovan Zakon o informacijski varnosti. Akt pravzaprav ne ureja informacijske varnosti, temveč samo prenaša Direktivo EU za varnost omrežij in informacijskih sistemov v nacionalni pravni red. Varnost omrežij in informacijskih sistemov je samo eden izmed sestavnih delov informacijske varnosti. Tako področji informacijske in tudi kibernetske varnosti ostajata pravno nedorečeni, še posebej ob dejstvu, da noben pravni akt ne določa vloge Slovenske vojske ob kibernetskem napadu (Štrucl, 2020, str. 3).

Anžič poudarja, da ustrezen koncept sistema zaščite omogoča ravnovesje med tveganji in nadzorom (Anžič, 2001, str. 255). To pomeni, da je treba vzpostaviti tak demokratični pravno-institucionalni okvir, ki bo omogočal zagotavljanje vseh oblik varnosti brez prevelikega poseganja v človekove pravice in bo hkrati zagotavljal vse oblike varnosti. Če zakonodajalec želi doseči tak koncept, mora vzpostaviti ustrezen terminološki okvir, ki bo omogočal izvajanje vladavine prava.

Ob koncu še opozorilo, da je treba pri sodobnem konceptu sistema zaščite zavzeti celostni pristop z vključitvijo strokovnega in akademskega področja. Žal daje kibernetski prostor številne sodobne varnostne izzive, tveganja in grožnje, pri čemer je večinoma uporabljen kibernetski prostor kot medij v informacijskem okolju, zato je še toliko pomembneje doseči konsistentnost na terminološkem področju, ki bo temeljna za uvedbo učinkovitega koncepta sistema zaščite.

3 PREDLOGI PREOBLIKOVANIH TERMINOV

Če želimo popolnoma slediti seriji standardov ISO27XXX, je v Republiki Sloveniji treba na novo opredeliti že sprejeti definiciji ali pa ju vsaj poenotiti v strateških in normativnih dokumentih. Zato smo pripravili predlog pomembnejših definicij s tega področja, ki sledijo smernicam ISO27XXX in analizi CISCO, predvsem z vidika ločevanja komunikacijskih in informacijskih sistemov.

Na to pomanjkljivost je opozoril že Weik, ki pravi, da komunikacijski sistemi niso samo komunikacijske (žične) povezave. Sodobni komunikacijski sistem namreč omogoča pridobivanje in distribucijo informacij v nekem času, oddaljeni nadzor sistemov in naprav, dostop računalnikov itn. (Weik, 1996, str. XII). Zato Weik opredeljuje komunikacijski sistem kot sistem ali objekt, to so na primer posamezna komunikacijska omrežja, relejne postaje, terminalna oprema, oddajniki, ki omogočajo prenos informacij med osebami in opremo (Weik, 1996, str. 159).

Zato menimo, da bi bilo treba definicije preoblikovati:

- **Zaščita informacij** predstavlja najvišji in najsplošnejši pojem zaščite informacij ne glede na njihovo obliko, pri čemer je treba vzpostaviti »/…/ *procese zaščite in obrambe podatkov in informacij ter komunikacijsko-informacijskih sistemov, z namenom zagotoviti njihovo razpoložljivost, zaupnost, celovitost, avtentičnosti in nezatajljivost*«.
- **Informacijska varnost** kot podskupina zaščite informacij predstavlja tehnične in netehnične ukrepe zaščite ter obrambe podatkov in informacij ne glede na obliko ter komunikacijsko-informacijskih sistemov pred »/…/ *nepooblaščenim dostopom, uporabo, razkritjem, motnjami, spremembami ali uničenjem zaradi zagotovitve razpoložljivosti, zaupnosti in celovitosti informacij*«.
- **Kibernetska varnost** kot podskupina informacijske varnosti predstavlja »/…/ *celoto aktivnosti, tehnične in netehnične ukrepe, katerih namen je zaščititi informacijsko-komunikacijsko opremo, komunikacijsko-informacijska omrežja,*

strojno in programsko opremo ter informacije in podatke, ki jih ti vsebujejo in obravnavajo, kar vključuje programsko opremo in druge elemente kibernetskega prostora, pred vsemi grožnjami, vključno z grožnjami nacionalni varnosti«.

– **Kibernetska obramba** kot podskupina kibernetske varnosti predstavlja »/…/ *celoto pasivne in aktivne ter tehnične in netehnične ukrepe ter dejavnosti, ki vključujejo preprečevanje, onemogočanje in odzivanje na kibernetske incidente ter obrambo kibernetskega napada v informacijskem okolju*«.
– **Kibernetski prostor** »/…/ *je virtualno okolje, v katerem poteka interakcija med ljudmi, programsko opremo in storitvami na internetu z uporabo komunikacijsko-informacijske tehnologije in omrežij*« (Štrucl, 2020, str. 233).

Ob takem preoblikovanju terminologije bi bilo upoštevano, da je v današnjem tehnološkem razvoju težko ločevati med komunikacijsko in informacijsko terminologijo, hkrati pa bi vzpostavili hierarhijo zagotavljanja varnosti in obrambe v informacijskem okolju. Taka razmejitev je nujna tako zaradi razumevanja problematike kot vzpostavitve ustrezne pravne in institucionalne ureditve varovanja informacij ter podatkov.

Sklep

V prispevku smo prikazali bistvene ugotovitve glede terminološke zmede v sodobnem varnostnem okolju v povezavi z varnostjo kibernetskega prostora. Terminološka zmeda je več kot očitna, tako na mednarodnem kot nacionalnem področju. Ugotovljeno je bilo, da ni sprejete enotne mednarodne terminologije, ki bi državam omogočala enotno in učinkovito odzivanje na sodobne grožnje. Različno pojmovanje na primer kibernetske varnosti vzpostavlja različne koncepte sistemov zaščite, kar v mednarodnem okolju povzroča neusklajeno odzivanje in ukrepanje ob sodobnih varnostnih grožnjah.

Če kot primer analiziramo normativno ureditev Republike Slovenije, ugotovimo, da normativni dokumenti niso terminološko usklajeni že na nacionalni ravni. Pri tem lahko izpostavimo na primer definiciji kibernetskega prostora in informacijskega okolja, v katerih je v Zakonu o informacijski varnosti opredeljeno, da je kibernetski prostor globalno informacijsko okolje. Informacijsko okolje pa je celota družbenih omrežij in kibernetskega prostora, kar po našem mnenju pomeni, da je kibernetski prostor v širšem pomenu besede enak informacijskemu okolju, kar pa ne drži. Če ti definiciji primerjamo še z definicijami v mednarodnem okolju, ugotovimo, da terminološka normativna ureditev Republike Slovenije ne vsebuje vseh glavnih neoprijemljivih elementov kibernetskega prostora, kot so aktivnosti, aplikacije, storitve ipd.

Koncept sistema zaščite proti sodobnim grožnjam ne temelji samo na terminu kibernetska varnost, temveč morata država in mednarodna skupnost vzpostaviti koncept sistema zaščite, ki temelji na terminih od zaščite informacij do kibernetske obrambe, ob upoštevanju definicije neprekinjenega delovanja. To v praksi pomeni, da mora subjekt določiti vrednost informacije in lastno vrednost, katera tveganja je pripravljen sprejeti in za kakšno ceno, da še zmeraj dosega določeno stopnjo zaščite

vseh oblik informacij, ki so hranjene ali obdelane v elektronskih in neelektronskih sistemih, da bi se tako zagotovile zaupnost, celovitost, razpoložljivost, nezatajljivost in avtentičnost informacij ter sistemov.

Menimo, da imamo v Republiki Sloveniji dovolj znanja in izkušenj tako v javnem sektorju kot na strokovnem in akademskem področju. To bi lahko pripomoglo k oblikovanju enotne terminologije vsaj na nacionalni ravni.

Literatura

1. *Anžič, A., 2001. Mednarodni terorizem – sistemski globalni in nacionalno-varnostni pristop. Ljubljana: Varstvoslovje. Let. 3, št. 4, 254–261.*
2. *Challenges to effective EU cybersecurity policy, 2019. Brussels: European Court of Auditors.*
3. *Cyber definition. NATO CCDCOE. https://ccdcoe.org/cyber-definitions.html, 14. 8. 2019.*
4. *Cyberspace – What is it? CISCO: https://blogs.cisco.com, 28. 3. 2019.*
5. *Clark, D., 2010. Characterizing cyberspace: past, present and future. ECIR Working Paper. Massachusetts Institute of Technology, Cambrige: Massachusetts.*
6. *Denning, E. D., 2013. Framework and Principles for Active Cyber Defens. Monterey: Naval Postgraduate School.*
7. *Dhawan, A., 2016. Understanding difference between Cyber Security & Information Securit. Social Network For CISO (Chief Information Security Officers). https://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information, 7. 5. 2019.*
8. *Dutton, J., 2019. Three pillars of cyber security. IT Governance. https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security, 27. 5. 2019.*
9. *ENISA overview of cybersecurity and related terminology. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology, 8. 7. 2019.*
10. *Falessi, N., Gavrila, R., Klejnstrup, M. R., & Moulinos, K., 2012. National Cyber Security Strategies. Practical Guide on Development and Execution. Heraklion: ENISA.*
11. *Framework for Improving Critical Infrastructure Cybersecurity, 2019. Gaithersburg: National Institute of Standards and Technology.*
12. *Galinec, D., 2018. Resilience is key. per Concordiam. Let. 9, št. 1, str. 15–21.*
13. *Gibson, W., 1997. Nevromant. Ljubljana: Cankarjeva založba.*
14. *Glossary of Key Information Security Terms, NIST IR 7298 Revision 2, 2011. Gaithersburg: National Institute of Standards and Technology.*
15. *Information Assurance versus Information Security. Novainfosec. https://www.novainfosec.com/2011/08/30/information-assurance-versus-information-security/, 27. 3. 2019.*
16. *Information Security Resources. SANS. https://www.sans.org/information-security/, 14. 6. 2018.*
17. *Joint Concept for Operating in the Information Environment (JCOIE), 2018. Washington: United States Department od Defence.*
18. *Joint Publication 3-12 Cyberspace Operations, 2018. Washington: Joint Chiefs of Staff.*
19. *Kosseff, J., 2018. Defining Cybersecurity Law. Iowa Law Review. Let. 103, št. 3, str. 985–1030.*
20. *Košir, M., 2018. Vloga Slovenske vojske pri zagotavljanju kibernetske varnosti slovenske družbe. Maribor: Slovenska vojska, Center vojaških šol.*

21. *Klimburg, A., 2012. National Cyber Security Framework Manual. Tallinn: NATO CCD COE Publications.*
22. *Klump, R., 2018. Information Assurance vs. Cyber Security vs. Information Security: Clarifying the Differences. Lewis University. https://www.lewisu.edu/experts/wordpress/index.php/information-assurance-vs-cyber-security-vs-information-security-clarifying-the-differences/, 10. 3. 2019.*
23. *Longley, D., Shain, M., in Caelli, W., 1992. Information Security: Dictionary of Concepts, Standards and Terms. New York: Stockton Press.*
24. *McDaniel, G., 1994. IBM Dictionary of computing. New York: McGraw – Hill.*
25. *Multinational Cyber Defence Education and Training Common Taxonomy, Draft: 2.05 (2016). NATO.*
26. *Probert, E. D., 2019. Organisational Structures & Incident Management for Cybersecurity in the America. ITU: SlideShare.*
27. *Rathmell, A., Daman, S., O'Brien, K., in Anhal, A., 2004. Engaging the Board: Corporate Governance and Information Assurance. Santa Monica: RAND Europe.*
28. *Strehovec, J., 1997. V svetu visokoadrenalinske tehnologije. V W. Gibson, Nevromant (Spremna beseda). Ljubljana: Cankarjeva založba.*
29. *Strategija kibernetske varnosti RS. Sklep Vlade RS, št. 38100-12/2015/5, z dne 25. 2. 2016.*
30. *Štrucl, D., 2020. Pravni in institucionalni vidiki ureditve kibernetske varnosti in obrambe Republike Slovenije. Ljubljana: Nova univerza, Evropska pravna fakulteta.*
31. *Uredba o informacijski varnosti v državni upravi. Uradni list RS, št. 29/18.*
32. *Weik, H., M., 1996. Communications Standard Dictionary, 3th Edition. Boston, MA: Springer.*
33. *The basics of ISO 22301. Advisera. https://advisera.com/27001academy/what-is-iso-22301/, 19. 3. 2019.*
34. *Zakon o informacijski varnosti. Uradni list RS, št. 30/18.*