Riikliku küberturvalisuse indeksi metoodika analüüs

Projekt "Usaldusväärsete infoühiskondade kujundamine arengumaades"

28 April 2020

TALLINNA ÜLIKOOL

ESTONIA DEVELOPMENT COOPERATION

Kokkuvõte

Käesoleva analüüsi eesmärgiks on tuua välja riikliku küberturvalisuse indeksi (NCSI) metoodika tugevused ja nõrkused võrreldes teiste samalaadsete küberturvalisuse taset hindavate metoodikatega, arvestades üldise kriisijuhtimise etappide kaetust ja rahvusliku küberturvalisuse strateegia koostamise juhendile vastavust. Seejuures on lähtutud NCSI eesmärkidest ja eeldusest, et säilib NCSI metoodika põhiolemus, mille kohaselt riikide küberturvalisuse indeksi väärtus leitakse avalike andmete – õigusaktide, ametlike dokumentide ja veebilehtede – alusel.

Analüüsi tulemusena tehakse ettepanekud riikliku küberturvalisuse indeksi metoodika täiustamiseks. Analüüsil on tuginetud küberturvalisuse taset hindavate enamkasutatavate metoodikate kirjeldustele, neid käsitlevatele publikatsioonidele ning muudele asjakohastele allikatele.

Analüüs on teostatud projekti „Usaldusväärsete infoühiskondade kujundamine arengumaades“ raames E-riigi Akadeemia SA ja Tallinna Ülikooli vahel sõlmitud lepingu alusel. Analüüsi rahastas Eesti Välisministeerium arengukoostöö ja humanitaarabi vahenditest.

Sisukord

1. Probleemipüstitus

Küberturvalisus on valdkond, mis suuresti mõjutab infoühiskonna arendamise tehnoloogiate loomist ja rakendamist. Seetõttu on arusaadav, et suurel osal riikidest on loodud küberturvalisuse strateegiad, poliitikad ja tegevuskavad. Samas on küberturvalisuse valdkond äärmiselt lai ning sellealased käsitlused eri riikides käsitlevad küllaltki erinevaid aspekte. Valdkonna ulatust iseloomustab kasvõi seegi, et Wikipedia artiklis „Cyber security" on viidatud 234-le artiklile (17.11.2019). 2018.a Tallinna Ülikoolis läbi viidud 43 riigi küberturvalisuse strateegiate ja muude poliitikadokumentide analüüs (vt Lisa 2) näitas, et nende dokumentide ulatus varieerub riigiti oluliselt. Ülikool analüüsis dokumente 33 aspektist ning näiteks Tšehhi Vabariigi küberturvalisuse strateegia[1] käsitles neist 19 aspekti, Šveitsi vastav 2012. aasta dokument[2] vaid kolme aspekti[3].

Samavõrd varieeruv on ka mõiste „küberturvalisus" (ingl.k. *cyber security*, ka *cybersecurity*) määratlus, mis võib olla nii väga üldine kui ka konkreetsem. Üldise sõnastuse näitena võib tuua Kolumbia poliitikadokumendis oleva küberturvalisuse definitsiooni, mis on „Riigi võime minimeerida küberohte või -intsidente oma kodanikele"[4]. Konkreetsema määratluse näiteks on Ungari küberjulgeoleku strateegias pakutud sõnastus: „Pidev ja kavandatud poliitiliste, juriidiliste, majanduslike, hariduslike, teadlikkuse tõstmise ja tehniliste meetmete rakendamine küberruumis esinevate riskide juhtimiseks, mis muudavad küberruumi usaldusväärseks keskkonnaks ühiskondlike ja majanduslike protsesside sujuvaks toimimiseks ning tagavad riskide vastuvõetava taseme küberruumis"[5]. Tõenäoliselt on mõnevõrra lihtsam rahvusvaheliselt laialdasele kokkuleppele jõuda, kui küberturvalisuse mõiste on määratletud üldiselt, kuid juba praegu on mitmed riigid aluseks võtnud ITU[6] põhjalikuma definitsiooni „Küberturvalisus on vahendite, poliitikate, turvakontseptsioonide, turvameetmete, juhendite, riskijuhtimise käsitluste, meetmete, väljaõppe, parimate

[1] „National Cyber Security Strategy of the Czech Republic", https://ccdcoe.org/uploads/2018/10/CS_organisation_CZE_032016.pdf

[2] „National Strategy for the Protection of Switzerland Against Cyber Risks", 2012 (analüüsi tegemise ajal ei olnud 2018. a versioon veel avaldatud), https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf

[3] Ühekordsel viitamisel mingile veebiallikale on selle aadress allmärkusena, kõikidel muudel juhtudel on allikas kasutatud kirjanduse loetelus.

[4] „*The state's capacity to minimize the level of exposure of its citizens to cyber threats or incidents*", *Policy Guidelines on Cybersecurity and Cyberdefence*, National Council on Economic and Social Policy, Republic of Columbia, https://www.sites.oas.org/cyber/Documents/Colombia%20-%20National%20Cybersecurity%20and%20Cyberdefense%20Policy.pdf

[5] „Continuous and planned taking of political, legal, economic, educational, awareness-raising and technical measures to manage risks in cyberspace that transforms the cyberspace into a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risks in cyberspace", *National Cyber Security Strategy of Hungary*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/HU_NCSS.pdf

[6] International Telecommunication Union

praktikate, tagatiste ja tehnoloogiate kogum, mida saab kasutada küberkeskkonna ja organisatsiooni ning kasutaja varade kaitsmiseks. Organisatsiooni ja kasutaja vara hulka kuuluvad võrgustatud arvutusseadmed, personal, infrastruktuur, rakendused, teenused, telekommunikatsioonisüsteemid ning kogu küberkeskkonnas edastatud ja / või salvestatud teave. Küberturvalisuse eesmärk on tagada organisatsiooni ja kasutaja varade turvaomaduste saavutamine ja säilitamine küberkeskkonna asjakohaste turvariskide vastu. Üldised turvalisuse eesmärgid hõlmavad järgmist: kättesaadavus; terviklikkus, mis võib hõlmata autentsust ja tõesust; konfidentsiaalsus" [ITU-T, 2008]. Küberturvalisuse üldine definitsioon antud ka standardis ISO/IEC 27032: 2012 „Guideline for cybersecurity" (eesti keeles EVS-ISO/IEC 27032:2018 *Infotehnoloogia. Turbemeetodid. Küberturbe juhised*). Küberturvalisuse mõiste määratlemiseks on loodud lausa omaette töörühmi, seda nii Eestis kui ka rahvusvaheliselt. Nii näiteks avaldati 2016. aastal ENISA[7] raames läbi viidud sellealase esindusliku uuringu „Definition of Cybersecurity – Gaps and overlaps in standardisation" tulemused [ENISA, 2016]. Nende poolt tehtud ettepanekutest räägime lähemalt 3. peatükis.

Küberturvalisus muutus aktuaalseks internetipõhiste teenuste massilise kasutuselevõtu järel. IT-süsteemide koostoimeks on vajalik süsteemidel omavahel suhelda, milleks omakorda on aga vajalikud teatud kokkulepped. See on põhjuseks, miks infotehnoloogia on kõige standardiseeritum valdkond - 17.11.2019 seisuga oli selles valdkonnas publitseeritud 3210 standardit ning väljatöötamisel lisaks 563 standardit, mis on üle kolme korra rohkem kui teisel kohal olev maanteesõidukeid käsitlevate standardite arv (912 standardit ja väljatöötamisel 273)[8]. Kuigi hariduse sisu kohta pole põhimõtteliselt rahvusvahelisi standardeid loodud, on ACM[9] IKT-hariduse kohta välja töötanud õppekavasoovitused[10], sh küberturvalisuse-alase kõrghariduse kohta[11]. Selleks, et olla edukas küberkuritegevuse vastu võitlemisel, on vajalik riikide koostöö oluliselt suuremal määral kui muude kuritegevusliikide vastu võitlemisel.

Riigi küberturvalisuse taseme ja võimekuse hindamiseks ning edasise tegevuse kavandamiseks on vajalikud asjakohased mõõdikud ja indeksid (agregeeritud mõõdikud). Metoodika loomisel (sh mõõdikute määratlemisel) tuleb arvestada järgmiste nõuetega:

1. *Adekvaatsus*: metoodika peab olema eesmärgipärane, st võimaldama adekvaatselt hinnata eesmärgina sätestatud tingimuste täidetust või täidetuse taset.

[7] European Union Agency for Network and Information Security

[8] https://www.iso.org/technical-committees.html

[9] Association for Computing Machinery

[10] https://www.acm.org/education/curricula-recommendations

[11] https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

2. ***Lihtsus***: metoodika rakendamine peab olema administratiivselt jõukohane (sh mõõdikute väärtused võimalikult lihtsalt leitavad/hinnatavad).
3. ***Paindlikkus***: metoodika peaks olema dünaamiliselt täiendatav, st arvestama vajadusega käsitleda edaspidi täiendavaid aspekte.

Nõuete komplekt sõltub omakorda tervest reast tingimustest, nagu näiteks eesmärgist, rahaliste ja inimressursside olemasolust, rakendusvaldkonna ulatusest jne. Nii näiteks esitatakse artiklis „Requirements for IT Security Metrics – an Argumentation Theory Based Approach" [Yasisin, Schryen, 2015] IT turvalisuse meetrika jaoks järgmised soovitused:

- Tõkestatud (*bounded*) – mõõdikute väärtused peavad olema nii alt- kui ülaltpoolt tõkestatud (fikseeritud peab olema vähim ja suurim võimalik väärtus).
- Kvantitatiivselt mõõdetav (*metrically scaled*) – mõõdikute väärtused peab olema võimalik leida.
- Usaldusväärne (*reliable*) – kordushindamine peab andma sama tulemuse.
- Valiidne (*valid*) – mõõtmisinstrument mõõdab ka tegelikult seda mida on soovitud mõõta.
- Objektiivne (*objective*) – hindamistulemus ei tohi sõltuda hindajast, sama tulemus saadakse, kui hindamine viiakse läbi kellegi teise poolt.
- Konteksti arvestav (*context-specific*) – võimaldab mõõdiku abil hinnata, mil määral on konkreetsel juhtumil võimalik väärtust luua.
- Automaatselt arvutatav (*computed automatically*) – see tagab praktilise rakenduse mugavuse ja majandusliku efektiivsuse, st see soovitus ei käi meetrika kvaliteedi kohta.

Peatükkides 8, 9 ja 10 näeme, et NCSI puhul võib küsimusi tekkida vaid adekvaatsuse osas. Probleemi käsitletakse peatükis 8. Küberturvalisuse hindamise metoodikate adekvaatsuse küsimuse tõstatamine on väga asjakohane ning seda näitab kasvõi asjaolu, et esmapilgul kahe suhteliselt sarnaste eesmärkidega ja sarnase metoodika (GCI ja NCSI) rakendamisel tuli näiteks Ida-Euroopa riikide (Bulgaaria, Moldova, Poola, Rumeenia, Slovakkia, Tšehhi, Ukraina, Ungari, Valgevene, Venemaa) indeksi väärtuste korrelatsioonikordajaks -0,1 (GCI 2018. aasta ja NCSI 2019. aasta andmed). See näitab, et GCI ja NCSI arvestavad riikide küberturvalisuse taseme hindamisel erinevaid aspekte. Valim oli küll väike, kuid selge indikatsiooni nende meetodite sisulise erinevuse kohta annab see siiski.

2. Uuringumetoodika

Mistahes metoodika analüüsimisel on esmatähtis määratleda käsitletava valdkonna ulatus. Seetõttu analüüsime esmalt küberturvalisuse mõiste määratlust, võttes aluseks esmalt riiklikud küberturvalisuse alased strateegiad ja muud poliitikadokumendid ning seejärel enim kasutatavad küberturvalisuse hindamise metoodikad. Kuna küberturvalisuse tagamise ning küberintsidentide vastumeetmeid võib käsitleda kui kriisijuhtimist, siis hindame riikliku küberturvalisuse indeksi NCSI metoodika ja kriisijuhtimise 5-etapilise metoodika (kriisi ärahoidmine, kahju leevendamine, kriisiks valmisolek, kriisi tekkimisel vastumeetmed, kriisist taastumine) kooskõla. Seejärel analüüsitakse riikliku küberturvalisuse indeksi metoodika kooskõla rahvusliku küberturvalisuse strateegia koostamise juhendiga, aga samuti NCSI metoodika adekvaatsust, lihtsust ja paindlikkust (muutmisvalmidust).

12. peatükis esitame ettepanekud riikliku küberturvalisuse indeksi metoodika täiendamiseks. Meie ettepanekute tuginevad muuhulgas enamkasutatavate küberturvalisuse hindamismetoodikate võrdleva analüüsi tulemustele.

Käesolev uuring põhineb peamiselt dokumentide (riiklikud poliitikadokumendid ning valdkondlikud raamistikud, mudelid, metoodikad ja teadusartiklid) analüüsile ning vähem rahvusliku küberturvalisuse indeksi metoodika senise rakendamise kogemusele.

3. Küberturvalisuse mõiste määratlusest

Eesti küberturvalisuse alastes strateegiadokumentides „Küberjulgeoleku strateegia 2008-2013“ ja „Küberjulgeoleku strateegia 2014-2017“ ei ole küberturvalisuse ja küberjulgeoleku mõisteid defineeritud. See on ka mõistetav, kuna küberturvalisuse valdkonna laiast ulatusest tulenevalt jääks mistahes definitsioon üldsõnaliseks ning vajaks praktiliseks kasutamiseks täiendavaid selgitusi. Selles võib veenduda näiteks viimases strateegias „Küberturvalisuse strateegia 2019-2022“ [MKM, 2018] toodud definitsiooni põhjal, mille kohaselt küberturvalisus on „seisund, kus võrgu- ja infosüsteemid on kaitstud ohtude realiseerumise eest“. 2019-2022.a küberturvalisuse strateegia loomise käigus metoodika väljatöötamiseks loodud töögrupp käsitles muuhulgas ka erinevates riikides kasutatavaid küberturvalisuse definitsioone ning jõudis järeldusele, et „olemasolevad definitsioonid ei vasta eesmärgiks seatud kolmele kriteeriumile – **üldistusvõime, lühidus** ja **süsteemsus**“.

Töörühm otsustas detailsetest definitsioonidest loobuda ning piirduda mõistete üldise kirjeldamisega.[12]

Järeldusele, et küberturvalisusel puudub üldkasutatav definitsioon, jõudsime ka Lisas 2 kirjeldatud Tallinna Ülikooli analüüsis 43 riigi küberturvalisuse alaste strateegiate ja muude poliitikadokumentide kohta. Samas on küberturvalisus siiski vajalik määratleda, nagu seda soovitas ka Cybersecurity Coordination Group (CSCG)[13]: „Euroopa Komisjon peaks looma selge ja ühise arusaama küberturvalisuse skoobist, tuginedes algatusele, mille CSCG kavatseb käivitada, et selgitada peamisi termineid ja määratlusi, mida kasutatakse Euroopa Liidu küberturvalisuse standardimisel ja suhtlemisel"[14]. Selles seisukohas olev sõna "skoop" on hoopis produktiivsem küberturvalisuse valdkonna määratlemisel – kui definitsioon üldjuhul ei erista administratiivset/organisatoorset taset (rahvusvaheline, riiklik, institutsioon, üksikisik) või ka valdkonda (õigusloome, järelevalve, haridus jne), siis skoobikirjelduses on seda võimalik teha. Seda kinnitavad ka dokumendis „Definition of Cybersecurity – Gaps and overlaps in standardisation" [ENISA, 2016] esitatud järeldused, mis põhinevad ETSI[15], ISO/IEC JTC1/SC27, ITU, NIST[16], NATO CCD COE[17], ja CNSS[18] dokumentide analüüsil. Põhjendus on sarnane eespooltooduga: „Probleem on selles, et küberturvalisus on kõikehõlmav mõiste ja pole võimalik luua definitsiooni, mis kataks küberjulgeoleku valdkonna kogu ulatuse"[19].

Siit kerkib küsimus, mida võtta küberturvalisuse skoobi määratlemisel aluseks. Selle üle otsustamiseks teeme ettepaneku lähtuda riikliku küberturvalisuse indeksi NCSI eesmärgist: ***hinnata riigi valmisolekut küberohu vältimiseks ja küberintsidentide haldamiseks***. Et küberohu vältimise ja küberintsidentide haldamise võimekuse suurendamine on sätestatud eesmärgina paljude riikide asjakohastes strateegiadokumentides, siis küberturvalisuse skoobi määratlemiseks võibki lähtuda nendes strateegiadokumentides enim käsitletud valdkondadest. Lisas 2 kirjeldatud analüüsi põhjal on strateegiadokumentide sisu kirjeldavateks märksõnadeks (märksõnade sageduse alanevas järjekorras):

1) Cyberspace/environment, Internet, Network systems

---

[12] Vt Küberturvalisuse strateegia 2019-2022 alusdokumenti „Strateegia valdkondlik metoodika", https://www.mkm.ee/et/eesmargid-tegevused/infouhiskond/kuberturvalisus

[13] Cybersecurity Coordination Group loodi 2011. aastal Euroopa standardiorganisatsioonide (CEN, CENELIC, ETSI) poolt kübervaldkonna nõuandva institutsioonina ning reorganiseeriti 2016. aastal küberturvalisuse fookusrühmaks, https://www.cencenelec.eu/standards/Sectorsold/DefenceSecurityPrivacy/Security/Pages/Cybersecurity.aspx

[14] „The EC should establish a clear and common understanding of the scope of Cyber Security, based on an initiative the CSCG plans to launch to clarify the key terms and definitions used in the standardisation of and communication related to Cyber Security within the European Union", *Recommendations for a Strategy on European Cyber Security Standardisation*, https://www.din.de/resource/blob/61520/377b6def0b8679a61c0252b5d1930c52/cscg-white-paper-data.pdf

[15] European Telecommunications Standards Institute

[16] National Institute of Standards and Technology

[17] NATO Cooperative Cyber Centre of Excellence

[18] Committee on National Security Systems

[19] „The problem is that Cybersecurity is an enveloping term and it is not possible to make a definition to cover the extent of the things Cybersecurity covers."

2) Information, Data
3) Protection
4) Services, Processes, Functioning, Operations
5) Systems, Hardware, Software
6) ICT infrastructure
7) Confidentiality
8) Integrity
9) Availability, accessibility
10) Users (persons)
11) Threats, dangers, risks
12) Legal persons
13) Public organisations
14) Ensurement, assurance
15) Cyber devices, ICT devices

Sellest loetelust võib teha järgmised järeldused:

a) Domineerib IT-süsteemide toimimise tagamine.
b) Erinevate institutsioonide roll on sätestatud kaudselt („legal persons“ ja „public organisations“ on nimekirja lõpuosas).
c) Hariduse temaatika on suhteliselt väikese osakaaluga.
d) Suhteliselt vähe on käsitletud ka riskide ja ohtude hindamist.

Samuti tuleb tõdeda, et mitmed olulised valdkonnad (näiteks rahvusvaheline koostöö) on erinevates strateegiadokumentides küll olulistena ära nimetatud, kuid sellega seonduvad probleemid, eesmärgid ja tegevusvaldkonnad jäänud paljudel juhtudel konkretiseerimata.

Samas on mõnevõrra üllatav tõdeda [ITU 2019, lk 11], et ITU andmetel vaid 46% nende liikmesriikidest kasutasid riigi küberturvalisuse hindamiseks mingeid mõõdikuid, samas kui ITU leidis 2018. aastal ligikaudu 80% oma liikmete GCI väärtuse (vastava küsimustiku täitis ligikaudu 66%, vt punktis 4.1 toodud GCI metoodika kirjeldust).

4. Enamlevinud küberturvalisuse taset hindavad metoodikad

Analüüsisime viite kõige enam kasutamist leidvat küberturvalisuse taseme hindamise metoodikat. Need määratlesime lihtsa Google-otsingu abil, lähtudes analüüsis „Index of Cybersecurity Indices 2017" [ITU, 2017] toodud küberturvalisuse hindamise metoodikate loetelust (14 metoodikat) ning nendele metoodikatele tehtud viidete arvust. Otsingusõnadena kasutasime vastava indeksi nimetust: „Global Cybersecurity Index", „Cyber Readiness Index 2.0" jne. Tabelis 1 on nende kohta 21.11.2019 tehtud Google-otsingul näidatud viidete arv (sulgudes tegelik viidete arv).

Tabel 1. Enim kasutatavad küberturvalisuse hindamise metoodikad

Jrk.nr	Nimi	Organisatsioon	Viidete arv
1.	Global Cybersecurity Index[20] (GCI)	ITU	38 100 (170)
2.	Cyber Readiness Index 2.0[21] (CRI 2.0)	Potomac Institute for Policy Studies	23 100 (90)
3.	The Index of Cyber security[22] (The Index of Cybersecurity)	New York University	26 200 (67)
4.	Cybersecurity Capacity Maturity Model (CCMM)[23]	Oxford University CESER	9 550 (139)
5.	National Cyber Security Index[24] (NCSI)	eGA	8 930 (97)
6.	EU Cybersecurity Dashboard[25]	BSA	5 080 (89)

Olgu lisatud, et mitmed artiklis „Index of Cybersecurity Indices 2017" käsitletud metoodikad ei käsitlenud mitte riikide, vaid institutsioonide küberturvalisuse või konkreetsete küberturvalisuse aspektide hindamist. Näiteks IBM X-Force Threat Intelligence Index[26] analüüsib toimunud küberintsidente ja pakub lahendusi nende ennetamiseks.

[20] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[21] https://www.potomacinstitute.org/academic-centers/cyber-readiness-index

[22] https://wp.nyu.edu/awm1/

[23] https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0

[24] https://ncsi.ega.ee/

[25] http://cybersecurity.bsa.org/

[26] https://www.ibm.com/security/data-breach/threat-intelligence

ITU poolt 2018. aastal läbiviidud riikide taset hindavate metoodikate analüüsil [ITU 2019; Annex E: Index of cybersecurity indices 2018] vaatluse all olnud 17-st metoodikast vaid kuus sobivad riikide võrdlemiseks ja järjestamiseks – Cyber Maturity in the Asia-Pacific Region, NCSI, GCI, CyberGreen Index, The Accenture Security Index ja Cyber Power Index. Tabelisse 1 on kuuest lisatud vaid GCI ja NCSI, kuna ülejäänud neli on siiani suhteliselt vähe kasutust leidnud. Märgime, et ITU käsitles 2017. aastal avaldatud publikatsioonis „Index of cybersecurity indices 2017" ka metoodikat CRI 2.0 [ITU 2017], mis on lisatud meie tabelisse, kuid ITU jättis selle metoodika 2019. aastal avaldatud 17 metoodika võrdlusest välja.

Alajaotustes 4.1 - 4.5 kirjeldame lühidalt Tabelis 1 toodud metoodikaid. NCSI lühikirjelduse esitame eraldi 5. peatükis. Kõikide vaadeldud metoodikate võrdlev analüüs (sh tugevused ja nõrkused ning ühised probleemid) on toodud 11. peatükis.

4.1. Globaalne küberturvalisuse indeks (GCI)

Järgnev kokkuvõte põhineb põhiosas allikal „Global Cybersecurity Index (GCI) 2018" [ITU 2019]. Metoodika põhieesmärgiks on mõõta riikide kübervõimekuse taset ja selle suurendamise alast tegevust, sh panust regionaalse ja globaalse võimekuse suurendamisse. Selle metoodika kohaselt hinnatakse riikide küberturvalisuse võimekust järgmistes valdkondades (sulgudes on mõõdikute nimed „Global Cybersecurity Index (GCI) 2018" sõnastuses):

Tabel 2. Globaalse küberturvalisuse indeksi mõõdikud ja nende kaalud

Mõõdikud	Kaalud
Õigusalased meetmed:	
• Küberkuritegevust käsitlevad õigusaktid (*cybercrime legislation*)	0,079
• Küberturvalisuse reguleerimine (*cybersecurity regulation*)	0,079
• Rämpsposti ohjeldamist käsitlevad õigusaktid (*containment/curbing of spam legislation*)	0,042
Tehnilised meetmed:	
• CERT/CIRT/CSIRT olemasolu	0,065
• Küberturvalisuse standardite rakendamise raamistik organisatsioonidele (*cybersecurity standards implementation framework for organizations*)	0,035
• Standardiorganisatsioon (*standardization body*)	0,030

• Rämpsposti käsitlemiseks kasutusele võetud tehnilised mehhanismid ja võimalused (*technical mechanisms and capabilities deployed to address Spam*) • Pilve kasutamine küberturvalisuse eesmärgil (*use of cloud for cybersecurity purpose*) • Laste veebikaitsemehhanismid (*child online protection mechanisms*)	0,024 0,019 0,027
Organisatoorsed meetmed: • Riiklik küberturvalisuse strateegia (*national cybersecurity strategy*) • Vastutav amet (*responsible agency*) • Küberturvalisuse mõõdikud (*cybersecurity metrics*)	 0,092 0,063 0,045
Võimekuse arendamise meetmed: • Avalikkuse teadlikkuse tõstmise kampaaniaid (*public awareness campaigns*) • Raamistik küberturvalisuse valdkonna spetsialistide atesteerimiseks ja akrediteerimiseks, küberjulgeolekualased koolituskursused (*framework for the certification and accreditation of cybersecurity professionals, professional training courses in cybersecurity*) • Küberjulgeoleku-alased haridusprogrammid või akadeemilised õppekavad (*educational programmes or academic curricular in cybersecurity*) • Küberturvalisuse teadus- ja arendusprogrammid (*cybersecurity R&D programmes*) • Stimuleerivad mehhanismid (*incentive mechanisms*) • Kodumaine küberturvalisuse tööstus (*home grown cybersecurity industry*)	 0,036 0,032 0,032 0,026 0,024 0,023
Rahvusvaheline koostöö: • Kahepoolsed lepingud (*bilateral agreements*) • Mitmepoolsed lepingud (*multilateral agreements*) • Osalemine rahvusvahelistel foorumitel/ühendustes (*participation in international fora/associations*) • Avaliku ja erasektori partnerlus (*public-private partnerships*) • Asutustevahelised/asutustesisesed partnerlused (*inter-agency/intra-agency partnerships*) • Parimad praktikad (*best practices*)	 0,038 0,038 0,036 0,034 0,026 0,028

Globaalse küberturvalisuse indeksi leidmise võib jagada kolme etappi:

1) riigid täidavad küsimustiku (50 küsimust), lisades sellele asjakohased veebilingid ja dokumendid (lähtudes nende jaoks eelnevalt koostatud juhendist),

2) ITU kontrollib esitatud informatsiooni ning vajadusel küsib täpsustusi ja/või täiendavat informatsiooni,

3) ITU viib läbi hindamise.

Hindamine toimub avalike dokumentide põhjal, mistõttu hinnang sõltub mitte niivõrd küberturvalisuse tasemest, kuivõrd asjakohaste avalike dokumentide olemasolust: „Igal aastal pühendumuse tase muutub, vastavalt sellele kuivõrd riigid on informatsiooni avalikkusele erinevate meediakanalite kaudu kättesaadavaks teinud“ ja „Globaalne küberturvalisuse indeks ei mõõda riikide valmisoleku taset reageerida küberrünnakutele, esikümnes esindatus ei kajasta tingimata tegelikku olukorda riigis ja vastupidi ” ([ITU 2019], lk 16)[27]. Vähe sellest, riigi küberturvalisuse taseme hinnang sõltub oluliselt ka küsimustiku täitmise kvaliteedist: „Selle ulatusliku andmekogumise edukus sõltub suuresti küsimustikule vastamise määrast“[28] (*ibid*, lk 53).

4.2. Potomaci poliitikauuringute instituudi kübervalmisoleku indeks 2.0

Järgnev kokkuvõte põhineb põhiosas allikal „Cyber Readiness Index 2.0“ [Hathaway jt 2015]. Metoodika hindab seitsmes rühmas kokku ligikaudu 70 mõõdiku väärtust kolmel tasemel: andmed puuduvad (*insufficient evidence*), osaliselt toimiv (*partially operational*), täielikult toimiv (*fully operational*). Hinnatavad rühmad on:

1) Riiklik strateegia (*National strategy*). Strateegia peab mitte ainult vastama võimekuse tunnustele, vaid olema ka kvaliteetne ja realistlik (olema kooskõlas riigi majandusliku võimekusega).
2) Intsidentide lahendamine (*Incident response*). See hõlmab muuhulgas preventiivseid, hariduse ning avaliku ja erasektori koostöö aspekte.
3) Võitlus küberkuritegevuse vastu ja seadusandlus (*E-crime and law enforcement*). Muuhulgas hõlmab see arvutisüsteemide hoidmist viirustest vabana.

[27] „Each year, the level of commitment changes according to the information made available to the public, and through the different media and data provided by countries” ja “GCI does not measure the level of preparedness of countries to respond to cyber-attacks, being represented in the top ten does not necessarily reflect the actual situation in the country and vice versa”.

[28] „the success of this extensive data-gathering effort depends heavily on the response rate to the questionnaire”.

4) Infojagamine *(information sharing*). Käsitleb küberintsidentide alase informatsiooni kogumise ja analüüsi aspekte.

5) Investeerimine teadus- ja arendustegevusse. Arvestab investeeringuid erialaõppesse (eelkõige doktoriõppesse), aga ka ettevõtete panustamist TA-tegevusse.

6) Diplomaatia ja kaubandus (*Diplomacy and trade*). Kaubanduse all on mõeldud IKT kasutamise või küberinfrastruktuuri, kriitiliste teenuste ja tehnoloogiate rahvusvahelisi, piirkondlikke ja/või üleriigilisi aspekte.

7) Küberkaitsevõime (*Defense and crisis response*). Fookus on riigi tasemel võimekuse arendamisel.

Igas rühmas kirjeldatakse neli võimekuse tunnust/elementi:

- Võimekust tagavad dokumendid (*Statement*),
- Võimekust tagavad institutsioonid (*Organization*),
- Vajalikud ressursid (*Resources*),
- Tegevused (*Implementation*).

Iga rühma kui terviku kohta antakse hinnang skaalal 0 ... 5 (5 märgib täielikku valmisolekut), kusjuures iga rühma kohta antav hinnang on järgmine: 5 korral „täielikult toimiv", vahemikus [3; 5) „osaliselt toimiv", vahemikus [0; 3) „andmed puuduvad".

Kuigi artikli „Cyber Readiness Index 2.0" [Hathaway jt 2015] kohaselt on selle metoodikaga hinnatud 125 riigi kübervalmisolekut (sh Eesti), on avalikult kättesaadavaks tehtud vaid 11 riigi analüüsid[29]. Metoodikale on viidatud suhteliselt rohkearvuliselt eelkõige seetõttu, et avalikustatud riikide analüüsid on erakordselt põhjalikud.

4.3. New York'i ülikooli küberturvalisuse indeks

Indeks on välja töötatud New York'i ülikooli Tandoni tehnoloogiakoolis. See indeks ei mõõda riikide taset, vaid mõõdab indeksi autorite poolt personaalselt valitud küberkaitsespetsialistide küsitlusmise[30] kaudu saadud avaliku ja erasektori institutsioonide informatsiooni infrastruktuuri küberturvalisuse riskitaseme hinnangut (*perceived risk*). Hinnangud avaldatakse igakuiselt[31].

[29] https://www.potomacinstitute.org/academic-centers/cyber-readiness-index
[30] https://wp.nyu.edu/awm1/respondents/
[31] https://wp.nyu.edu/awm1/

Metoodika põhineb küsimustikul, kus tuleb hinnata riskitasemeid 5-tasemelisel skaalal võrreldes eelmise kuuga (kiiresti langenud, langenud, ei ole muutunud, tõusnud, kiiresti tõusnud). Küsimused on jaotatud kuude rühma: rünnaku teostajad (5 küsimust), vahendid (5 küsimust), ründajate soovitud efekt (3 küsimust), rünnaku sihtmärgid (7 küsimust), kaitsemehhanismid (2 küsimust), üldhinnang (3 küsimust)[32]. Näiteks esimeses rühmas tuleb hinnata riske järgmiste gruppide osas: organisatsioonisisesed isikud, strateegilised konkurendid, häkkerid, kurjategijad, riiklikud institutsioonid.

Seega on nimetus *Küberturvalisuse indeks* mõnevõrra eksitav, täpsem oleks *Küberriski indeks* või *Küberturvalisuse riski indeks*, nii nagu on nimetatud indeksi koostamist selgitava veebilehe pealkirjas[33].

Kuna selle indeksi eesmärk ja ulatus on oluliselt kitsam NCSI eesmärgist mõõta riikide valmisolekut küberohtude ennetamiseks ja küberintsidentide juhtimiseks, siis võib selle 11. peatükis teostatud metoodikate võrdlusanalüüsist välja jätta. Suhteliselt suur viidete arv sellele indeksile tuleneb eelkõige kahest asjaolust. Esiteks on see indeks välja töötatud ülikoolis ja seetõttu viitab sellele indeksile suhteliselt suur arv teadusartikleid. Teiseks käsitlevad seda indeksit mitmed ITU publikatsioonid.

4.4. Küberturvalisuse võimekuse küpsusmudel

Küberturvalisuse võimekuse küpsusmudel (*Cybersecurity Capacity Maturity Model for Nations*) on välja töötatud Oxfordi ülikooli Martini kooli globaalse küberturvalisuse võimekuse keskuse poolt.

Järgnev kokkuvõte põhineb põhiosas dokumendil „Cybersecurity Capacity Maturity model for Nations (CMM)" [GCSCC, 2016]. Hinnatakse viit valdkonda (*dimensions*), mille raames vaadeldakse tervet rida tegureid (*factors*). Neid on kokku 24 (tegurite identifikaatoritena kasutame ülalviidatud dokumendis kasutatud tähistusi):

1) **Küberturvalisuse poliitika ja strateegia** (*Cybersecurity Policy and Strategy*)
   - D1.1 Rahvuslik küberturvalisuse strateegia (*National Cybersecurity Strategy*)
   - D1.2 Juhtumitele reageerimine (*Incident Response*)
   - D1.3 Kriitilise taristu kaitse (*Critical Infrastructure Pr*otection)
   - D1.4 Kriisihaldus (*Crisis Management*)

[32] https://wp.nyu.edu/awm1/survey/
[33] https://wp.nyu.edu/awm1/rationale/

D1.5 Küberkaitse korraldus (*Cyber Defence Consideration*)

D1.6 Kommunikatsioonisüsteemid (*Communications Redundancy*)

2) **Küberkultuur ja ühiskond** (*Cyber Culture and Society*)

D2.1 Küberturvalisust tähtsustav mõtteviis (*Cybersecurity Mind-set*)

D2.2 Kasutajate usaldus veebiteenuste suhtes (*Trust and Confidence on the Internet*)

D2.3 Kasutajate arusaam isikuandmete kaitsest veebis (*User Understanding of Personal Information Protection Online*)

D2.4 Teatamismehhanismid (*Reporting Mechanisms*)

D2.5 Meedia ja sotsiaalmeedia (*Media and Social Media*)

3) **Küberturvalisuse alane haridus, koolitus ja oskused** (Cybersecurity Education, Training and Skills)

D3.1 Teadlikkuse alane koolitus (*Awareness-raising*)

D3.2 Küberturvalisuse alane koolitus (*Framework for Education*)

D3.3 Küberturvalisuse spetsialistide koolitus (*Framework for Professional Training*)

4) **Õiguslik ja regulatiivne raamistik** (*Legal and Regulatory Frameworks*)

D4.1 Õiguslikud raamistikud (*Legal Frameworks*)

D4.2 Kriminaalõigussüsteem (*Criminal Justice System*)

D4.3 Ametlikud ja mitteametlikud koostööraamistikud küberkuritegevuse vastu võitlemiseks (*Formal and Informal Cooperation Frameworks to Combat Cybercrime*)

5) **Standardid, organisatsioonid ja tehnoloogiad** (Standards, Organisations and Technologies)

D5.1 Standardid ja head praktikad (*Adherence to Standards*)

D5.2 Internetiteenuste ja taristu usaldusväärsus (*Internet Infrastructure Resilience*)

D5.3 Tarkvara kvaliteedi ja funktsionaalsuse nõuded (*Software Quality Protection*)

D5.4 Tehnilised turvakontrollid (*Technical Security Controls*)

D5.5 Krüptokontrollid (*Cryptographic Controls*)

D5.6 Küberturvalisuse alased tooted (*Cybersecurity Marketplace*)

D5.7 Avalikustamine (*Responsible Disclosure*)

Iga teguri küpsusetaset hinnatakse 1-8 mõõdiku abil. Küpsustasemeteks on:

- Algtase (*start-up*): küberturvalisust tagavaid tegevusi läbi ei viida.
- Kujunev (*formative*): tegevus on kaootiline (*ad-hoc*), mittesüsteemne.
- Juurdunud (*established*): mõõdiku-alane tegevus on määratletud ja toimib.

- Strateegiline (*strategic*): määratletud on prioriteedid ja eraldatud selleks vajalikud ressursid.
- Dünaamiline (*dynamic*): kiire ja momendi olukorda arvestav otsustusprotsess, vajadusel strateegiamuudatused ja ressursside ümberjaotus.

Iga mõõdiku jaoks on fikseeritud küpsustaset määravad kriteeriumid. Kasutatakse ka vahepealseid hindeid (näiteks *Established to Strategic*). Tuleb siiski märkida, et küpsusmudeli analüüs on läbi viidud põhiosas vaid arenguriikide kohta. Euroopa Liidu riikidest on lisaks Suurbritanniale (kus see mudel on välja töötatud) hinnatud vaid Küprose ja Leedu küberturvalisuse võimekust[34].

Küberturvalisuse võimekuse küpsusmudel erineb teistest laialt levinud küpsusmudelitest (näiteks *Project Management Capability Maturity Model*[35]) selle poolest, et ei määratleta ühte integreeritud küpsustaset, vaid leitakse küpsustase eraldi iga teguri osas.

4.5. BSA Euroopa Liidu riikide küberturvalisuse indeks (EU Cybersecurity Dashboard)

Euroopa Liidu riikide küberturvalisuse indeks on töötatud välja The Software Alliance[36] poolt. Tegu ei ole Euroopa Liidu ametliku küpsustaseme määramise metoodikaga, mistõttu on indeksi nimi eksitav. Järgnev kokkuvõte põhineb põhiosas allikal „EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace" [BSA 2015] ja metoodikas kasutatavate mõõdikute hindamiskriteeriumitel „Methodology and Criteria for the Cybersecurity Reports"[37].

Kokku on 25 mõõdikut, mis on jagatud eri suurusega viide rühma (sulgudes on vastavas rühmas olevate mõõdikute arv):

- Õiguslikud alused (*Legal foundations*, 12),
- Täidesaatvad üksused (*Operational entities*, 6),
- Avaliku ja erasektori partnerlus (*Public-private partnerships*, 3),
- Sektoripõhised küberturbekavad (*Sector specific cybersecurity plans*, 3),
- Haridus (*Education*, 1).

[34] https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-assessments-around-world

[35] https://www.pmis-consulting.com/consulting/project-management-capability-maturity-model/

[36] https://www.bsa.org/

[37] http://cybersecurity.bsa.org/assets/PDFs/methodology_eucybersecurity.pdf

Metoodika hindab põhiosas dokumentide – õigusaktide, strateegiate, plaanide – olemasolu. Enamik mõõdikuid (v.a. kaks aastaarvu küsivat) on hinnatud skaalal *jah/ei/osaliselt*. Seejuures viiel juhul väärtust *osaliselt* ei omistata. Kõikide Euroopa Liidu liikmesriikide kohta tehtud analüüsid on avalikult kättesaadavad[38]. Riigi kohta tehtud analüüs hõlmab keskmiselt 2,5 lehekülge. Mõne riigi mõne mõõdiku hinnanguks on antud N/A või ka „-„ s.t ei kohaldata (*not applicable*). Väikseim arv (2014. aasta seisuga) *ei*-hinnanguid (4) oli antud Hollandile ja Suurbritanniale.

Eestile oli antud *ei*-hinnanguid viis; need olid antud järgmistele küsimustele:

- Kas on olemas seadusandlikke akte või poliitika, mis nõuab, et igal teenuseid pakkuval organisatsioonil (*agency*) oleks teabejuht (CIO) või julgeolekuametnik (CSO)?
- Kas kavandamisel on uusi avaliku ja erasektori partnerlusi või on need käimas (kui jah, siis millisele fookusvaldkonnale)?
- Kas on olemas ühine avaliku ja erasektori kava, mis käsitleks küberturvalisust?
- Kas on määratletud valdkondlikud turvalisuse prioriteedid?
- Kas on läbi viidud valdkonnapõhiseid küberturvalisuse riskihindamisi?

Samas, kuna need analüüsid on tehtud 2014. aastal, ei pruugi need hinnangud tänapäeval enam adekvaatsed olla.

5. Riikliku küberturvalisuse indeksi metoodika lühikirjeldus

Eesti välja töötatud riiklik küberturvalisuse indeks (NCSI) mõõdab riigi tegevusi nii küberohtude ennetamisel kui ka toimunud intsidentide tagajärgede likvideerimisel. Nende küberohtude ohjamiseks peab riigil olema asjakohane võimekus küberturvalisuse tagamiseks ning intsidentide juhtimiseks ja üldise küberturvalisuse arendamiseks. Metoodikas arvestatavad mõõdikud on määratletud selliselt, et minimeerida järgmisi ohte[39]:

- e-teenused ei ole kättesaadavad (*denial of e-services*)
- andmete terviklus on rikutud juurdepääsuõiguseta isikute poolt (*data integrity breach*)

[38] http://cybersecurity.bsa.org/countries.html#estonia

[39] https://www.ncsi.ega.ee/methodology/

- juurdepääsuõiguseta isikute ligipääs konfidentsiaalsetele andmetele (*data confidentiality breach*).

Mõõdikud (kokku on neid 46) on jaotatud kolme kategooriasse, igaühes 4 alarühma (sulgudes vastavas alarühmas olevate mõõdikute arv):

Üldised küberturvalisuse mõõdikud

1. Küberturvalisuse poliitikakujundamine (4)
2. Küberohtude analüüs ja informatsioon (3)
3. Haridus ja professionaalne areng (5)
4. Panustamine globaalsesse küberturvalisusse (4)

Küberturvalisuse baasmõõdikud

5. Digiteenuste kaitse (3)
6. Elutähtsate teenuste kaitse (4)
7. E-isikutuvastus ja usaldusteenused (7)
8. Isikuandmete kaitse (2)

Intsidentide ja kriisijuhtimise mõõdikud

9. Küberintsidentide vastustamine (3)
10. Küberkriiside haldamine (4)
11. Küberkuritegevuse vastane võitlus (4)
12. Militaarsed küberoperatsioonid (3)

Mõõdikute täielik loetelu on toodud 6. peatükis tabelis 3.

Mõõdiku väärtus võib maksimaalselt olla kas 1, 2 või 3 punkti ning selle omistab ekspertrühm, lähtudes järgmisest skaalast:

- On olemas valdkonda reguleeriv õigusakt – 1
- On olemas valdkonnaga tegelev institutsioon – 2-3
- Toimib ametlik koostööformaat – 2
- Küberturvalisust suurendavad toimingud on läbi viidud – 1-3.

Riikliku küberturvalisuse indeksi väärtus leitakse avalike andmete – õigusaktide, ametlike dokumentide, ametlike veebilehtede – alusel. Andmete esitamiseks on loodud sellealane veebipõhine sisestuskeskkond[40]. Nii sisestuskeskkonnas kui ka tulemuste kuvamise keskkonnas on ära toodud nii hindamiskriteerium kui ka viide dokumendile ja/või veebilehele, mis tõendab kriteeriumi täidetust.

[40] https://www.ncsi.ega.ee/data-collection/

Maksimaalselt on võimalik saada 77 punkti, st ühe punkti „väärtus“ 100-punktilisel skaalal on ligikaudu 1,3 punkti (=100/77). Juhul kui kahe riigi punktisummad on võrdsed, siis kõrgemale asetatakse riik, mille üldine IKT arengutase on madalam. Viimane arvutatakse IKT arenguindeksi (*ICT Development Index*, IDI) ja võrgustumisvalmiduse indeksi (*Networked Readiness Index*, NRI) keskväärtusena.

6. NCSI analüüs kriisijuhtimise etappide katvuse seisukohalt

Riigi tasemel on esmatähtis tagada mehhanismid ulatuslike ja/või kriitiliste küberintsidentide ennetamiseks, vastumeetmete rakendamiseks ja tagajärgede likvideerimiseks. Seetõttu võib küberturvalisuse tagamist käsitleda kui kriisijuhtimist ning hinnata seda kriisijuhtimise mudeli kohaselt. Kriisijuhtimise mudelid jagavad juhtimise neljaks või viieks etapiks, kusjuures 4-etapilised mudelid erinevad 5-etapilistest põhiliselt selle poolest, et vaatlevad kaht etappi (kriisi ärahoidmine ja selle leevendamine) ühe etapina.

Hindame rahvusliku küberturvalisuse indeksi raames kavandatud tegevuste kooskõla 5-etapilise kriisijuhtimise mudeliga. Etappideks on:

1) Kriisi ennetamine (*crisis* ***prevention***). Küberturvalisuse seisukohast tähendab see küberintsidentide ennetamist, näiteks tulemüüride olemasolu või kasutajate poolt küberhügieenireeglite järgimist.
2) Kahju leevendamine (***mitigation*** *of loss*). See hõlmab meetmeid nii taristu (näiteks andmebaaside peegeldamine) kui näiteks ka regulatsioonide jaoks (näiteks andmebaaside arhiveerimise kohustus).
3) Kriisiks valmisolek (*crisis* ***preparedness***). See on äärmiselt ulatuslik valdkond, hõlmates nii küberohu äratundmist, aga ka kõikvõimalikke muid küberturvalisust tagavaid planeerimise, koolituse, süsteemiarenduse ja muid meetmeid.
4) Kriisile reageerimine (***response*** *to a crisis*). See hõlmab küberintsidendi toimumise ajal toimuvat inimressursside tegevuse ja tehnoloogiliste vahendite kasutuse koordineerimist, aga samuti küberintsidendi laienemist tõkestavaid tegevusi.
5) Kriisist taastumine (***recovery*** *from the crisis*). Küberintsidendist taastumine koosneb tegevustest, mille eesmärgiks on saavutada intsidendieelne süsteemide toimimine.

Märgime, et erinevad allikad kasutavad mõnevõrra erinevaid kriisijuhtimise etappide nimetusi. Näiteks Ameerika Ühendriikide sisejulgeoleku ministeerium kasutab nimetusi *prevention*, *mitigation*, *protection*, *response* ja *recovery*[41].

Alljärgnevas tabelis 3 seame kõik riikliku küberturvalisuse indeksi mõõdikud vastavusse kriisijuhtimise etappidega. Iga mõõdiku puhul on arvestatud selle mõju kuni kolme kriisijuhtimise etapis. Näiteks riigi küberturvalisuse strateegia (mõõdik 1.3) hõlmab teatud määral ka küberintsidendi vastumeetmete ja taastumist toetavaid aspekte, kuid küberintsidendi ärahoidmise, kahjuleevenduse ja valmisoleku aspekte tuleks siiski lugeda olulisemateks.

Mõõdiku nime järel on esitatud sulgudes selle mõõdiku identifikaator NCSI hindamistabelis (vt näiteks Eesti kohta koostatud tabelit https://ncsi.ega.ee/country/ee/).

Tabel 3. NCSI kooskõla kriisijuhtimise 5-etapilise mudeliga

Jrk. nr.	Mõõdik	Kriisi ennetamine	Kahju leevendamine	Kriisiks valmisolek	Kriisile reageerimine	Kriisist taastumine
1.	Küberturvalisuse riikliku poliitika üksus (1.1)	*	*	*		
2.	Riigitasemel küberturvalisuse koordinatsiooniüksus (1.2)			*	*	
3.	Riigi küberturvalisuse strateegia (1.3)	*	*	*		
4.	Küberturvalisuse rakendusplaan (1.4)	*	*	*		
5.	Küberohtude analüüsiüksus (2.1)		*	*		
6.	Iga-aastased küberohtude analüüsid (2.2)			*		
7.	Küberturvalisuse veebileht (2.3)	*		*		
8.	Üldhariduse õppekavades küberturvalisuse kompetentsid (3.1)	*		*		
9.	Küberturvalisuse bakalaureuseõppekava (3.2)			*	*	
10.	Küberturvalisuse magistrikava (3.3)			*	*	*
11.	Küberturvalisuse doktorikava (3.4)			*	*	*
12.	Küberturvalisuse spetsialiste ühendav erialaühing (3.5)			*		

[41] https://www.fema.gov/mission-areas

13.	Küberkuritegevuse konventsioon on ratifitseeritud (4.1)		*			
14.	Regulaarne esindatus rahvusvahelises koostöövormingus (4.2)				*	
15.	Riigis rahvusvaheline küberkaitseorganisatsioon (4.3)				*	*
16.	Kolme aasta jooksul välisriigis küberkaitsevõimekuse projekt (4.4)			*		
17.	Digiteenuste osutajate küberturvalisuse alane vastutus (5.1)	*				
18.	Küberturvalisuse standard avalikule sektorile (5.2)	*				
19.	Kompetentne järelevalveasutus (5.3)	*	*	*		
20.	Elutähtsa teenuse osutajat sätestav õigusakt (6.1)	*				
21.	Elutähtsa teenuse osutaja haldab IKT riske (6.2)	*	*	*		
22.	Elutähtsa teenuse osutajate järelevalveasutus (6.3)	*	*	*		
23.	Teenuseosutajate turbemeetmete regulaarne monitooring (6.4)			*		
24.	Isikukoodi olemasolu (7.1)	*				
25.	Krüptosüsteemide nõuded (7.2)	*				
26.	Elektrooniline isikutuvastus (7.3)		*			
27.	Digiallkiri (7.4)					
28.	Ajatembeldamine (7.5)					
29.	Elektroonilised usaldusteenused on reguleeritud (7.6)	*				
30.	Elektrooniliste usaldusteenuste järelevalve (7.7)	*	*	*		
31.	Isikuandmete kaitse seadus (8.1)	*				
32.	Isikuandmete kaitse järelevalveasutus (8.2)	*				
33.	Küberintsidentide tuvastamis- ja vastustamisüksus (9.1)			*	*	*
34.	Küberintsidentide raporteerimiskohustus (9.2)	*	*	*		
35.	Rahvusvahelise koordineerimise kontaktpunkt (9.3)			*	*	
36.	Küberintsidentide kriisihaldusplaan (10.1)				*	*
37.	Riigitasemel kriisihaldusõppused (10.2)			*		
38.	Osavõtt rahvusvahelistest kriisihaldusõppustest (10.3)			*		
39.	Vabatahtlike rakendamine küberkaitses on seadustatud (10.4)			*	*	*
40.	Küberkuriteod on kriminaliseeritud (11.1)	*				
41.	Küberkuritegude vastu võitlemise üksus (11.2)	*		*	*	
42.	Küberkuritegude ekspertiisiüksus (11.3)			*		

43.	Küberkuritegude 24/7 rahvusvaheline kontaktpunkt (11.4)		*		*	
44.	Küberoperatsioonide militaarüksus (12.1)			*		
45.	Kaitsejõud on viinud läbi küberkaitseõppuseid (12.2)			*		
46.	Militaarüksus on osalenud rahvusvahelistel küberõppusel (12.3)			*		
	KOKKU	20	12	29	12	6

Tabeli 3 kommentaarid on järgmised:

1. Küberintsidendi ennetamise ja kahjuleevenduse eristamine on sageli tinglik. Näiteks intsidendi osalist ärahoidmist võib käsitleda ka kui kahjuleevendust.
2. Arvestatud on ka kaudset mõju. Näiteks asjaolu, et elektrooniline isikutuvastus (mõõdik 7.3) võimaldab nimeliselt fikseerida andmebaaside poole pöördumised, vähendab isikuandmete väärkasutuse riske.
3. Kaudse mõju suuruse hindamisel on olulise ja mitteolulise mõju eristamine subjektiivne, kuna selleks puuduvad selged kriteeriumid. Nii näiteks on digiallkirja (7.4) ja ajatembeldamise (7.5) mõju hinnatud tabelis 6 väheoluliseks. Samas võib nende mõju edaspidi uute tehnoloogiate ja teadmiste lisandudes osutuda tulevikus oluliseks.

Järeldused tabelist 3.

1. NCSI nõuete täitmine tagab suhteliselt hea valmisoleku küberintsidentideks ja nende ärahoidmise; intsidentide vastu- ja taastusmeetmed on vähem tähtsustatud. Kuna intsidendi ärahoidmis- ja kahjuleevenduse meetmete eristus on kohati tinglik, võib ka kahjuleevenduse etappi lugeda piisavalt tähtsustatuks.
2. Järgmised mõõdikud on küberintsidentide juhtimisega seonduvalt vähemolulised: digiallkiri (7.4), ajatembeldamine (7.5), mistõttu võiks kaaluda indeksist nende ärajätmist.
3. NCSI tähtsustab küberturvalisuse alast formaalõpet (mõõdikud 3.1-3.4) samas kui mitteformaalne õpe pole indeksis kajastatud. Sätestatud on küll küberintsidentidest raporteerimiskohustus (mõõdik 9.2) ja iga-aastane küberohtude analüüside koostamine (mõõdik 2.2), kuid kogemuse operatiivset levitamist pole hõlmatud.

7. NCSI vastavus rahvuslikule küberturvalisuse strateegia koostamise juhendile

Sisulise hinnangu andmiseks sellele, kuivõrd NCSI katab kõik küberturvalisuse strateegia olulised aspektid, on sobivaim võtta aluseks Rahvusvahelise Telekommunikatsiooni Liidu (ITU), Maailmapanga Rahvaste Ühenduse sekretariaadi (ComSec), Rahvaste Ühenduse telekommunikatsiooniorganisatsiooni (CTO) ning NATO Küberkaitsekoostöö keskuse (NATO CCD COE) juhtimisel loodud rahvusliku küberturvalisuse strateegia koostamise juhend "Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity" [ITU, ComSec, CTO, NATO CCD COE 2018]. Selles määratletakse seitse fookusrühma ning 33 elementi, mida riiklikud küberturvalisuse strateegiad peaksid hõlmana.

NCSI metoodikas olevate mõõdikute ja rahvusliku küberturvalisuse strateegia koostamise juhendis olevate elementide vastavus on toodud tabelis 4. Tabeli esimeses veerus on strateegia koostamise juhendis loetletud strateegiaelemendi järjekorranumber, teises veerus elemendi nimetus ja kolmandas veerus antud elemendile vastavate NCSI mõõdikute identifikaatorit number. NCSI identifikaatorite numbrid ja nimed on toodud varem tabelis 3. Strateegia elementide nimetustes on mõnel juhul parema arusaadavuse huvides tõlget laiendatud. Juhul kui NCSI mõõdik ei kata strateegia koostamise juhendi elementi piisavalt või seos on kaudne, siis on mõõdik asetatud sulgudesse.

Tabel 4. NCSI kooskõla rahvusliku küberturvalisuse strateegia koostamise juhendiga

Ident.	Elemendi nimetus	NCSI vastavad mõõdikud
1.1	Strateegia on heaks kiidetud valitsuse tasemel	1.3
1.2	Loodud on kompetentne küberturvalisuse võimuorgan	1.1
1.3	Tagatud on valitsusesisene koostöö	1.2
1.4	Tagatud on sektoritevaheline koostöö	(1.2, 3.5, 6.3)
1.5	Tagatud on adekvaatsed ressursid	9.1, 11.2, 11.3, 11.4, 12.1
1.6	Strateegiaga kaasnevad selle rakenduskavad	1.4

2.1	Valitsusasutuste ja kriitilise taristu operaatorite jaoks on määratletud kooskõlaline riskihalduse käsitlus	6.2
2.2	Küberturvalisuse riskihalduseks on kasutusel ühtne metoodika	(5.2)
2.3	Riigile oluliste sektorite jaoks on leitud riskide profiilid	(6.2)
2.4	Riigi kriitiliste üksuste jaoks on kehtestatud küberturvalisuse poliitikad	5.2, 6.1
3.1	Riigis on loodud küberintsidentide lahendamise võimekus	3.2, 3.3, 3.4, 9.1, (2.1, 2.2)
3.2	Koostatud on küberturvalisuse kriisiohjeplaanid	10.1
3.3	Olemas on teabejagamise mehhanismid	(2.3, 9.2)
3.4	Viiakse läbi riigisiseseid ja rahvusvahelisi küberkaitseõppuseid	10.2, 10.3, 12.2, 12.3
4.1	Loodud on riskihalduskavad kriitilise taristu ja teenuste kaitsmiseks	6.2
4.2	Kriitilise taristu ja teenuste kaitsmiseks on loodud selge juhtimismudel	5.1
4.3	Kriitilise taristu ja teenuste jaoks on kehtestatud väljundipõhised (*outcomes-based*) küberturvalisuse nõuded	(6.4)
4.4	Rakendatud on turupõhised stiimulid küberturvalisuse põhimõtete järgimiseks	(5.3, 6.3, 6.4, 7.7)
4.5	Kriitilise taristu ja teenuste turvalisuse suurendamiseks on loodud jätkusuutlikud avaliku ja erasektori partnerlussuhted	(6.3)
5.1	Arendatakse küberturvalisuse õppekavu	3.1, 3.2, 3.3, 3.4
5.2	Stimuleeritakse laiapõhjalist digiturvalisuse koolitust	(3.5, 10.4)
5.3	Täidetakse koordineeritud digiturvalisuse teadlikkuse tõstmise programme	(2.3)
5.4	Toetatakse digiturvalisuse innovatsiooni ja teadus-arendustegevust	2.1, 2.2, 3.4, 11.3
6.1	Kehtestatud on küberkuritegevuse seadusandlus	11.1
6.2	Üksikisiku õigused ja vabadused on kaitstud	8.1, 8.2

6.3	Loodud on taristu ja IKT süsteemide konfidentsiaalsuse, terviklikkuse ja kättesaadavuse rikkumist ennetavad mehhanismid.	7.1, 7.2, 7.3, 7.6, 7.7
6.4	Toetatud on õiguskaitse suutlikkust suurendavad meetmed (sh asjaosaliste koolitus)	(2.3)
6.5	Kehtestatud on organisatsioonidevahelised järelevalveasutused	5.3, 6.3
6.6	Küberkuritegevuse alased rahvusvahelised kokkulepped on ratifitseeritud.	4.1
7.1	Küberturvalisus on välispoliitika üks prioriteete	
7.2	Osaleb rahvusvahelistel foorumitel ja koostöökogudes	4.2, 4.3
7.3	Formaalne ja mitteformaalne koostöö on toetatud	4.4, 9.3
7.4	Riiklikud algatused on kooskõlas rahvusvahelistega	

Kommentaarid tabeli 4 juurde.

1. Rahvusliku küberturvalisuse strateegia koostamise juhend sisaldab elemente, mida ei ole võimalik avalike avalike dokumentidega hinnata, kuna need on kas kvalitatiivsed (elemendid 1.4 ja 7.4) või eeldavad konfidentsiaalsust (elemendid 2.3 ja 4.1; osaliselt ka 4.3).
2. Rahvusliku küberturvalisuse strateegia koostamise juhendi elementidest on NCSI metoodikaga suhteliselt väheselt või kaudselt kaetud järgmised elemendid: 2.2, 4.3, 4.4, 4.5, 5.2, 5.3, 6.4, 7.1.
3. NCSI mõõdikutest on rahvusliku küberturvalisuse strateegia koostamise juhendi elementidega suhteliselt vähem seotud järgmised NCSI mõõdikud: 7.4, 7.5.

Järeldused tabelist 4.

1. NCSI metoodikaga on suhteliselt hästi kaetud järgmised rahvusliku küberturvalisuse strateegia koostamise juhendi fookusvaldkonnad: valitsemine (*governance*), valmisolek ja vastupanuvõime (*preparedness and resilience*), seadusandlus ja regulatsioonid (*legislation and regulation*) ning rahvusvaheline koostöö (*international cooperation*). Osaliselt on kaetud riiklik küberturvalisuse riskihaldus (*risk management in national cybersecurity*), kriitiline taristu ja olulised teenused (*critical infrastructure services and essential services*), võimekuse arendamine ning teadlikkuse suurendamine (*capability and capability building and awareness raising*).

2. NCSI mõõdikud on heas kooskõlas rahvusliku küberturvalisuse strateegia koostamise juhendiga. Vaid digiallkiri (NCSI mõõdik 7.4) ja ajatembeldamine (7.5) ei ole otseselt seotud rahvusliku küberturvalisuse strateegia koostamise juhendi ühegi elemendiga.
3. NCSI poolt on suhteliselt vähem tähtsustatud laiapõhjaline teavitus ja koolitus (3.3, 5.2, 5.3).
4. Lisas 2 kirjeldatud riiklike küberturvalisuse strateegiadokumentide analüüs näitas, et koolituse problemaatika on ka üldiselt riiklikes strateegiadokumentides suhteliselt vähe tähtsustatud (analüüsi üldised tulemused on toodud 3. peatükis).

8. NCSI metoodika adekvaatsus

Metoodika adekvaatsuse all mõistame seda, kuivõrd kooskõlaline on metoodika indeksile seatud eesmärgiga (vt p 1.4.1).

NCSI eesmärgi sõnastus on järgmine: *Riiklik küberturvalisuse indeks mõõdab riikide valmisolekut küberohtude ennetamiseks ja küberintsidentide juhtimiseks. NCSI on ka andmebaas avalikult kättesaadavate tõendusmaterjalidega ja vahend küberjulgeoleku riikliku suutlikkuse suurendamiseks*.

Seega olulised märksõnad on: „riikide valmisolek“, „küberohtude ennetamine“, „küberintsidentide juhtimine“, „andmebaas avalikult kättesaadavate tõendusmaterjalidega“, „vahend küberjulgeoleku riikliku suutlikkuse suurendamiseks“.

Käsitleme järgnevalt iga märksõna eraldi. Siinkohal on asjakohane märkida, et kuigi ettevõtete jaoks on koostatud mitmeid küberturvalisuse suurendamise raamistikke ja juhendeid (vt näiteks [CREST, 2013] või [Cyber Security Coalition, 2015]), siis riigi tasemel sarnaseid raamistikke ja juhendeid pole koostatud.

a) *Riigi valmisolek*.

Riigi roll küberohtude ennetamisel ja küberintsidentide juhtimisel on eelkõige asjakohaste regulatsioonide, institutsioonide ja ressursside tagamine. Üldise kriisijuhtimise mudeli kohaselt hõlmab see roll nii küberohu äratundmist, aga ka kõikvõimalikke küberturvalisust tagavaid planeerimis-, koolitus-, süsteemiarenduse ja muude meetmete rakendamist.

Konkreetsemalt on riigi valmisoleku tagamiseks vajalik:

- seadusandluse olemasolu ja elluviimine
- strateegia ja tegevuskavade olemasolu

- kompetentse kaadri olemasolu
- järelevalveinstitutsioonide olemasolu ja toimimine.

6. peatükis läbiviidud analüüs näitas, et NCSI metoodika hindab adekvaatselt riigi kriisiks valmisoleku komponente. Tabelist 3 tehtud järelduste kohaselt ei kata NCSI mõõdikud vaid kompetentse kaadri olemasolu toetavat mitteformaalset õpet. Rahvusliku küberturvalisuse strateegia koostamise juhendi (peatükk 7) kohaselt läheksid selle alla elemendid 5.2 (stimuleeritakse laiapõhjalist digiturvalisuse koolitust) ja osaliselt ka 6.4 (toetatud on õiguskaitse suutlikkust suurendavad meetmed).

b) *Küberohtude ennetamine*.

Küberohtude ennetamine sõltub eelkõige digivahendite kasutajate käitumisest ning tehnoloogiliste süsteemide kaitstusest. Üldise kriisijuhtimise mudeli kohaselt tähendab see näiteks tulemüüride olemasolu või kasutajate poolt küberhügieenireeglite järgimist.

Konkreetsemalt on riigi küberturvalisuse alal valmisoleku tagamiseks vajalik:

- analüüsivõimekuse olemasolu ja selle rakendamine
- kriitilise taristu kaitsmine
- riigisisene ja rahvusvaheline koostöö
- rahvaharidus.

6. peatükis esitatud NCSI ja kriisijuhtimise etappide võrdluse põhjal on küberohtude ennetamise hindamine NCSI metoodika kohaselt väga adekvaatne. Tabelist 4 järeldub, et NCSI mõõdikud ei kata täielikult:
1) analüüsivõimekuse rakendamist (element 2.2 – *küberturvalisuse riskihalduseks on kasutusel ühtne metoodika*),
2) riigisisest koostööd (element 1.4 – *tagatud on sektoritevaheline koostöö*, 4.4 – *rakendatud on turupõhised stiimulid küberturvalisuse põhimõtete järgimiseks*, 4.5 – *kriitilise taristu ja teenuste turvalisuse suurendamiseks on loodud jätkusuutlikud avaliku ja erasektori partnerlussuhted*)
3) rahvaharidust (5.2 – *stimuleeritakse laiapõhjalist digiturvalisuse koolitust*, 5.3 – *täidetakse koordineeritud digiturvalisuse teadlikkuse tõstmise programme*).

c) *Küberintsidentide juhtimine*.

Küberintsidentide juhtimine tähendab küberintsidendi tuvastamist, intsidendi toimumise ajal inimressursside tegevuse ja tehnoloogiliste vahendite kasutuse koordineerimist ning samuti küberintsidendi laienemist tõkestavaid tegevusi. Selleks on vajalik:

- kohustus teavitada küberintsidendist

- professionaalse kaadri olemasolu
- kriisihalduse institutsioonide olemasolu ja toimimine

Kuigi 6. peatükis läbi viidud NCSI ja kriisijuhtimise etappide võrdluse kohaselt on küberintsidentide juhtimine (veerg *Kriisile reageerimine* tabelis 3) NCSI mõõdikutega kaetud, ei kata NCSI mõõdikud piisavalt küberintsidentidest saadud kogemuse levitamist. Rahvusliku küberturvalisuse strateegia koostamise juhendis (peatükk 7) läheks küberintsidentidest saadud kogemuse levitamise alla strateegia element 3.3 (*olemas on teabejagamise mehhanismid*).

d) ***Andmebaas avalikult kättesaadavate tõendusmaterjalidega***.

Kuna NCSI metoodika kohaselt on hindamise aluseks veebis avaldatud lingid riikide asjakohastele allikatele, siis on see nõue täidetud.

e) ***Vahend küberjulgeoleku riikliku suutlikkuse suurendamiseks***.

See nõue eeldab ligipääsu hea praktika kirjeldusele punktide a), b) ja c) all loetletud adekvaatsuse märksõnade osas. Formaalselt on NCSI metoodika puhul see nõue täidetud – hinnatud riikide asjakohastele dokumentidele on veebiviited ning nendele on vaba ligipääs. Asjaolu, et mõõdikute väärtuste hindamiseks on kehtestatud skaalad, annab võimaluse otsustada nõuete täidetuse taseme üle. Samas ei ole eriti häid praktikaid ega ka NCSI metoodika kohaselt riikide küberturvalisuse taset hindava ekspertrühma soovitusi välja toodud.

Kokkuvõtvalt võib NCSI metoodika adekvaatsust hinnata heaks. Ettepanekud NCSI metoodika adekvaatsuse suurendamiseks on esitatud 12. peatükis.

9. NCSI metoodika lihtsus

Metoodika lihtsuse mõõdikuna kasutame töömahtu, mis on vajalik NCSI metoodika rakendamiseks mingi konkreetse riigi küberturvalisuse taseme hindamisel. Seejuures jaguneb töömaht kaheks komponendiks:

a) Esmahindamiseks vajalik töömaht
b) Kordushindamiseks vajalik töömaht.

Kumbki komponent jaguneb omakorda kaheks:

a) Hinnatavas riigis tehtava töö maht

b) Hindaja (antud juhul E-riigi Akadeemia töötajate) töö maht.

Kuna mistahes mõõdiku hindamine toimub (avalikus) veebis oleva informatsiooni põhjal, siis on riigi NCSI väärtuse leidmiseks kuluv aeg võrdeline ühe veebilehe määratlemiseks ning analüüsimiseks kuluva ajaga. Kuigi ühe mõõdiku puhul võib aluseks olla ka rohkem kui üks veebileht, on praktikas mitmele veebilehele viidatud vaid üksikute mõõdikute puhul tegeliku töö kogumaht sellest ei muutu.

Hindaja seisukohalt rohkem aeganõudev võib olla selliste mõõdikute väärtuste hindamine, mille hindevahemikud on suuremad. Samas kuna ligi poolte mõõdikute väärtus on kas 0 või 1, siis mudeli lihtsuse huvides võib skaalade erinevuse jätta arvestamata. Mõõdiku, mille hindeskaala on näiteks 0 ... 3, tegelik väärtus võib olla 0, st selle hindamiseks ei kulu rohkem aega kui väiksema hindeskaalaga mõõdiku väärtuse hindamiseks.

Seega võib esmahinnangu (E) ja kordushinnangu (K) maksimaalse töömahu hinnanguks kasutada valemeid

$E = 46 \cdot (c_1 + c_2 + c_3)$

$K = c \cdot (c_1 + c_2 + c_3)$

kus

c_1 – hinnatava poolt ühe veebiaadressi määratlemiseks kuluv keskmine aeg (mõõta võib näiteks tundides)

c_2 – hinnatava poolt ühe näitaja kommenteerimiseks kuluv keskmine aeg

c_3 – hindaja poolt ühe mõõdiku hindamiseks kuluv keskmine aeg

c – keskmine näitajate arv kordushindamisel (alternatiivina võib võtta c = 1).

On selge, et igal konkreetsel juhul võivad c_1, c_2 ja c_3 väärtused varieeruda väga suures ulatuses. Näiteks c_3 puhul võib see olla null, kuid võib olla näiteks ka paar tundi, kui otsuse tegemiseks on vaja süüvida esitatud dokumentide sisusse. Juhul kui hindamisel lisada näidismõõdiku tunnus (vt soovitusi 12. peatükis), siis mõõdiku hindamiseks kuluvat aega see oluliselt ei suurenda.

Kokkuvõtteks võib NCSI väärtuse arvutamist pidada ja lihtsaks ning metoodika lihtsust suurepäraseks. Seega ei ole NCSI praeguseid protseduure otstarbekas muuta.

10. NCSI metoodika paindlikkus

Metoodika paindlikkuse all on silmas peetud selle järgmiseid kriteeriume:

a) Metoodika on täiendatav, st võimaldab uue mõõdiku lisamist, olemasoleva muutmist või kaotamist.

b) Metoodika on dünaamiline, st mingi mõõdiku lisamine, muutmine või kaotamine ei põhjusta teiste mõõdikute ümberarvestust.

Kuna NCSI on andmebaasipõhine, siis uue mõõdiku lisamine, olemasoleva muutmine või kaotamine tähendab NCSI eksperdi jaoks vaid muudatuste sisseviimist ncsi.ega.ee veebi andmebaasi. NSCI metoodika igakordse muutmisega kaasneb terve rida ühekordseid tegevusi, nagu näiteks mõõdiku sisuline hindamine, metoodika juhendi täiendamine jmt.

Dünaamilisus on tagatud metoodika olemusega, kuna mõõdiku hindamine toimub sõltumatult teiste mõõdikute väärtustest. Seega vastab NCSI suurepäraselt paindlikkuse kriteeriumitele.

11. Küberturvalisuse hindamismetoodikate võrdlev analüüs

Tabelites 5 ja 6 esitame vaadeldud metoodikate (v.a. New York'i küberturvalisuse indeksi) olulisemad tugevused ja nõrkused koos põhjendustega ning hindame nende metoodikate adekvaatsust, lihtsust ja paindlikkust.

Metoodikate olulisemate tugevuste ja nõrkuste määratlemisel arvestame nii suhtelisi (võrdluses teiste metoodikatega) kui ka absoluutseid aspekte. Absoluutsete aspektide all on arvestatud kooskõla üldise kriisijuhtimise mudeli (vt peatükk 6) ja rahvusliku küberturvalisuse strateegia koostamise juhendiga (vt peatükk 7). NCSI vastavuse analüüs üldise kriisijuhtimise mudeliga ja rahvusliku küberturvalisuse strateegia koostamise juhendiga on viidud läbi 6. ja 7. peatükis.

Tabel 5. Vaadeldud metoodikate olulisemad tugevused.

Metoodika	Metoodika tugevused	Põhjendus

Globaalne küberturvalisuse indeks GCI	1. Käsitleb põhjalikult rahvusvahelisse koostöösse panustamist. 2. Motiveerib riike oma küberturvalisust täiustama.	• Rahvusvahelist koostööd käsitleb kuus mõõdikut (25% mõõdikute koguarvust). • Metoodika kasutamine on küberturva-lisuse hindamisel laialt levinud.
Potomaci poliitikauuringute instituudi kübervalmisoleku indeks CRI 2.0	1. Metoodikat kirjeldav põhidokument annab küberturvalisuse suurendamiseks tegevusjuhiseid. 2. Iga konkreetse riigi analüüs on väga põhjalik.	• Metoodikat kirjeldav põhidokument toob iga hinnatava rühma osas erinevatest riikidest häid näiteid. • Raportite maht on üldjuhul vahemikus 20-40 lehekülge.
Küberturvalisuse võimekuse küpsusmudel CCMM	1. Küpsustasemete määratle-mise juhend on põhjalik. 2. Iga konkreetse riigi küpsuse määratlemise järgselt tehakse soovitusi küpsustaseme tõstmiseks.	• Iga mõõdiku ja iga taseme jaoks on olemas kriteeriumid. • Näiteks Leedule on tehtud küberturvalisuse suurendamiseks kokku 105 ettepanekut.
BSA EL küberturvalisuse indeks	1. Mõõdikute hindamiskriteeriumite määratlemiseks on loodud lihtne juhend.	• Mõõdikute hindamiskriteeriumid on koondatud ülevaatlikku tabelisse.
Riiklik küberturvalisuse indeks NCSI	1. Väga ülevaatlik ning tagasivaateid ja riikide võrdlusi võimaldav veebileht. 2. Motiveerib riike pidevalt küberturvalisust täiustama. 3. Kõik riigi hinnangul arvestatud tõendid on avalikud. 4. Metoodika on dünaamiliselt muudetav/täiendatav.	• Riikide hinnangud on illustreeritud rohke graafikaga, sh on indeksi kolme aasta dünaamika kujutatud graafiliselt. • Operatiivselt andmetega täiendatav, mistõttu iga aktsepteeritud täiendus kajastub riigi indeksis jooksvalt. • Tagab metoodika usaldusvääruse ning võimaldab riikidel üksteiselt õppida. • Võimaldab paindlikult arvestada küberturvalisuse uusi aspekte.

Kokkuvõtvalt võib öelda, et NCSI eristub teistest positiivselt eelkõige kasutajasõbraliku veebiliidese ning hindamisel aluseks võetavate materjalide avalikkuse poolest. Kuigi see metoodika ei paku riikide küberturvalisuse suurendamiseks soovitusi (nagu näiteks CCMM

või CRI 2.0), on tänu materjalide avalikkusele riikidel üksteise heast praktikast võimalik õppida.

Täiendavalt võib lisada järgmised kommentaarid:

1. Tabelis 5 loetletud metoodikatest kolme (GCI, BSA EL küberturvalisuse indeks, NCSI) ühise omadusena võib mainida asjaolu, et nende rakendamine ei ole eriti töömahukas.
2. Kuigi NCSI veebiliides on võrreldes teiste analüüsitud metoodikate veebilehtedega selgelt parim, on selleski mõned kergesti kõrvaldatavad probleemid, nagu näiteks:
    a. Mõõtühikuks on 1,3 punkti, kuid tulemus väljastatakse veebis täpsusega 0,01 (pdf-väljatrükkides täisarvuna).
    b. Pdf-faili salvestamisel lokaalsele andmekandjale pakutakse salvestatava faili nimeks alati „download".

Tabel 6. Vaadeldud metoodikate olulisemad nõrkused

Metoodika	Metoodika nõrkused	Põhjendus
Globaalne küberturvalisuse indeks GCI	1. Valdkondade kaalud on võrdsed (0,2) samas kui nende koosseisus olevate mõõdikute kaalud on täpsusega 0.001.	• Kaalud ei ole põhjendatud (mistõttu teistsuguste kaalude kasutamisel muutuks ka riikide järjestus).
	2. Riikide analüüsid ei ole avalikud.	• Ei võimalda teiste riikide kogemusest õppida.
Potomaci poliitikauuringute instituudi kübervalmisoleku indeks CRI 2.0	1. Metoodika ei ole riike eristav.	• Kõrgeimalt hinnatud riikide tase on kõigi seitsme rühma osas hinnatud kui „osaliselt toimiv".
	2. Metoodika detailne kirjeldus ei ole avalikult kättesaadav.	• Puudub võimalus eneseanalüüsiks.
	3. Enamiku riikide kohta koostatud raportid ei ole avalikud.	• Ei võimalda teiste riikide kogemusest õppida.
Küberturvalisuse võimekuse küpsusmudel CCMM	1. Suhteliselt töömahukas.	• Riigi hindamisaruande mahuks on 50-60 lehekülge.
	2. Küberturvalisuse võimekuse hindamine on läbi viidud vaid mõne	• Ei võimalda edukate riikide kogemusest õppida.

	üksiku arenenud riigi kohta.	
BSA EL küberturvalisuse indeks	1. Ei peegelda aktuaalset seisu.	• Metoodikat on rakendatud vaid 2014. aastal ühekordse projektina.
Riiklik küberturvalisuse indeks NCSI	1. Võrreldes teiste analüüsitud metoodikatega olulisi nõrkuseid ei leitud.	

Nõrkuste osas võib täiendavalt lisada järgmised kommentaarid:

1. CRI 2.0 probleemiks on ka asjaolu, et hinnangute jaotus on äärmiselt ebaühtlane. Näiteks hindega „täielikult toimiv" ei ole avalikustatud analüüsides hinnatud mitte ühegi riigi mitte ühtegi rühma. Seega on sisuliselt tegemist binaarse hindeskaalaga – *andmed puuduvad* ja *osaliselt toimiv*. Ka pole metoodikat piisavalt kirjeldatud, mistõttu seda saab rakendada vaid selle autorite kitsas seltskond. Pole avaldatud isegi mõõdikute täielikku loetelu; nende osaline nimekiri (61 mõõdikut) sisaldub vaid allikas [Hathaway 2016].
2. NCSI metoodika nõrkused üldise kriisijuhtimise mudeli ja rahvusliku küberturvalisuse strateegia koostamise juhendi suhtes on välja toodud 6 ja 7 peatükis.

Järgnevas tabelis 7 hindame vaadeldud metoodikaid adekvaatsuse, lihtsuse ja muudetavuse seisukohalt. Hinnangute andmisel oleme kasutanud järgmist skaalat:

5 – suurepärane

4 – väga hea

3 – hea

2 – rahuldav

1 – nõrk

Tabel 7. Vaadeldud metoodikate adekvaatsuse, lihtsuse ja paindlikkuse hinnangud

Metoodika	Eesmärk	Adekvaatsus	Lihtsus	Paindlikkus
Globaalne küberturvalisuse indeks GCI	Mõõta riikide pühendumust küberturvalisuse tagamisele ning neid võrrelda.	3	4	3

Kübervalmisoleku indeks CRI 2.0	Hinnata riikide taset 7 indikaatori osas.	3	3	2
Küberturvalisuse võimekuse küpsusmudel CCMM	Hinnata riikide küberturvalisuse võimekuse taset 24 tunnuse (teguri) osas.	4	2	3
BSA EL küberturvalisuse indeks	Hinnata riikide küberturvalisuse poliitikat kujundava 25 tunnuse olemasolu.	1	5	1
Rahvuslik küberturvalisuse indeks NCSI	Mõõta riikide valmisolekut küberohtude ennetamiseks ja küberintsidentide juhtimiseks.	4	5	5

Võtame järgnevate hinnangute võrdlusaluseks 8., 9. ja 10. peatükis kirjeldatud NCSI metoodika adekvaatsuse, lihtsuse ja paindlikkuse hinnangud (vastavalt 4, 5 ja 5). Vaid CCMM järgi mõõdetakse **mõõdikute/kriteeriumite täitmise määra** (viis taset, vt alajaotus 4.4). Teiste metoodikate puhul ei arvesta kriteeriumite täitmise määra, vaid üksnes olemasolu (on/ei ole). Sisuliselt ei hinda taset ka kübervalmisoleku indeks CRI 2.0, kuna kõikide hinnatud mõõdikute väärtuseks on omistatud *osaliselt toimiv*. Seetõttu on nendel kübervõimekuse suurendamiseks suhteliselt madal rakenduslik väärtus, kuna ei paku vastuseid küsimusele *Kuidas*?

Vaid GCI ja NCSI võimaldavad võrrelda riike omavahel. Samas omavad kõik metoodikad teatud väärtust, kuna hõlmavad mitmeid mõõdikud, mida on otstarbekas arvestada ka NCSI mõõdikute komplekti täiendamisel (vt 12. peatükki).

Vaadeldud metoodikate ühise omadusena võib mainida asjaolu, et hindamise raamistik ei arvesta hinnatava riigi spetsiifikat, mis põhineks analüüsitava institutsiooni protsesside kvalitatiivsel analüüsil, sarnaselt näiteks NASA SEL SPI tarkvaraarenduse metoodikaga [McGarry jt 1994]. Samas on selge, et sellise metoodika rakendamine oleks võrreldamatult töömahukam, eeldades muuhulgas mahukat eelanalüüsi ja hindajate kohtvisiite. Ka puudub vaadeldud metoodikates ilmutatud kujul esitatud seos (st veenev põhjendus) metoodika eesmärkide ja valitud kriteeriumite vahel, nii nagu seda on peatükis 8 tehtud rahvusliku küberturvalisuse indeksi metoodika analüüsil.

Kirjeldatud metoodikate ühiseks jooneks on ka asjaolu, et need on positivistlikud, st arvestavad vaid küberturvalisust suurendavaid faktoreid ning jätavad arvestamata seda vähendavad faktorid, näiteks riigi poliitikaid/praktikaid, mis toetavad küberkuritegevust (nii

näiteks on Venemaa ja Hiina GCI pingereas suhteliselt kõrgetel kohtadel, vastavalt 26. ja 27. kohal).

Võrreldes erinevaid metoodikaid, tuleb nõustuda artiklis „The Balanced Digitalization and Digital Security: Case of Regional Authorities" [Kuusisto & Kuusisto, 2019; lk 270] väljendatud hinnanguga, et „keerukad turvalisuse hindamise kontseptsioonid pole veel rahvusvaheliselt piisavalt määratletud, korraldatud ja reguleeritud"[42], misjärel jõutakse seisukohale, et „juhtimise ja juhtimise toetamiseks kasutatavate näitajate kavandamisel ja kasutamisel on vaja põhjalikku analüüsi asjakohaste ja sobivate mõõdikukomplektide valimiseks ja moodustamiseks"[43]. Tõsi küll, selle seisukohani jõuti vaid kümne riigi GCI- ja NCSI-väärtuste võrdlemise järel. Nende korral oli indeksihulkade korrelatsioonikordaja väärtuseks lausa 0,73, kuid juba indeksite kõige väiksema väärtusega riigi (Jordaania) väljajätmisel oli korrelatsioonikordaja väärtuseks üksnes 0,27.

12. Ettepanekud riikliku küber-turvalisuse indeksi metoodika täiustamiseks

Järgnevalt esitatavad ettepanekud põhinevad eelkõige riikliku küberturvalisuse indeksi NCSI võrdlusanalüüsil kriisijuhtimise 5-etapilise metoodika ja rahvusliku küberturvalisuse strateegia koostamise juhendiga. Pakutud uute mõõdikute sõnastustes on arvestatud teiste küberturvalisuse hindamise metoodikates kasutatud sõnastustega. Seejuures oleme lähtunud sellest, et metoodika olemus (avalike dokumentide põhisus) jääks samaks.

Ettepanekud on jagatud kahte rühma:

a) Ettepanekud metoodika täiendamiseks;

b) Ettepanekud metoodika rakendamise osas.

Metoodika täiendamise osas on kolm sisulist ettepanekut:

[42] "the complex security evaluation concepts are not yet internationally defined, organized and regulated to a sufficient level"

[43] "when planning and using indicators for supporting governance and management, a thorough analysis is needed for selecting and forming relevant and suitable indicator sets"

1) **Jätta mõõdikute komplektist välja mõõdikud 7.4** (digiallkiri) ja **7.5** (ajatembeldamine). Kumbki ei osutunud oluliseks ei 5-etapilise metoodika ega rahvusliku küberturvalisuse strateegia koostamise juhendi seisukohalt. Ka ei ole digiallkirjastamist ja ajatembeldamist mitte ühegi teise analüüsitud metoodika mõõdikute seas.

2) Lisada mõõdikute komplekti järgmised mõõdikud:

    a. **Küberturvalisuse riskihalduseks on kasutusel ühtne metoodika** (*A common methodology for managing cybersecurity risks is identified*). Sisuliselt on see nõue NCSI metoodika praeguses versioonis sätestatud vaid avalikule sektorile, ja sedagi kaudses sõnastuses (mõõdik 5.2 – Küberturbestandard avalikule sektorile). Riskihaldus on ilmutatud kujul mainitud vaid ühes (46-st) NCSI mõõdikus (mõõdik 6.2). Suhteliselt hästi on kaetud vaid küberohtude hindamine: NCSI mõõdikud 2.1 (Küberohtude analüüsiüksus) ja 2.2 (Iga-aastased küberohtude analüüsid). Samas on ohuhinnangud vaid riskihalduse üheks – kuigi oluliseks – komponendiks. Näiteks moodustavad riske käsitlevad mõõdikud rahvuslikus küberturvalisuse strateegia koostamise juhendis terve fookusrühma (7-st fookusrühmast).

    b. **Toimib küberkaitsespetsialistide süstemaatiline täiendkoolitus** (*There is systematic non-formal training of cyber defense specialists*). Kuna IKT valdkond areneb väga kiiresti, siis spetsialistide täiendkoolitus on vähemalt sama oluline kui tasemeõpe. Sisuliselt on küberkaitsespetsialistide täiendkoolitus teistes küberturvalisuse hindamise metoodikates kaetud. Samas on nendes olevate mõõdikute nimetused väga üldsõnalised, näiteks *Küberturvalisuse alane koolitus* (CCMM D3.2) või *Küberjulgeolekualased koolituskursused* (GCI), mistõttu annavad väga suure tõlgendusruumi.

    c. **Küberkaitse alal toimivad avaliku ja erasektori vahelised koostöömehhanismid** (*There are public-private cooperation mechanisms in the field of cyber defense*). Riikliku küberturvalisuse indeksi mõõdikute seas koostöö aspekt pole ilmutatud kujul mainitud. Samas on koostöö erinevad aspektid kõikides teistes küberturvalisuse hindamise metoodikates ja raamistikes väga olulisel kohal. Mõningaid näiteid: sektoritevaheline koostöö (rahvuslik küberturvalisuse strateegia koostamise juhend), avaliku ja erasektori partnerlus (EL küberturvalisuse töölaud), asutustevahelised/asutustesisesed partnerlused (Globaalne küberturvalisuse indeks), ametlikud ja mitteametlikud koostööraamistikud küberkuritegevuse vastu võitlemiseks (Küberturvalisuse võimekuse küpsusmudel).

d. **Toimivad küberkaitse alase teabe ja parimate praktikate operatiivse jagamise mehhanismid** (*Mechanisms for the operational sharing of cyber defense information and best practices have been established*). Nagu eespool mainitud, sätestatud on küll küberintsidentidest raporteerimiskohustus (NCSI mõõdik 9.2) ja iga-aastaste küberohtude analüüside publitseerimine (NCSI mõõdik 2.2), kuid küberkaitse ja -intsidentide alase kogemuse operatiivset levitamist pole hõlmatud. Samas on senise kogemuse kasutamine nii küberintsidentide ennetamisel kui ka juhtimisel äärmiselt oluline.

Lisaks tuleks kaaluda paar olulise küberturvalisuse aspekti lisamist indeksi, kuid samas tuleb möönda, et neid aspekte on dokumentide alusel suhteliselt raske hinnata:
1) laia elanikkonna digiturvalisuse teadlikkuse tõstmine ja
2) laia elanikkonna küberturvalisuse alane harimine.

Samas saab neid aspekte hinnata kaudselt elanikkonna teadlikkuse tõstmist ja küberturvalisuse alast harimist toetavate mehhanismide olemasolu kaudu. NCSI metoodikas on sellekohasteks mõõdikuteks 2.3 (*Küberturvalisuse veebileht*) ja 3.1 (*Üldhariduse õppekavades küberturvalisuse kompetentsid*). Ka kuuluks selliste mehhanismide hulka ülal punkti d all nimetatud mõõdik (*Toimivad küberkaitsealase teabe ja parimate praktikate operatiivse jagamise mehhanismid*).

Metoodika rakendamise osas on järgmised ettepanekud:

1) ***Esitada riikide tulemused täisarvuks ümardatuna***. Alternatiiv: esitada tulemus vahemikus [0; 1] (kahe kohaga peale koma), et oleks samas skaalas GCI hinnangutega.
2) ***Lisada andmebaasi näidismõõdiku tunnus***. Sellega saaks eksperdid märgistada konkreetsete riikide eriti heatasemelisi praktikaid peegeldavad mõõdikud, mida nad soovitavad teistel riikidel arvestada eeskujudena. See võimaldaks näiteks riikide puhul, millel on mingi mõõdiku väärtuseks null, kuvada veebis riikide loetelu, mille korral antud mõõdik omab näidismõõdiku tunnust. See võimaldaks muuhulgas viia näiteks ka ühesuguse indeksi väärtusega riikide järjestamise uutele alustele – asetada ettepoole riik, millel on suuremale arvule mõõdikutele omistatud näidismõõdiku staatus. Samuti tugevdaks see NCSI metoodikas kvalitatiivse komponendi osakaalu.

3) ***Avaldada NCSI metoodika põhjalik kirjeldus tervikliku publikatsioonina***. Praegu on metoodika kirjeldus avaldatud veebilehena ja näiteks ka artiklis [Rikk 2018], kuid puudub põhjalik terviklik käsitlus.

4) ***NCSI metoodika kirjelduses (eelmine punkt) tuua selgelt välja selle spetsiifika ja erinevuse teistest riikide küberturvalisuse taset mõõtvatest metoodikatest***, eelkõige GCI-st. Selgeks eristavaks aspektiks (NCSI kasuks) on metoodika veebilahendus. Seejuures võiks viidata ka mujal läbiviidud võrdlusuuringute tulemustele. Näiteks artikkel „Comparative Analysis of the Cybersecurity Indices and Their Applications" [Kravets 2019] võtab GCI ja NCSI võrdluse kokku järgmiselt: „NCSI on kõige asjakohasem, täpsem ja kajastab hetkeseisu"[44] ja NCSI „Pakub andmetöötluseks kaasaegseid teenuseid (tarkvara)"[45]. ITU toob oma võrdlusanalüüsis „Index of Cybersecurity Indices 2017" NCSI-st erinevusena ära selle, et NCSI hõlmab muuhulgas ka küberküpsust (*cyber maturity*) ja küberohte (*cyber threats*), mida GCI ei kata.

5) Muuta riigi tulemuslikkust esitava rapordi pdf-faili vaikimisi pakutav nimi ***informatiivseks***, näiteks nimekujuga NCSI-Riiginimi-kuupäev.

13. Kokkuvõte

Analüüsitud metoodikatest kõige elujõulisem on GCI, kuna seda toetab ITU. Seetõttu ei oleks otstarbekas käsitleda NCSI metoodikat kui konkureerivat, vaid kui lisaväärtust pakkuvat metoodikat.

Sellest tulenevalt võikski metoodika edasiarendamisel põhieesmärgiks olla selle rakendajatele võimalikult suure lisaväärtuse pakkumine.

Metoodika staatuse tõstmiseks võiks selle arendamisse kaasata NATO küberkaitsekeskuse (CCD COE – NATO *Cooperative Cyber Defence Centre of Excellence*) ning taotleda selle NATO-poolset tunnustamist.

Samuti võiks metoodika populaarsuse tõstmiseks sellega siduda erinevaid akadeemilisi ja teavitusüritusi, nagu näiteks:

[44] „NCSI is the most relevant, accurate and reflects the current state"
[45] „is provided with modern services (software) for data processing"

- Regulaarsete konverentside korraldamine (näiteks koostöös ülikoolide ja NATO küberkaitsekeskusega).
- Koostada ja levitada (näiteks seminaride vormis) parimaid praktikaid.
- Informeerida NCSI metoodika eelistest Eesti kõrgeid ametiisikuid (sh president, peaminister, Eesti esindaja ÜRO julgeolekunõukogus).

Juba praegu on NCSI rakendamine vaieldamatult kõige kasutajasõbralikum. Arvestades rahvusvaheliselt Eesti kõrget IT-alast renomeed, on NCSI veelgi laialdasemaks levikuks väga head eeldused.

Viidatud kirjanduse loetelu

1. BSA (2015). EU Cybersecurity Dashboard. A Path to a Secure European Cyberspace. http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf
2. CREST (2013), Cyber Security Incident Response Guide. Loetud aadressil http://www.crest-approved.org/wp-content/uploads/CSIR-Procurement-Guide.pdf
3. Cyber Security Coalition (2015). Cyber Security Incident Management Guide. Centre for Cyber Security. https://www.cybersecuritycoalition.be/content/uploads/cybersecurity-incident-management-guide-EN.pdf
4. ENISA (2016). Definition of Cybersecurity – Gaps and overlaps in standardisation. https://www.enisa.europa.eu/publications/definition-of-cybersecurity
5. GCSCC (2016). Cybersecurity Capacity Maturity model for Nations (CMM). Revised Edition. Global Cyber Security Capacity Centre. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf
6. Hathaway, M. (2016). Measuring and Assessing the Cybersecurity Challenge: Cyber Readiness Index 2.0. Esitlus GFCE (Global Forum on Cyber Expertise) aastakoosolekul. Loetud aadressil https://www.thegfce.com/binaries/gfce/documents/speeches/annual-meeting-2016/06/13/presentation9/12.12-12.45-cyber-readiness-index.pdf
7. Hathaway, M., Demchak, C., Kerben, J., McArdle, J., Spidalieri, F. (2015). Cyber Readiness Index 2.0. Potomac Institute for Policy Studies. https://www.potomacinstitute.org/images/CRIndex2.0.pdf
8. ITU (2017). Index of Cybersecurity Indices 2017, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/2017_Index_of_Indices.pdf
9. ITU, ComSec, CTO, NATO CCD COE (2018). Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity. ISBN: 978-92-61-27791-8. https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf
10. ITU (2019). Global Cybersecurity Index (GCI) 2018. ISBN: 978-92-61-28201-1. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
11. ITU-T (2008). X.1205: Overview of cybersecurity. ITU-T Recommendations, X Series: Data Networks, Open System Communications and Security. International Telecommunication Union (ITU). https://www.itu.int/rec/T-REC-X.1205-200804-I

12. Kravets, V. M. (2019). Comparative Analysis of the Cybersecurity Indices and Their Applications. Theoretical and Applied Cybersecurity, Vol. 1, No. 1. http://tacs.ipt.kpi.ua/article/view/169090

13. Kuusisto, K., Kuusisto, R. (2019). The Balanced Digitalization and Digital Security: Case of Regional Authorities. Proceedings of the 18th European Conference on Cyber Warfare and Security (Edited by Tiago Cruz and Paolo Simoes), 4.-5.07.2019. ISBN: 978-1-912764-29-7.

14. McGarry, F., Pajerski, R., Page, G., Waligora, S., Basili, V., Zelkowitz, M. (1994). Software Process Improvement in the NASA Software Engineering Laboratory. Carnegie Mellon University. https://resources.sei.cmu.edu/asset_files/TechnicalReport/1994_005_001_16334.pdf

15. MKM (2018). Küberturvalisuse strateegia 2019-2022. https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf

16. Othman, S.H., Beydoun, G., Sugumaran, V. (2014). Development and validation of a Disaster Management Model (DMM), Inf. Process. Manag., 50, No. 2, 235-271.

17. Rikk, R. (2018). National Cyber Security Index 2018. e-Governance Academy. https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf

18. Yasasin, E., Schryen, G., (2015). Requirements for IT Security Metrics – an Argumentation Theory Based Approach. 23rd European Conference on Information Systems (ECIS). Münster, 26.-29.05. 2015.

Lisa 1. Lühendite ja mõistete selgitus[46]

ACM	Association for Computing Machinery
BSA	The (Business) Software Alliance
CCMM	Cybersecurity Capacity Maturity Model
CERT	Kriitiliste arvutiintsidentide lahendamise teenistus (*Computer Emergency Response Team*)
CIRT	Arvutiintsidentide lahendamise teenistus (*Computer Incident Response Team*)
CRI 2.0	Cyber Readiness Index 2.0
CSCG	Cybersecurity Coordination Group
CSIRT	Arvutiturbeintsidentide lahendamise teenistus (*Computer Security Incident Response Team*)
ENISA	European Union Agency for Network and Information Security
ETSI	European Telecommunications Standards Institute
GCI	ITU Global Cybersecurity Index
indeks	mingi mõõdikute hulga alusel leitud agregeeritud mõõdik
ITU	International Telecommunication Union
mõõdik	Mingi väljundi kvalitatiivne või kvantitatiivne kirjeldus. Antud juhul väikseima hinnatava suuruse tähenduses.
NASA SEL SPI	NASA Software Engineering Laboratory Software Process Improvement
NCSI	National Cyber Security Index
NIST	US National Institute of Standards and Technology

[46] Küberturvalisuse põhimõisted on defineeritud dokumendis „Küberturvalisuse strateegia 2019-2022" [MKM 2018].

Lisa 2. Riikide küberturvalisuse-alaste strateegiadokumentide analüüsi kokkuvõte

2018. aasta esimesel poolaastal viis Raul Rikk oma doktoriõpingute raames läbi uuringu, mille eesmärgiks oli selgitada välja valdavad küberturvalisuse skoobimääratlused riiklikes strateegia- ja poliitikadokumentides.

Vaatluse alla võeti kõik riigid (43 riiki), kelle vastavaid ingliskeelseid dokumente õnnestus 2018. aasta alguse seisuga kätte saada. Lisaks vaadeldi olulisemaid rahvusvaheliste institutsioonide (ITU, Euroopa Liit, ISO/IEC, NIST, ETSI) asjakohaseid dokumente.

Vaadeldud riikideks olid: Afganistan, Austria, Filipiinid, Hispaania, Holland, Horvaatia, Eesti, Iirimaa, Iisrael, India, Itaalia, Jamaika, Jordaania, Katar, Keenia, Kolumbia, Küpros, LAV, Läti, Leedu, Luksemburg, Malta, Moldaavia, Montenegro, Nigeeria, Norra, Poola, Portugal, Ruanda, Saudi Araabia, Slovakkia, Sloveenia, Saksamaa, Soome, Suurbritannia, Šveits, Trinidad ja Tobago, Tšehhi, Türgi, Uganda, Ungari, USA, Uus-Meremaa.

Igast riigist käsitleti vaid kõige olulisemat alusdokumenti. Selle nimetuseks oli 33-l juhul *strateegia* (*strategy*), viiel juhul *poliitika* (*policy*) ning viiel juhul midagi muud (*programm*, *plaan*, *kontseptsioon*).

Uuringumetoodikaks oli tekstianalüüs.

Põhitulemuseks oli vaadeldud dokumentides kasutatud küberturvalisuse valdkonna terminite märksõnapilv. Need koondati 33-e klassi, millest igaüks käsitles teatud aspekti ning viidi läbi sagedusanalüüs. Kõige enam esinenud klasse iseloomustanud märksõnade loetelu on toodud käesoleva dokumendi peatükis 2 *Küberturvalisuse valdkonna määratlemisest*.

Eraldi sai analüüsitud mõiste *küberturvalisus* (*cybersecurity*, *cyber security*) definitsioone. Osutus, et 12-l juhul ei olnud mõistet „küberturvalisus“ ilmutatud kujul määratletud. Nendest kolmel juhul oli defineeritud mõiste „küberruum“ (*cyberspace*). Seitsmel juhul oli kasutatud rahvusvaheliste institutsioonide (ITU, NIST, ISO/IEC) definitsioone.

Vaadeldud dokumentide variatiivsus oli erakordselt suur, seda nii skoobi (hõlmatud aspektide arv) kui ka sügavuse (üldsõnalisus *versus* konkreetsus) poolest.

Selle analüüsi tulemused koondati tabelisse, kus iga riigi ja vaadeldud rahvusvahelise institutsiooni kohta märgiti analüüsitud dokumendi nimi, selle avaldamise aasta, põhimõiste (kübertuvalisus, küberruum) nimi, põhimõiste definitsioon (kui see puudus, siis dokumendis sätestatud tegevuse põhieesmärk) ning iga vaadeldud aspekti kohta selle käsitluse olemasolu või mitteolemasolu dokumendis.