EUROPEAN UNION AGENCY
FOR CYBERSECURITY

RIIKIDE SUUTLIKKUSE HINDAMISE RAAMISTIK

DETSEMBER 2020

ENISA

Euroopa Liidu Küberturvalisuse Amet (ENISA) on Euroopa Liidu asutus, mille eesmärk on saavutada küberturvalisuse ühtlane kõrge tase kogu Euroopas. 2004. aastal asutatud ning ELi küberturvalisuse määrusega tugevdatud Euroopa Liidu Küberturvalisuse Amet osaleb ELi küberpoliitikas, suurendab IKT-toodete, -teenuste ja -protsesside usaldusväärsust küberturvalisuse sertifitseerimiskavade abil, teeb koostööd liikmesriikide ja ELi organitega ning aitab Euroopal valmistuda tuleviku küberprobleemideks. Jagades teadmisi ning suurendades suutlikkust ja teadlikkust teeb amet koostööd peamiste sidusrühmadega, et tugevdada usaldust sidusmajanduse vastu, edendada Euroopa Liidu taristu kerksust ning tagada kokkuvõttes Euroopa ühiskonna ja kodanike digitaalne turvalisus. Lisateave: www.enisa.europa.eu.

KONTAKTANDMED

Autorite kontaktaadress: team@enisa.europa.eu.
Selle dokumendiga seotud meediapäringud: press@enisa.europa.eu.

AUTORID

Anna Sarri, Pinelopi Kyranoudi – Euroopa Liidu Küberturvalisuse Amet (ENISA)
Aude Thirriot, Federico Chiarelli, Yang Dominique-Wavestone

TÄNUAVALDUS

ENISA soovib tänada ja tunnustada kõiki eksperte, kes osalesid ja andsid väärtusliku panuse sellesse aruandesse, eelkõige järgmisi (tähestiku järjekorras).

Digitaalühiskonna arendamise keskbüroo (Ungari), Marin Ante Pivčević

Küberturbekeskus (Belgia)

Taani küberturbekeskus CFCS (Center for Cybersikkerhed), Thomas Wulff

Küberkuritegevuse vastase võitluse Euroopa keskus – EC3, Alzofra Martinez Álvaro

Küberkuritegevuse vastase võitluse Euroopa keskus – EC3, Adrian-Ionut Bobeica

Saksamaa föderaalne siseministeerium, Sascha-Alexander Lettgen

Infoturbe amet (Sloveenia Vabariik), Marjan Kavčič

Itaalia valitsus (Itaalia)

Malta IT-asutus (Malta), Katia Bonello ja Martin Camilleri

Justiits- ja avaliku julgeoleku ministeerium (Norra), Robin Bakke

Digitaalpoliitika ministeerium (Kreeka), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali ja Sotiris Vasilos

Majandus- ja kommunikatsiooniministeerium (Eesti), Anna-Liisa Pärnalaas

Riiklik küber- ja infoturbeamet (Tšehhi Vabariik), Veronika Netolická

Riikliku julgeoleku amet (Slovakkia)

Riikliku julgeoleku teenistus (Hispaania), Maria Mar Lopez Gil

NCTV, justiits- ja julgeolekuministeerium (Madalmaad)

Portugali riiklik küberjulgeolekukeskus (Portugal), Alexandre Leite ja Pedro Matos

Küberjulgeolekupoliitika osakond, keskkonna-, kliima- ja sideministeerium (Iirimaa), James Caffrey

Oxfordi Ülikool – ülemaailmne küberturbesuutlikkuse keskus, Carolin Weisser Harris

Samuti soovib ENISA tänada kõiki eksperte, kes andsid väärtusliku panuse uuringusse, kuid eelistavad jääda anonüümseks.

ÕIGUSTEAVE

Kui ei ole märgitud teisiti, kuuluvad väljaandes esitatud arvamused ja tõlgendused ENISA-le. Väljaannet ei saa käsitada ENISA või ENISA asutuste õigusmeetmena, v.a kui see on vastu võetud määruse (EL) 2019/881 kohaselt.
Väljaanne ei pruugi kajastada hetkeolukorda ning ENISA võib seda aeg-ajalt ajakohastada.

Kolmandaid isikuid on tsiteeritud, nagu asjakohane. ENISA ei vastuta käesolevas väljaandes viidatud välisallikate, sh väliste veebikohtade sisu eest.

Väljaanne on teavitava olemusega. See peab olema kättesaadav tasuta. ENISA ega ükski ENISA nimel tegutsev isik ei vastuta väljaandes sisalduva teabe võimaliku kasutamise korral.

AUTORIÕIGUSE MÄRGE

ISBN: 978-92-9204-479-4

DOI: 10.2824/307015

KATALOOGINUMBER: TP-02-21-253-ET-N

1. SISUKORD

SÕNASTIK

LÜHEND	MÄÄRATLUS
AI	Tehisintellekt
C2M2	Küberturbesuutlikkuse küpsusmudel
CCRA	Ühiskriteeriumide tunnustamise kokkulepe
CCSMM	Kogukondliku küberturbe küpsusmudel
CII	Elutähtis teabetaristu
CMM	Riikide küberturbesuutlikkuse küpsusmudel
CMMC	Küberturbe küpsustaseme sertifitseerimismudel
CPI	Kübervõimsuse indeks
CSIRT	Küberturbeintsidentide lahendamise üksused
CVD	Turbenõrkuste koordineeritud teatamine
DPA	Andmekaitseseadus
DSM	Digitaalne ühtne turg
ECCG	Euroopa küberturvalisuse sertifitseerimise rühm
ECSM	Euroopa küberturvalisuse kuu
ECSO	Euroopa Küberturvalisuse Organisatsioon
EFTA	Euroopa Vabakaubanduse Assotsiatsioon
EL	Euroopa Liit
EQF	Euroopa kvalifikatsiooniraamistik
GCI	Ülemaailmne küberturvalisuse indeks
GDPR	Isikuandmete kaitse üldmäärus
GDS	Valitsuse digiteenus
IA-CM	Avaliku sektori siseauditi suutlikkuse mudel
IKT	Info- ja kommunikatsioonitehnoloogia
ISMM	NISTi küberturberaamistiku infoturbe küpsusmudel
ITU	Rahvusvaheline Telekommunikatsiooni Liit
LEA	Õiguskaitseasutus
MS	Liikmesriik
NCSS	Riiklikud küberturbestrateegiad

NIS	Võrgu- ja infoturve
NIST	Riiklik standardi- ja tehnoloogiainstituut (USA)
NLO	Riiklikud kontaktametnikud
OES	Oluliste teenuste operaatorid
OT	Käidutehnoloogia
PET	Privaatsust soodustavad tehnoloogiad
PIMS	Privaatsusteabe haldussüsteem
PPP	Avaliku ja erasektori partnerlused
Q-C2M2	Katari küberturbesuutlikkuse küpsusmudel
R&D	Teadus- ja arendustegevus
SOG-IS MRA	Infosüsteemide turvalisuse vanemametnike rühma vastastikuse tunnustamise leping
VKEd	Väikesed ja keskmise suurusega ettevõtjad

KOMMENTEERITUD KOKKUVÕTE

Et praegused küberohud üha mitmekesistuvad ning küberründed intensiivistuvad ja sagenevad, peavad ELi liikmesriigid tõhusalt reageerima, arendades edasi ja kohandades oma riiklikke küberturbestrateegiaid. Alates sellest, kui ENISA avaldas 2012. aastal esimesed riiklike küberturbestrateegiate uuringud, on ELi liikmesriigid ja EFTA riigid palju arendanud oma strateegiaid ja neid rakendanud.

Aruandes tutvustatakse ENISA tegevust riikide suutlikkuse hindamise raamistiku (NCAF) koostamisel.

Raamistiku eesmärk on pakkuda liikmesriikidele võimalust hinnata oma küpsustaset ise, keskendudes riikliku küberturbestrateegia eesmärkide hindamisele. See aitab neil suurendada ja arendada küberturbesuutlikkust strateegilisel ja operatiivtasandil.

Vahend annab lihtsa ja esindava ülevaade liikmesriigi küberturbeküpsusest. Riikide suutlikkuse hindamise raamistik on vahend, mis aitab liikmesriikidel:

- anda kasulikku teavet pikaajalise strateegia väljatöötamiseks (nt head tavad, suunised);
- tuvastada riiklikus küberturbestrateegias puuduvad elemendid;
- suurendada veelgi küberturbesuutlikkust;
- toetada poliitiliste meetmete vastutust;
- suurendada üldsuse ja rahvusvaheliste partnerite usaldusväärsust;
- toetada teavitustegevust ja edendada mainet läbipaistva organisatsioonina;
- eeldada tulevikuprobleeme;
- tuvastada saadud kogemusi ja parimaid tavasid;
- luua arutelude toetamiseks küberturbesuutlikkuse lähtealus kogu ELis;
- hinnata riikide küberturbesuutlikkust.

Raamistik koostati ENISA valdkonnaekspertide ning 19 liikmes- ja EFTA riigi esindajate toetusel[1]. Aruande sihtrühm on poliitikakujundajad, eksperdid ja riigiametnikud, kes vastutavad riikliku küberturbestrateegia ning laiemal tasandil ka küberturbesuutlikkuse kavandamise, rakendamise ja hindamise eest või on nendega seotud.

[1] Küsitleti järgmiste liikmesriikide ja EFTA riikide esindajaid: Belgia, Eesti, Hispaania, Horvaatia, Iirimaa, Itaalia, Kreeka, Liechtenstein, Madalmaad, Malta, Norra, Portugal, Rootsi, Saksamaa, Slovakkia, Sloveenia, Taani, Tšehhi Vabariik, Ungari.

Riikide suutlikkuse hindamise raamistikus on 17 strateegilist eesmärki ja see jaguneb 4 peamiseks teemade klastriks.

- 1. klaster: küberturbe juhtimine ja standardid
  1. Riiklike kübervaldkonna hädaolukorra lahendamise plaani koostamine
  2. Põhiliste turbemeetmete kehtestamine
  3. Digitaalse identiteedi tagamine ja usalduse suurendamine digitaalsete avalike teenuste vastu

- 2. klaster: suutlikkuse suurendamine ja teadlikkus
  4. Küberturbeõppuste korraldamine
  5. Intsidentidele reageerimise suutlikkuse loomine
  6. Kasutajate teadlikkuse suurendamine
  7. Koolitus- ja õppekavade tugevdamine
  8. Teadus- ja arendustegevuse edendamine
  9. Turbemeetmetesse investeerimise stiimulite pakkumine erasektorile
  10. Tarneahela küberturbe täiustamine

- 3. klaster: õiguslikud ja reguleerivad raamistikud
  11. Elutähtsa teabetaristu, oluliste teenuste operaatorite ja digitaalse teenuse osutajate kaitse
  12. Küberkuritegevuse käsitlemine
  13. Intsidentidest teatamise mehhanismide loomine
  14. Privaatsuse ja andmekaitse tugevdamine

- 4. klaster: koostöö
  15. Avaliku ja erasektori partnerluse loomine
  16. Avalik-õiguslike asutuste koostöö institutsionaliseerimine
  17. Osalemine rahvusvahelises koostöös

1. SISSEJUHATUS

2016. aasta juulis avaldatud küberturvalisuse direktiivis nõutakse, et ELi liikmesriigid võtaksid vastu riikliku võrgu- ja infosüsteemide turvalisuse strateegia (riikliku küberturbestrateegia), nagu on sätestatud artiklites 1 ja 7. Sellises kontekstis on riiklik küberturbestrateegia määratletud kui raamistik, millega kehtestatakse strateegilised põhimõtted, suunised, strateegilised eesmärgid, prioriteedid, asjakohased poliitikad ja reguleerivad meetmed. Riikliku küberturbestrateegia kavandatav eesmärk on saavutada ja säilitada võrgu ja süsteemide turvalisuse kõrge tase, mis võimaldab liikmesriikidel leevendada võimalikke ohte. Lisaks võib riiklik küberturbestrateegia soodustada ka tööstuse, majanduse ja ühiskonna arengut.

ELi küberturvalisuse määruses on sätestatud, et ENISA edendab parimate tavade levitamist riikliku küberturvalisuse strateegia määratlemisel ja rakendamisel, toetades liikmesriike küberturvalisuse direktiivi vastuvõtmisel ning kogudes väärtuslikku tagasisidet nende kogemuste kohta. Selleks on ENISA loonud mitu vahendit, et aidata liikmesriikidel arendada, rakendada ja hinnata oma riiklikke küberturbestrateegiaid.

Oma volituste raames on ENISA eesmärk luua riikide suutlikkuse enesehindamise raamistik, et mõõta eri riikide küberturbestrateegiate küpsustaset. Käesoleva aruande eesmärk on tutvustada enesehindamise raamistiku koostamisel tehtud uuringut.

1.1 UURINGU KÄSITLUSALA JA EESMÄRGID

Uuringu põhieesmärk on luua riikide suutlikkuse enesehindamise raamistik (NCAF), et mõõta liikmesriikide küberturbesuutlikkuse taset. Täpsemalt peaks raamistik võimaldama liikmesriikidel teha järgmist:

- hinnata riiklikku küberturbesuutlikkust;
- suurendada teadlikkust riigi küpsustasemest;
- tuvastada täiustatavad valdkonnad;
- suurendada küberturbesuutlikkust.

See raamistik peaks aitama liikmesriikidel ja eelkõige riiklikel poliitikakujundajatel korraldada enesehindamismenetluse, mille eesmärk on täiustada riikide küberturbesuutlikkust.

1.2 METOODIKA

Riikide suutlikkuse enesehindamise raamistiku arendamise metoodika aluseks on neli põhietappi.

1. **Dokumentide analüüs:** esiteks vaadati põhjalikult läbi olemasolev kirjandus, et koguda parimad tavad, kuidas arendada riikliku küberturbestrateegia rakendamise küpsustasemete hindamise raamistikku. Dokumentide analüüs keskendub küberturbesuutlikkuse suurendamise ja strateegia määratlemise asjakohaste dokumentide süstemaatilisele analüüsile, olemasolevatele liikmesriikide riiklikele küberturbestrateegiatele ja olemasolevate küberturbe küpsusmudelite võrdlemisele. Olemasolevate küpsusmudelite võrdlusanalüüsiks kasutati käesoleva uuringu jaoks arendatud analüüsiraamistikku. Analüüsiraamistik tugineb Beckeri küpsusmudelite

väljatöötamise metoodikale[2], millega luuakse üldine ja kooskõlastatud kord küpsusmudelite kavandamiseks ning sätestatakse selged nõuded küpsusmudelite arendamiseks. Analüüsiraamistikku kohandati veelgi, et see vastaks käesoleva uuringu vajadustele.

2. **Ekspertide ja sidusrühmade seisukohtade kogumine:** dokumentide analüüsil kogutud andmete ja analüüsi esialgsete järelduste põhjal tuvastati siin etapis eksperdid, kellel on kogemusi riikliku küberturbestrateegia või küpsusmudelite väljatöötamisel ja rakendamisel, ning kutsuti nad intervjuule. ENISA võttis ühendust oma riiklike küberturbestrateegiate eksperdirühma ja riiklike kontaktametnikega, et leida iga liikmesriigi asjaomased eksperdid. Lisaks küsitleti mõnda küpsusmudelite arendamisel osalenud eksperti. Kokku peeti 22 intervjuud, neist 19 liikmesriikide (ja EFTA riikide) küberturbeasutuste esindajatega.
3. **Kokkuvõtete tegemise sisendi analüüs:** dokumentide analüüsil ja küsitlemisel kogutud andmeid analüüsiti, et tuvastada parimad tavad riiklike küberturbestrateegiate hindamise enesehindamise raamistiku arendamisel, et mõista liikmesriikide vajadusi ja määrata, mis andmete kogumine eri Euroopa riikides on teostatav[3]. See analüüs võimaldas peenhäälestada eelmistes etappides arendatud esialgset mudelit ning täpsustada mudelis sisalduvaid näitajaid, küpsustasemeid ja nende mõõtmeid.
4. **Mudeli lõplik vormistamine:** seejärel vaatasid ENISA valdkonnaeksperdid läbi riikide suutlikkuse enesehindamise raamistiku ajakohastatud versiooni, mille eksperdid kinnitasid 2020. aasta oktoobris seminaril, mis toimus enne selle avaldamist.

1.3 SIHTRÜHM

Aruande sihtrühm on poliitikakujundajad, eksperdid ja riigiametnikud, kes vastutavad riikliku küberturbestrateegia ning laiemal tasandil ka kübeturbesuutlikkuse arendamise, rakendamise ja hindamise eest või on nendega seotud. Lisaks võivad selles dokumendis esitatud tulemused olla väärtuslikud küberturbepoliitika ekspertidele ja teadlastele riigi või Euroopa tasandil.

[2] J. Becker, R. Knackstedt, and J. Pöppelbuß, “Developing Maturity Models for IT Management: A Procedure Model and its Application,” Business & Information Systems Engineering, vol. 1, no. 3, pp. 213–222, Jun. 2009.
[3] Selle uuringu raames tähendab käesoleva aruande väljend „Euroopa riigid“ ELi 27 liikmesriiki.

2. TAUST

2.1 VARASEM TEGEVUS RIIKLIKE KÜBERTURBESTRATEEGIATE OLELUSTSÜKLIGA

Nagu on märgitud ELi küberturvalisuse määruses, on ENISA üks peamisi eesmärke toetada liikmesriike riiklike võrgu- ja infosüsteemide turbestrateegiate väljatöötamisel, edendada nende strateegiate levitamist ja jälgida nende rakendamist. ENISA on oma volituste raames koostanud sel teemal mitu dokumenti, et edendada heade tavade jagamist ja toetada riiklike küberturbestrateegiate rakendamist kogu ELis.

- Riikliku küberturbestrateegia väljatöötamise ja rakendamise etapi praktiline juhend[4], 2012
- Küberruumis turvalisuse tugevdamiseks tehtava riikide tegevuse suuna määramine[5], 2012
- Esimene ENISA raamistik liikmesriikide riiklike küberturbestrateegiate hindamiseks[6], 2014.
- Veebipõhine interaktiivne riiklike küberturbestrateegiate kaart[7], 2014
- Riiklike küberturbestrateegiate heade tavade juhend[8], 2016
- Riiklike küberturbestrateegiate hindamisvahend[9], 2018
- Riiklike küberturbestrateegiate innovatsiooni head tavad[10], 2019

A LISA. annab lühiülevaate ENISA peamistest väljaannetest sel teemal.

Eespool nimetatud juhendeid ja dokumente analüüsiti dokumentide analüüsi etapi osana. Eelkõige on riikide suutlikkuse hindamise raamistiku aluseks riiklike küberturbestrateegiate hindamisvahend.[11] Riikide suutlikkuse hindamise raamistik tugineb eesmärkidele, mida käsitletakse riiklike küberturbestrateegiate veebipõhises hindamisvahendis

[4] NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] An evaluation framework for NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] Riiklike küberturbestrateegiate interaktiivne kaart (ENISA, 2014, ajakohastatud 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Dokumendiga ajakohastatakse 2012. aasta juhendit: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] Riiklike küberturbestrateegiate hindamisvahend (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
[11] Riiklike küberturbestrateegiate hindamisvahend (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

2.2 EUROOPA RIIKLIKES KÜBERTURBESTRATEEGIATES TUVASTATUD ÜHISED EESMÄRGID

Liikmesriikide erinevused raskendavad ühiste tegevuste või tegevuskavade tuvastamist erinevates riiklikes kontekstides, õigusraamistikes ja poliitilistes tegevuskavades. Samas on liikmesriikide riiklikes küberturbestrateegiates sageli strateegilised eesmärgid, mis on seotud samade teemadega. Seega tuvastati ENISA varasema tegevuse ja liikmesriikide riiklike küberturbestrateegiate analüüsi põhjal 22 strateegilist eesmärki. Neist 15 oli tuvastatud juba ENISA varasema tegevusega, 2 lisati käesoleva uuringuga ja 5 eesmärki tuvastati tuleviku jaoks.

2.2.1 Liikmesriikide ühised strateegilised eesmärgid

Tuginedes ENISA varasemale tegevusele, täpsemalt riiklike küberturbestrateegiate hindamisvahendile[12], on järgmises tabelis loetletud eespool nimetatud 15 strateegilist eesmärki, mida tavaliselt käsitlevad liikmesriikide küberturbestrateegiad. Eesmärgid kirjeldavad teema üldist käsitlust riigis. Allpool kirjeldatud eesmärkide lisateave on ENISA riiklike küberturbestrateegiate heade tavade aruandes[13].

Tabel 1. Liikmesriikide ühised strateegilised eesmärgid, mida käsitletakse riiklikes küberturbestrateegiates

Nr	Riikliku küberturbe strateegilised eesmärgid	Eesmärgid
1	**Riiklike kübervaldkonna hädaolukorra lahendamise plaanide koostamine**	▶ Esitada ja selgitada kriteeriumid, millega määratleda olukorda kriisina ▶ Määratleda kriisiga toimetuleku peamised protsessid ja meetmed ▶ Määratleda selgelt eri sidusrühmade rollid ja kohustused küberkriisi ajal ▶ Esitada ja selgitada kriteeriumid, millal kriis on läbi ja/või kes on pädev seda teatama
2	**Põhiliste turbemeetmete kehtestamine**	▶ Ühtlustada eri tavad, mida järgivad avaliku ja erasektori organisatsioonid ▶ Luua pädevate ametiasutuste ja organisatsioonide ühiskeel ning avatud turvalised sidekanalid ▶ Võimaldada eri sidusrühmadel kontrollida ja võrrelda oma küberturbesuutlikkust ▶ Jagada küberturbe heade tavade teavet igas majandussektoris ▶ Aidata sidusrühmadel prioriseerida oma investeeringuid turbesse
3	**Küberturbeõppuste korraldamine**	▶ Tuvastada, mida on vaja testida (kavad ja protsessid, inimesed, taristu, reageerimisvõime, koostöövõime, teabevahetus jt) ▶ Luua selgete volitustega riiklik küberõppuste kavandamise üksus ▶ Lõimida küberturbeõppused riikliku küberturbestrateegia või riikliku kübervaldkonna hädaolukorra lahendamise kava olelustsüklisse
4	**Intsidentidele reageerimise suutlikkuse loomine**	▶ Mandaat – see on seotud volituste, rollide ja kohustustega, mille peab üksusele määrama valitsus ▶ Teenuste portfell – see hõlmab teenuseid, mida üksus osutab oma haldusalas või kasutab üksusesiseseks toimimiseks ▶ Tegevussuutlikkus – see käsitleb tehnilisi ja tegevusnõudeid, mida üksus peab järgima ▶ Koostöösuutlikkus – see hõlmab nõudeid teabe jagamise kohta teiste üksustega, keda eelmised kolm kategooriat ei hõlma,

[12] Riiklike küberturbestrateegiate hindamisvahend (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[13] Dokumendiga ajakohastatakse 2012. aasta juhendit: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

Nr	Riikliku küberturbe strateegilised eesmärgid	Eesmärgid
		nt poliitikakujundajad, kaitsevägi, reguleerivad asutused, (elutähtsa teabetaristu) operaatorid, õiguskaitseasutused.
5	Kasutajate teadlikkuse suurendamine	▶ Tuvastada küber- või infoturbega seotud teadmiste lüngad ▶ Täita lüngad teadlikkuse tõstmise või teadmistebaasi arendamise/tugevdamise kaudu
6	Koolitus- ja õppekavade tugevdamine	▶ Suurendada olemasoleva infoturbega seotud tööjõu tegevussuutlikkust ▶ Julgustada õppureid liituma ja seejärel valmistada neid ette küberturvalisuse valdkonda sisenemiseks ▶ Edendada ja soodustada suhteid infoturbe akadeemiliste keskkondade ja infoturbesektori vahel ▶ Viia küberturbekoolitus kooskõlla ärivajadustega
7	Teadus- ja arendustegevuse edendamine	▶ Tuvastada haavatavuste tegelikud põhjused, mitte üksnes parandada nende tagajärgi ▶ Tuua kokku eri valdkondade teadlased, et leida lahendusi mitmemõõtmelistele ja keerukatele probleemidele, näiteks füüsilistele küberohtudele ▶ Ühendada valdkonna vajadused ja teadusuuringute tulemused, toetades sellega üleminekut teoorialt praktikale ▶ Leida viisid, kuidas olemasolevaid kübertaristuid toetavate toodete ja teenuste küberturbetaset peale säilitamise ka tõsta
8	Turbemeetmetesse investeerimise stiimulite pakkumine erasektorile	▶ Tuvastada võimalikud stiimulid, mis suunaksid eraettevõtteid investeerima turbemeetmetesse ▶ Pakkuda ettevõtetele stiimuleid, mis julgustavad investeerima turbemeetmetesse
9	Elutähtsa teabetaristu, oluliste teenuste operaatorite ja digitaalse teenuse osutajate kaitse	▶ Tuvastada elutähtsad teabetaristud ▶ Tuvastada ja maandada elutähtsa teabetaristu asjakohased riskid
10	Küberkuritegevuse käsitlemine	▶ Luua õigusakte küberkuritegevuse valdkonnas ▶ Suurendada õiguskaitseasutuste tõhusust
11	Intsidentidest teatamise mehhanismide loomine	▶ Koguda teadmisi üldise ohukeskkonna kohta ▶ Hinnata intsidentide mõju (nt turberikkumised, võrgurikked, teenuse katkemine) ▶ Koguda teadmisi olemasolevate ja uute haavatavuste ja rünnakuliikide kohta ▶ Ajakohastada vastavalt turbemeetmeid ▶ Rakendada küberturvalisuse direktiivi sätteid intsidentidest teatamise kohta
12	Privaatsuse ja andmekaitse tugevdamine	▶ Toetada privaatsuse ja andmekaitsega seotud põhiõiguste tugevdamist
13	Avaliku ja erasektori partnerluse loomine	▶ Heidutamine (ründajate heidutamiseks) ▶ Kaitse (uute julgeolekuohtude uurimine) ▶ Tuvastamine (teabe jagamine, et käsitleda uusi ohte) ▶ Reageerimine (intsidendi esialgse mõjuga toimetuleku suutlikkuse osutamine) ▶ Taastumine (intsidendi lõpliku mõju parandamise suutlikkuse osutamine)
14	Avalik-õiguslike asutuste koostöö institutsionaliseerimine	▶ Suurendada koostööd avaliku sektori asutuste vahel, kellel on küberturbega seotud kohustused ja pädevus ▶ Vältida avalik-õiguslike asutuste pädevuste ja ressursside kattumist ▶ Täiustada ja institutsionaliseerida avaliku sektori asutuste koostööd küberjulgeoleku eri valdkondades
15	Osalemine rahvusvahelises koostöös (mitte ainult ELi liikmesriikidega)	▶ Saada kasu ühise teadmistebaasi loomisest ELi liikmesriikide vahel ▶ Luua sünergiad riiklike küberturbeasutuste vahel ▶ Võimaldada ja suurendada võitlust piiriülese kuritegevuse vastu

2.2.2 Täiendavad strateegilised eesmärgid

Dokumentide analüüsi ja ENISA korraldatud küsitluste alusel tuvastati täiendavad strateegilised eesmärgid. Liikmesriigid käsitlevad neid teemasid üha enam oma riiklikes küberturbestrateegiates või koostavad nende alusel tegevuskavu. Esitatud on ka liikmesriikide rakendatavate meetmete näited. Kui näide pärineb avalikult kättesaadavast allikast, lisatakse viide. Kui näited põhinevad konfidentsiaalsetel intervjuudel ELi liikmesriikide ametnikega, viiteid ei lisata.

Tuvastati järgmised täiendavad strateegilised eesmärgid:

- tarneahela küberturbe täiustamine;
- digitaalse identiteedi tagamine ja usalduse suurendamine digitaalsete avalike teenuste vastu.

Tarneahela küberturbe täiustamine

Väikesed ja keskmise suurusega ettevõtjad (VKE) on Euroopa majanduse alus. Nad moodustavad 99% kõigist ELi ettevõtetest[14]. 2015. aastal olid VKEd loonud hinnanguliselt ligikaudu 85% uutest töökohtadest ja andsid kaks kolmandikku erasektori kogutööhõivest ELis. Et VKEd osutavad teenuseid suurtele ettevõtetele ja teevad üha rohkem koostööd avaliku halduse asutustega[15], tuleb märkida, et vastastikku seotud tänapäeva kontekstis on VKEd küberrünnete seisukohast nõrk lüli. VKEd on küberrünnete suhtes kõige haavatavamad, kuid sageli ei saa nad endale lubada piisavat investeerimist küberturbesse[16]. Tarneahela küberturbe täiustamisel tuleb seega keskenduda VKEdele.

Lisaks sellisele süsteemsele lähenemisviisile võivad liikmesriigid keskenduda ka konkreetsete oluliseks peetavate IKT-teenuste ja -toodete küberturbele: elutähtsas teabetaristus kasutatav IKT-tehnoloogia, sidesektoris jõustatavad turbemehhanismid (kontroll internetiteenuse osutaja tasandil), eiDASe määruses määratletud usaldusteenused ja pilveteenuse osutajad. Näiteks kohustus Poola oma 2019.–2024. aasta riiklikus küberturbestrateegias[17] arendama riikliku küberturbe hindamise ja sertifitseerimise süsteemi kui tarneahela kvaliteedi tagamise mehhanismi. See sertifitseerimissüsteem viiakse kooskõlla IKT digitaalsete toodete, teenuste ja protsesside sertifitseerimise ELi raamistikuga, mis on kehtestatud ELi küberturvalisuse määrusega (2019/881).

Seega on tarneahela küberturbe täiustamine äärmiselt oluline. Seda on võimalik saavutada, kehtestades muu hulgas tugevad poliitikad VKEde toetamiseks, andes suuniseid küberturbenõuete kohta avaliku halduse hankemenetlustes, edendades koostööd erasektoris, luues avaliku ja erasektori partnerlusi, edendades turbenõrkustest teatamise koordineeritud mehhanisme[18], luues toodete sertifitseerimise kava, hõlmates VKEde digitaalsetes algatustes küberturvalisuse komponente ja rahastades oskuste arendamist.

[14] https://ec.europa.eu/growth/smes_et
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
[16] https://www.eesc.europa.eu/et/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study
[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Digitaalse identiteedi tagamine ja usalduse suurendamine digitaalsete avalike teenuste vastu

2020. aasta veebruaris esitas Euroopa Komisjon dokumendis „Euroopa digituleviku kujundamine“[19] nägemuse ELi digiüleminekust, et pakkuda kaasavaid tehnoloogiaid, mis toimivad inimeste heaks ja austavad ELi põhiväärtusi. Dokumendis rõhutatakse eelkõige avaliku halduse asutuste digiülemineku olulisust kogu Euroopas. Sellest tulenevalt on ülimalt tähtis suurendada usaldust valitsuse vastu seoses digitaalse identiteediga ja avalike teenuste vastu. See on veelgi olulisem, sest avaliku sektori tehingud ja andmevahetus on sageli tundlikku laadi.

Mitu riiki on väljendanud kavatsust käsitleda teemat oma riiklikus küberturbestrateegias, näiteks Taani, Eesti, Prantsusmaa, Luksemburg, Malta, Hispaania, Madalmaad ja Ühendkuningriik. Mõni neist on väljendanud ka seisukohta, et seda strateegilist eesmärki võiks käsitleda laiema kava osana.

- Eesti on sidunud sellega seotud tegevuskava „Elektroonilise identiteedi turvalisus ja elektroonilise isikutuvastamise võime“ laiema 2020. aasta digitaalarengu tegevuskavaga Eestis.
- Prantsusmaa riiklikus küberturbestrateegias märgitakse, et digitaaltehnoloogia eest vastutav riigisekretär jälgib tegevuskava koostamist, et „kaitsta Prantsusmaa kodanike digitaalelu, privaatsust ja isikuandmeid“.
- Madalmaade riiklikus küberturbestrateegias märgitakse, et küberturvet avaliku halduse asutustes ning seoses kodanikele ja ettevõtjatele pakutavate avalike teenustega käsitletakse üksikasjalikumalt laiemas digivalitsuse tegevuskavas.
- Et Ühendkuningriigi valitsus jätkab rohkemate oma teenuste veebipõhiseks muutmist, on valitsuse digitaalteenistus (*Government Digital Service*, GDS) määratud Ühendkuningriigi riikliku küberturbekeskuse (*National Cybersecurity Centre*, NCSC) toel tagama, et kõik valitsuse loodud või hangitud uued digitaalteenused oleksid vaikimisi turvalised.

2.2.3 Muud kaalutletud strateegilised eesmärgid

Dokumentide analüüsimisel ja ENISA peetud küsitluste osana analüüsiti ka muid strateegilisi eesmärke. Otsustati siiski, et neid eesmärke ei kasutata enesehindamise raamistikus. C LISA. Muud uuritud eesmärgid

loetleb iga sellise eesmärgi määratluse, mida võib rakendada tulevastes aruteludes riikliku küberturbestrateegia võimalikuks täiustamiseks.

Tulevikukaalutlustena analüüsiti järgmisi strateegilisi eesmärke.

- Valdkonnaomaste küberturbestrateegiate arendamine
- Väärinfo levitamise kampaaniate vastane tegevus
- Turvalised tipptasemel tehnoloogiad (5G, tehisintellekt, kvantarvutus jt)
- Andmesuveräänsuse tagamine
- Küberkindlustusvaldkonna arendamise stiimulite pakkumine

[19] Euroopa digituleviku kujundamine, COM(2020) 67 final: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52020DC0067&from=et

2.3 VÕRDLUSUURINGU PÕHIJÄRELDUSED

Olemasolevate küberturbe küpsusmudelite dokumendianalüüsi eesmärk oli koguda teavet ja tõendeid, et toetada riikide suutlikkuse enesehindamise raamistiku kavandamist riikliku küberturbestrateegia raames. Sellega seoses tehti olemasolevate mudelite ulatuslik kirjandusülevaade, et täiendada küberturbe küpsusmudelite esialgse analüüsi tulemusi ja olemasolevaid riiklikke küberturbestrateegiaid, mida on käsitletud peatükkides 2.1 ja 2.2. See süstemaatiline ülevaade toetab hindamisraamistiku küpsustasemete valimist ja põhjendamist ning eri mõõtmete ja näitajate määratlemist.

Küpsusmudelite süstemaatilise ülevaate raames kaalutleti ja analüüsiti põhiomaduste alusel 10 mudelit. Käesolevas uuringus läbi vaadatud mudelite põhiomaduste kokkuvõtlik ülevaade on tabelis Tabel 2. Analüüsitud küpsusmudelite ülevaade ja üksikasjalik analüüs on lisas A LISA..

Tabel 2. Analüüsitud küpsusmudelite ülevaade

Mudeli nimetus	Küpsustasemete arv	Atribuutide arv	Hindamismeetod	Tulemuste esitus
Riikide küberturbesuutlikkuse küpsusmudel (CMM)	5	5 põhimõõdet	Koostöö kohaliku organisatsiooniga mudeli peenhäälestamiseks enne selle kohaldamist riigi kontekstis	5-osaline radiaaldiagramm
Küberturbesuutlikkuse küpsusmudel (C2M2)	4	10 põhivaldkonda	Enesehindamise metoodika ja vahendid	Sektordiagrammid ega tulemuskaart
Elutähtsa taristu küberturvalisuse täiustamise raamistik	– (4 astet)	5 põhifunktsioni	Enesehindamine	–
Katari küberturbesuutlikkuse küpsusmudel (Q-C2M2)	5	5 põhivaldkonda	–	–
Küberturbe küpsustaseme sertifitseerimismudel (CMMC)	5	17 põhivaldkonda	Kolmandast isikust audiitorite hinnang	–
Kogukondliku küberturbe küpsusmudel (CCSMM)	5	6 põhimõõdet	Hindamine kogukondades riiklike ja föderaalsete õiguskaitseasutuste osalusel	–
NISTi küberturvalisuse raamistiku infoturbe küpsusmudel (ISMM)	5	23 hinnatavat valdkonda	–	–
Avaliku sektori siseauditi suutlikkuse mudel (IA-CM)	5	6 elementi	Enesehindamine	–
Ülemaailmne küberturvalisuse indeks (GCI)	–	5 sammast	Enesehindamine	Paremusjärjestus
Kübervõimsuse indeks (CPI)	–	4 kategooriat	Organisatsiooni Economist Intelligence Unit võrdlusuuring	Paremusjärjestus

See süstemaatiline ülevaade võimaldas teha järeldusi olemasolevates mudelites sisalduvate parimate tavade kohta, et toetada praeguse küpsusmudeli kontseptuaalse raamistiku väljatöötamist. Eelkõige toetas võrdlusuuring küpsustasemete määratlemisel, mõõtmeklastrite loomisel ja näitajate valimisel ning mudeli tulemuste asjakohase visualiseerimismetoodika arendamisel. Kõigi nende elementide kõige asjakohasemad tulemused on tabelis Tabel 3.

Tabel 3. Võrdlusuuringu põhijäreldused

Omadus	Põhijäreldus
Küpsustasemed	▶ Küberturbesuutlikkuse hindamisraamistike viietasandiline küpsusskaala on üldiselt aktsepteeritud ja suudab pakkuda detailseid hindamistulemusi (iga mudeli küpsustasemete määratluste üksikasjalik ülevaade: vt Tabel 6 Küpsustasemete võrdlus). ▶ Kõigi mudelite kohta on iga küpsustaseme kõrgetasemeline määratlus, mida seejärel kohandatakse mõõtmete või mõõtmete klastritega. ▶ Küberturbesuutlikkuse küpsuse mõõtmisel hinnatakse tavaliselt kaht põhiaspekti: strateegiate küpsus ja strateegiate rakendamiseks kehtestatud protsesside küpsus.
Atribuudid	▶ Olemasolevate küpsusmudelite atribuutide võrdlusanalüüsil on tulemused heterogeensed ja atribuute on mudeli kohta keskmiselt 4–5. ▶ Ligikaudu 4 või 5 atribuudil põhinev mudel pakub riikidele sobival tasemel andmete detailsust, rühmitades asjakohased mõõtmed ja tagades tulemuste loetavuse (iga mudeli atribuutide kirjeldus: vt Tabel 7. Atribuutide/**mõõtmete võrdlus**). ▶ Põhiprintsiip, mida kõik mudelid klastrite määratlemisel kasutavad, põhineb igasse klastrisse rühmitatud elementide kooskõlal.
Hindamismeetod	▶ Hindamismeetod oleneb analüüsitud mudelist. ▶ Kõige tavalisem hindamismeetod põhineb enesehindamisel.
Tulemuste esitus	▶ Oluline on esitada tulemused eri detailsusega. ▶ Visualiseerimismeetodid peaksid olema iseenesest mõistetavad ja kergesti loetavad.

Kontseptuaalne mudel koostati küpsusmudelite võrdlusanalüüsi ja ENISA varasema tegevuse põhjal. Samuti otsustati kasutada *ENISA interaktiivset veebipõhist vahendit*, et töötada välja iga atribuudi jaoks kasutatavad küpsusnäitajad.

2.4 RIIKLIKU KÜBERTURBESTRATEEGIA HINDAMISE PROBLEEMID

Liikmesriigid kohtavad küberturbesuutlikkuse suurendamisel paljusid probleeme, täpsemalt tagamisel, et nende suutlikkus oleks kooskõlas uusima arenguga. Allpool on uuringus liikmesriikide tuvastatud ja nendega arutatud probleemide kokkuvõte.

- **Koordineerimisel ja koostöö raskused:** küberturbetegevuse koordineerimine riigi tasandil, et tagada tõhus reageerimine küberturbeprobleemidele, võib olla keerukas, sest osaleb palju sidusrühmi.
- **Puuduvad hindamise tegemise vahendid:** sõltuvalt kohalikust kontekstist ja küberturbe riiklikust juhtimisstruktuurist võib riikliku küberturbestrateegia ja selle eesmärkide hindamine kesta üle 15 inimtööpäeva.
- **Vähene toetus küberturbesuutlikkuse arendamisele:** mõni liikmesriik märkis, et eelarve põhjendamiseks ja küberturbesuutlikkuse arendamise toetuse saamiseks peavad nad kõigepealt korraldama hindamisetapi, et tuvastada lüngad ja piirangud.
- **Raskused edu ja muutuste seostamisel strateegiaga:** ohud muutuvad pidevalt ja tehnika areneb, seega tuleb tegevuskavu pidevalt kohandada. Samas on riikliku küberturbestrateegia hindamine ja muudatuste seostamine strateegiaga keerukas. See omakorda raskendab riikliku küberturbestrateegia piirangute ja puuduste tuvastamist.
- **Raskused riikliku küberturbestrateegia tõhususe mõõtmisel:** eri valdkondade, näiteks edenemise, rakendamise, küpsuse ja tõhususe mõõtmiseks saab koguda tulemusi. Kuigi edenemise ja rakendamise mõõtmine on tõhususe mõõtmisega võrreldes suhteliselt lihtne, on viimane riikliku küberturbestrateegia tulemuste ja mõju hindamisel otstarbekam. ENISA korraldatud küsitluste põhjal märkis palju liikmesriike,

et riikliku küberturbestrateegia tõhususe kvantitatiivne mõõtmine on oluline, kuid samas ka väga keerukas, mõnel juhul üsna võimatu.

- **Raskused ühise raamistiku vastuvõtmisel:** ELi liikmesriigid tegutsevad poliitika, organisatsioonide, kultuuri, ühiskonna struktuuri ja riikliku küberturbestrateegia küpsuse poolest eri kontekstides. Mõni uuringu raames küsitletud liikmesriik märkis, et kõigile sobiva ainsa enesehindamise raamistiku põhjendamine ja kasutamine võib olla keerukas.

2.5 RIIKIDE SUUTLIKKUSE HINDAMISE EELISED

Alates 2017. aastast on kõigil ELi liikmesriikidel olemas küberturbestrateegia[20]. Kuigi areng on positiivne, on samuti oluline, et liikmesriigid saaksid neid riiklikke küberturbestrateegiaid nõuetekohaselt hinnata, andmaks strateegilisele planeerimisele ja rakendamisele lisaväärtust.

Üks riikide suutlikkuse hindamise raamistiku eesmärke on hinnata küberturbesuutlikkust riiklikes küberturbestrateegiates sätestatud prioriteetide alusel. Põhimõtteliselt hinnatakse raamistikus liikmesriikide küberturbesuutlikkuse küpsust riikliku küberturbestrateegia eesmärkidega määratletud valdkondades. Seega toetavad raamistiku rakendamisel saadud tulemused liikmesriikide poliitikakujundajaid riikliku küberturbestrateegia määratlemisel, andes neile ülevaate olukorrast riigis[21]. Riikide suutlikkuse hindamise raamistiku lõppeesmärk on aidata liikmesriikidel tuvastada täiustatavad valdkonnad ja suurendada suutlikkust.

Raamistiku eesmärk on võimaldada liikmesriikidel teha oma küpsustaseme enesehindamine, keskendudes riikliku küberturbestrateegia eesmärkidele, mis aitavad suurendada ja arendada küberturbesuutlikkust strateegilisel ja operatiivtasandil.

Tuginedes praktilisemale lähenemisviisile, mille aluseks on ENISA intervjuud mitme küberturbeasutusega liikmesriikides, tuvastati riikide suutlikkuse raamistiku järgmised eelised:

- anda kasulikku teavet pikaajalise strateegia väljatöötamiseks (nt head tavad, suunised);
- tuvastada riiklikus küberturbestrateegias puuduvad elemendid;
- suurendada veelgi küberturbesuutlikkust;
- toetada poliitiliste meetmete vastutust;
- suurendada üldsuse ja rahvusvaheliste partnerite usaldusväärsust;
- toetada teavitustegevust ja edendada mainet läbipaistva organisatsioonina;
- eeldada tulevikuprobleeme;
- tuvastada saadud kogemusi ja parimaid tavasid;
- luua arutelude toetamiseks küberturbesuutlikkuse lähtealus kogu ELis;
- hinnata riikide küberturbesuutlikkust.

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[21] Weiss, C.H. (1999). The interface between evaluation and public policy. Evaluation, 5(4), 468-486.

3. RIIKIDE SUUTLIKKUSE HINDAMISE RAAMISTIKU METOODIKA

3.1 ÜLDEESMÄRK

Riikide suutlikkuse hindamise raamistiku **põhieesmärk** on mõõta **liikmesriikide** küberturbesuutlikkuse küpsustaset, et aidata riikidel hinnata oma riiklikku küberturbesuutlikkust, suurendada teadlikkust riigi küpsustasemest, tuvastada täiustamist vajavad valdkonnad ja suurendada küberturbesuutlikkust.

3.2 KÜPSUSTASEMED

Raamistiku aluseks on **viis küpsustaset**, mis määratlevad etapid, mida liikmesriigid läbivad küberturbesuutlikkuse suurendamisel riikliku küberturbestrateegia iga eesmärgiga hõlmatud valdkonnas. Tasemed väljendavad üha suuremat küpsust alates esialgsest **1. tasemest**, kus liikmesriikidel ei ole selgelt määratletud lähenemisviisi küberturbesuutlikkuse suurendamiseks riikliku küberturbestrateegia eesmärkidega hõlmatud valdkondades, ja lõpetades **5. tasemega**, kus küberturbesuutlikkuse suurendamise strateegia on dünaamiline ja kohandub keskkonna arenguga. Järgmises tabelis (Tabel 4) on küpsustasemete skaala ja iga küpsustaseme kirjeldus.

Tabel 4. ENISA riikide suutlikkuse hindamise raamistiku viietasandiline küpsusskaala

1. TASE – ESIALGNE/AJUTINE	2. TASE – VARAJANE MÄÄRATLEMINE	3. TASE – KEHTESTAMINE	4. TASE – OPTIMEERIMINE	5. TASE – KOHANDATAVUS
Liikmesriigil puudub selgelt määratletud lähenemisviis küberturbesuutlikkuse suurendamiseks riikliku küberturbestrateegia eesmärkidega hõlmatud valdkondades. Riigil võib siiski olla olemas üldeesmärke ja uuringuid (tehnilisi, poliitilisi, poliitikauuringuid), et täiustada riigi suutlikkust.	Riiklik lähenemisviis suutlikkuse suurendamiseks riikliku küberturbestrateegia eesmärkidega hõlmatud valdkondades on määratletud. Tulemuste saavutamiseks vajalikud tegevuskavad või tegevused on olemas, kuid varajases etapis. Lisaks võivad olla tuvastatud ja/või kaasatud aktiivsed sidusrühmad.	Riikliku küberturbestrateegia eesmärkidega hõlmatud valdkonnas suutlikkuse suurendamise tegevuskava on selgelt määratletud ja seda toetavad asjaomased sidusrühmad. Tavasid ja tegevusi jõustatakse ja rakendatakse riiklikul tasandil ühtselt. Tegevused on määratletud ja dokumenteeritud koos selge vahendite eraldamise ja juhtimise ning tähtaegadega.	Tegevuskava hinnatakse korrapäraselt: see on prioriteetne, optimeeritud ja kestlik. Küberturbesuutlikkuse suurendamise meetmete tulemuslikkust mõõdetakse korrapäraselt. Tuvastatud on edutegurid, probleemid ja lüngad meetmete rakendamisel.	Küberturbesuutlikkuse suurendamise strateegia on dünaamiline ja kohandatav. Pidev tähelepanu keskkonna arengule (tehnika areng, ülemaailmsed konfliktid, uued ohud jt) aitab kaasa kiirele otsustussuutlikkusele ja võimele võtta kiiresti meetmeid olukorra parandamiseks.

3.3 KLASTRID JA ENESEHINDAMISE RAAMISTIKU ÜLDSTRUKTUUR

Enesehindamise raamistik koosneb **neljast klastrist:** I) küberturbe juhtimine ja standardid, II) suutlikkuse suurendamine ja teadlikkus, III) õiguslikud ja regulatiivsed raamistikud ning IV) koostöö. Iga klaster hõlmab üht riigi küberturbesuutlikkuse suurendamise peamist teemavaldkonda ja sisaldab eesmärgikogumit, mille liikmesriigid võivad lisada riiklikku küberturbestrateegiasse, eelkõige järgmist.

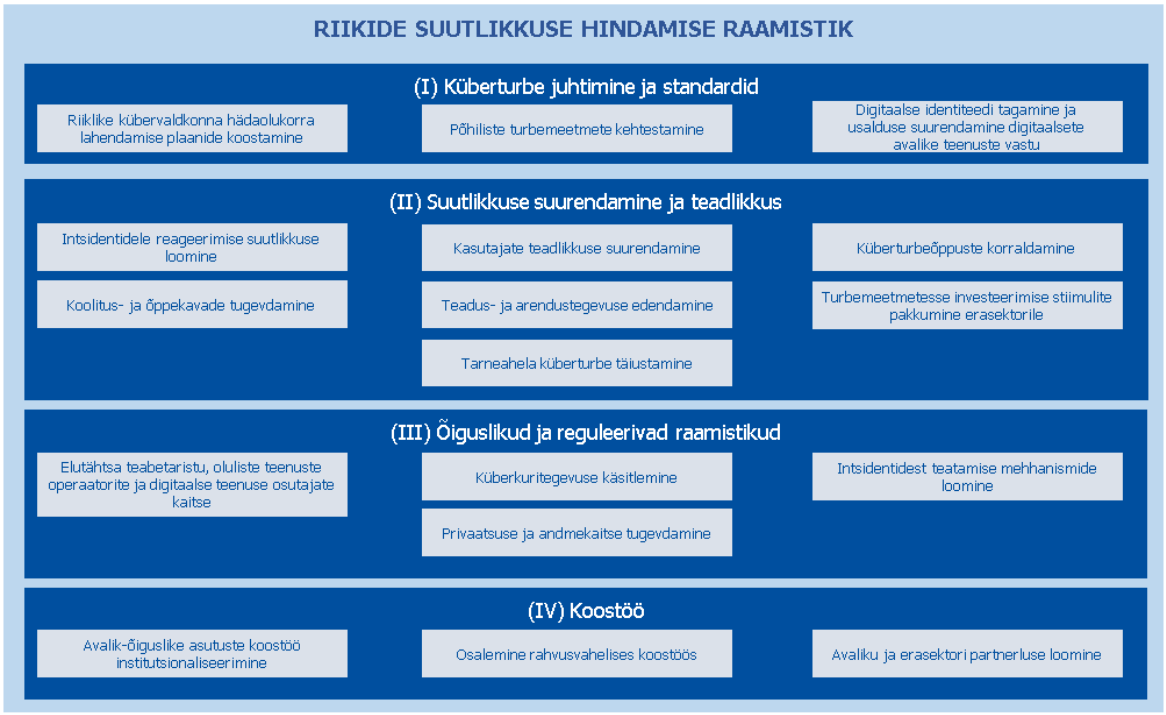
- **(I) Küberturbe juhtimine ja standardid**: see klaster mõõdab liikmesriikide suutlikkust saavutada küberturbe valdkonnas nõuetekohane juhtimine, kehtestada standardid ja head tavad. See mõõde arvestab küberkaitse ja kerksuse eri aspekte, toetades ühtlasi riikliku küberjulgeolekusektori arengut ja suurendades usaldust valitsuse vastu.
- **(II) Suutlikkuse suurendamine ja teadlikkus**: see klaster hindab liikmesriikide suutlikkust teadvustada küberturbe riske ja ohte ning neid käsitleda. Lisaks hindab see mõõde riigi suutlikkust pidevalt suurendada küberturbesuutlikkust ning teadmiste ja oskuste üldist taset valdkonnas. Samuti käsitleb see küberturbeturu arengut ja küberturbe teadus- ja arendustegevuse saavutusi**.** Sellesse klastrisse on koondatud kõik eesmärgid, mis toetavad suutlikkuse suurendamist.
- **(III) Õiguslikud ja reguleerivad raamistikud:** see klaster mõõdab liikmesriikide suutlikkust kehtestada vajalikud õiguslikud ja reguleerivad instrumendid, et käsitleda ja vastustada kasvavat küberkuritegevust ja seonduvaid küberintsidente ning kaitsta elutähtsat teabetaristut. Lisaks hindab see mõõde ka liikmesriikide suutlikkust luua õigusraamistik kodanike ja ettevõtjate kaitseks, näiteks seoses turbe ja privaatsuse tasakaalustamisega.
- **(IV) Koostöö:** see klaster hindab riiklikul ja rahvusvahelisel tasandil eri sidusrühmade koostööd ja teabevahetust kui olulist vahendit pidevalt muutuva ohukeskkonna paremaks mõistmiseks ja sellele reageerimiseks.

Mudelis sisalduvad eesmärgid on sellised, mille liikmesriigid on ühiselt vastu võtnud ning mis on valitud peatükis 2.2 loetletud eesmärkide hulgast. Eelkõige hindab mudel järgmisi eesmärke.

- 1. Riiklike kübervaldkonna hädaolukorra lahendamise plaanide koostamine (I)
- 2. Põhiliste turbemeetmete kehtestamine (I)
- 3. Digitaalse identiteedi tagamine ja usalduse suurendamine digitaalsete avalike teenuste vastu (I)
- 4. Intsidentidele reageerimise suutlikkuse loomine (II)
- 5. Kasutajate teadlikkuse suurendamine (II)
- 6. Küberturbeõppuste korraldamine (II)
- 7. Koolitus- ja õppekavade tugevdamine (II)
- 8. Teadus- ja arendustegevuse edendamine (II)
- 9. Turbemeetmetesse investeerimise stiimulite pakkumine erasektorile (II)
- 10. Tarneahela küberturbe täiustamine (II)
- 11. Elutähtsa teabetaristu, oluliste teenuste operaatorite ja digitaalse teenuse osutajate kaitse (III)
- 12. Küberkuritegevuse käsitlemine (III)
- 13. Intsidentidest teatamise mehhanismide loomine (III)
- 14. Privaatsuse ja andmekaitse tugevdamine (III)
- 15. Avalik-õiguslike asutuste koostöö institutsionaliseerimine (IV)
- 16. Osalemine rahvusvahelises koostöös (IV)
- 17. Avaliku ja erasektori partnerluse loomine (IV)

Neli klastrit ja nende aluseesmärgid on ühendatud mudeliks, millega saada terviklik ülevaade liikmesriikide küberturbesuutlikkuse küpsusest. Järgmisel joonisel (Joonis 1) on enesehindamise raamistiku üldstruktuur ja eri elementide (eesmärgid, klastrid ja enesehindamise raamistik) seos riigi tulemuslikkuse hindamisega.

Joonis 1. Enesehindamise raamistiku struktuur



Enesehindamise raamistiku iga eesmärgi kohta on mitu näitajat, mis jagunevad viie küpsustaseme vahel. Iga näitaja põhineb jah-ei-küsimusel. Näitaja võib olla kohustuslik või mitte.

3.4 PUNKTISUMMA ARVUTAMISE MEHHANISM

Enesehindamise raamistikus **punktisumma arvutamisel** arvestatakse ülalnimetatud elemente ja peatükis 3.5 loetletud põhimõtteid. Mudeliga arvutatav punktisumma tugineb kahe parameetri väärtusele: **küpsustase** ja **hõlmavus.** Mõlemat parameetrit saab arvutada eri tasanditel: i) eesmärkide kaupa, ii) eesmärkide klastrite kaupa või iii) üldiselt.

Tulemused eesmärgi tasandil

Küpsustaseme punktisumma annab ülevaate riigi küpsustasemest, näidates, mis suutlikkus on olemas ja mis tavasid kasutatakse. Küpsustaseme punktisumma arvutatakse vastavalt kõrgeimale tasemele, mille korral vastaja täitis kõik vajalikud nõuded (vastas jaatavalt kõigile kohustuslikele küsimustele). Lisaks peavad olema täidetud kõigi eelnevate küpsustasemete nõuded.

Hõlmavus näitab kõigi positiivse vastusega näitajate osakaalu, olenemata nende tasemest. See on täiendav väärtus, mis arvestab kõiki eesmärki mõõtvaid näitajaid. Hõlmavus arvutatakse eesmärgi alla kuuluvate küsimuste koguarvu ja jaatavate vastustega küsimuste arvu suhtena.

Oluline on märkida, et edaspidi tähendab selles dokumendis sõna „***punktisumma***“ nii küpsustaseme kui ka hõlmavuse väärtusi.

Joonisel 2 on punktisummade arvutamise mehhanism eesmärkide kaupa ja see annab visuaalse ülevaate hindamismehhanismist, mida kirjeldatakse peatükis 3.1 ja täiendavalt allpool.

Joonis 2. Punktisumma arvutamise mehhanism eesmärkide kaupa

Joonis 2 kujutab näidet, kuidas arvutada küpsustaset eesmärkide kaupa. NB! Vastaja täitis kõik esimese kolme küpsustaseme nõuded ja ainult osaliselt 4. taseme nõuded. Seega näitab punktisumma, et ***vastaja küpsustase on küberturbeõppuste korraldamise eesmärgi korral 3. tasemel.***

Samas ei kajasta joonise (Joonis 2) näide eesmärgi küpsustase teavet, mis on saadud positiivse punktisummaga näitajatest ja mis ületavad 3. küpsustaset. Sellisel juhul võib hõlmavus anda ülevaate kõigist eesmärgi saavutamiseks vastaja rakendatud elementidest, olenemata vastaja tegelikust küpsustasemest. Praegusel juhul on eesmärgi alla kuuluvate küsimuste koguarvu ja jaatavate vastustega küsimuste arvu suhe 19 : 27, st ***hõlmavus on 70%.***

Et arvestada liikmesriikide eripära ja ühtlasi saada järjepidev ülevaade, arvutatakse punktisumma klastri tasandil ja üldisel tasandil kahe eri valimi põhjal.

- **Üldpunktisummad:** üks tervikvalim, mis hõlmab klastri või üldraamistiku kõiki eesmärke (1–17).
- **Eripunktisummad:** üks erivalim, mis hõlmab ainult liikmesriigi valitud eesmärke (tavaliselt vastavalt riigi küberturbestrateegia eesmärkidele) klastris või üldraamistikus.

Punktid klastri tasandil

Iga klastri põhiküpsustase arvutatakse kõigi selle klastri eesmärkide küpsustasemete aritmeetilise keskmisena.

Iga klastri eriküpsustase arvutatakse selle klastri nende eesmärkide küpsustasemete aritmeetilise keskmisena, mida liikmesriik otsustas hinnata (tavaliselt vastavalt riigi küberturbestrateegia eesmärkidele).

Näiteks Joonis 1 näitab, et klaster I (küberturbe juhtimine ja standardid) koosneb kolmest eesmärgist. Eeldades, et vastaja otsustas hinnata ainult kaht esimest eesmärki, kuid mitte kolmandat, ja eeldades, et kahe esimese eesmärgi küpsustasemed on vastavalt 2 ja 4, on klastri küpsustase kõiki eesmärke arvestades 2. tase (klastri I üldine küpsustase = (2 + 4) : 3).

Teisalt ainult hindaja valitud erieesmärke arvestades on klastri küpsustase 3. tase (klastri I eriküpsustase = (2 + 4) : 2).

Iga klastri põhihõlmavus arvutatakse klastri alla kuuluvate küsimuste koguarvu ja jaatavate vastustega küsimuste arvu suhtena.

Iga klastri erihõlmavus arvutatakse kahe arvu suhtena: klastri nende küsimuste koguarv, mis on seotud eesmärkidega, mida liikmesriik otsustas hinnata (tavaliselt vastavalt riigi küberturbestrateegia eesmärkidele), ja jaatavate vastustega küsimuste arv.

Punktisummad üldisel tasandil

Riigi üldine põhiküpsustase arvutatakse raamistiku kõigi eesmärkide (1–17) küpsustasemete aritmeetilise keskmisena.

Riigi üldine eriküpsustase arvutatakse raamistiku nende eesmärkide küpsustasemete aritmeetilise keskmisena, mida liikmesriik otsustas hinnata (tavaliselt vastavalt riigi küberturbestrateegias olevatele eesmärkidele).

Riigi üldine põhihõlmavus arvutatakse raamistikuga hõlmatud kõigi eesmärkide (1–17) alla kuuluvate küsimuste koguarvu ja jaatavate vastustega küsimuste arvu suhtena.

Riigi üldine erihõlmavus arvutatakse kahe arvu suhtena: raamistiku eesmärkide alla kuuluvate nende küsimuste koguarv, mida liikmesriik otsustas hinnata (tavaliselt vastavalt riigi küberturbestrateegia eesmärkidele), ja jaatavate vastustega küsimuste arv.

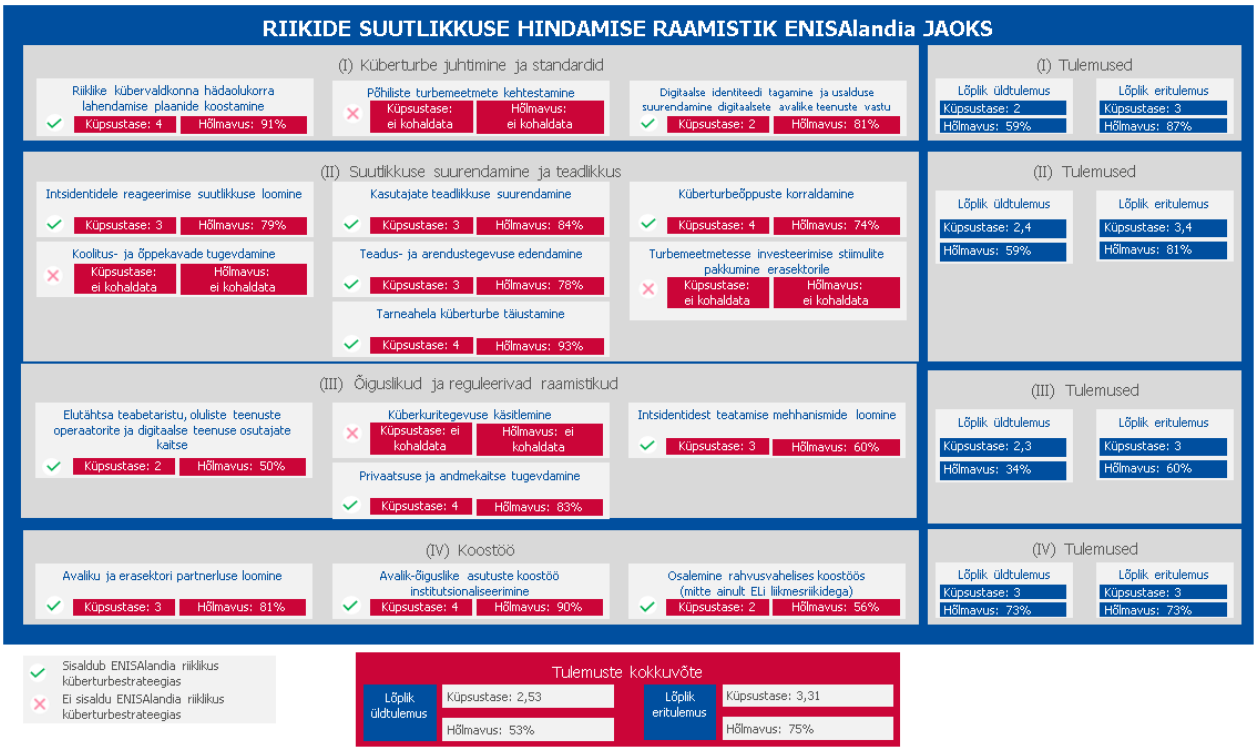
Iga näitaja kohta saavad vastajad valida kolmanda variandi „ei tea / ei ole kohaldatav“. Sellisel juhul näitajat tulemuste koguarvutuses ei kasutata.

Küpsustasemed klastri ja üldtasandil arvutatakse aritmeetilise keskmisena, et näidata muudatust kahe hindamise vahel. Alternatiiv, mis seisneb klastrite ja üldise küpsustaseme arvutamisel kõige vähem küpsema eesmärgi küpsustasemena – kuigi see on küpsuse seisukohast asjakohane – ei arvesta edenemist muude eesmärkidega hõlmatud valdkondades.

Et klastri ja üldtasand liidetakse aruandluse eesmärgil, on otsustatud kasutada aritmeetilist keskmist. Täpsemaks aruandluseks kasutage eesmärkide tasandi punktisummasid.

Joonisel 3 on kokkuvõte punktisumma arvutamise mehhanismidest mudeli eri tasanditel (eesmärk, klaster, üldine).

Joonis 3. Üldine punktisumma arvutamise mehhanism



3.5 ENESEHINDAMISE RAAMISTIKU NÕUDED

Selles peatükis esitatud riikide suutlikkuse hindamise raamistik põhineb liikmesriikide tõstatatud vajadustel ja tugineb järgmistele nõuetele.

- Liikmesriik kasutab riigi suutlikkuse hindamise raamistikku vabatahtlikkuse alusel enesehindamise raamistikuna.
- Riikide suutlikkuse hindamise raamistiku eesmärk on mõõta liikmesriikide küberturbesuutlikkust seoses 17 eesmärgiga. Liikmesriik võib siiski ise valida hinnatavad eesmärgid ja hinnata ainult osa 17 eesmärgist.
- Enesehindamise raamistiku eesmärk on mõõta liikmesriigi küberturbesuutlikkuse küpsustaset.
- Hindamise tulemusi ei avaldata, v.a kui liikmesriik otsustab seda teha omal algatusel.
- Liikmesriik saab esitada hindamistulemused, märkides riigi küberturbesuutlikkuse, eesmärkide klastri või isegi üheainsa eesmärgi küpsustaseme.
- Kõik hinnatud eesmärgid on hindamisraamistikus võrdselt asjakohased, seega on neil sama tähtsus. Sama kehtib selles kasutatavate näitajate kohta.
- Liikmesriik saab jälgida oma tegevust aja jooksul.

Enesehindamise raamistiku eesmärk on toetada liikmesriike küberturbesuutlikkuse suurendamisel. See hõlmab seetõttu ka soovitusi või suuniseid, millest Euroopa riigid saavad juhinduda oma küpsustaseme täiustamisel.

NB! Need soovitused või suunised põhinevad ENISA väljaannetel ja teistelt riikidelt saadud kogemustel ning tuginevad enesehindamise tulemustele.

4. RIIKIDE SUUTLIKKUSE HINDAMISE RAAMISTIKU NÄITAJAD

4.1 RAAMISTIKU NÄITAJAD

Selles peatükis esitatakse ENISA riikide suutlikkuse hindamise raamistiku näitajad. Järgmised alapeatükid jagunevad klastriteks.

Tabelis on iga klastri kohta esitatud terviklik näitajate kogum küpsustasemega seotud küsimustena. Küsimustik on enesehindamise peamine vahend. Iga eesmärgi kohta tuleb arvestada kaht näitajate kogumit:

- strateegia küpsuse üldküsimused (9 küsimust), mis on iga küpsustaseme puhul märgitud punktidega a–c ja mis korduvad iga eesmärgi korral;
- küberturbesuutlikkuse (319 küsimust), mis on iga küpsustaseme korral nummerdatud skaalal 1–10 vastavalt eesmärgiga hõlmatud valdkonnale.

Igale küsimusele on lisatud silt (0/1), mis näitab, kas küsimus on küpsustaseme jaoks kohustuslik näitaja (1) või mitte (0).

Igal küsimusel on tunnusnumber, mis koosneb järgmistest osadest:

- eesmärgi number,
- küpsustase,
- küsimuse number.

Näiteks tähendab küsimuse number 1.2.4, et see on strateegilise eesmärgi (I) „Riiklike kübervaldkonna hädaolukorra lahendamise plaanide koostamine“ 2. küpsustaseme 4. küsimus.

NB! Kui ei ole märgitud teisiti, käsitletakse küsimuses riigi tasandit. Kõigis küsimustes tähendab „teie“ liikmesriiki üldiselt ja mitte hindavat isikut ega valitsusasutust.

Iga eesmärgi määratlus on peatükis 2.2 – Euroopa riiklikes küberturbestrateegiates tuvastatud ühised eesmärgid.

4.1.1 1. klaster: küberturbe juhtimine ja standardid

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
1 – Riiklike kübervaldkonna hädaolukorra lahendamise plaanide koostamine	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						
	1	Kas olete alustanud riiklike kübervaldkonna hädaolukorra lahendamise plaanide koostamist, näiteks sätestanud nende üldeesmärgid, ulatuse ja/või põhimõtted?	1	Kas teil on olemas doktriin / riiklik strateegia, mis käsitleb küberturvet kriisitegurina (st kava, poliitika jne)?	1	Kas teil on olemas riikliku tasandi küberkriiside ohjamise kava?	1	Kas olete rahul riiklikus kübervaldkonna hädaolukorra lahendamise plaanis hõlmatud elutähtsate sektorite arvu või protsendiga?	1	Kas teil on kasutusel kogemuste analüüsimise protsess, mida rakendada pärast küberõppusi või tegelikke kriise riiklikul tasandil?	1
	2	Kas üldiselt ollakse seisukohal, et küberintsidendid on kriisitegur, mis võib ohustada riiklikku julgeolekut?	0	Kas teil on olemas keskus, mille kaudu saada teavet ja teavitada otsustajaid? See tähendab mis tahes meetodeid, platvorme või asukohti, millega tagatakse, et kõigil kriisile reageerijatel on juurdepääs samale reaalajas kättesaadavale teabele küberkriisi kohta.	1	Kas teil on riiklikul tasandil kasutusel küberkriisimenetlused?	1	Kas korraldate riikliku kübervaldkonna erandolukorra planeerimisega seotud tegevusi (õppusi) piisavalt sageli?	1	Kas teil on olemas riikliku plaani regulaarseks katsetamise protsess?	1
	3	Kas kübervaldkonna erandolukorra planeerimise valdkonnas on tehtud uuringuid (tehnilisi, operatiivseid, poliitilisi)?	0	Kas riiklike kübervaldkonna erandolukorra planeerimise ja plaanide teostamise järelevalvesse on kaasatud vastavad ressursid?	1	Kas teil on teabevahetusüksus, kes on saanud erikoolituse küberkriisidele reageerimiseks ja üldsuse teavitamiseks?	1	Kas teil on piisavalt inimesi, kes tegelevad kriisiplaneerimisega, vaatavad üle omandatud kogemusi ja teevad muudatusi?	1	Kas teil on olukorrateadlikkuse suurendamiseks asjakohased vahendid ja platvormid?	1
	4	-		Kas teil on riiklikul tasandil küberohtude hindamise metoodika, mis sisaldab mõju hindamise menetlusi?	0	Kas kaasate kõiki asjaomaseid riiklikke sidusrühmi (riiklik julgeolek, riigikaitse, kodanikukaitse, õiguskaitse, ministeeriumid, ametiasutused jne)?	1	Kas teil on piisavalt koolitatud inimesi, et reageerida küberkriisidele riiklikul tasandil?	1	Kas kasutate kübervaldkonna hädaolukorra lahendamise plaani seireks ja täiustamiseks erilist küpsusmudelit?	0

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
	5	-		-		Kas teil on olemas asjakohased kriisiohjerajatised ja kriisiruumid?	1	-		Kas teil on olemas ressursid, mis on suunatud kas ohtude ennetamisele või tegevusele küberjulgeoleku tuleviku nimel, et käsitleda tulevikukriise ja homseid probleeme?	0
	6	-		-		Kas kaasate vajaduse korral rahvusvahelisi sidusrühmi ELis?	0	-		-	
	7	-		-		Kas teete vajaduse korral koostööd rahvusvaheliste sidusrühmadega ELi-välistes riikides?	0	-		-	
2 – Põhiliste turbemeetmete kehtestamine	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						
	1	Kas olete teinud uuringu, et tuvastada **avaliku sektori** organisatsioonidega seotud nõuded ja lüngad, mis põhinevad rahvusvaheliselt tunnustatud standarditel, nt ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS jne?	1	Kas turbemeetmed on kasutusele võetud kooskõlas rahvusvaheliste/riiklike standarditega?	1	Kas põhilised turbemeetmed on kohustuslikud?	1	Kas on olemas põhiliste turbemeetmete sageda ajakohastamise protsess?	1	Kas teil on olemas IKT tugevdamise protsess, kui meetmed ei leevenda intsidente?	1

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
	2	Kas olete teinud uuringu, et tuvastada **eraõiguslike** organisatsioonidega seotud nõuded ja lüngad, mis põhinevad rahvusvaheliselt tunnustatud standarditel, nt ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS jne?	1	Kas põhiliste turbemeetmete määratlemisel konsulteeritakse erasektori ja muude sidusrühmadega?	1	Kas rakendate elutähtsates sektorites horisontaalseid turbemeetmeid?	1	Kas on kehtestatud seiremehhanism, et analüüsida põhiliste turbemeetmete kasutuselevõttu?	1	Kas hindate nende uute standardite asjakohasust, mida arendatakse vastuseks ohtude uusimale arengule?	1
	3	-		-		Kas rakendate elutähtsates sektorites sektoriomaseid turbemeetmeid?	1	Kas on olemas riiklik asutus, kes kontrollib, kas põhilisi turbemeetmeid jõustatakse või mitte?	1	Kas teil on olemas riiklik koordineeritud nõrkustest teatamise kord või edendate seda?	1
	4	-				Kas põhilised turbemeetmed on kooskõlas asjakohaste sertifitseerimissüsteemidega?	1	Kas teil on kehtestatud kord nõuetele mittevastavate organisatsioonide tuvastamiseks teatud ajavahemiku jooksul?	1	-	
	5	-		-		Kas põhiliste turbemeetmete jaoks on kehtestatud riski enesehindamise protsess?	1	Kas on olemas auditiprotsess, et tagada turbemeetmete nõuetekohane rakendamine?	1	-	
2 – Põhiliste turbemeetmete kehtestamine	6	-		-		Kas vaatate riigiasutuste hankeprotsesside käigus üle kohustuslikud põhilised turbemeetmed?	0	Kas määratlete või julgustate aktiivselt turvaliste standardite vastuvõtmist elutähtsate IT-/OT-toodete (meditsiiniseadmed, andmesidega ja autonoomsed sõidukid, professionaalsed raadioseadmed, rasketööstuse seadmed jne) arendamisel?	0	-	
3 – Digitaalse identiteedi tagamine ja usalduse suurendamine digitaalsete avalike teenuste vastu	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete seda käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
3 – Digitaalse identiteedi tagamine ja usalduse suurendamine digitaalsete avalike teenuste vastu	1	Kas olete teinud uuringuid või puuduste analüüse, et tuvastada, kas kodanikele ja ettevõtjatele on vaja turvalisi digitaalseid avalikke teenuseid?	1	Kas koostate riskianalüüse, et määrata varade või teenuste riskiprofiil, enne kui teisaldate need pilve või osalete digiülemineku projektides?	1	Kas edendate privaatsuslõime metoodikat kõigis e-riigi projektides?	1	Kas kogute näitajaid küberintsidentide kohta, mis on seotud digitaalsete avalike teenuste rikkumistega?	1	Kas osalete Euroopa töörühmades, et vastata standarditele ja/või töötada välja uusi nõudeid elektrooniliste usaldusteenuste jaoks (e-allkirjad, e-templid, registreeritud e-andmevahetusteenused, ajatemplid, veebikohtade autentimine), nt ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU jne?	1
	2	-		Kas teil on kasutusel strateegia, millega luua kodanike ja ettevõtjate jaoks turvalised riiklikud e-identimise süsteemid või neid edendada?	1	Kas kaasate turvaliste digitaalsete avalike teenuste kavandamisse ja osutamisse erasektori sidusrühmi?	1	Kas olete rakendanud e-identimise vahendite vastastikust tunnustamist teiste liikmesriikidega?	1	Kas osalete aktiivselt vastastikuste eksperdihinnangute koostamisel e-identimise süsteemidest Euroopa Komisjonile teatamise osana?	1
	3	-		Kas teil on strateegia, millega luua või edendada kodanike ja ettevõtjate jaoks turvalisi riiklikke elektroonilisi usaldusteenuseid (e-allkirju, e-templeid, registreeritud e-andmevahetusteenus, ajatemplit, veebikohtade autentimist)?	1	Kas rakendate kõigi digitaalsete avalike teenuste korral minimaalset turvalisuse lähtetaset?	1	-		-	
	4	-		Kas teil on valitsuse pilvandmetöötluse strateegia (valitsusele ja avaliku sektori asutustele, näiteks ministeeriumidele, riigiasutustele ja haldusasutustele suunatud pilvandmetöötlusstrateegia), mis arvestab mõju turbele?	0	Kas kodanikele ja ettevõtjatele on kättesaadavad e-identimise süsteemid, mille usaldusväärsuse tase on märkimisväärne või kõrge, nagu on määratletud eIDASe määruse (EL) nr 910/2014 lisas?	1	-		-	
	5	-		-		Kas teil on digitaalseid avalikke teenuseid, mis nõuavad e-identimise süsteeme, mille usaldusväärsuse tase on märkimisväärne või kõrge, nagu on määratletud eIDASe määruse (EL) nr 910/2014 lisas?	1	-		-	
	6	-		-		Kas teil on kodanikele ja ettevõtjatele usaldusteenuse osutajaid (e-allkiri, e-tempel, registreeritud e-andmevahetusteenus, ajatempel, veebikohtade autentimine)?	1	-		-	

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
	7	-		-		Kas toetate põhiliste turbemeetmete vastuvõtmist kõigi pilveteenuste kasutuselevõtumudelite korral (nt privaatsed, avalikud, hübriidsed, IaaS, PaaS, SaaS)?	0	-		-	

4.1.2 2. klaster: suutlikkuse suurendamine ja teadlikkus

Riikliku küberturbestrateegia eesmärk	Nr	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
4 – Intsidentidele reageerimise suutlikkuse loomine	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete seda käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						
	1	Kas teil on olemas mitteametlik intsidentidele reageerimise suutlikkus, mida hallatakse avalikus ja erasektoris või nende vahel?	1	Kas teil on vähemalt üks ametlik riiklik küberturbeintsidentide lahendamise üksus?	1	Kas teil on küberturvalisuse direktiivi II lisas viidatud sektorites olemas intsidentidele reageerimise suutlikkus?	1	Kas olete määratlenud ja edendanud intsidentidele reageerimise menetluste ja intsidentide klassifitseerimise süsteemide standardtavasid?	1	Kas teil on olemas mehhanismid nullpäeva turbeaukude varajaseks avastamiseks, tuvastamiseks, ennetamiseks, neile reageerimiseks ja nende leevendamiseks?	1
	2	-		Kas teie riiklikul või riiklikel küberturbeintsidentide lahendamise üksusel või üksustel on selgelt määratletud sekkumise ulatus, nt sõltuvalt sihtsektorist, intsidendi tüübist, mõjust?	1	Kas teie riigis on olemas riikliku küberturbeintsidentide lahendamise üksuse koostöömehhanism intsidentidele reageerimiseks?	1	Kas hindate oma intsidentidele reageerimise suutlikkust, tagamaks, et teil on piisavalt ressursse ja oskusi küberturvalisuse direktiivi I lisa punktis 2 sätestatud ülesannete täitmiseks?	1	-	
	3	-		Kas teie riiklikul või riiklikel küberturbeintsidentide lahendamise üksusel või üksustel on selgelt määratletud suhted teiste riiklike sidusrühmadega seoses riikliku küberturbemaastiku ja intsidentidele reageerimise tavadega (nt õiguskaitseasutused, kaitsevägi, internetiteenuste osutajad, riiklik küberjulgeolekukeskus)?	0	Kas teie riikliku või riiklike küberturbeintsidentide lahendamise üksuse või üksuste intsidentidele reageerimise suutlikkus on kooskõlas küberturvalisuse direktiivi I lisaga, st kättesaadavuse, füüsilise julgeoleku, talitluspidevuse, rahvusvahelise koostöö, intsidentide seire, varajase hoiatamise, intsidentidele reageerimise, riskianalüüsi ja olukorrateadlikkuse, erasektoriga koostöö, standardpraktikate jms alusel?	1	-		-	

Riikliku küberturbestrateegia eesmärk	Nr	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
4 – Intsidentidele reageerimise suutlikkuse loomine	4	-				Kas teil on kasutusel koostöömehhanism teiste naaberriikidega seoses intsidentidega?	1	-		-	
	5	-		-		Kas olete ametlikult määratlenud selged intsidentide käsitlemise poliitikad ja menetlused?	1	-		-	
	6	-		-		Kas teie riiklik või riiklikud küberturbeintsidentide lahendamise üksus või üksused osalevad küberturbeõppustel nii riiklikul kui ka rahvusvahelisel tasandil?	1	-		-	
	7	-		-		Kas teie riiklik või riiklikud küberturbeintsidentide lahendamise üksus või üksused on seotud intsidendile reageerimise ja julgeolekurühmade foorumiga (FIRST)?	0	-		-	
5 – Kasutajate teadlikkuse suurendamine	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete seda käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						
	1	Kas valitsus, erasektor või tavakasutajad tunnistavad vähemalt minimaalselt vajadust teadvustada küberturvalisuse ja privaatsuse küsimusi?	1	Kas olete tuvastanud kasutajate teadlikkuse suurendamiseks konkreetse sihtrühma, näiteks tavakasutajad, noored, ärikasutajad (mida saab jaotada üksikasjalikumalt: VKEd, oluliste teenuste operaatorid, digitaalse teenuse osutajad jne)?	1	Kas olete kampaaniate jaoks välja töötanud teavituskavad/-strateegia?	1	Kas töötate välja parameetrid oma kampaania hindamiseks planeerimise etapis?	1	Kas teil on olemas mehhanismid, millega tagatakse, et teadlikkuse tõstmise kampaaniad on pidevalt asjakohased ja arvestavad tehnika arengut, ohtude muutumist, õigusakte ja riikliku julgeoleku suuniseid?	1

Riikliku küberturbestrateegia eesmärk	Nr	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
5 – Kasutajate teadlikkuse suurendamine	2	Kas avaliku sektori asutused korraldavad oma organisatsioonis küberteadlikkuse suurendamise kampaaniaid vastavalt vajadusele, näiteks pärast küberturbeintsidenti?	0	Kas olete koostanud projektikava, et suurendada teadlikkust infoturbe ja privaatsuse küsimustes?	1	Kas teil on olemas protsess sisu loomiseks valitsuse tasandil?	1	Kas hindate oma kampaaniaid pärast nende teostamist?	1	Kas teete korrapäraseid hindamisi või uuringuid, et mõõta küberturbe ja privaatsusega seotud hoiakute või käitumise muutusi era- ja avalikus sektoris?	1
	3	Kas avaliku sektori asutused korraldavad vastavalt vajadusele üldsusele küberteadlikkuse kampaaniaid, näiteks pärast küberturbeintsidenti?	0	Kas teil on kättesaadavad ja kergesti tuvastatavad ressursid (nt ühtne veebiportaal, teadlikkuse suurendamise materjalid) kõigile kasutajatele, kes soovivad täiendada teadmisi küberturbe ja privaatsuse teemal?	1	Kas teil on olemas teadlikkuse tõstmise sihtvaldkondade tuvastamise mehhanismid (nt ENISA ohtude kaardistamise aruanne, riiklikud ohud, rahvusvahelised ohud, tagasiside riiklikelt küberkuritegevusvastastelt keskustelt jne)?	1	Kas teil on olemas mehhanismid sihtrühma jaoks kõige asjakohasema meedia- või teabevahetuskanali leidmiseks, et maksimeerida sihtrühmadeni jõudmist ja kaasamist? Näiteks digitaalmeedia eri liigid, brošüürid, e-kirjad, õppematerjalid, plakatid tiheda liiklusega piirkondades, televisioon, raadio jne.	1	Kas konsulteerite käitumisspetsialistidega, et kohandada kampaaniat sihtrühmale?	1
	4	-		-		Kas viite sisu loomisel sidusrühmi kokku ekspertide ja teabevahetusüksustega?	1			-	
	5	-		-		Kas kaasate ja rakendate oma teavitustegevuses erasektorit, et tutvustada ja levitada sõnumeid laiemale üldsusele?	1	-		-	
	6	-		-		Kas valmistate ette erilisi teadlikkusalgatusi avaliku sektori, erasektori, akadeemiliste ringkondade või kodanikuühiskonna juhtidele?	1	-		-	
	7	-		-		Kas osalete ENISA Euroopa küberturvalisuse kuu kampaaniates?	0	-		-	
6 – Küberturbeõppuste korraldamine	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		

Riikliku küberturbestrateegia eesmärk	Nr	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
6 – Küberturbeõppuste korraldamine	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						
	1	Kas korraldate riiklikul või üleeuroopalisel tasandil kriisiõppusi muudes sektorites (v.a küberturve)?	1	Kas teil on riiklikul tasandil olemas küberturbeõppuste kava?	1	Kas kaasate kõiki seotud avaliku halduse asutusi (isegi kui stsenaarium on valdkonnaomane)?	1	Kas koostate pärast meetme rakendamist aruandeid/hindamisaruandeid?	1	Kas teil on olemas saadud kogemuste analüüsimise suutlikkus kübervaldkonnas (aruandlusprotsessid, analüüs, leevendusmeetmed)?	1
	2	Kas olete eraldanud vahendeid kriisiohjeõppuste kavandamiseks ja tegemiseks?	1	Kas teete või prioriseerite küberkriisiohjamise õppusi elutähtsate ühiskondlike funktsioonide ja elutähtsa taristu jaoks?	1	Kas kaasate õppuste kavandamisel ja korraldamisel erasektorit?	1	Kas testite riiklikke kavu ja menetlusi?	1	Kas olete kehtestanud omandatud kogemuste analüüsi protsessi?	1
	3	-		Kas olete määranud koordineeriva asutuse, kes teeb küberturbeõppuste koostamise ja kavandamise järelevalvet (avaliku sektori asutus, konsultatsioonifirma jt)?	0	Kas korraldate valdkonnaomaseid õppusi riiklikul ja/või rahvusvahelisel tasandil?	1	Kas osalete küberturbeõppustel üleeuroopalisel tasandil?	1	Kas kohandate õppuste stsenaariume vastavalt uusimale arengule (tehnika areng, ülemaailmsed konfliktid, ohud jt)?	1
	4	-		-		Kas korraldate õppusi kõigis elutähtsates sektorites, mida mainitakse küberturvalisuse direktiivi II lisas?	1	-		Kas ühtlustate oma kriisiohjemenetlusi teiste liikmesriikidega, et tagada tõhus üleeuroopaline kriisiohje?	1
	5	-		-		Kas korraldate sektorivahelisi ja/või sektoriüleseid küberturbeõppusi?	1	-		Kas teil on olemas mehhanism strateegiate, plaanide ja menetluste kiireks kohandamiseks vastavalt õppustel saadud kogemustele?	0
	6	-		-		Kas korraldate küberturbeõppusi, mis on kohandatud eri tasanditele (tehniline ja operatiivtasand, menetlustasand, otsustustasand, poliitiline tasand jne)?	0	-		-	
7 – Koolitus- ja õppekavade tugevdamine	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete seda käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		

Riikliku küberturbestrateegia eesmärk	Nr	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						
	1	Kas kaalutlete küberturbe koolitus- ja õppekavade koostamist?	1	Kas koostate küberturbekursusi?	1	Kas teie riigis käsitletakse küberturbekultuuri õpilaste haridustee varajases etapis? Näiteks kas küberturvet käsitletakse põhikoolis ja gümnaasiumis?	1	Kas julgustate era- ja avaliku sektori töötajaid end akrediteerima või sertifitseerima?	1	Kas teil on olemas mehhanismid, millega tagatakse, et koolitused ja õppekavad on pidevalt asjakohased, arvestades praegust ja kujunemisjärgus tehnoloogia arengut, ohtude muutumist, õigusakte ja riikliku julgeoleku suuniseid?	1
	2	-		Kas teie riigi ülikoolid pakuvad küberturbe doktoriõpet eraldi erialana, mitte arvutiteaduse õppeainena?	1	Kas teie riigis on olemas riiklikud teaduslaborid ja haridusasutused, mis on spetsialiseerunud küberturbele?	1	Kas teie riik on töötanud välja küberturbe koolitus- või mentorlusprogramme, et toetada riiklikke idufirmasid ja VKEsid?	1	Kas olete rajanud küberturbe akadeemilisi tippkeskusi, mis toimiksid teadus- ja hariduskeskustena?	1
	3	-		Kas kavatsete koolitada haridustöötajaid (olenemata valdkonnast) infoturbe ja privaatsuse küsimustes, nt veebiturbe, isikuandmete kaitse ja küberkiusamise teemal?	1	Kas edendate/rahastate küberturvalisuse erikursusi ja õppekavu liikmesriikide tööhõiveameti töötajatele?	1	Kas toetate aktiivselt infoturbekursuste lisamist kõrgharidusse peale arvutiteaduse üliõpilaste ka muudele erialadele, näiteks selle kutseala vajadustele kohandatud kursusi?	1	Kas akadeemilised asutused osalevad küberturbe haridus- ja teadusvaldkonna arutelude juhtimises rahvusvahelisel tasandil?	0
	4	-		-		Kas teil on olemas küberturbe kursused ja/või eriõppekava EQFi (Euroopa kvalifikatsiooniraamistik) 5.–8. taseme jaoks?	1	Kas hindate korrapäraselt infoturbe valdkonna oskuste puudust (küberturbe töötajate puudust)?	1	-	
	5	-		-		Kas julgustate ja/või toetate algatusi internetiturbe kursuste lisamiseks põhi- ja keskhariduse õppekavadesse?	1	Kas edendate võrgustike loomist ja teabe jagamist akadeemiliste asutuste vahel nii riiklikul kui ka rahvusvahelisel tasandil?	1		

Riikliku küberturbestrateegia eesmärk	Nr	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
7 - Koolitus- ja õppekavade tugevdamine	6	-		-		Kas rahastate või pakute tasuta algtaseme küberturbekoolitusi kodanikele?	0	Kas kaasate erasektorit mis tahes vormis küberturbe haridusalgatustesse, nt kursuste kavandamisse ja pidamisse, õppepraktikasse, tööpraktikasse jne?	1	-	
	7	-		-		Kas korraldate aasta infoturbeüritusi (nt häkkimisvõistlusi või -maratone)?	0	Kas rakendate rahastamismehhanisme, et soodustada küberturbe valdkonna akadeemiliste kraadide omandamist (nt stipendiumid, tagatud õpipoisiõpe/praktika, tagatud töökohad konkreetsel tegevusalal või rollid avalikus sektoris)?	0	-	
8 – Teadus- ja arendustegevuse edendamine	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete seda käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						
	1	Kas olete teinud uuringuid või analüüse, et tuvastada küberturbe teadus- ja arendustegevuse prioriteedid?	1	Kas teil on kehtestatud teadus- ja arendustegevuse prioriteetide määratlemise protsessid (nt tekkivad teemad uut tüüpi küberrünnete heidutamise, nende vastaseks kaitseks, nende avastamiseks ja nendega kohanemiseks)?	1	Kas teil on kavas siduda teadus- ja arendustegevuse algatused reaalmajandusega?	1	Kas teadus- ja arendustegevuse küberturbealgatused on kooskõlas asjakohaste strateegiliste eesmärkidega, nt digitaalse ühtse turu, programmi „Horisont 2020“, digitaalse Euroopa ja ELi küberturbestrateegiaga?	1	Kas teete riiklikul tasandil koostööd mis tahes rahvusvaheliste küberturbe teadus- ja arendustegevuse algatustega?	1
	2	-		Kas teadus- ja arendustegevuse prioriseerimises osaleb erasektor?	1	Kas teil on olemas küberjulgeolekuga seotud riiklikke projekte?	1	Kas teadus- ja arendustegevuse algatuste jaoks on olemas hindamissüsteem?	1	Kas teadus- ja arendustegevuse prioriteedid on kooskõlas kehtivate või tulevaste eeskirjadega (riiklikul tasandil)?	1

Riikliku küberturbestrateegia eesmärk	Nr	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
8 – Teadus- ja arendustegevuse edendamine	3	-		Kas akadeemilised ringkonnad osalevad teadus- ja arendustegevuse prioriseerimisel?	1	Kas teil on olemas kohalikud/piirkondlikud idufirmade ökosüsteemid ja muud võrgustikukanalid (nt tehnoloogiapargid, innovatsiooniklastrid, võrgustikuüritused/-platvormid), et edendada innovatsiooni (sh küberturbe idufirmadele)?	1	Kas ülikoolide ja muude uurimisasutustega on sõlmitud koostöölepinguid?	1	Kas osalete ühe või mitme uusima teadus- ja tehnoloogiavaldkonna teema arutelude juhtimisel rahvusvahelisel tasandil?	0
	4	-		Kas on olemas riiklikud teadus- ja arendustegevuse algatused, mis on seotud küberturbega?	0	Kas akadeemilistes ringkondades ja erasektoris investeeritakse küberturbe teadus- ja arendustegevusse?	1	Kas on olemas tunnustatud asutus, mis teeb küberturbe teadus- ja arendustegevuse järelevalvet?	0	-	
	5	-		-		Kas teil on ülikoolides rakendusuuringute õppetoole, mis ühendavad uurimisteemasid ja turuvajadusi?	1	-		-	
	6	-		-		Kas teil on sihtotstarbelisi küberturbe teadus- ja arendustegevuse rahastamisprogramme?	0	-		-	
9 – Turbemeetmetesse investeerimise stiimulite pakkumine erasektorile	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete seda käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						
	1	Kas on olemas tööstuspoliitika või poliitiline tahe ergutada küberjulgeolekutööstuse arengut?	1	Kas stiimulite väljatöötamisel osaleb erasektor?	1	Kas küberturbesse investeerimise edendamiseks on olemas majandus-, regulatiiv- või muud liiki stiimuleid?	1	Kas on olemas erasektoris tegutsejaid, kes reageerivad stiimulitele turbemeetmetesse investeerimisega, nt küberturbele spetsialiseerunud investorid ja spetsialiseerumata investorid?	1	Kas teie küberturbeteemadele suunatud stiimulite valik tugineb viimastele ohusuundumustele?	1

Riikliku küberturbestrateegia eesmärk	Nr	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
9 – Turbemeetmetesse investeerimise stiimulite pakkumine erasektorile	2	–		Kas olete tuvastanud konkreetsed arendatavad küberturbeteemad (nt krüptograafia, privaatsus, autentimise uus vorm, tehisintellekti kasutamine küberturbes jne)?	0	Kas pakute küberturbe idufirmadele ja VKEdele tuge (nt maksusoodustusi)?	1	Kas pakute erasektorile stiimuleid, mis võimaldavad keskenduda tipptasemel tehnoloogiate (nt 5G, tehisintellekt, esemevõrk, kvantandmetöötlus jne) turvalisusele?	1	–	
	3	–		–		Kas pakute maksusoodustusi või muid finantsstiimuleid erasektori investoritele, kes investeerivad küberturbe idufirmadesse?	1	–		–	
	4	–		–		Kas soodustate küberturbe idufirmade ja VKEde juurdepääsu riigihangetele?	0	–		–	
	5	–		–		Kas erasektorile stiimulite pakkumiseks on olemas eelarve?	0	–		–	
10 – Tarneahela küberturbe täiustamine	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete seda käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						
	1	Kas olete teinud uuringu tarneahela haldamise turbe heade tavade kohta, mida kasutatakse eri tegevusalade ja/või avaliku sektori hangetes?	1	Kas hindate küberturvet elutähtsate sektorite kogu IKT-teenuste ja -toodete tarneahelas (vastavalt küberturvalisuse direktiivi (2016/1148) II lisale)?	1	Kas kasutate IKT-põhiste toodete ja teenuste turvalisuse sertifitseerimise kava? Näiteks SOG-IS MRA Euroopas (infosüsteemide turvalisuse vanemametnike rühm, vastastikuse tunnustamise leping), ühiste kriteeriumite tunnustamise kokkulepe (CCRA), riiklikud algatused, valdkondlikud algatused jne.	1	Kas olete kehtestanud protsessi IKT-teenuste ja -toodete tarneahela küberturvalisuse hindamiste ajakohastamiseks elutähtsates sektorites (vastavalt küberturvalisuse direktiivi (2016/1148) II lisale)?	1	Kas teil on varajaste ohumärkide avastamiseks tarneahela põhielementides olemas tuvastusmehhanismid, näiteks turbekontrollid internetiteenuste osutaja tasandil, turbemehhanismid peamistes taristukomponentides jne?	1

Riikliku küberturbestrateegia eesmärk	Nr	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
10 – Tarneahela küberturbe täiustamine	2	-		Kas rakendate avaliku halduse asutuste hankepoliitikas standardeid, et tagada IKT-toodete ja -teenuste pakkujate vastavus infoturbe põhinõuetele, nt standardeid ISO/IEC 27001 ja 27002, ISO/IEC 27036 jne?	1	Kas edendate IKT-toodete ja -teenuste arendamisel aktiivselt turvalisuse ja lõimprivaatsuse parimaid tavasid, nt turvalise tarkvara arendamise olelustsükli, esemevõrgu olelustsükli korral?	1	Kas teil on olemas protsess, millega tuvastada küberturbe puudused elutähtsate sektorite tarneahelas (vastavalt küberturvalisuse direktiivi (2016/1148) II lisale)?	1	-	
	3	-		-		Kas arendate ja pakute keskseid katalooge, kus on üksikasjalik teave olemasolevate infoturbe- ja privaatsusstandardite kohta, mida saab kohandada VKEdele ja mida need saavad rakendada?	1	Kas teil on olemas mehhanismid, millega tagatakse oluliste teenuste operaatorite jaoks kriitilise tähtsusega IKT-toodete ja -teenuste küberkerksus (võime jääda kättesaadavaks ja turvaliseks ka küberintsidendi korral), näiteks testimise, korrapäraste hindamiste, ohustatud elementide tuvastamise vms kaudu?	1	-	
	4	-				Kas osalete aktiivselt ELi IKT-alaste digitaaltoodete, -teenuste ja -protsesside sertifitseerimisraamistiku väljatöötamises vastavalt ELi küberturvalisuse määrusele (määrus (EL) 2019/881), näiteks osaledes Euroopa küberturvalisuse sertifitseerimise rühmas (ECCG), edendades tehniliste standardite ja korra arendamist IKT-toodete ja -teenuste turvalisuse tagamiseks?	0	Kas edendate VKEdele suunatud sertifitseerimiskavade väljatöötamist, et toetada infoturbe- ja privaatsusstandardite vastuvõtmist?	0	-	
	5	-		-		Kas pakute VKEdele mis tahes liiki stiimuleid turbe- ja privaatsusstandardite vastuvõtmiseks?	0	Kas olete kehtestanud vahendeid, et julgustada suurettevõtjaid suurendama oma tarneahelates väikeettevõtete küberturvet, nt küberturbekeskus, koolitus ja teadlikkuse suurendamise kampaaniad?	0	-	
	6	-		-		Kas julgustate tarkvaramüüjaid toetama VKEsid, tagades, et väikestele organisatsioonidele suunatud toodetes kasutatakse turvalisi vaikekonfiguratsioone?	0	-		-	

4.1.3 3. klaster: õiguslikud ja reguleerivad raamistikud

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
11 – Elutähtsa teabetaristu, oluliste teenuste operaatorite ja digitaalse teenuse osutajate kaitse	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete seda käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						
	1	Kas on olemas üldine arusaam, et elutähtsa teabetaristu operaatorid panustavad riigi julgeolekusse?	1	Kas teil on olemas oluliste teenuste tuvastamise metoodika?	1	Kas olete rakendanud küberturvalisuse direktiivi (2016/1148)?	1	Kas teil on kehtestatud riskiregistri ajakohastamise kord?	1	Kas koostate ja ajakohastate ohtude kaardistamise aruandeid?	1
	2	-		Kas teil on olemas elutähtsa teabetaristu tuvastamise metoodika?	1	Kas olete rakendanud Euroopa kodanikualgatuse direktiivi (2008/114) Euroopa elutähtsate taristute identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta?	1	Kas olete kasutusele võtnud muid mehhanisme, et mõõta, kas oluliste teenuste operaatorite rakendatavad tehnilised ja korralduslikud meetmed võrgu- ja infosüsteemide turberiskide juhtimiseks on asjakohased? Näiteks regulaarsed küberturbeauditid, riiklik raamistik standardmeetmete rakendamiseks, valitsusepoolsed tehnilised vahendid, nagu tuvastusmehhanismid või süsteemiomane konfiguratsiooniülevaade jne.	1	Kas suudate kaardistatud ohtude uusima arengu põhjal lisada oma elutähtsa teabetaristu kaitse tegevuskavasse uue valdkonna?	1
	3	-		Kas teil on olemas oluliste teenuste operaatorite tuvastamise metoodika?	1	Kas teil on olemas oluliste teenuste tuvastatud operaatorite riiklik register elutähtsate sektorite kaupa?	1	Kas vaatate oluliste teenuste tuvastatud operaatorite nimekirja läbi ja seejärel ajakohastate seda hiljemalt iga kahe aasta järel?	1	Kas suudate kaardistatud ohtude uusima arengu põhjal kohandada oma elutähtsa teabetaristu kaitse tegevuskava jaoks uusi nõudeid?	1

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
11 – Elutähtsa teabetaristu, oluliste teenuste operaatorite ja digitaalse teenuse osutajate kaitse	4	-		Kas teil on olemas digitaalse teenuse osutajate tuvastamise metoodika?	1	Kas teil on olemas digitaalsete teenuste tuvastatud osutajate riiklik register?	1	Kas olete kasutusele võtnud muid mehhanisme, et mõõta, kas digitaalse teenuse osutajate rakendatavad tehnilised ja korralduslikud meetmed võrgu- ja infosüsteemide turberiskide juhtimiseks on asjakohased? Näiteks regulaarsed küberturbeauditid, riiklik raamistik standardmeetmete rakendamiseks, valitsusepoolsed tehnilised vahendid, nagu tuvastusmehhanismid või süsteemiomane konfiguratsiooniülevaade jne.	1	-	
	5	-		Kas teil on üks või mitu riiklikku asutust, kes teevad elutähtsa teabetaristu kaitse ning võrgu- ja infosüsteemide turvalisuse järelevalvet, nt vastavalt küberturvalisuse direktiivi (2016/1148) nõuetele?	1	Kas teil on olemas tuvastatud või teadaolevate riskide riiklik register?	1	Kas vaatate digitaalsete teenuste tuvastatud osutajate nimekirja läbi ja seejärel ajakohastate seda hiljemalt iga kahe aasta järel?	1	-	
	6	-		Kas töötate välja sektoripõhiseid kaitsekavu, sealhulgas põhilisi küberturvalisuse meetmeid (kohustuslikud või suunised)?	0	Kas teil on olemas elutähtsa teabetaristu sõltuvuste kaardistamise metoodika?	1	Kas kasutate turvalisuse sertifitseerimise süsteemi (riigisisest või rahvusvahelist), et aidata oluliste teenuste operaatoritel ja digitaalse teenuse osutajatel tuvastada turvalisi IKT-tooteid, nt Euroopas SOG-IS MRA, riiklikud algatused jne?	1	-	
	7	-		-		Kas kasutate riskijuhtimistavasid, et tuvastada, kvantifitseerida ja juhtida elutähtsa teabetaristuga seotud riske riiklikul tasandil?	1	Kas kasutate turvalisuse sertifitseerimise kava või kvalifitseerimismenetlust, et hinnata oluliste teenuste operaatoritega koostööd tegevaid teenuseosutajaid (nt intsidentide avastamise, intsidentidele reageerimise, küberturbeauditite, pilveteenuste, kiipkaartide jms valdkonnas tegutsevad teenuseosutajad)?	1	-	

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
11 – Elutähtsa teabetaristu, oluliste teenuste operaatorite ja digitaalse teenuse osutajate kaitse	8	-		-		Kas osalete konsultatsiooniprotsessis, et tuvastada piiriüleseid sõltuvusi?	1	Kas teil on olemas mehhanismid oluliste teenuste operaatorite ja digitaalse teenuse osutajate küberturvalisuse põhimeetmetele vastavuse taseme mõõtmiseks?	0	-	
	9					Kas teil on ühtne kontaktpunkt, kes vastutab võrgu- ja infosüsteemide turvalisusega seotud küsimuste koordineerimise eest riiklikul tasandil ja piiriülese koostöö eest liidu tasandil?	1	Kas olete kehtestanud meetmeid, et tagada elutähtsa teabetaristu teenuste järjepidevus? Näiteks kriisiennetus, elutähtsate infosüsteemide taastamise kord, talitluspidevus ilma infotehnoloogiata, võrguühenduseta varundamise kord jne.	0		
	10					Kas määratlete põhilised küberturbemeetmed (kohustuslikud või suunised) digitaalse teenuse osutajatele ja kõigile sektoritele, mis on loetletud küberturvalisuse direktiivi (2016/1148) II lisas?	1				
	11	-		-		Kas pakute küberintsidentide avastamise vahendeid või meetodeid?	1	-		-	
12 – Küberkuritegevuse käsitlemine	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete seda käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
	1	Kas olete teinud uuringu, et leida küberkuritegevuse tõhusa käsitlemise õiguskaitsenõuded (õiguslik alus, ressursid, oskused jne)?	1	Kas teie riiklik õigusraamistik on täielikult kooskõlas asjaomase ELi õigusraamistikuga, sealhulgas direktiiviga 2013/40/EL, milles käsitletakse ründeid infosüsteemide vastu? Näiteks seoses ebaseadusliku juurdepääsuga infosüsteemidele, süsteemi ebaseadusliku häirimise, ebaseadusliku andmetesse sekkumise, ebaseadusliku pealtkuulamise, kuritegude sooritamise vahenditega jms.	1	Kas teil on prokuratuurides olemas küberkuritegevusele keskenduvad üksused?	1	Kas kogute statistikat vastavalt direktiivi 2013/40/EL (infosüsteemide vastu suunatud ründeid käsitlev direktiiv) artikli 14 lõikele 1?	1	Kas korraldate riiklikul ja/või mitmepoolsel tasandil asutustevahelisi koolitusi või seminare õiguskaitseasutustele, kohtunikele, prokuröridele ja küberturbeintsidentide lahendamise riiklikele/valitsuse üksustele?	1
	2	Kas olete teinud uuringu, et leida , mida vajavad prokurörid ja kohtunikud küberkuritegevuse tõhusal käsitlemisel (õiguslik alus, ressursid, oskused jne)?	1	Kas teil on kehtestatud õigussätteid, mis käsitlevad identiteedi ja isikuandmete vargust veebis?	1	Kas teil on olemas sihtotstarbeline eelarve küberkuritegevusega tegelevatele üksustele?	1	Kas kogute eraldi statistikat küberkuritegevuse kohta, nt operatiivstatistikat, küberkuritegevuse suundumuste statistikat, küberkuritegevuse tulu ja tekitatud kahju statistikat jne?	1	Kas osalete kuritegevuse tõkestamiseks rahvusvahelise tasandi kooskõlastatud tegevustes, näiteks kuritegelikesse häkkimisfoorumitesse, organiseeritud küberkuritegevuse rühmitustesse ja pimeveebi turgudele infiltreerumine ja robotivõrkude mahavõtmisel osalemine vms?	1
	3	Kas teie riik on allkirjastanud Euroopa Nõukogu Budapesti küberkuritegevuse konventsiooni?	1	Kas teil on kehtestatud õigussätteid, mis käsitlevad intellektuaalomandi ja autoriõiguste rikkumisi veebis?	1	Kas olete asutanud keskse asutuse/üksuse, mis koordineerib tegevust küberkuritegevuse vastase võitluse valdkonnas?	1	Kas hindate õiguskaitseasutuste, kohtute ja küberturbeintsidentide lahendamise riiklike üksuste töötajatele küberkuritegevuse vastase koolituse piisavust?	1	Kas küberturbeintsidentide lahendamise üksuste, õiguskaitseasutuste ja kohtute (prokurörid ja kohtunikud) ülesanded on küberkuritegevusega seotud koostöö tegemisel selgelt eraldatud?	1
	4			Kas teil on kehtestatud õigussätteid, mis käsitlevad ahistamist veebis või küberkiusamist?	1	Kas olete loonud koostöömehhanisme küberkuritegevuse vastases võitluses osalevate asjaomaste riiklike asutuste vahel, sealhulgas õiguskaitseasutuste ja riiklike küberturbeintsidentide lahendamise üksuste vahel?	1	Kas teete regulaarseid hindamisi, et tagada õiguskaitseasutuste küberkuritegevusüksustele piisavate ressursside (inimesed, eelarve ja vahendid) olemasolu?	1	Kas teie õigusraamistik hõlbustab koostööd küberturbeintsidentide lahendamise üksuste / õiguskaitseasutuste ning kohtute (prokurörid ja kohtunikud) vahel?	1

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
12 – Küberkuritegevuse käsitlemine	5			Kas teil on kehtestatud õigussätteid, mis käsitlevad arvutipettusi, näiteks kooskõlas Euroopa Nõukogu Budapesti küberkuritegevuse konventsiooniga?	1	Kas teete küberkuritegevuse vastase võitluse valdkonnas teiste liikmesriikidega koostööd ja jagate nendega teavet?	1	Kas teete regulaarseid hindamisi, et tagada on prokuratuuri küberkuritegevusüksustele piisavate ressursside (inimesed, eelarve ja vahendid) olemasolu?	1	Kas osalete ELi sidusrühmadega (õiguskaitseasutused, küberturbeintsidentide lahendamise üksused, ENISA, Europoli EC3 jne) jagatavate standardsete vahendite ja metoodikate, vormide ning menetluste väljatöötamisel ja haldamisel?	1
	6	-		Kas teil on kehtestatud õigussätteid, mis käsitlevad laste kaitset veebis, nt direktiivi 2011/93/EL ja Euroopa Nõukogu Budapesti küberkuritegevuse konventsiooni sätete kohaselt?	1	Kas teete küberkuritegevuse vastase võitluse valdkonnas koostööd ELi asutustega (nt Europoli EC3, Eurojusti, ENISAga) ja jagate nendega teavet?	1	Kas teil on küberkuritegevuse kohtuasjade menetlemiseks eraldi kohtuasutused või kohtunikud?	1	Kas olete kehtestanud tipptasemel mehhanisme, mis heidutavad inimesi küberkuritegevuse vastu huvi tundmast või selles osalemast?	0
	7	-		Kas olete nimetanud operatiivse riikliku kontaktpunkti, et vahetada teavet ja vastata teiste liikmesriikide kiireloomulistele päringutele seoses õigusrikkumistega, mis on sätestatud direktiivis 2013/40/EL (infosüsteemide vastu suunatud ründeid käsitlev direktiiv)?	1	Kas teil on olemas piisavad vahendid küberkuritegevuse käsitlemiseks (näiteks küberkuritegevuse taksonoomia ja klassifikatsioon, elektrooniliste tõendite kogumise vahendid, arvutikriminalistika, usaldusväärsed jagamisplatvormid jne)?	1	Kas olete kehtestanud mis tahes meetmeid, mis on suunatud küberkuritegevuse ohvrite (tavakasutajad, VKEd, suurettevõtted) toetamisele ja abistamisele?	1	Kas teie riigis kasutatakse ELi tegevuskava ja/või õiguskaitsealast hädaolukordadele reageerimise protokolli (EU LE ERP), et reageerida efektiivselt ulatuslikele küberintsidentidele?	0
	8			Kas teie õiguskaitseasutuses on spetsiaalne küberkuritegevuse üksus?	1	Kas teil on elektrooniliste tõendite käsitlemiseks olemas standardne töökord?	1	Kas olete küberrünnetele reageerimiseks loonud asutustevahelise raamistiku ja koostöömehhanismid kõigi asjaomaste sidusrühmade vahel (nt õiguskaitseasutused, riiklikud küberturbeintsidentide lahendamise üksused, kohtuasutused), koos erasektoriga, kui asjakohane (nt oluliste teenuste operaatorid, teenuseosutajad)?	1	-	
	9			Kas olete küberkuritegevuse konventsiooni artikli 35 kohaselt määranud ööpäev läbi kättesaadava kontaktpunkti?	1	Kas teie riik osaleb ELi asutuste (nt Europol, Eurojust, OLAF, Cepol, ENISA) pakutavates ja/või toetatavates koolitusvõimalustes?	0	Kas teie õigusraamistik toetab küberturbeintsidentide lahendamise üksuste ja õiguskaitseasutuste koostööd?	1	-	

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
12 – Küberkuritegevuse käsitlemine	10	-		Kas olete ulatuslikele küberrünnetele reageerimiseks määranud kogu ööpäeva kättesaadava operatiivse riikliku kontaktpunkti ELi õiguskaitsealase hädaolukordadele reageerimise protokolli (EU LE ERP) jaoks?	1	Kas teie riik kaalutleb Euroopa Nõukogu küberkuritegevuse konventsiooni 2. lisaprotokolli vastuvõtmist?	0	Kas teil on kasutusel mehhanismid (nt vahendid, menetlused), millega toetada küberkuritegevuse vastase võitluse valdkonnas teabevahetust ja koostööd küberturbeintsidentide lahendamise üksuste ja õiguskaitse ning potentsiaalselt ka kohtute (prokurörid ja kohtunikud) vahel?	1	-	
	11			Kas pakute küberkuritegevuse vastases võitluses osalevatele sidusrühmadele (õiguskaitseasutused, kohtud, küberturbeintsidentide lahendamise üksused) regulaarselt erikoolitusi, näiteks koolitusi küberruumiga seotud kuritegude registreerimise / nende asjus süüdistuse esitamise kohta, koolitusi elektrooniliste tõendite kogumise ja tervikluse tagamise kohta kogu digitaalse järelevalveahela ja arvutikriminalistika menetluste raames?	1						
	12			Kas teie riik on ratifitseerinud Euroopa Nõukogu Budapesti küberkuritegevuse konventsiooni või sellega ühinenud?	1			-	-	-	
	13	-		Kas teie riik on allkirjastanud ja ratifitseerinud Euroopa Nõukogu Budapesti küberkuritegevuse konventsiooni lisaprotokolli (arvutisüsteemide kaudu sooritatud rassistliku ja ksenofoobse olemusega tegude kriminaliseerimine)?	0	-	-	-		-	
13 – Intsidentidest teatamise mehhanismide loomine	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete seda käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
13 – Intsidentidest teatamise mehhanismide loomine	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						
	1	Kas teil on küberintsidentide jaoks olemas mitteametlikud mehhanismid teabevahetuseks erasektori organisatsioonide ja riiklike ametiasutuste vahel?	1	Kas teil on kasutusel intsidentidest teatamise süsteemid kõigi küberturvalisuse direktiivi II lisas loetletud sektorite jaoks?	1	Kas teil on kehtestatud kohustuslik intsidentidest teatamise süsteem, mis toimib praktikas?	1	Kas teil on kasutusel ühtlustatud menetlus sektoripõhiste intsidentidest teatamise süsteemide jaoks?	1	Kas koostate intsidentide aastaaruandeid?	1
	2	-		Kas olete rakendanud sideteenuste osutajatele kohaldatavaid teavitamise nõudeid kooskõlas direktiivi (EL 2018/1972) artikliga 40? Direktiivi kohaselt peavad liikmesriigid tagama, et üldkasutatavate elektroonilise side võrkude ja üldkasutatavate elektroonilise side teenuste pakkujad teatavad pädevale asutusele ilma põhjendamatu viivituseta igast turbeintsidendist, mis on oluliselt mõjutanud võrkude või teenuste toimimist.	1	Kas on olemas koordineerimis-/koostöömehhanism intsidentidest teatamise kohustuste kohta seoses isikuandmete kaitse üldmääruse, küberturvalisuse direktiivi artikli 40 (varasem artikkel 13a) ja eIDASe määrusega?	1	Kas teil on kehtestatud intsidentidest teatamise süsteem ka muude sektorite jaoks kui need, mis on hõlmatud küberturvalisuse direktiiviga?	1	Kas intsidenditeate saanud üksuses koostatakse küberturvalisuse ülevaatearuandeid või muid analüüse?	1
	3	-		Kas olete vastavalt eIDASe määruse (määrus (EL) nr 910/2014) artiklile 19 rakendanud usaldusteenuse osutajatele kohaldatavat teavitamise kohustust? Artiklis 19 sätestatakse muude nõuete hulgas, et usaldusteenuse osutajad peavad teavitama järelevalveasutust olulistest intsidentidest või rikkumistest.	1	Kas teil on olemas piisavad vahendid, et tagada eri teavituskanalite kaudu jagatud teabe konfidentsiaalsus ja terviklus?	1	Kas mõõdate intsidentidest teatamise menetluste tõhusust (näiteks näitajad intsidentide kohta, millest teatati asjakohaste kanalite kaudu, intsidendist teatamise aeg jne)?	1	-	

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
	4	-		Kas olete vastavalt küberturvalisuse direktiivi artiklile 16 rakendanud digitaalse teenuse osutajatele kohaldatavat teavitamise kohustust? Artiklis 16 sätestatakse, et digitaalse teenuse osutajad peavad teatama pädevale asutusele või riiklikule küberturbeintsidentide lahendamise üksusele põhjendamatu viivituseta igast intsidendist, millel on oluline mõju nende poolt liidus osutatavale III lisas sätestatud teenusele.	1	Kas teil on teatamise soodustamiseks platvorm/vahend?	0	Kas teil on riiklikul tasandil olemas intsidentide liigitamise ja algpõhjuste kategooriate ühtne taksonoomia?	0	-	
	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete seda käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						
	1	Kas olete teinud uuringuid või analüüse, et tuvastada täiustatavad valdkonnad kodanike privaatsuse paremaks kaitsmiseks?	1	Kas riiklik andmekaitseasutus on kaasatud küberturbe probleemvaldkondade käsitlemisse (nt uute küberturbe õigusaktide ja nõuete koostamine, määratletud minimaalsed turbemeetmed)?	1	Kas edendate avaliku ja/või erasektori jaoks turbemeetmete ja lõimitud andmekaitse parimaid tavasid?	1	Kas teete korrapäraseid hindamisi, et tagada andmekaitseasutustele piisavate ressursside (inimesed, eelarve ja vahendid) olemasolu?	1	Kas teil on olemas tehnika uusima arengu seire mehhanismid, et kohandada neile vastavalt asjakohaseid suuniseid ja õigussätteid/-kohustusi?	1
	2	Kas olete töötanud riiklikul tasandil välja õigusliku aluse isikuandmete kaitse üldmääruse (määrus (EL) 2016/679) jõustamiseks, näiteks säilitanud või kehtestanud määruses esitatud nõuete suhtes konkreetsemaid sätteid või piiranguid?	0	-		Kas olete korraldanud selleteemalisi teadlikkuse tõstmise ja koolitusprogramme?	1	Kas julgustate organisatsioone ja ettevõtjaid omandama ISO/IEC 27701:2019 sertifikaadi privaatse teabe haldamise süsteemi (PIMS) kohta?	1	Kas osalete aktiivselt teadus- ja arendustegevuse raames tehtavates algatustes seoses privaatsust soodustavate tehnoloogiatega või edendate neid?	0

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
	3	-		-		Kas kooskõlastate juhtumitest teatamise menetlusprotsesse andmekaitseasutusega?	1	-		-	
	4	-		-		Kas edendate ja toetate infoturbe ja privaatsuse tehniliste standardite väljatöötamist? Kas need on spetsiaalselt kohandatud väikestele ja keskmise suurusega ettevõtjatele (VKE)?	0	-		-	
	5	-		-		Kas teil on olemas praktilised ja laiendatavad suunised, et toetada eri liiki vastutavaid töötlejaid privaatsuse ja andmekaitse õiguslike nõuete ja kohustuste täitmisel?	0	-		-	

4.1.4 4. klaster: koostöö

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
15 – Avaliku ja erasektori partnerluse loomine	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete seda käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						
	1	Kas üldiselt ollakse arusaamisel, et avaliku ja erasektori partnerlus aitab eri vahendite abil (nt ühine huvi küberturbesektori arengu vastu, koostöö asjakohase küberturvalisuse õigusraamistiku loomisel, teadus- ja arendustegevuse edendamine) kaasa küberturvalisuse taseme tõstmisele riigis?	1	Kas teil on olemas avaliku ja erasektori partnerluste loomise riiklik tegevuskava?	1	Kas olete loonud riiklikke avaliku ja erasektori partnerlusi?	1	Kas olete loonud sektoriteüleseid avaliku ja erasektori partnerlusi?	1	Kas suudate kohandada või luua avaliku ja erasektori partnerlusi vastavalt tehnika ja õigusaktide uusimale arengule?	1
	2	-		Kas olete kehtestanud avaliku ja erasektori partnerluste haldamiseks õigusliku või lepingulise aluse (eriõigusaktid, mitteavalikustamise lepingud, intellektuaalomand)?	1	Kas olete loonud sektoripõhiseid avaliku ja erasektori partnerlusi?	1	Kas keskendute olemasolevate avaliku ja erasektori partnerluste korral ka avaliku sektori koostööle avaliku sektori ning erasektori koostööle erasektoriga?	1		
	3	-		–		Kas rahastate avaliku ja erasektori partnerluste loomist?	1	Kas edendate avaliku ja erasektori partnerlusi väikeste ja keskmise suurusega ettevõtjate (VKE) seas?	1	-	

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
15 – Avaliku ja erasektori partnerluse loomine	4	-		–		Kas avaliku ja erasektori partnerlusi juhivad üldiselt avaliku sektori asutused (avaliku sektori kontaktpunkt haldab ja koordineerib avaliku ja erasektori partnerlust, avaliku sektori asutused lepivad eelnevalt kokku, mida soovivad saavutada, avaliku halduse asutused edastavad erasektorile selged suunised oma vajaduste ja piirangute kohta jne)?	1	Kas mõõdate avaliku ja erasektori partnerluste tulemusi?	1	-	
	5	-		–		Kas olete Euroopa Küberturvalisuse Organisatsiooni (ECSO) avaliku ja erasektori lepingulise partnerluse liige?	0	-		-	
	6	-		-		Kas teil on avaliku ja erasektori partnerlusi, mis keskenduvad küberturbeintsidentide lahendamise üksuste tegevustele?	0	-		-	
	7					Kas teil on avaliku ja erasektori partnerlusi, mis keskenduvad elutähtsa teabetaristu kaitse probleemidele?	0				
	8	-		-		Kas teil on avaliku ja erasektori partnerlusi, mis keskenduvad küberteadlikkuse suurendamisele ja oskuste arendamisele?	0	-		-	
16 – Avalik-õiguslike asutuste koostöö institutsionaliseerimine	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete seda käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
	1	Kas teil on mitteametlikke koostöökanaleid avalik-õiguslike asutuste vahel?	1	Kas teil on olemas küberturbele keskenduv riiklik koostöökava, näiteks nõuandekogud, juhtrühmad, foorumid, nõukogud, küberkeskused või eksperdirühmad?	1	Kas koostöökavas osalevad avaliku sektori asutused?	1	Kas olete taganud, et küberturbele keskendunud koostöökanalid on olemas vähemalt järgmiste avaliku sektori asutuste vahel: luureteenistused, riigisisesed õiguskaitseasutused, prokuratuurid, valitsusasutused, riiklikud küberturbeintsidentide lahendamise üksused ja kaitsevägi?	1	Kas avalik-õiguslikele asutustele antakse ühtset miinimumteavet kaardistatud ohtude uusima arengu ja küberturbe olukorrateadlikkuse kohta?	1
	2	-		-		Kas olete loonud teabevahetuseks koostööplatvorme?	1	Kas hindate tõhusa koostöö edendamiseks koostöökavade edukust ja puudusi?	1	-	
16 – Avalik-õiguslike asutuste koostöö institutsionaliseerimine	3	-		-		Kas olete määratlenud koostööplatvormide ulatuse (nt ülesanded ja kohustused, probleemsete valdkondade arv)?	1	-		-	
	4	-		-		Kas korraldate aastakoosolekuid?	1	-		-	
	5	-		-		Kas teil on olemas eri geograafiliste piirkondade pädevate asutuste koostöömehhanismid, näiteks piirkonna turbekorrespondentide võrgustik, küberturbeametnik piirkondlikes majanduskodades jne?	1	-		-	
17 – Osalemine rahvusvahelises koostöös (mitte ainult ELi liikmesriikidega)	a	Kas käsitlete seda eesmärki oma praeguses riiklikus küberturbestrateegias või kavatsete seda käsitleda järgmises väljaandes?	1	Kas on olemas mitteametlikke tavasid või tegevusi, mis aitavad saavutada eesmärki koordineerimata viisil?	1	Kas teil on olemas tegevuskava, mis on ametlikult määratletud ja dokumenteeritud?	1	Kas vaatate oma tegevuskava läbi, et hinnata kava tulemuslikkust?	1	Kas teil on olemas mehhanismid, millega tagatakse, et tegevuskava kohandatakse dünaamiliselt keskkonna arenguga?	1
	b			Kas olete määratlenud oma tegevuskavas eeldatavad tulemused, juhtpõhimõtted või põhitegevused?	1	Kas teie tegevuskavas on esitatud selge ressursside jaotus ja juhtimine?	1	Kas vaatate oma tegevuskava läbi, et tagada selle nõuetekohane prioriseerimine ja optimeerimine?	1		
	c			Kui asjakohane: kas teie tegevuskava rakendatakse ja kas see on piiratud ulatuses juba tõhus?	0						

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
17 – Osalemine rahvusvahelises koostöös (mitte ainult ELi liikmesriikidega)	1	Kas teil on olemas rahvusvaheline kaasamisstrateegia?	1	Kas teil on koostöölepinguid teiste riikidega (kahepoolsed, mitmepoolsed) või partnereid teistes riikides (näiteks teabe jagamiseks, suutlikkuse suurendamiseks, abiks jne)?	1	Kas vahetate teavet strateegilisel tasandil (nt kõrgetasemeline poliitika, riskitaju jne)?	1	Kas teie riigi avalik-õiguslikud küberturbeasutused osalevad rahvusvahelistes koostöökavades?	1	Kas juhite mitmepoolsete kokkulepete raames arutelusid ühel või mitmel teemal?	1
	2	Kas teil on kasutusel mitteametlikud koostöökanalid teiste riikidega?	1	Kas teil on olemas ühtne kontaktpunkt, mis võib täita sidefunktsiooni, et tagada piiriülene koostöö liikmesriikide ametiasutustega (koostöörühmad, küberturbeintsidentide lahendamise üksuste võrgustik jne)?	1	Kas vahetate teavet taktikalisel tasandil (nt ohusubjektide bülletään, teabe jagamise ja analüüsimise keskused, taktikad, tehnikad ja menetlused jne)?	1	Kas hindate regulaarselt rahvusvahelise koostöö algatuste tulemusi?	1	Kas juhite rahvusvaheliste aluslepingute või konventsioonide raames arutelusid ühel või mitmel teemal?	1
	3	Kas riigi juhtivisikud on väljendanud kavatsust osaleda küberturvalisuse rahvusvahelises koostöös?	1	Kas teil on olemas konkreetsed inimesed, kes osalevad rahvusvahelises koostöös?	1	Kas vahetate teavet operatiivtasandil (nt operatiivkoostöö teave, toimuvad intsidendid, turberikke indikaatorid jne)?	1	-		Kas juhite rahvusvahelistes eksperdirühmades arutelusid või läbirääkimisi ühel või mitmel teemal? Näiteks küberruumi stabiilsuse ülemaailmses komisjonis (GCSC), ENISA võrgu- ja infoturbe koostöörühmas, ÜRO infoturbe valitsusekspertide rühmas (GGE) jne.	1
	4	-		-		Kas osalete rahvusvahelistel küberturbeõppustel?	1	-		-	
	5	-		-		Kas osalete rahvusvahelistes suutlikkuse suurendamise algatustes (nt koolitused, oskuste arendamine, standardmenetluste koostamine jne)?	0	-		-	
	6	-		-		Kas olete sõlminud teiste riikidega vastastikuse abi lepinguid? Näiteks õiguskaitseasutuste tegevus, kohtumenetlused, intsidentidele reageerimise suutlikkuse vastastikkus, küberturbevarade jagamine jne.	0	-		-	

Riikliku küberturbestrateegia eesmärk	#	1. tase	K	2. tase	K	3. tase	K	4. tase	K	5. tase	K
	7	-		-		Kas olete allkirjastanud või ratifitseerinud küberturvalisuse valdkonna rahvusvahelisi lepinguid või konventsioone (nt rahvusvaheline käitumisjuhend küberturvalisuse valdkonnas, küberkuritegevuse konventsioon)?	0	-		-	

4.2 RAAMISTIKU KASUTAMISE SUUNISED

Selle peatüki eesmärk on tutvustada liikmesriikidele suuniseid ja soovitusi raamistiku kasutuselevõtuks ja küsimustiku täitmiseks. Alljärgnevad soovitused põhinevad peamiselt liikmesriikide esindajatega peetud intervjuude tagasisidel.

- **Valmistuge andmete kogumise ja konsolideerimise koordineerimistegevusteks.** Enamik liikmesriike mõistab, et sellise enesehindamismenetlus kestab ligikaudu 15 inimtööpäeva. Enesehindamise tegemisel tuleb kaasata paljusid sidusrühmi. Seega on soovitatav määrata ettevalmistavaks etapiks piisavalt aega, et tuvastada kõik asjaomased sidusrühmad valitsusasutustes, avalik-õiguslikes asutustes ja erasektoris.
- **Tuvastage keskasutus, kes vastutab enesehindamise valmimise eest riiklikul tasandil.** Et riikide suutlikkuse hindamise raamistiku kõigi näitajate kohta andmete kogumisel võib osaleda arvukalt sidusrühmi, on soovitatav keskorgani või -asutuse olemasolu, kelle ülesandeks on enesehindamise valmimine kõigi asjaomaste sidusrühmadega suheldes ja nende tegevust koordineerides.
- **Kasutage hindamismenetlust kui võimalust vahetada küberturbeteemadel teavet ja suhelda.** Liikmesriikide jagatud kogemused näitasid, et arutelud (individuaalsete intervjuude või ühisseminaridena) on hea viis edendada dialoogi küberturbe teemadel ning jagada ühiseid vaateid ja pöörata tähelepanu täiustatavatele valdkondadele. Lisaks sellele, et tulemuste jagamine aitab esile tõsta olulisi saavutusi, võib see edendada ka küberturbeteemasid.
- **Kasutage hindamise objektiks olevate eesmärkide valimisel riiklikku küberturbestrateegiat.** Riikide suutlikkuse hindamise raamistiku 17 eesmärgi väljatöötamisel lähtuti liikmesriikide riiklikes küberturbestrateegiates sageli käsitletud eesmärkidest. Riiklikes küberturbestrateegiates käsitletavaid eesmärke tuleks kasutada hindamise objektide valimise vahendina. Riiklik küberturbestrateegia ei tohiks hindamist siiski piirata. Et riiklik küberturbestrateegia keskendub loomulikult prioriteetidele, on ei hõlma strateegia sihilikult teatud valdkondi. Samas ei tähenda see, et teatud suutlikkust ei võiks esineda. Näiteks kui teatud eesmärk puudub riiklikus küberturbestrateegias, kuid riigil on selle eesmärgiga seoses olemas küberturbesuutlikkus, võib seda eesmärki hinnata.
- **Riikliku küberturbestrateegia kohaldamisala muutumisel tagage, et punktisumma tõlgendamine on kooskõlas strateegia muutusega.** Riikliku küberturbestrateegia olelustsükkel on mitmeaastane. Mõne liikmesriigi riiklikku küberturbestrateegiat jõustatakse tavaliselt 3–5 aasta tegevuskavaga, mille kohaldamisala muutub küberturbestrateegia kahe järjestikuse väljaande vahel. Seda silmas pidades tuleb erilist tähelepanu pöörata enesehindamise tulemuste esitamisele küberturbestrateegia kahe väljaande vahel: kohaldamisala muutmine võib mõjutada küpsuse lõplikku punktisummat. Soovitatav on võrrelda strateegiliste eesmärkide kogu ulatuse punkte aastate lõikes (st üldpunkte).

Meeldetuletus punktisumma arvutamise mehhanismi kohta – hõlmavuse näide
Punktisumma arvutamise mehhanism koosneb kahest punktide tasandist:
(i) **üldine põhihõlmavus** põhineb enesehindamise raamistiku kõigil strateegilistel eesmärkidel;
(ii) **üldine erihõlmavus** põhineb liikmesriigi valitud strateegilistel eesmärkidel (tavaliselt vastavalt riigi küberturbestrateegia eesmärkidele).

Olemuselt (punktisumma arvutamise mehhanism: vt punkt 3.1) on üldine erihõlmavus suurem või võrdne kui üldine põhihõlmavus, sest viimane võib hõlmata eesmärke, mida liikmesriik ei käsitle ning mis seepärast vähendavad üldist põhihõlmavust. Kui liikmesriik lisab uue eesmärgi, suureneb üldhõlmavus (hõlmatud on rohkem küpsusnäitajaid), kuid üldine eriküpsus võib väheneda (kui uus lisatud eesmärk on algetapis ja seega madala küpsustasemega).

- **Enesehindamise küsimustiku täitmisel pidage meeles, et peamine eesmärk on toetada liikmesriike küberturbesuutlikkuse suurendamisel.** Seepärast soovitatakse enesehindamisel valida vastus, millega nõustutakse kõige rohkem, isegi kui mõnikord on konkreetselt vastata keerukas. Kui vastus küsimusele on teatud ulatuses „JAH“, kuid teises ulatuses „EI“, peaksid liikmesriigid arvestama, et eitava vastuse korral on vaja meetmeid: kas parandusmeetmete kava või kavatsust panustada täiustatavasse valdkonda, mida arvestada edasise arengu korral.

5. JÄRGMISED SAMMUD

5.1 TULEVASED TÄIUSTUSED

Liikmesriikide esindajate küsitlemisel ja dokumentide analüüsi etapis tuvastati võimaliku edasise arenguna ka järgmised soovitused praeguse riikide suutlikkuse hindamise raamistiku täiustamiseks.

- **Arendada hindamissüsteemi, et saavutada suurem täpsus.** Näiteks saab binaarsete JAH/EI-vastuste asemel rakendada hõlmavusprotsenti, millega saab paremini arvestada suutlikkuse konsolideerimise keerukust riigi tasandil. Esimese sammuna valiti JAH/EI-vastustega lihtne lähenemisviis.
- **Võtta kasutusele kvantitatiivsed näitajad, et mõõta liikmesriikide küberturbestrateegiate tõhusust.** Riikide suutlikkuse hindamise raamistik keskendub liikmesriikide küberturbesuutlikkuse küpsustaseme hindamisele. Seda saab täiendada näitajatega, millega mõõta liikmesriikide poolt nende suutlikkuse arendamiseks rakendatud tegevuste ja tegevuskavade tõhusust. Praeguses etapis ei tundunud selliste tõhususnäitajate lisamine realistlik järgmistel põhjustel: vähe tagasisidet kasutajatelt; keeruline on leida asjakohaseid näitajaid, mis seovad väljundi riikliku küberturbestrateegia rakendamisega; raske on välja töötada realistlikke näitajaid, mida saab hiljem koguda. Seda teemat võidakse siiski käsitleda tulevikus.
- **Üleminek enesehindamismenetluselt hindamispõhisele lähenemisviisile.** Raamistiku võimalik tulevane areng võib olla üleminek hindamispõhisele lähenemisviisile, millega hinnata liikmesriikide küberturbesuutlikkuse küpsust järjepidevamalt. Kolmanda isiku tehtav hindamine võib minimeerida võimalikku erapoolikust.

A LISA. DOKUMENTIDE ANALÜÜSI TULEMUSTE ÜLEVAADE

A lisas on kokkuvõte ENISA varasemast tegevusest riiklike küberturbestrateegiatega ja ülevaade avalikult kättesaadavatest küberturbesuutlikkuse küpsuse mudelitest. Mudelite valimisel ja läbivaatamisel arvestatakse järgmisi eeldusi.

- Kõik mudelid ei põhine rangel uurimismetoodikal.
- Mudelite ülesehitust ja tulemusi ei selgitata alati põhjalikult, selgitades iga mudelit iseloomustavate elementide seoseid.
- Mõni mudel ei sisalda arendamise, ülesehituse ja hindamismetoodika üksikasju.
- Mõni meie leitud mudel ja vahend ei sisalda üldse ülesehituse ja sisu üksikasju ning neid ei ole seega loetletud.
- Ülevaate mudelite valik põhineb geograafilisel ulatusel. Põhitähelepanu pööratakse küberturbesuutlikkuse küpsuse mudelitele, mis on koostatud Euroopa riikide tulemuslikkuse hindamiseks. Geograafilist ulatust on siiski oluline laiendada, et analüüsida küpsusmudelite koostamise häid tavasid kogu maailmas.

See asjakohaste avalikult kättesaadavate küberturbesuutlikkuse küpsuse mudelite süstemaatiline ülevaade koostati kohandatud analüüsiraamistiku abil, mis põhines Beckeri määratletud küpsusmudelite arendamise meetoditel[22]. Iga olemasoleva küpsusmudeli korral analüüsiti järgmisi elemente.

- **Küpsusmudeli nimetus:** küpsusmudeli nimetus ja peamised viited.
- **Asutus:** mudeli väljatöötamise eest vastutav avalik-õiguslik või eraõiguslik asutus.
- **Üldeesmärk ja sihtrühm:** mudeli üldine kohaldamisala ja eeldatav sihtrühm (eeldatavad sihtrühmad).
- **Tasemete arv ja määratlus:** mudeli küpsustasemete arv ja üldkirjeldus.
- **Atribuutide arv ja nimetus:** küpsusmudeli atribuutide arv ja nimetus. Atribuutide analüüsil on kolm eesmärki:
  - jaotada küpsusmudel kergesti mõistetavateks osadeks;
  - liita mitu atribuuti samale eesmärgile vastavateks atribuutide klastriteks;
  - esitada küpsustaseme subjekti kohta eri vaatenurki.
- **Hindamismeetod:** küpsusmudeli hindamise meetod.
- **Tulemuste esitus:** määrata küpsusmudeli tulemuste visualiseerimise meetod. Selle etapi loogika seisneb selles, et liiga keerukad küpsusmudelid võivad mitte toimida, seepärast peab tulemuste esitamise viis vastama praktilistele vajadustele.

[22] J. Becker, R. Knackstedt, and J. Pöppelbuß, “Developing Maturity Models for IT Management: A Procedure Model and its Application,” Business & Information Systems Engineering, vol. 1, no. 3, pp. 213–222, Jun. 2009.
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Varasem tegevus riiklike küberturbestrateegiatega

ENISA avaldas 2012. aastal varajase tegevuse osana kaks riiklikke küberturbestrateegiaid käsitlevat dokumenti. Esimene oli riikliku küberturbestrateegia arendamise ja rakendamise faasi praktiline juhend[23], mis pakkus välja konkreetsed meetmed riikliku küberturbestrateegia rakendamiseks ning esitas riikliku küberturbestrateegia neljaetapiline olelustsükkel: strateegia arendamine, strateegia rakendamine, strateegia hindamine ja strateegia säilitamine. Teine oli küberturbe tugevdamise riikliku tegevuse suuna määramist käsitlev dokument[24], mis kirjeldas küberturbestrateegiate olukorda ELis ja mujal 2012. aastal ning tegi ettepaneku, et liikmesriigid peaksid määrama oma riiklikes strateegiates sisalduvad ühisteemad ja erinevused.

2014. aastal avaldati esimene ENISA raamistik liikmesriikide riikliku küberturbestrateegia hindamiseks[25]. See raamistik sisaldab riikliku küberturbestrateegia hindamise soovitusi ja häid tavasid, samuti suutlikkuse suurendamise vahendeid (nt tuvastatud eesmärgid, sisendid, väljundid, peamised tulemusnäitajad jne). Neid vahendeid kohandatakse strateegilise planeerimise etapis eri küpsustasemetel olevate riikide erinevate vajadustega. Samal aastal avaldas ENISA veebipõhise riiklike küberturbestrateegiate interaktiivse kaardi[26], mis võimaldab kasutajatel kiiresti tutvuda kõigi liikmesriikide ja EFTA riikide riiklike küberturbestrateegiatega, sealhulgas nende strateegiliste eesmärkide ja rakendamise heade näidetega. Kaart töötati algselt välja riiklike küberturbestrateegiate hoidlana (2014) ja 2018. aastal ajakohastati seda rakendusnäidetega. Alates 2019. aastast toimib kaart teabekeskusena, mis koondab liikmesriikide esitatud andmeid nende tegevuse kohta riikliku küberturbe tõhustamisel.

Riiklike küberturbestrateegiate heade tavade juhendis[27] (2016) loetletakse 15 strateegilist eesmärki. Juhendis analüüsitakse ka iga liikmesriigi küberturbestrateegia rakendamise astet ning tuvastatakse rakendamise lüngad ja probleemid.

2018. aastal avaldas ENISA riiklike küberturbestrateegiate hindamisvahendi[28]. See on interaktiivne enesehindamisvahend, mis aitab liikmesriikidel hinnata oma riikliku küberturbestrateegiaga seotud strateegilisi prioriteete ja eesmärke. Vahend annab lihtsate küsimuste kaudu liikmesriikidele konkreetseid soovitusi iga eesmärgi rakendamiseks. Riiklike küberturbestrateegiate innovatsiooni heade tavade dokumendis[29] (2019) käsitletakse küberturbe ja riikliku küberturbestrateegia innovatsiooni. Dokumendis kirjeldatakse probleeme ja häid tavasid innovatsiooni eri mõõtmete raames, nagu seda tajuvad valdkonna eksperdid. Eesmärk on aidata kavandada tulevasi innovaatilisi strateegilisi eesmärke.

A.1 Riikide küberturbesuutlikkuse küpsusmudel (CMM)

Riikide küberturbesuutlikkuse küpsusmudel (CMM) töötati välja ülemaailmses küberturbesuutlikkuse keskuses (Capacity Centre), mis kuulub Oxfordi Ülikooli all tegutseva Oxford Martini Kooli alla. Suutlikkuskeskuse eesmärk on küberturbesuutlikkuse küpsusmudeli kasutuselevõtu abil suurendada küberturbesuutlikkuse arendamise ulatust ja tõhusust Ühendkuningriigis ja rahvusvahelisel tasandil. See küpsusmudel on suunatud otse riikidele, kes

[23] NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] An evaluation framework for NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] National Cybersecurity Strategies - Interactive Map (ENISA, 2014, ajakohastatud 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Dokumendiga ajakohastatakse 2012. aasta juhendit: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] Riiklike küberturbestrateegiate hindamisvahend (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

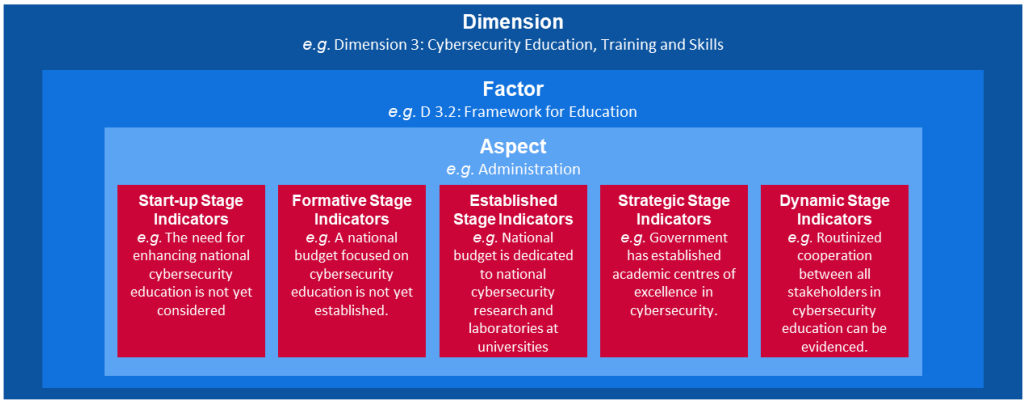
soovivad suurendada oma riiklikku küberturbesuutlikkust. Algselt 2014. aastal kasutusele võetud küberturbesuutlikkuse küpsusmudel vaadati läbi 2016. aastal pärast seda, kui seda kasutati 11 riigi küberturbe suutlikkusnäitajate analüüsil.

Atribuudid/mõõtmed

Küberturbesuutlikkuse küpsusmudeli kohaselt koosneb küberturbesuutlikkus **viiest mõõtmest,** mis moodustavad küberturbesuutlikkuse klastrid. Iga klaster esindab eri uurimissuunda küberturbesuutlikkuse analüüsimisel ja mõistmisel. Viie mõõtme raames kirjeldavad **tegurid** küberturbesuutlikkuse olemasolu üksikasju. Need üksikasjad on elemendid, mis aitavad iga mõõtme korral tõhustada küberturbesuutlikkuse küpsustaset. Igal teguril on mitu **aspekti**, mis esindavad teguri eri komponente. Aspektidena jagunevad näitajad väiksemateks klastriteks, mida on lihtsam mõista. Iga aspekti hinnatakse seejärel **näitajate** abil, et kirjeldada etappe, meetmeid või komponente, mis viitavad konkreetsele küpsustasemele (mis on määratletud järgmises punktis) konkreetse aspekti, teguri või mõõtme raames.

Need terminid võivad olla kihilised, nagu on kujutatud järgmisel joonisel.

Joonis 4. Küberturbesuutlikkuse küpsusmudeli näitajad



Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Mõõde nt 3. mõõde: küberturbeharidus, -koolitus ja -oskused
Factor e.g. D 3.2: Framework for Education	Tegur nt D 3.2: haridusraamistik
Aspect e.g. Administration	Aspekt nt haldus
Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Algetapi näitajad nt riikliku küberturbehariduse tõhustamise vajadust ei ole veel käsitletud
Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Kujundava etapi näitajad nt küberturbeharidusele keskenduvat riiklikku eelarvet ei ole veel määratud
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Rakendamisetapi näitajad nt olemas on riiklik eelarve, mis on suunatud riiklikele küberturbeuuringutele ja -laboritele ülikoolides
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Strateegilise etapi näitajad nt valitsus on loonud küberturbehariduse akadeemilise tippkeskuse
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Dünaamilise etapi näitajad nt kõigi küberturbehariduse sidusrühmade tõendatud regulaarne koostöö

Viie mõõtme kirjeldus on järgmine.

i Küberturbepoliitika ja -strateegia väljatöötamine (6 tegurit)
ii Vastutustundliku küberturbekultuuri edendamine ühiskonnas (5 tegurit)
iii Küberturbeteadmiste arendamine (3 tegurit)
iv Tõhusate õigus- ja regulatiivraamistike loomine (3 tegurit)
v Riskide ohjamine standardite, organisatsioonide ja tehnoloogia abil (7 tegurit)

Küpsustasemed

Küberturbesuutlikkuse küpsusmudelis on **5 küpsustaset**, et määrata riigi olek seoses küberturbesuutlikkuse konkreetse teguri/aspektiga. Need tasemed annavad ülevaate olemasolevast küberturbesuutlikkusest.

- **Algetapp:** selles etapis küberturbeküpsus puudub või on väga algeline. Võivad toimuda esialgsed arutelud küberturbesuutlikkuse suurendamise üle, kuid konkreetseid meetmeid ei ole võetud. Selles etapis puuduvad vaadeldavad tõendid.
- **Kujundav etapp:** aspektide mõnd omadust on hakatud arendama ja sõnastama, kuid see võib olla ajutine, korrapäratu, vähe määratletud või lihtsalt n-ö uudne. Sellise tegevuse kohta on siiski olemas selged tõendid.
- **Rakendamisetapp**. Aspekti elemendid on paigas ja toimivad. Samas ei ole ressursside suhtelist määramist siiski põhjalikult kaalutletud. Seoses n-ö suhteliste investeeringutega aspekti eri elementidesse on tehtud vähe kompromisse. Aspekt siiski toimib ja on määratletud.
- **Strateegiline etapp**. Tehtud on valikuid, mis aspekti osad on konkreetse organisatsiooni või riigi jaoks olulised ja mis vähem olulised. Strateegilises etapis on need valikud tehtud, olenevalt riigi või organisatsiooni olukorrast.
- **Dünaamiline etapp**. Selles etapis on kehtestatud selged mehhanismid strateegia muutmiseks olenevalt asjaoludest, näiteks ohukeskkonna tehnoloogia, ülemaailmse konflikti või olulise muutuse tõttu ühes probleemses valdkonnas (nt küberkuritegevus või privaatsus). Dünaamilised organisatsioonid on välja töötanud strateegiate sujuva muutmise meetodid. Seda etappi iseloomustavad kiire otsustamine, ressursside ümberjaotamine ja muutuva keskkonna pidev jälgimine.

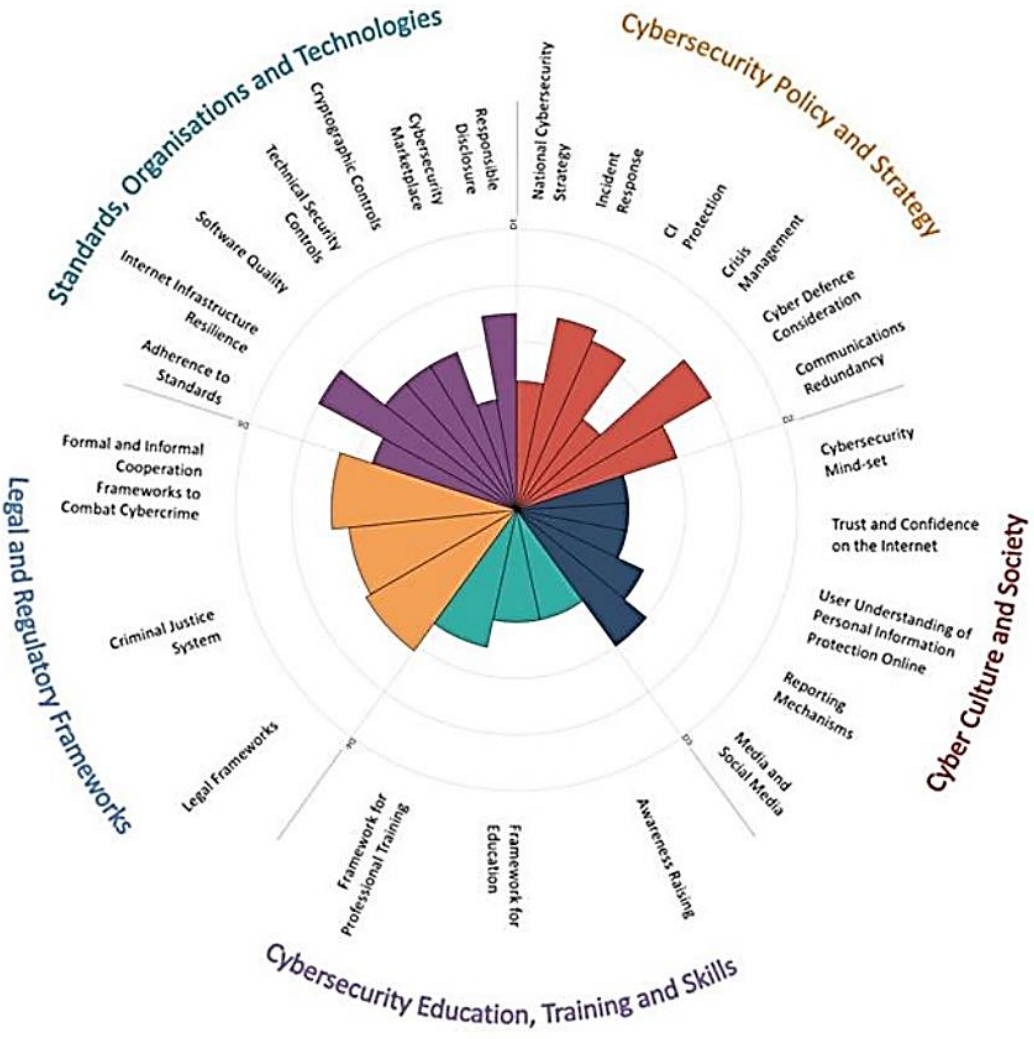
Hindamismeetod

Et suutlikkuskeskusel puudub põhjalik ja üksikasjalik arusaam iga mudelit rakendava riigi sisekontekstist, tehakse koostööd rahvusvaheliste organisatsioonide ning riikide ministeeriumide või organisatsioonidega. Küberturbesuutlikkuse küpsusmudeli viie mõõtme küpsustaseme hindamiseks kohtuvad suutlikkuskeskus ja vastuvõttev organisatsioon 2–3 päeva jooksul avaliku ja erasektori asjaomaste riiklike sidusrühmadega, et pidada küberturbesuutlikkuse küpsusmudeli mõõtmetele keskenduvate sihtrühmade arutelusid. Igat mõõdet arutavad sidusrühmade eri klastrid vähemalt kaks korda. See on aluseks esialgsele andmekogumile edasiseks hindamiseks.

Tulemuste esitusviis

Küberturbesuutlikkuse küpsusmudel annab ülevaate iga riigi küpsustasemest radiaaldiagrammiga, millel on 5-osa (üks osa iga mõõtme kohta). Iga mõõde esindab viiendikku sektordiagrammist, kus iga teguri viis küpsustaset ulatuvad diagrammi keskpunktist väljapoole; nagu allpool näidatud, on „algetapp“ diagrammi keskpunktile kõige lähemal ja „dünaamiline etapp“ sellest kõige kaugemal.

Joonis 5. Küberturbesuutlikkuse küpsusmudel: tulemuste ülevaade



Standards, Organisations and Technologies	Standardid, organisatsioonid ja tehnoloogiad
Legal Regulatory Frameworks	Õigus- ja regulatiivraamistikud
Cybersecurity Education, Training and Skills	Küberturbeharidus, -koolitus ja -oskused
Cybersecurity Policy and Strategy	Küberturbepoliitika ja -strateegia
Cyber Culture and Society	Küberkultuur ja ühiskond
Responsible Disclosure	Vastutustundlik teatamine
Cybersecurity market place	Küberturvalisuse turg
Cryptographic Controls	Krüptograafilised kontrollmehhanismid
Technical Security Controls	Tehnilised turbekontrollid
Software Quality	Tarkvara kvaliteet
Internet Infrastructure Resilience	Internetitaristu kerksus
Adherence to Standards	Standardite järgimine
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Ametlikud ja mitteametlikud küberkuritegevuse vastu võitlemise koostööraamistikud
Criminal Justice System	Kriminaalõigussüsteem
Legal Frameworks	Õigusraamistikud
Framework for Professional Training	Kutsekoolituse raamistik
Framework for Education	Haridusraamistik
Awareness Raising	Teadlikkuse suurendamine
Media and Social Medai	Meedia ja sotsiaalmeedia
Reporting Mechanisms	Aruandlusmehhanismid
User Understanding of Personal Information Protection Online	Kasutaja arusaam isikuandmete kaitsest internetis
Trust and Confidence on the Internet	Usaldus interneti vastu
Cybersecurity Mind-set	Küberturbe mõtteviis
Communications Redundancy	Sidevahendite rohkus
Cyber Defence Consideration	Küberkaitse kaalutlused

Crisis Management	Kriisiohje
CI Protection	Elutähtsa taristu kaitse
Incident Response	Intsidentidele reageerimine
National Cybersecurity Strategy	Riiklik küberturbestrateegia

Ülemaailmse küberturbesuutlikkuse keskus, Oxford Martini Kool, Oxfordi Ülikool, 2017.

A.2 Küberturbesuutlikkuse küpsusmudel (C2M2)

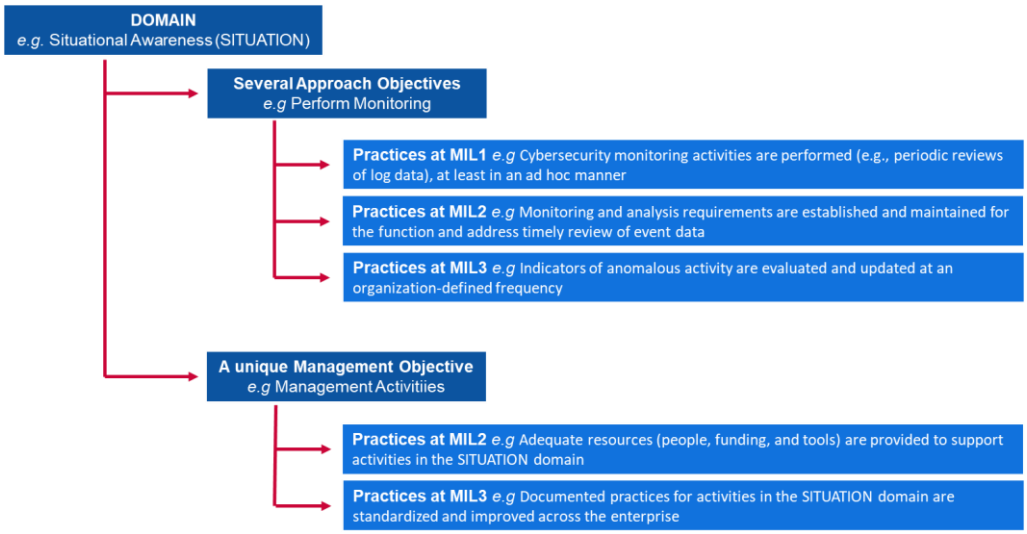
Küberturbesuutlikkuse küpsusmudeli (C2M2) töötas välja USA energeetikaministeerium koostöös erasektori ja avaliku sektori ekspertidega. Suutlikkuskeskuse eesmärk on aidata mis kõigil organisatsioonidel valdkonnast, liigist ja suurusest olenemata hinnata ja täiustada oma küberturbekavu ning tugevdada oma digitaalset tegevuskerksust. Küberturbesuutlikkuse küpsusmudel keskendub selliste küberturbetavade rakendamisele ja haldamisele, mis seonduvad teabe, infotehnoloogia (IT) ja käidutehnoloogia (OT) varadega ja keskkondadega, milles need toimivad. Küberturbesuutlikkuse küpsusmudelis määratletakse küpsusmudelid järgmiselt: „omaduste, atribuutide, näitajate või mustrite kogum, mis kajastab võimekust ja arengut konkreetses valdkonnas“. Algselt 2014. aastal kasutusele võetud küpsusmudel vaadati läbi 2019. aastal.

Atribuudid/mõõtmed

Küberturbesuutlikkuse küpsusmudel koosneb **kümnest valdkonnast**, mis loogiliselt rühmitab küberturbetavad. Iga tavade kogum sisaldab tegevusi, mida organisatsioon saab teha, et luua ja arendada selles valdkonnas oma suutlikkust. Lisaks on iga valdkond seotud **unikaalse halduseesmärgiga** ja **lähenemisviisi mitme eesmärgiga.** Nii lähenemisviisil põhinevate kui ka halduseesmärkide raames kirjeldatakse **mitu tava**, et anda ülevaade institutsionaliseeritud tegevustest.

Nende mõistete seoste kokkuvõte on järgmisel joonisel.

Joonis 6. Küberturbesuutlikkuse küpsusmudeli näitajad



Domain eg Situational Awareness (SITUATION)	**Valdkond**, nt olukorrateadlikkus (OLUKORD)
Several Approaches Objectives e.g. Perform Monitoring	**Mitu lähenemisviisiga seotud eesmärki**, nt järelevalve tegemine
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Tavad tasemel MIL1**, nt küberturbeseire (nt logiandmete korrapärane ülevaatamine) toimub vähemalt ajutiselt
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Tavad tasemel MIL2**, nt seire- ja analüüsinõuded on kehtestatud, neid peetakse toimivuse tagamiseks ja rakendatakse sündmuste andmete õigeaegseks läbivaatuseks

Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency
A unique Management Objectve e.g. Management Activities
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise

Tavad tasemel MIL3, nt anomaalse tegevuse näitajaid hinnatakse ja ajakohastatakse organisatsiooni määratud sagedusega
Unikaalne halduseesmärk, nt haldustegevus
Tavad tasemel MIL2, nt piisavad ressursid (inimesed, rahastus ja vahendid), et toetada OLUKORRA valdkonna tegevusi
Tavad tasemel MIL3, nt dokumenteeritud tavasid OLUKORRA valdkonnas standarditakse ja täiustatakse kogu ettevõttes

Kümme valdkonda on järgmised:

i Riskijuhtimine (RISK)
ii Varade, muutuste ja konfiguratsioonide haldamine (VARAD)
iii Identiteedi ja juurdepääsu haldamine (JUURDEPÄÄS)
iv Ohtude ja haavatavuse haldamine (OHUD)
v Olukorrateadlikkus (OLUKORD)
vi Sündmustele ja intsidentidele reageerimine (REAGEERIMINE)
vii Tarneahela ja väliste sõltuvuste haldamine (SÕLTUVUSED)
viii Personalihaldus (PERSONAL)
ix Küberturbe arhitektuur (ARHITEKTUUR)
x Küberturbekava juhtimine (PROGRAMM)

Küpsustasemed

Küberturbesuutlikkuse küpsusmudel koosneb **neljast küpsustasemest** (MIL0–MIL3), et määrata küpsuse suurenemine kahel tasemel: lähenemisviiside põhjal ja halduslik. Küpsusnäitajate tasemed on vahemikus MIL0–MIL3 ja neid tuleb rakendada iga valdkonna kohta eraldi.

- **MIL0**. Tavad puuduvad.
- **MIL1**. Esialgsed tavad on olemas, kuid need võivad olla ajutised.
- **MIL2**. Haldustunnused:
  - tavad on dokumenteeritud;
  - protsessi toetamiseks on olemas piisavad ressursid;
  - tavasid rakendavatel töötajatel on piisavad oskused ja teadmised;
  - määratud on vastutusalad ja volitused tavade rakendamiseks.

  Lähenemisviisiga seotud tunnused:
  - tavad on täielikumad või arenenumad kui tasemel MIL1.
- **MIL3**. Haldustunnused:
  - tegevusi juhivad poliitikad (või muud organisatsiooni suunised);
  - valdkondlike tegevuste jaoks on olemas tulemuslikkuse eesmärgid, mida jälgitakse nende saavutamise hindamiseks;
  - valdkondlike tegevuste jaoks kasutusel olevad dokumenteeritud tavad on standarditud ja neid täiustatakse kogu ettevõtte ulatuses.

  Lähenemisviisiga seotud tunnused:
  - tavad on täielikumad või arenenumad kui tasemel MIL2.

Hindamismeetod

Küberturbesuutlikkuse küpsusmudel on ette nähtud kasutamiseks koos **enesehindamise metoodika** ja vahendite komplektiga (saadaval taotluse alusel), et organisatsioon saaks hinnata ja täiustada oma küberturbekava. Vahendite komplekti abil saab enesehindamise teha ühe päevaga, kuid täpsemaks hindamiseks saab komplekti kohandada. Lisaks saab küberturbesuutlikkuse küpsusmudelit kasutada uue küberturbekava väljatöötamise alusena.

Mudeli sisu on esitatud kõrgel abstraktsioonitasemel, et seda saaksid tõlgendada organisatsioonid tüübist, struktuurist, suurusest ja valdkonnast olenemata. Mudeli laialdane kasutamine valdkonnas võib toetada valdkonna küberturbesuutlikkuse võrdlusanalüüsi.

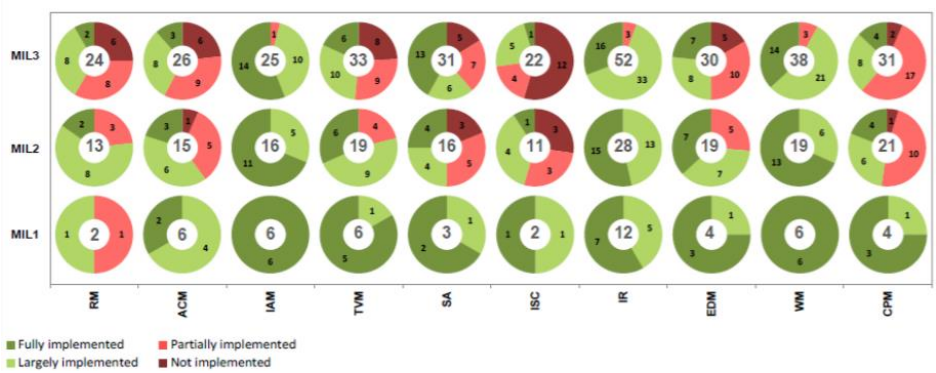
Tulemuste esitusviis

Küberturbesuutlikkuse küpsusmudeli alusel tehtud küsitluse tulemuste põhjal koostatakse hindamisaruanne. Aruandes esitatakse tulemused kahel viisil: eesmärkide kaupa, kus tavade küsimuste vastused on jaotatud valdkonna ja selle eesmärkide kaupa, ja valdkondade kaupa,

kus vastused on kõigi valdkondade ja küpsusnäitajate tasemete kaupa. Mõlema esitusviisiga kasutatakse sektordiagramme (või rõngasdiagramme), üks iga vastuse kohta, ning foorisüsteemiga hindamismehhanismi. Joonisel (Joonis 7) tähistavad rõngasdiagrammi punased sektorid küsimuste arvu, millele vastati „Ei ole rakendatud“ (tumepunane) või „Osaliselt rakendatud“ (helepunane). Rohelised sektorid tähistavad küsimuste arvu, millele vastati „Suures osas rakendatud“ (heleroheline) või „Täielikult rakendatud“ (tumeroheline).

Joonise näide (Joonis 7) kujutab punktisummade kaarti pärast küpsuse hindamist. X-teljel on küberturbesuutlikkuse küpsusmudeli 10 valdkonda ja Y-teljel küpsustasemed (MIL). Joonise riskijuhtimise valdkonnas (RM) on kolm sektordiagrammi, üks iga küpsustaseme jaoks (ML1, ML2, ML3). Riskijuhtimise valdkonna kohta rõhutatakse joonisel, et 1. küpsustaseme (ML1) saavutamiseks tuleb hinnata kaht küsimust. Praegusel juhul on ühele vastatud „Suures osas rakendatud“ ja teisele „Osaliselt rakendatud“. 2. küpsustasemel (ML2) tuleb mudeli järgi hinnata 13 küsimust. 2 küsimust 13st on 1. tasemel (ML1) ja 11 küsimust 2. tasemel (ML2). Sama kehtib ka 3. taseme (ML3) kohta.

Joonis 7. Küberturbesuutlikkuse küpsusmudel – valdkondade vaate näide



Fully implemented	Täielikult rakendatud
Largely implemented	Suures osas rakendatud
Partially implemented	Osaliselt rakendatud
Not implemented	Ei ole rakendatud
MIL1	MIL1
MIL2	MIL2
MIL3	MIL3
RM	RM (RISK)
ACM	ACM (VARAD)
IAM	IAM (JUURDEPÄÄS)
TVM	TVM (OHUD)
SA	SA (OLUKORD)
ISC	ISC (TEABEVAHETUS)
IR	IR (REAGEERIMINE)
EDM	EDM (SÕLTUVUSED)
WM	WM (PERSONAL)
CPM	CPM (PROGRAMM)

Allikas: USA energeetikaministeerium, elektrienergia tarne ja energiakindluse amet, 2015.

A.3 Elutähtsa taristu küberturvalisuse täiustamise raamistik

Elutähtsa taristu küberturvalisuse täiustamise raamistik töötati välja USA riiklikus standardi- ja tehnoloogiainstituudis (NIST). Raamistik keskendub küberturbetegevuse suunamisele ja riskide juhtimisele organisatsioonis. Raamistik on suunatud kõigile organisatsioonidele, olenemata suurusest, küberturberiski tasemest ja küberturbe keerukusest. See on raamistik, mitte mudel, seepärast erineb selle ülesehitus varem analüüsitud mudelite omast.

Raamistik koosneb kolmest osast: raamistiku põhialused, rakendusastmed ja raamprofiilid.

- **Raamistiku põhialus** on küberturbe meetmete, soovitud tulemuste ja kohaldatavate võrdlusaluste kogum, mis on elutähtsa taristu sektoritel ühine. See sarnaneb küberturbesuutlikkuse küpsusmudelites kasutatavate atribuutide või valdkondadega.
- **Raamistiku rakendusastmed** (edaspidi „astmed“) annavad taustteavet, kuidas organisatsioon käsitab küberturberiske ja mis protsessidega seda riski juhitakse. Astmed on vahemikus 1 (osaline) kuni 4 (paindlikkus) ning kirjeldavad järk-järgult rangemaks ja keerukamaks muutuvaid küberturberiskide juhtimise tavasid. Astmed ei kirjelda küpsustaset, pigem on nende eesmärk toetada organisatsioonis otsustamist, kuidas hallata küberturberiske ning mis valdkonnad on organisatsioonis prioriteetsemad ja võiksid saada lisavahendeid.
- **Raamprofiil** (edaspidi „profiil“) kajastab tulemusi, mis põhinevad tegevusvajadustel, mille organisatsioon on valinud raamistiku kategooriate ja alamkategooriate seast. Profiil põhineb standardite, suuniste ja tavade vastavusel raamistiku põhialustega konkreetse rakendusstsenaariumi korral. Profiile saab kasutada riskiseisundi täiustamise võimaluste tuvastamisel, võrreldes selleks praegust profiili (hetkeolukord) sihtprofiiliga (soovitav olukord).

Raamistiku põhialused

Raamistiku põhialused on viis **funktsiooni**. Koos annavad need funktsioonid kõrgetasemelise strateegilise ülevaate organisatsiooni küberturberiskide juhtimise olelustsüklist. Raamistiku põhialus tuvastab iga funktsiooni aluseks olevad põhilised **kategooriad ja alamkategooriad** ning ühitab need informatiivsete võrdlusalustega, näiteks iga alamkategooria olemasolevate standardite, suuniste ja tavadega.

Funktsioonid ja kategooriad on järgmised.

i **Tuvastamine:** töötada välja organisatsiooniline arusaam sellest, kuidas hallata süsteemide, inimeste, varade, andmete ja suutlikkuste küberturberiske.
   - Alamkategooriad: varahaldus; tegevuskeskkond; juhtimine; riskihindamine; riskijuhtimise strateegia.

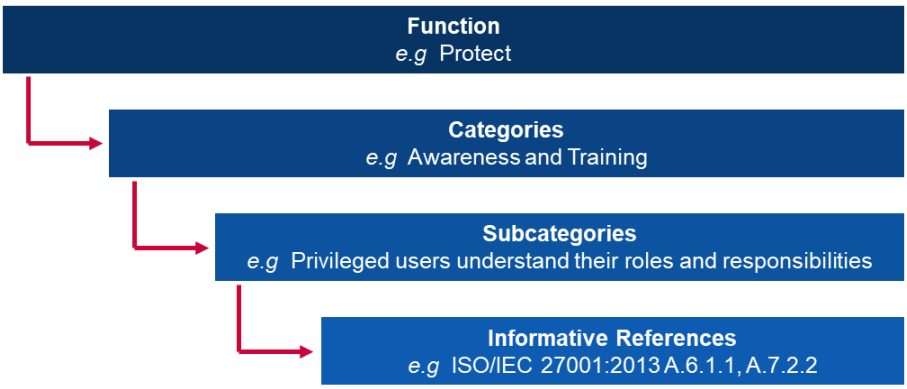
ii **Kaitse:** töötada välja asjakohased kaitsemeetmed elutähtsate teenuste osutamise tagamiseks ning neid rakendada.
   - Alamkategooriad: identiteedihaldus ja juurdepääsukontroll; teadlikkus ja koolitused; andmeturve; teabekaitseprotsessid ja -menetlused; säilitamine; kaitsev tehnoloogia.

iii **Avastamine:** töötada välja asjakohased tegevused küberturbesündmuse tuvastamiseks ja neid rakendada.
   - Alamkategooriad: anomaaliad ja sündmused; pidev turbeseire; avastamisprotsessid.

iv **Reageerimine:** töötada välja asjakohased tuvastatud küberintsidendi korral meetmete võtmise tegevused ja neid rakendada.
   - Alamkategooriad: reageerimise kavandamine; teabevahetus; analüüs; leevendamine; täiustamine.

v **Taastamine:** töötada välja asjakohased tegevused kerksuskavade kasutuselevõtuks ja mis tahes suutlikkuste või teenuste taastamiseks, mis said küberintsidendi tõttu kahjustada, ning neid tegevusi rakendada.
   - Alamkategooriad: taaste kavandamine; täiustamine; teabevahetus.

Joonis 8. Elutähtsa taristu küberturvalisuse täiustamise raamistiku näide



Function e.g Project
Categories e.g Awarness and Training
Subcategories e.g Privileged useres understand their roles and responsibilities
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Funktsioon, nt projekt
Kategooriad, nt teadlikkus ja koolitused
Alamkategooriad, nt volitatud kasutajad mõistavad oma rolle ja kohustusi
Informatiivsed viited, nt ISO/IEC 27001:2013 A.6.1.1, A.7.2.2

Astmed

Elutähtsa taristu küberturvalisuse täiustamise raamistik tugineb **4 astmele**, millest igaüks on määratletud kolmel teljel: riskijuhtimise protsess, lõimitud riskijuhtimisprogramm ja välisosalus. Astmeid ei tohiks käsitada küpsustasemetena, vaid raamistikuna, mis annab organisatsioonide seisukohtadele küberturberiskide ja nende haldamise protsesside konteksti.

- **1. aste: osaline**
  - **Riskijuhtimise protsess**: organisatsiooni küberturberiskide juhtimise tavad ei ole ametlikud, riske juhitakse ajutiselt ja mõnikord reageerivalt.
  - **Lõimitud riskijuhtimisprogramm**: küberturberiskide teadvustamine on organisatsiooni tasandil piiratud. Organisatsioon juhib küberturberiske korrapäratult ja juhtumipõhiselt ning võivad puududa protsessid, millega organisatsioonis jagada küberturbe teavet.
  - **Välisosalus**: organisatsioon ei mõista oma rolli laiemas ökosüsteemis seoses sellega, kellest ta sõltub ja kes sõltub temast. Organisatsioon üldiselt ei teadvusta enda pakutavate ja kasutatavate toodete ning teenuste kübertarneahela riske.
- **2. aste: riskiteadlikkus**
  - **Riskijuhtimise protsess**: juhtkond on heaks kiitnud riskijuhtimise tavad, kuid need ei pruugi olla kehtestatud kogu organisatsiooni hõlmava poliitikana.
  - **Lõimitud riskijuhtimisprogramm**: organisatsiooni tasandil teadvustatakse küberturberiske, kuid ei ole kehtestatud kogu organisatsiooni hõlmavat küberturberiskide juhtimise lähenemisviisi. Organisatsiooni ja väliste varade küberriski hindamine toimub, kuid tüüpiliselt ei ole see korratav ja ega korduv.
  - **Välisosalus**: organisatsioon üldiselt mõistab oma rolli laiemas ökosüsteemis seoses kas sellega, kellest ta sõltub, või sellega, kes sõltub temast, kuid mitte mõlemat. Lisaks teadvustab organisatsioon enda pakutavate ja kasutatavate toodete ning teenuste kübertarneahela riske, kuid ei käsitle neid järjepidevalt ega ametlikult.
- **3. aste: korratavus**
  - **Riskijuhtimise protsess**: organisatsiooni riskijuhtimise tavad on ametlikult heaks kiidetud ja kehtestatud poliitikana. Organisatsiooni küberturbetavasid ajakohastatakse korrapäraselt, lähtudes riskijuhtimise protsessi rakendamisest seoses tegevus-/missiooninõuete ning ohtude ja tehnika muutustega.
  - **Lõimitud riskijuhtimisprogramm**: küberturberiskide juhtimiseks on kasutusel kogu organisatsiooni hõlmav lähenemisviis. Määratletud on riskipõhised poliitikad, protsessid ja menetlused, neid rakendatakse eesmärgipäraselt ja vaadatakse läbi.

Kõrgema juhtkonna esindajad tagavad küberturvalisuse arvestamise organisatsiooni kõigi tegevusliinide kaudu.
    - **Välisosalus**: organisatsioon mõistab laiemas ökosüsteemis oma rolli ning seda, kellest ta sõltub ja kes sõltub temast. Samuti võidakse panustada kogukonna riskiteadlikkuse suurendamisse. Organisatsioon teadvustab enda pakutavate ja kasutatavate toodete ja teenuste kübertarneahela riske.
- **4. aste: kohandatavus**
    - **Riskijuhtimise protsess**: organisatsioon kohandab oma küberturbetavasid, tuginedes varasemale ja praegusele küberturbetegevusele, sealhulgas saadud kogemustele ja prognoosivatele näitajatele.
    - **Lõimitud riskijuhtimisprogramm**: küberturberiskide juhtimiseks on kasutusel kogu organisatsiooni hõlmav lähenemisviis, mis kasutab riskipõhiseid poliitikaid, protsesse ja menetlusi, et käsitleda võimalikke küberturbesündmusi.
    - **Välisosalus**: organisatsioon mõistab laiemas ökosüsteemis oma rolli ning seda, kellest ta sõltub ja kes sõltub temast. Samuti panustatakse kogukonna riskiteadlikkuse suurendamisse.

Hindamismeetod

Elutähtsa taristu küberturvalisuse täiustamise raamistiku eesmärk on võimaldada organisatsioonidel hinnata oma riske ise, et muuta küberturbekäsitlus ja seonduvad investeeringud ratsionaalsemaks, tõhusamaks ja väärtuslikumaks. Investeeringute tõhususe analüüsimiseks peab organisatsioonil olema kõigepealt selge arusaam organisatsiooni eesmärkidest, nende eesmärkide seosest ja toetavatest küberturbetulemustest. Raamistiku põhialustele tuginevad küberturbetulemused toetavad investeeringute tõhususe ja küberturbetegevuste enesehindamist.

A.4 Katari küberturbesuutlikkuse küpsusmudel (Q-C2M2)

Katari küberturbesuutlikkuse küpsusmudel (Q-C2M2) töötati 2018. aastal välja Katari Ülikooli õiguskolledžis. Q-C2M2 põhineb mitmel olemasoleval mudelil ning selle eesmärk on luua põhjalik hindamismetoodika Katari küberturberaamistiku täiustamiseks.

Atribuudid/mõõtmed

Küpsusmudeli aluseks on USA riikliku standardi- ja tehnoloogiainstituudi (NIST) raamistikus esitatud lähenemisviis, mille kohaselt kasutatakse mudeli peamiste valdkondadena viit põhifunktsiooni. Need viis põhifunktsiooni kohalduvad Katari kontekstis, sest need on ühised kõigile elutähtsa taristu sektoritele, mis on Katari küberturberaamistikus oluline element. Katari küberturbesuutlikkuse küpsusmudelis on **viis valdkonda**, iga valdkond jaguneb omakorda mitmeks alamvaldkonnaks, mis hõlmavad kogu küberturbesuutlikkuse küpsuse skaalat.

Viis valdkonda on järgmised.

i **Mõistmise valdkond** koosneb neljast alamvaldkonnast: küberjuhtimine, varad, riskid ja koolitused.
ii **Turvalisuse valdkonna** alamvaldkonnad on andmeturve, tehnoloogiaturve, juurdepääsukontrolli turve, sideturve ja töötajate julgeolek.
iii **Kokkupuute valdkonna**alamvaldkonnad on seire, intsidentide haldamine, avastamine, analüüs ja teatamine.
iv **Reageerimise valdkonna**alamvaldkonnad on reageerimise kavandamine, leevendamine ja reageerimisega seotud teabevahetus.
v **Kestlikkuse valdkonna** alamvaldkonnad on taaste kavandamine, järjepidevuse haldamine, täiustamine ja välissõltuvused.

Küpsustasemed

Q-C2M2 mudelis on **5 küpsustaset,** mis mõõdavad riigiasutuste või valitsusväliste organisatsioonide suutlikkuse taset põhifunktsioonide tasandil. Tasemete eesmärk on hinnata küpsust eelmises punktis kirjeldatud viies valdkonnas.

- **Algatamine:** mõnes valdkonnas on kasutusel ajutised küberturvalisuse tavad ja protsessid.
- **Rakendamine:** vastu on võetud poliitikad kõigi küberturbetegevuste rakendamiseks vastavates valdkondades, eesmärgiga saada rakendamine teatud ajaks valmis.
- **Arendamine:** rakendatud on küberturbetegevuste vastavates valdkondades arendamise ja täiustamise poliitikad ja tavad, eesmärgiga soovitada rakendamiseks uusi tegevusi.
- **Kohandamine:** küberturbetegevused vaadatakse uuesti läbi ning kasutusele võetakse tavad, mis põhinevad varasematest kogemustest ja meetmetest tulenevatel prognoosivatel näitajatel.
- **Paindlikkus**: jätkatakse kohandamisetapi tingimuste täitmist, rõhutades rohkem paindlikkust ja kiirust valdkondades meetmete rakendamisel.

Hindamismeetod

Katari küberturbesuutlikkuse küpsusmudeli uuringud on varajases etapis ja mudel ei ole veel rakendusvalmis. See on raamistik, mis võiks edaspidi olla aluseks Katari organisatsioonide jaoks üksikasjaliku hindamismudeli kasutuselevõtuks.

A.5 Küberturbe küpsustaseme sertifitseerimismudel (CMMC)

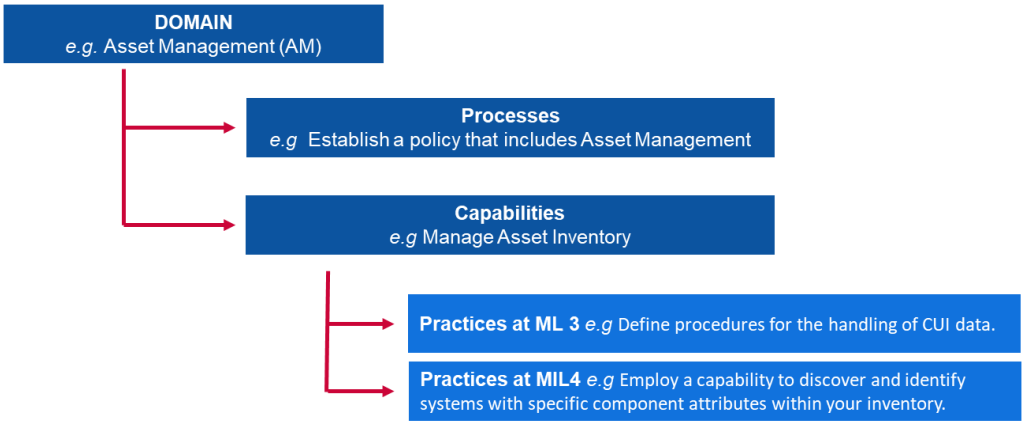
Küberturvalisuse küpsustaseme sertifitseerimismudeli (CMMC) programmi töötas välja USA kaitseministeerium koostöös Carnegie Melloni Ülikooli ja Johns Hopkinsi Ülikooli rakendusfüüsika laboriga. Kaitseministeeriumi peamine eesmärk mudeli väljatöötamisel oli kaitsta kaitsetööstusest pärit teavet. Küberturvalisuse küpsustaseme sertifitseerimismudelis käsitletava teabe klassifikatsioon on kas „föderaalne lepinguline teave“ (teave, mille on esitanud valitsus või mis on valituse jaoks koostatud sellise lepingu alusel ja mida ei avalikustata) või „reguleeritud salastamata teave“ (teave, mis nõuab kaitsemeetmeid või levitamise kontrollmehhanismide, mis vastavad õigusaktidele, nõuetele ja kogu valitsust hõlmavatele poliitikatele ning on nendega kooskõlas). Mudeli abil mõõdetakse küberturvalisuse küpsust ja esitatakse parimad tavad koos sertifitseerimiselemendiga, tagamaks iga küpsustasemega seotud tavade rakendamise. CMMC uusim versioon avaldati 2020. aastal.

Atribuudid/mõõtmed

Küberturvalisuse küpsustaseme sertifitseerimismudel koosneb **17 valdkonnast**, mis koondavad küberturbe protsesside ja suutlikkuste klastreid. Iga valdkond jaguneb omakorda mitmeks **protsessiks**, mis on valdkondade lõikes sarnased, ja üheks või mitmeks **suutlikkuseks**, mida käsitletakse viie küpstaseme raames. Suutlikkus igal asjakohasel küpsustasemel jaguneb üksikasjalikeks **tavadeks**.

Nende mõistete seos on järgmine.

Joonis 9. Küberturvalisuse küpsustaseme sertifitseerimismudeli näitajad



DOMAIN e.g. Asset Management (AM)	**VALDKOND** nt varahaldus (AM)
Processes e.g Establish a policy that includes Asset Management	**Protsessid** nt varahaldust hõlmava poliitika kehtestamine
Capabilities e.g Manage Asset Inventory	**Suutlikkused** nt varade loetelu haldamine
Practices at ML 3 e.g Define procedures for the handling of CUI data	**Tavad tasemel MIL3** nt reguleeritud salastamata teabe käitlemise korra määratlemine
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory	**Tavad tasemel MIL4** nt andmikku kuuluvate spetsiifiliste komponendiatribuutidega süsteemide avastamise ja tuvastamise suutlikkuse kasutamine

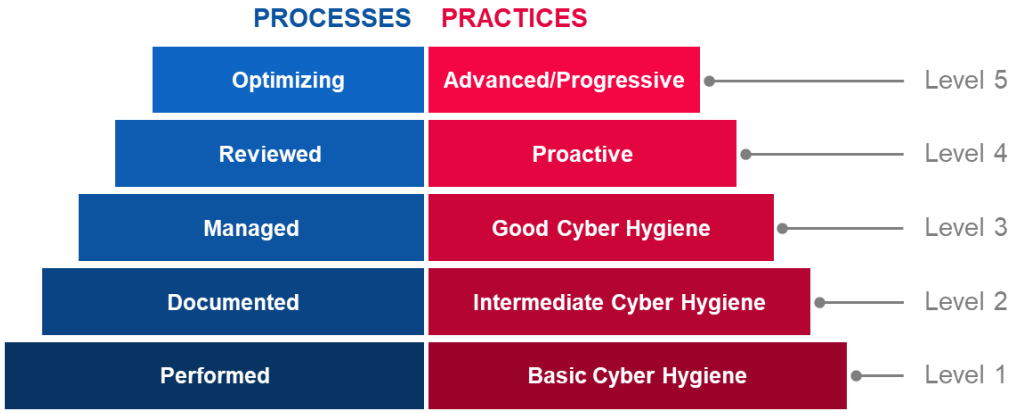
17 valdkonda on järgmised.

i Juurdepääsukontroll (AC)
ii Varahaldus (AM)
iii Auditeerimine ja aruandekohustus (AU)
iv Teadlikkus ja koolitused (AT)
v Konfiguratsioonihaldus (CM)
vi Tuvastamine ja autentimine (IA)
vii Intsidentidele reageerimine (IR)
viii Säilitamine (MA)
ix Andmekandjate kaitse (MP)
x Töötajate julgeolek (PS)
xi Füüsiline kaitse (PE)
xii Taastamine (RE)
xiii Riskijuhtimine (RM)
xiv Turvalisuse hindamine (CA)
xv Olukorrateadlikkus (SA)
xvi Süsteemi ja side kaitse (SC)
xvii Süsteemi- ja teabeterviklus (SI)

Küpsustasemed

Küberturvalisuse küpsustaseme sertifitseerimismudelis on **5 küpsustaset**, mis on määratletud protsesside ja tavade alusel. Küberturvalisuse küpsustaseme sertifitseerimismudeli teatud küpsustaseme saavutamiseks peab organisatsioon täitma selle taseme protsesside ja tavade eeltingimused. See tähendab samuti, et täidetud on ka kõik eeltingimused tasemest allpool.

Joonis 10. Küberturvalisuse küpsustaseme sertifitseerimismudeli küpsustasemed



PROCESSES	PROTSESSID
Optimizing	Optimeerimine
Reviewed	Läbivaatamine
Managed	Juhtimine
Documented	Dokumenteerimine
PRACTICES	TAVAD
Advanced/Progressive	Edasijõudnud/edasiliikuv
Proactive	Proaktiivne
Good Cyber Hygiene	Hea küberhügieen
Intermediate Cyber Hygiene	Keskmine küberhügieen
Basic Cyber Hygiene	Algtasemel küberhügieen
Level 5	5. tase
Level 4	4. tase
Level 3	3. tase
Level 2	2. tase
Level 1	1. tase

- **1. tase**
  - **Protsessid – teostamine**: organisatsioon võib suuta tavasid sooritada üksnes ajutiselt, võib-olla tuginedes dokumenteerimisele. Ei hinnata, kas protsessi küpsustase on 1. tasemel.
  - **Tavad – algtasemel küberhügieen**: 1. tase on seotud föderaalse lepingulise teabe kaitsega ning hõlmab üksnes tavasid, mis vastavad algtasemel kaitsenõuetele.
- **2. tase**
  - **Protsessid – dokumenteerimine**: 2. taseme saavutamiseks on vaja, et organisatsioon kehtestaks ja dokumenteeriks tavad ja poliitikad, millel põhineb organisatsiooni küberturvalisuse küpsustaseme sertifitseerimismudeliga seotud tegevus. Tavade dokumenteerimine võimaldab neid korrata. Organisatsioonid arendavad küpset suutlikkust, dokumenteerides protsesse ja rakendades neid seejärel vastavalt dokumenteeritule.
  - **Tavad – keskmine küberhügieen**: 2. tase on vaheetapp 1. ja 3. taseme vahel ning koosneb standardis NIST SP 800-171 eritletud turbenõuete alamhulgast ning tavadest, mis pärinevad muudest standarditest ja allikatest.
- **3. tase**
  - **Protsessid – juhtimine**: 3. taseme saavutamiseks on vaja, et organisatsioon koostab ja haldab kava, mis tõendab tavade rakendamise juhtimist, ning tagab kavale vajalikud ressursid. Kava võib sisaldada missiooni, eesmärkide, projektikavade, ressursside hankimise, nõutava koolituse ja asjaomaste sidusrühmade kaasamise teavet.
  - **Tavad – hea küberhügieen**: 3. tase keskendub reguleeritud salastamata teabe kaitsele ja hõlmab kõiki standardis NIST SP 800-171 eritletud turbenõudeid ning muudest standarditest ja allikatest pärit täiendavaid ohtude leevendamise tavasid.
- **4. tase**
  - **Protsessid – läbivaatamine**: 4. taseme saavutamiseks on vaja, et organisatsioon vaataks läbi tõhusustavad ja mõõdaks neid. Lisaks tõhusustavade mõõtmisele suudavad selle taseme organisatsioonid võtta vajaduse korral parandusmeetmeid ja teavitada järjepidevalt kõrgema tasandi juhtkonda olukorrast või probleemidest.
  - **Tavad – proaktiivne**: 4. tase keskendub reguleeritud salastamata teabe kaitsele ja hõlmab tõhustatud turbenõuete alamhulka. Need tavad suurendavad organisatsiooni suutlikkust avastada küberintsidente ja neile reageerida, käsitledes muutuvaid taktikaid, tehnikaid ja menetlusi ning kohanedes nendega.
- **5. tase**
  - **Protsessid – optimeerimine**: 5. taseme saavutamiseks on vaja, et organisatsioon standardiks ja optimeeriks protsesside rakendamist kogu organisatsiooni ulatuses.

- **Tavad – edasijõudnud/proaktiivne**: 5. tase keskendub reguleeritud salastamata teabe kaitsele. Täiendavad tavad suurendavad küberturbesuutlikkuse ulatust ja keerukust.

Hindamismeetod

Küberturvalisuse küpsustaseme sertifitseerimismudel on suhteliselt uus mudel, mis valmis 2020. aasta esimeses kvartalis. Seni ei ole seda kasutusele võetud üheski organisatsioonis. USA kaitseministeeriumi töövõtjad loodavad siiski jõuda sertifitseeritud kolmandast isikust audiitoriteni, kes teeksid auditeid. Kaitseministeerium eeldab, et töövõtjad rakendavad küberturvalisuse edendamiseks ja tundliku teabe kaitseks parimaid tavasid.

A.6 Kogukondliku küberturvalisuse küpsusmudel (CCSMM)

Kogukondliku küberturvalisuse küpsusmudeli (CCSMM) töötas välja Texase Ülikooli taristu tagamise ja turbe keskus. Kogukondliku küberturvalisuse küpsusmudeli eesmärk on paremini määratleda meetodid, millega määrata kogukonna praegune kübervalmidus, ning anda kogukondadele ettevalmistusel järgitav tegevuskava. Kogukondliku küberturvalisuse küpsusmudeli sihtrühm on peamiselt kohalikud omavalitsused või osariikide valitsused. Mudel töötati välja 2007. aastal.

Atribuudid/mõõtmed

Küpsustasemed on määratletud **6 põhimõõtme** kaudu, mis hõlmavad küberturvalisuse eri aspekte kogukondades ja organisatsioonides. Need mõõtmed on iga küpsustaseme jaoks selgelt määratletud (üksikasjalik teave: vt Joonis 31. Kogukondliku küberturvalisuse küpsusmudeli). 6 mõõdet on järgmised.

i Käsitletavad ohud
ii Mõõdikud
iii Teabe jagamine
iv Tehnoloogia
v Koolitused
vi Testimine

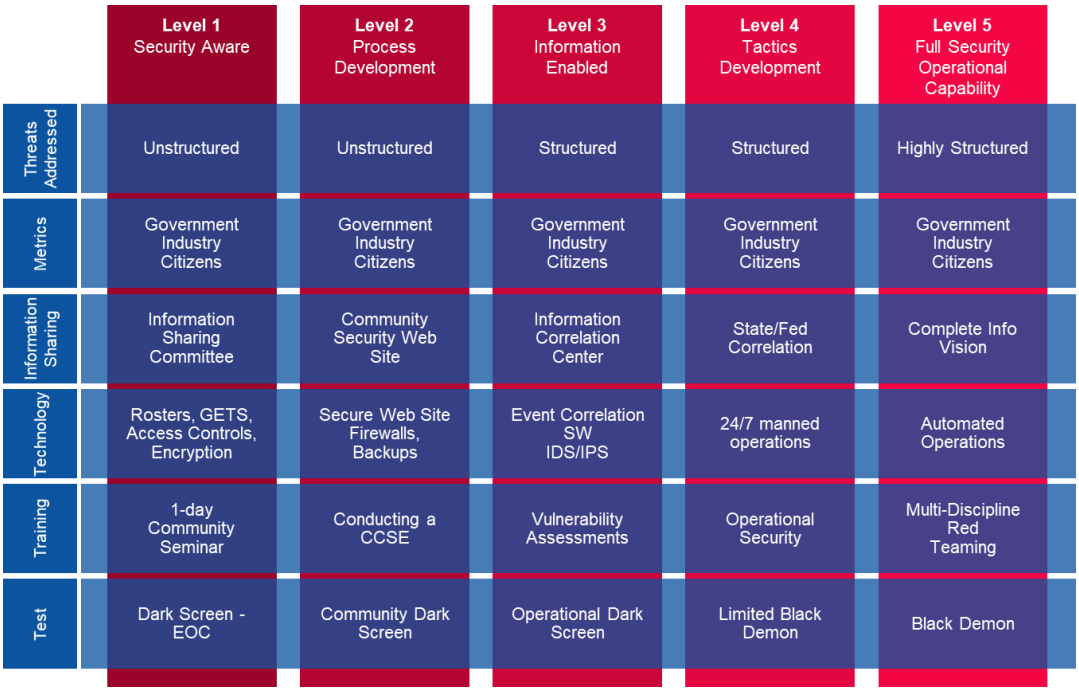
Küpsustasemed

Kogukondliku küberturvalisuse küpsusmudel tugineb **5 küpsustasemele**, mis põhinevad tasandi peamistel ohtudel ja tegevustel.

- **1. tase: turbeteadlikkus**
  Taseme tegevused on peamiselt seotud isikutele ja organisatsioonidele küberturbe ohtude, probleemide ja küsimuste teadvustamisega.
- **2. tase: protsesside arendamine**
  Taseme eesmärk on aidata kogukondadel luua ja täiustada turbeprotsesse, mida on vaja küberturbeprobleemide tõhusaks lahendamiseks.
- **3. tase: tõhus teabejagamine**
  Eesmärk on täiustada kogukonnasiseseid teabejagamise mehhanisme, et kogukond saaks tõhusalt seostada näiliselt eraldi teabeelemente.
- **4. tase: taktika arendamine**
  Tasandi elemendid keskenduvad paremate ja proaktiivsemate meetodite väljatöötamisele, mille abil rünnakuid tuvastada ja neile reageerida. Sellel tasemel peaks enamik ennetusmeetodeid olema juba olemas.

- **5. tase: täielik julgeolekualane operatiivsuutlikkus**
  Tase kajastab elemente, mis peavad olema kehtestatud, et organisatsioon oleks täielikult valmis käsitlema mis tahes liiki küberohte.

Joonis 31. Kogukondliku küberturvalisuse küpsusmudeli mõõtmete kokkuvõte tasemete järgi



Level 1	1. tase
Security Aware	Turbeteadlikkus
Level 2	2. tase
Process Development	Protsesside arendamine
Level 3	3. tase
Information Enabled	Tõhus teabejagamine
Level 4	4. tase
Tactics Development	Taktika arendamine
Level 5	5. tase
Full Security Operational Capability	Täielik julgeolekualane operatiivsuutlikkus
Threats Addressed	Käsitletavad ohud
Metrics	Mõõdikud
Information sharing	Teabe jagamine
Technology	Tehnoloogia
Training	Koolitused
Test	Testimine
Unstructured	Liigendamata
Governement	Valitsus
Industry	Tööstus
Citizens	Kodanikud
Information Sharing Committee	Teabe jagamise komisjon
Rosters, GETS, Assess Controls, Encryption	Nimekirjad, valitsuse hädaolukorra telekommunikatsiooniteenus, juurdepääsukontroll, krüptimine
1-dat Community Seminar	1-päevane kogukonnaseminar
Dark Screen – EOC	Õppus „Dark Screen“ – eriolukordade operatiivkeskus
Unstructured	Liigendamata
Governement	Valitsus
Industry	Tööstus
Citizens	Kodanikud
Community Security Web site	Kogukonnaturbe veebikoht
Secure Web Site Firewalls, Backups	Turvalise veebikoha tulemüürid, varundamine
Conudcting a CCSE	Kontrollpunkti sertifitseeritud turbeekspertide koolituse pidamine
Community Dark Screen	Kogukonnaõppus „Dark Screen“
Structured	Liigendatud

Governement	Valitsus
Industry	Tööstus
Citizens	Kodanikud
Information Correlation Center	Teabekorreleerimiskeskus
Event Correlation SW IDS/IPS	Sündmuste korreleerimise tarkvara (sissetungituvastuse/sissetungitõrje süsteemid)
Vulnerability Assessment	Haavatavuse hindamine
Operational Dark Screen	Operatiivõppus „Dark Screen“
Structured	Liigendatud
Governement	Valitsus
Industry	Tööstus
Citizens	Kodanikud
State/Fed Correlation	Riiklik/föderaalne korrelatsioon
24/7 manned operations	Pidevalt mehitatud operatsioonid
Operational Security	Operatiivjulgeolek
Limited Black Demon	Piiratud õppus „Black Demon“
Highly Structured	Üksikasjalikult liigendatud
Governement	Valitsus
Industry	Tööstus
Citizens	Kodanikud
Complete Info Vision	Täielik teabevisioon
Automated Operations	Automaatoperatsioonid
Multi-Discipline Red Teaming	Valdkondadevahelised punase tiimiga õppused
Black Demon	Black Demon

Hindamismeetod

Kogukondliku küberturvalisuse küpsusmudel on hindamisvahendina suunatud kogukondadele, keda peaksid selles toetama riiklikud ja föderaalsed õiguskaitseasutused. Mudeli eesmärk on aidata kogukonnal määratleda kõige olulisema, kõige tõenäolisemad sihtmärgid ja kaitstava (ning kaitse ulatuse). Nende eesmärkide järgi saab välja töötada kavad, et viia kogukonna iga aspekt nõutavale küberturvalisuse küpsustasemele. Kogukondliku küberturvalisuse küpsusmudeli rakendamisel saadud andmed aitavad määratleda eesmärke mitmesugustel testidel ja õppustel, millega saab mõõta olemasolevate kavade tõhusust.

A.7 NISTi küberturvalisuse raamistiku infoturbe küpsusmudel (ISMM)

Infoturbe küpsusmudel (ISMM) töötati välja Saudi Araabia kuningas Fahdi nimelise Naftakeemia ja Mineraloogia Ülikooli informaatika- ja tehnikakolledžis. See on uus küpsusmudel, millega mõõdetakse küberturbemeetmete rakendamise suutlikkust. Infoturbe küpsusmudeli eesmärk on võimaldada organisatsioonidel mõõta küberturbemeetmete rakendamise kulgu aja jooksul, kasutades sama mõõtevahendit korrapäraselt, et tagada soovitud turbeoleku säilimine. Infoturbe küpsusmudel töötati välja 2017. aastal.

Atribuudid/mõõtmed

Infoturbe küpsusmudel tugineb olemasolevatele hinnatavatele valdkondadele NISTi raamistikus, kuid lisab vastavushindamise mõõtme. Seega koosneb mudel **23 hinnatavast valdkonnast**, mille järgi analüüsitakse organisatsiooni turbeolekut. Hinnatavad 23 valdkonda on järgmised.

i Varahaldus
ii Tegevuskeskkond
iii Juhtimine
iv Riskihindamine
v Riskijuhtimise strateegia
vi Vastavushindamine
vii Juurdepääsukontroll
viii Teadlikkus ja koolitused
ix Andmeturve
x Infokaitseprotsessid ja -menetlused
xi Säilitamine

xii Kaitsetehnoloogia
xiii Anomaaliad ja sündmused
xiv Pidev turbeseire
xv Avastamisprotsessid
xvi Reageerimise kavandamine
xvii Reageerimisega seotud teabevahetus
xviii Reageerimise analüüs
xix Reageerimisega seotud leevendamine
xx Reageerimise täiustamine
xxi Taaste kavandamine
xxii Taastamise täiustamine
xxiii Taastamisega seotud teabevahetus

Küpsustasemed

Infoturbe küpsusmudel koosneb **5 küpsustasemest,** mida kättesaadavates dokumentides kahjuks ei kirjeldata üksikasjalikult.

- **1. tase:** protsesside teostamine
- **2. tase:** protsesside juhtimine
- **3. tase:** protsesside kehtestamine
- **4. tase:** protsesside prognoosimine
- **5. tase:** protsesside optimeerimine

Hindamismeetod

Infoturbe küpsusmudelis ei esitata organisatsioonide hindamise konkreetseid metoodikaid.

A.8 Avaliku sektori siseauditi suutlikkuse mudel (IA-CM)

Siseauditi suutlikkuse mudel (IA-CM) töötati välja Siseaudiitorite Instituudi Teadusuuringute Sihtasutuses eesmärgiga suurendada avalikus sektoris enesehindamise abil suutlikkust ja küberturbe põhimõtete edendamist. Auditispetsialistidele suunatud IA-CM annab mudelist ülevaate koos rakendusjuhendiga, mis aitab mudelit kasutada enesehindamise vahendina.

Kuigi mudel keskendub pigem siseauditite, mitte küberturbesuutlikkuse suurendamisele, on mudel suunatud avaliku sektori asutustele nende küpsustaseme enesehindamiseks ning seda saab protsesside ja tõhususe täiustamiseks rakendada üldiselt. Et kohaldamisala ei keskendu küberturbele, atribuute ei analüüsita. Siseauditi suutlikkuse mudel valmis 2009. aastal.

Küpsustasemed

Siseauditi suutlikkuse mudelis on **5 küpsustaset**, mis kirjeldavad siseaudititega seotud tegevuste omadusi ja suutlikkust igal tasemel. Mudelis sisalduvad suutlikkuse tasemed toetavad pidevat täiustamist.

- **1. tase: Esialgne**
  Puudub kestlik, korratav suutlikkus, sõltutakse üksiktoimingutest.
  - Ajutine või liigendamata.
  - Eraldi üksikauditid või dokumentide ja tehingute läbivaatamine täpsuse ja nõuetele vastavuse tagamiseks.
  - Tulemused sõltuvad ametikohal olija oskustest.
  - Ei ole kehtestatud muid kutsetavasid kui need, mille on kehtestanud kutseühingud.
  - Rahastamise kiidab heaks juhtkond vastavalt vajadusele.
  - Taristu puudub.
  - Audiitorid kuuluvad tõenäoliselt organisatsiooni suuremasse üksusesse.
  - Institutsiooniline suutlikkus on arendamata.
- **2. tase: taristu**
  Kestlikud ja korratavad tavad ja menetlused.
  - 2. taseme korral on põhiküsimus või -probleem, kuidas kehtestada ja säilitada korratavaid protsesse ning seega luua korratav suutlikkus.

- Luuakse siseauditite aruandlussuhteid, juhtimis- ja haldustaristuid ning kutsetavasid ja protsesse (siseauditi suunised, protsessid ja menetlused).
- Auditite kavandamine tugineb peamiselt juhtkonna prioriteetidele.
- Jätkuvalt toetutakse peamiselt konkreetsete isikute oskustele ja pädevustele.
- Osaline vastavus standarditele.

3. tase: lõimimine

Juhtimis- ja kutsetavasid kohaldatakse ühtselt.

- Siseauditite eeskirjad, protsessid ja menetlused on määratletud, dokumenteeritud ning lõimitud omavahel ja organisatsiooni taristuga.
- Siseauditite juhtimis- ja kutsetavad on välja kujunenud ja neid kohaldatakse kogu siseaudititegevuses ühtlaselt.
- Siseauditid hakkavad vastama organisatsiooni tegevusele ja riskidele.
- Siseauditid arenevad üksnes tavapärase siseauditi tegemisest rühmategevuseks, kus antakse nõu tulemuslikkuse ja riskijuhtimise kohta.
- Keskendutakse rühma moodustamisele, siseauditisuutlikkusele, sõltumatusele ja objektiivsusele.
- Üldiselt vastab standarditele.

4. tase: juhtimine

Teave lõimitakse kogu organisatsiooni ulatuses, et täiustada juhtimist ja riskijuhtimist.

- Siseauditi ja peamiste sidusrühmade ootused on vastavuses.
- Kehtestatud on tulemusmõõdikud, et mõõta ja jälgida siseauditi protsesse ja tulemusi.
- Siseauditit peetakse organisatsioonile olulist panust andvaks.
- Siseaudit on organisatsiooni juhtimise ja riskijuhtimise lahutamatu osa.
- Siseaudit on hästi juhitud tegevusüksus.
- Riske mõõdetakse ja juhitakse kvantitatiivselt.
- Olemas on vajalikud oskused ja pädevused ning suutlikkus neid uuendada ja jagada teadmisi (siseauditi raames ja kogu organisatsioonis).

5. tase: optimeerimine

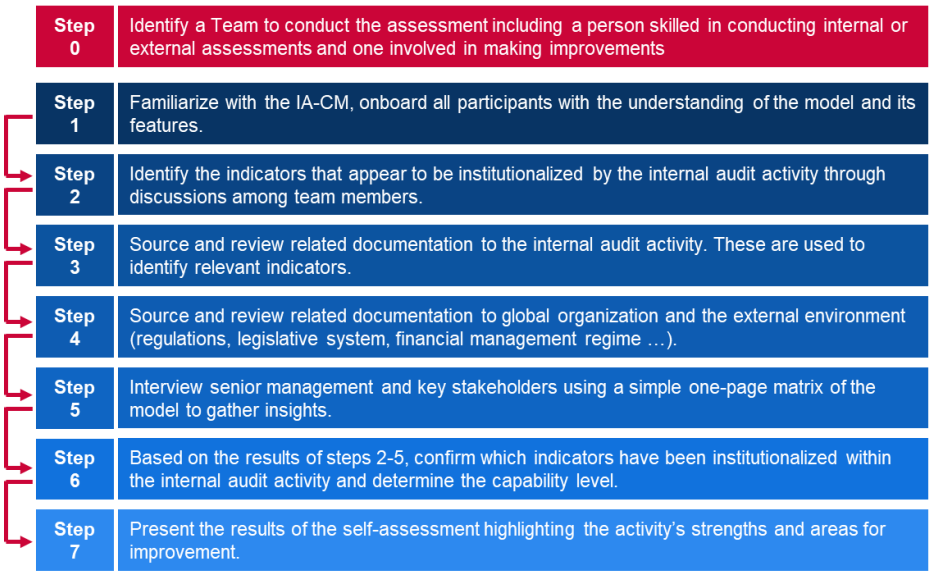
Õppimine organisatsiooni sees ja mujalt, et saavutada pidev areng.

- Siseaudit võimaldab organisatsioonil õppida pidevalt protsesse täiustades ja uuendades.
- Siseauditis kasutatakse organisatsioonisisest ja -välist teavet, et toetada strateegiliste eesmärkide saavutamist.
- Maailmatasemel/soovitatavad/parimad tavad.
- Siseaudit on organisatsiooni juhtimisstruktuuri oluline osa.
- Kõrgetasemelised kutse- ja erioskused.
- Individuaalsed, üksuse ja organisatsiooni tulemuslikkusnäitajad on täielikult lõimitud, et
- tulemuslikkust täiustada.

Hindamismeetod

Siseauditi suutlikkuse mudel on selgelt välja töötatud enesehindamiseks. Selles on mudeli kasutamise üksikasjalikud juhised ja kohandatavad näidisslaidid. Enne enesehindamise algust tuleb tuvastada konkreetne rühm, kuhu kuulub vähemalt üks siseauditite sise- või välishindamiste tegemise oskustega isik ja üks isik, kes osaleb valdkonna täiustamisel.

Joonis 12. Siseauditi suutlikkuse mudeli enesehindamise etapid



Step 0	0. etapp
Step 1	1. etapp
Step 2	2. etapp
Step 3	3. etapp
Step 4	4. etapp
Step 5	5. etapp
Step 6	6. etapp
Step 7	7. etapp
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Tuvastage hindav rühm, kuhu kuulub isik, kes on pädev tegema sise- või välishindamisi, ja isik, kes osaleb täiustamisel.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Tutvuge siseauditi suutlikkuse mudeliga, kaasates kõik osalejad, kes mõistavad mudelit ja selle omadusi.
Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Tuvastage näitajad, mis näivad olevat siseauditiga seotud tegevuste raames institutsionaliseerunud, arutades seda rühmaliikmetega.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Hankige siseauditiga seotud dokumentatsioon ja vaadake dokumendid läbi. Neid kasutatakse asjakohaste näitajate tuvastamisel.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Hankige ja vaadake läbi üldkorralduse ja väliskeskkonnaga seotud dokumentatsioon (nõuded, õigussüsteem, finantsjuhtimise kord jne).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Küsitlege kõrgemat juhtkonda ja peamisi sidusrühmi, kasutades teabe kogumiseks mudeli lihtsat üheleheküljelist maatriksit.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	2.–5. etapi tulemuste alusel kinnitage, mis näitajad on siseauditiga seotud tegevuste raames institutsionaliseerunud ja mis on suutlikkuse tase.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Esitage enesehindamise tulemused, tuues esile tegevuse eelised ja täiustatavad valdkonnad.

A.9 Ülemaailmne küberturvalisuse indeks (GCI)

Ülemaailmne küberturvalisuse indeks (GCI) on Rahvusvahelise Telekommunikatsiooni Liidu (ITU) algatus, mille eesmärk on vaadata läbi küberturbesse panustamine ja olukord kõigis ITU piirkondades (Aafrika, Põhja- ja Lõuna-Ameerika, Araabia riigid, Aasia ja Vaikse ookeani piirkond, SRÜ ja Euroopa) ning tuua esile riike, kes panustavad küberturbesse palju ja kasutavad soovitatavaid tavasid. Ülemaailmse küberturvalisuse indeksi eesmärk on aidata riikidel tuvastada täiustatavad küberturbevaldkonnad ning motiveerida neid võtma meetmeid oma koha parandamiseks paremusjärjestuses, aidates seega tõsta küberturbe üldtaset kogu maailmas.

Et GCI on indeks, mitte küpsusmudel, ei kasuta see küpsustasemeid, vaid punktisummasid riikide ja regioonide küberturbele pühendumise hindamiseks ja võrdlemiseks.

Atribuudid/mõõtmed

Ülemaailmne küberturvalisuse indeks (GCI) põhineb ülemaailmse küberturvalisuse tegevuskava (GCA) viiel sambal. Sambad moodustavad ülemaailmse küberturvalisuse indeksi viis osaindeksit ja igaüks neist sisaldab näitajate kogumit. Viis sammast ja näitajad on järgmised.

i **Juriidiline:** meetmed, mis põhinevad küberturvet ja küberkuritegevust käsitlevate õigusasutuste ja õigusraamistike olemasolul.
- Küberkuritegevust käsitlevad õigusaktid
- Küberturvalisuse nõuded
- Rämpsposti piiramise/vähendamise õigusaktid

ii **Tehniline:** meetmed, mis põhinevad küberturbe tehnikaasutuste ja raamistike olemasolul.
- CERT/CIRT/CSRIT
- Standardite rakendamise raamistik
- Standardiorganisatsioon
- Rämpsposti käsitlemiseks kasutusele võetud tehnilised mehhanismid ja suutlikkused
- Pilve kasutamine küberturvalisuse eesmärgil
- Laste võrgukeskkonnas kaitsmise mehhanismid

iii **Organisatsiooniline:** meetmed, mis põhinevad poliitika koordineerimise asutuste ja küberturvalisuse arendamise strateegiate olemasolul riiklikul tasandil.
- Riiklik küberturbestrateegia
- Vastutav asutus
- Küberturve

iv **Suutlikkuse suurendamine:** meetmed, mille aluseks on teadus- ja arendustegevus, haridus- ja koolitusprogrammid ning sertifitseeritud spetsialistid ja avaliku sektori asutused, kes või mis edendavad suutlikkuse suurendamist.
- Üldsuse teadlikkuse tõstmise kampaaniad
- Küberturvalisuse spetsialistide sertifitseerimise ja akrediteerimise raamistik
- Küberturvalisuse kutsekoolituskursused
- Küberturvalisuse õppekavad koolides ja ülikoolides
- Küberturvalisuse teadus- ja arendustegevuse programmid
- Stimuleerimismehhanismid

v **Koostöö:** partnerlusel, koostööraamistikel ja teabejagamisvõrgustikel põhinevad meetmed.
- Kahepoolsed kokkulepped
- Mitmepoolsed kokkulepped
- Osalemine rahvusvahelistel foorumitel / rahvusvahelistes ühendustes
- Avaliku ja erasektori partnerlused
- Asutustevahelised ja -sisesed partnerlused
- Parimad tavad

Hindamismeetod

Ülemaailmne küberturvalisuse indeks on enesehindamise vahend, mis põhineb binaarsetel, eelkodeeritud ja avatud küsimustega[30] küsitlusel. Binaarsete vastuste kasutamine välistab arvamustel põhineva hindamise ja võimaliku kallutatuse teatud liiki vastuste suunas. Eelkodeeritud vastused säästavad aega ja võimaldavad täpsemat andmeanalüüsi. Lisaks võimaldab lihtne kahetine skaala kiiremat ja keerukamat hindamist, sest ei nõua pikki vastuseid. See kiirendab ja lihtsustab vastamist ja edasist hindamist. Vastaja peab kinnitama ainult teatud eelnimetatud küberturbelahenduste olemasolu või puudumist. Vastuseid kogutakse ja asjakohaseid materjale laaditakse üles veebiküsitlusmehhanismiga, mis võimaldab eksperdirühmal eraldada saadud teabest häid tavasid ja temaatilisi kvalitatiivseid hinnanguid.

Ülemaailmse küberturvalisuse indeksi määramise protsess toimub järgmiselt.

- Kõigile osalejatele saadetakse kutse, milles teavitatakse neid algatusest ja palutakse teatada teabekeskus, kes vastutab kõigi asjakohaste andmete kogumise ja ülemaailmse küberturvalisuse indeksi veebiküsimustiku täitmise eest. Veebiküsitluse toimumise ajal kutsub ITU heakskiidetud teabekeskuse ametlikult küsimustikule vastama.
- Esmane andmete kogumine (riikide korral, kes ei vasta küsimustikule):
  - ITU koostab küsimustiku põhjal esialgse vastuste kavandi, kasutades avalikult kättesaadavaid andmeid ja veebiuuringuid;
  - küsimustiku vastuste kavand saadetakse läbivaatamiseks teabekeskustele;
  - teabekeskused täiustavad andmete täpsust ja tagastavad seejärel kavandi;
  - parandatud küsimustiku vastuste kavand saadetakse lõplikuks heakskiitmiseks uuesti igale teabekeskusele;
  - valideeritud küsimustikku kasutatakse analüüsimiseks, punktide andmiseks ja järjestamiseks.
- Teisene andmete kogumine (küsimustikule vastanud riikide korral):
  - ITU tuvastab puuduvad vastused, tõendavad dokumendid, lingid jne;
  - vajaduse korral suurendab teabekeskus vastuste täpsust;
  - parandatud küsimustiku vastuste kavand saadetakse lõplikuks heakskiitmiseks uuesti igale teabekeskusele;
  - valideeritud küsimustikku kasutatakse analüüsimiseks, punktide andmiseks ja järjestamiseks.

A.10 Kübervõimsuse indeks (CPI)

Kübervõimsuse indeks (CPI) töötati välja Booz Allen Hamiltoni rahastatud Economist Intelligence Uniti uurimisprogrammi raames 2011. aastal. Kübervõimsuse indeks on „dünaamiline kvantitatiivne ja kvalitatiivne mudel, […] mis mõõdab küberkeskkonna eriomadusi kübervõimsuse neljas alusvaldkonnas: õiguslik ja reguleeriv raamistik; majandus- ja sotsiaalkontekst; tehnoloogiataristu ja tööstusrakendused, analüüsides digitaalset arengut peamistel tegevusaladel“[31]. Kübervõimsuse indeksi eesmärk on võrrelda G20 riikide suutlikkust taluda küberründeid ja võtta kasutusele digitaalne taristu, mida on vaja eduka ja turvalise majanduse jaoks. Kübervõimsuse indeksiga esitatud võrdlusalus keskendub 19 G20 riigile (v.a EL). Indeks esitab riikide järjestuse iga näitaja kohta.

Atribuudid/mõõtmed

Kübervõimsuse indeks (CPI) põhineb kübervõimsuse neljal alusvaldkonnal. Iga kategooriat mõõdetakse seejärel mitme näitaja abil, mille tulemusel määratakse igale riigile eripunktisumma. Kategooriad ja sambad on järgmised.

i **Õigus- ja regulatiivraamistik**
- Valitsuse pühendumus küberarengule

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf
[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

- Küberkaitsepoliitika
- Kübertsensuur (või selle puudumine)
- Poliitiline tõhusus
- Intellektuaalomandi kaitse

ii **Majandus- ja sotsiaalkontekst**

- Haridustasemed
- Tehnilised oskused
- Kaubanduse avatus
- Innovatsiooni tase tegevuskeskkonnas

iii **Tehnoloogiataristu**

- Juurdepääs info- ja kommunikatsioonitehnoloogiale
- Info- ja kommunikatsioonitehnoloogia kvaliteet
- Info- ja kommunikatsioonitehnoloogia taskukohasus
- Kulutused infotehnoloogiale
- Turvaliste serverite arv

iv **Tööstusrakendused**

- Nutivõrgud
- E-tervis
- E-kaubandus
- Nutikas transport
- E-riik

Hindamismeetod

Kübervõimsuse indeksi mudel on kvantitatiivne ja kvalitatiivne punktiarvu mudel. Hindamise tegi Economist Intelligence Unit, kasutades kvantitatiivseid näitajaid kättesaadavatest statistilistest allikatest ja andmete puudumisel hinnanguid. Peamised allikad olid järgmised: Economist Intelligence Unit, ÜRO Hariduse, Teaduse ja Kultuuri Organisatsioon (UNESCO), Rahvusvaheline Telekommunikatsiooni Liit (ITU) ja Maailmapank.

A.11 Kübervõimsuse indeks (CPI)

Selles punktis on olemasolevate küpsusmudelite analüüsi põhitulemuste kokkuvõte. Tabel 5. Analüüsitud küpsusmudelite ülevaade annab ülevaate iga mudeli põhiomadustest vastavalt Beckeri mudeli muudetud versioonile. Tabel 6 Küpsustasemete võrdlus käsitleb analüüsitud mudelite küpsustasemete kõrgetasemelisi määratlusi. Tabel 7 annab ülevaate igas mudelis kasutatud mõõtmetest või atribuutidest.

Tabel 5. Analüüsitud küpsusmudelite ülevaade

Mudeli nimetus	Välja töötanud asutus	Eesmärk	Sihtmärk	Tasemete arv	Atribuutide arv	Hindamismeetod	Tulemuste esitus
Riikide küberturbesuutlikkuse küpsusmudel (CMM)	Ülemaailmne küberturbesuutlikkuse keskus Oxfordi Ülikool	Suurendada küberturbesuutlikkuse arendamise ulatust ja tõhusust rahvusvahelisel tasandil	Riigid	5	5 põhimõõdet	Koostöö kohaliku organisatsiooniga mudeli peenhääletamiseks enne selle kohaldamist riigi kontekstis	5-osaline radiaaldiagramm
Küberturbesuutlikkuse küpsusmudel (C2M2)	USA energeetikaministeerium (DOE)	Aidata organisatsioonidel hinnata ja täiustada oma küberturbekavu ning tugevdada oma digitaalset tegevuskerksust	Kõigi sektorite mis tahes liiki ja suurusega organisatsioonid	4	10 põhivaldkonda	Enesehindamise metoodika ja vahendid	Sektordiagrammidega tulemuskaart
Elutähtsa taristu küberturvalisuse täiustamise raamistik	USA riiklik standardi- ja tehnoloogiainstituut (NIST)	Raamistik, mille eesmärk on juhtida organisatsioonides küberturbetegevust ja hallata riske	Organisatsioonid	– (4 astet)	5 põhifunktsiooni	Enesehindamine	-
Katari küberturbesuutlikkuse küpsusmudel (Q-C2M2)	Katari Ülikooli õiguskolledž	Pakkuda toimivat mudelit, millega võrrelda, mõõta ja arendada Katari küberturvalisuse raamistikku	Katari organisatsioonid	5	5 põhivaldkonda	–	-
Küberturbe küpsustaseme sertifitseerimismudel (CMMC)	USA kaitseministeerium (DOD)	Edendada küberturvalisuse parimaid tavasid andmete kaitsmiseks	Kaitsetööstuse organisatsioonid	5	17 põhivaldkonda	Kolmandast isikust audiitorite hinnang	-
Kogukondliku küberturvalisuse küpsusmudel (CCSMM)	Texase Ülikooli taristu tagamise ja turbe keskus	Määrata kogukonna praegune kübervalmidus ning anda kogukondadele ettevalmistusel järgitav tegevuskava	Kogukonnad (kohalikud omavalitsused või osariikide valitsused)	5	6 põhimõõdet	Hindamine kogukondades riiklike ja föderaalsete õiguskaitseasutuste osalusel	-
NISTi küberturvalisuse raamistiku infoturbe küpsusmudel (ISMM)	Informaatika- ja tehnikakolledž Kuningas Fahdi nimeline Naftakeemia ja Mineraloogia Ülikool, Dhahran, Saudi Araabia	Võimaldada organisatsioonidel mõõta küberturbemeetmete rakendamise kulgu aja jooksul, et tagada soovitud turbeoleku säilimine	Organisatsioonid	5	23 hinnatavat valdkonda	–	-
Avaliku sektori siseauditi suutlikkuse mudel (IA-CM)	Siseaudiitorite Instituudi Teadusuuringute Sihtasutus	Suurendada avalikus sektoris enesehindamise abil suutlikkust ja küberturvalisuse põhimõtete edendamist	Avaliku sektori organisatsioonid	5	6 elementi	Enesehindamine	-
Ülemaailmne küberturvalisuse indeks (GCI)	Rahvusvaheline Telekommunikatsiooni Liit (ITU)	Vaadata läbi küberturvalisusesse panustamine ja olukord riikides ning aidata riikidel tuvastada täiustatavad küberturbevaldkonnad	Riigid	–	5 sammast	Enesehindamine	Paremusjärjestus

Kübervõimsuse indeks (CPI)	Economist Intelligence Unit ja Booz Allen Hamilton	Võrrelda G20 riikide suutlikkust taluda küberrünnetega ning võtta kasutusele digitaalne taristu, mida on vaja eduka ja turvalise majanduse jaoks	G20 riigid	–	4 kategooriat	Organisatsiooni Economist Intelligence Unit võrdlusuuring	Paremusjärjestus

Tabel 6 Küpsustasemete võrdlus

Mudel	1. tase	2. tase	3. tase	4. tase	5. tase
Riikide küberturbesuutlikkuse küpsusmudel (CMM)	**Algetapp** Küberturbesuutlikkus puudub või on väga algeline. Võivad toimuda esialgsed arutelud küberturbesuutlikkuse suurendamise üle, kuid konkreetseid meetmeid ei ole võetud. Selles etapis puuduvad vaadeldavad tõendid.	**Kujundav etapp** Aspektide mõnd omadust on hakatud arendama ja sõnastama, kuid see võib olla ajutine, korrapäratu, vähe määratletud või lihtsalt n-ö uudne. Sellise tegevuse kohta on siiski olemas selged tõendid.	**Rakendamisetapp** Aspekti elemendid on paigas ja toimivad. Samas ei ole ressursside suhtelist määramist siiski põhjalikult kaalutletud. Seoses n-ö suhteliste investeeringutega aspekti eri elementidesse on tehtud vähe kompromisse. Aspekt siiski toimib ja on määratletud.	**Strateegiline etapp** Tehtud on valikuid, mis aspekti osad on konkreetse organisatsiooni või riigi jaoks olulised ja mis vähem olulised. Strateegilises etapis on need valikud tehtud, olenevalt riigi või organisatsiooni olukorrast.	**Dünaamiline etapp** Kehtestatud on selged mehhanismid strateegia muutmiseks olenevalt asjaoludest, näiteks ohukeskkonna tehnoloogia, ülemaailmse konflikti või olulise muutuse tõttu ühes probleemses valdkonnas (nt küberkuritegevus või privaatsus). Dünaamilised organisatsioonid on välja töötanud strateegiate sujuva muutmise meetodid. Seda etappi iseloomustavad kiire otsustamine, ressursside ümberjaotamine ja muutuva keskkonna pidev jälgimine.
Küberturbesuutlikkuse küpsusmudel (C2M2)	**MIL0** Tavad puuduvad.	**MIL1** Esialgsed tavad on olemas, kuid need võivad olla ajutised.	**MIL2** Haldustunnused: tavad on dokumenteeritud; protsessi toetamiseks on olemas piisavad ressursid; tavasid rakendavatel töötajatel on piisavad oskused ja teadmised; määratud on vastutusalad ja volitused tavade rakendamiseks. Lähenemisviisiga seotud tunnused: tavad on täielikumad või arenenumad kui tasemel MIL1.	**MIL3** Haldustunnused: tegevusi juhivad poliitikad (või muud organisatsiooni suunised); valdkondlike tegevuste jaoks on olemas tulemuslikkuse eesmärgid, mida jälgitakse nende saavutamise hindamiseks; valdkondlike tegevuste jaoks kasutusel olevad dokumenteeritud tavad on standarditud ja neid täiustatakse kogu ettevõtte ulatuses. Lähenemisviisiga seotud tunnused: tavad on täielikumad või arenenumad kui tasemel MIL2.	–
NISTi küberturvalisuse raamistiku infoturbe	**Protsesside teostamine**	**Protsesside juhtimine**	**Protsesside kehtestamine**	**Protsesside prognoosimine**	**Protsesside optimeerimine**

küpsusmudel (ISMM)					
Katari küberturbesuutlikkuse küpsusmudel (Q-C2M2)	**Algatamine** Mõnes valdkonnas on kasutusel ajutised küberturvalisuse tavad ja protsessid.	**Arendamine** Rakendatud on küberturbetegevuste vastavates valdkondades arendamise ja täiustamise poliitikad ja tavad, eesmärgiga soovitada rakendamiseks uusi tegevusi.	**Rakendamine** Vastu on võetud poliitikad kõigi küberturbetegevuste rakendamiseks vastavates valdkondades, eesmärgiga saada rakendamine teatud ajaks valmis.	**Kohandamine** Küberturbetegevused vaadatakse uuesti läbi ning kasutusele võetakse tavad, mis põhinevad varasematest kogemustest ja meetmetest tulenevatel prognoosivatel näitajatel.	**Paindlikkus** Jätkatakse kohandamisetapi tingimuste täitmist, rõhutades rohkem paindlikkust ja kiirust valdkondades meetmete rakendamisel.
Küberturbe küpsustaseme sertifitseerimismudel (CMMC)	**Protsessid: teostamine** Et organisatsioon võib suuta tavasid rakendada üksnes ajutiselt, võib-olla tuginedes dokumenteerimisele, ei hinnata, kas protsessi küpsustase on 1. tasemel. **Tavad: algtasemel küberhügieen** 1. tase on seotud föderaalse lepingulise teabe kaitsega ning hõlmab üksnes tavasid, mis vastavad algtasemel kaitsenõuetele.	**Protsessid: dokumenteerimine** 2. taseme saavutamiseks on vaja, et organisatsioon kehtestaks ja dokumenteeriks tavad ja poliitikad, millel põhineb organisatsiooni küberturvalisuse küpsustaseme sertifitseerimismudeliga seotud tegevus. Tavade dokumenteerimine võimaldab neid korrata. Organisatsioonid arendavad küpset suutlikkust, dokumenteerides protsesse ja rakendades neid seejärel vastavalt dokumenteeritule. **Tavad: keskmine küberhügieen** 2. tase on vaheetapp 1. ja 3. taseme vahel ning koosneb standardis NIST SP 800-171 eritletud turbenõuete alamhulgast ning tavadest, mis pärinevad muudest standarditest ja allikatest.	**Protsessid: juhtimine** 3. taseme saavutamiseks on vaja, et organisatsioon koostab ja haldab kava, mis tõendab tavade rakendamise juhtimist, ning tagab kavale vajalikud ressursid. Kava võib sisaldada missiooni, eesmärkide, projektikavade, ressursside hankimise, nõutava koolituse ja asjaomaste sidusrühmade kaasamise teavet. **Tavad: hea küberhügieen** 3. tase keskendub reguleeritud salastamata teabe kaitsele ja hõlmab kõiki standardis NIST SP 800-171 eritletud turbenõudeid ning muudest standarditest ja allikatest pärit täiendavaid ohtude leevendamise tavasid.	**Protsessid: läbivaatamine** 4. taseme saavutamiseks on vaja, et organisatsioon vaataks läbi tõhustavad ja mõõdaks neid. Lisaks tõhustavade mõõtmisele suudavad selle taseme organisatsioonid võtta vajaduse korral parandusmeetmeid ja teavitada järjepidevalt kõrgema tasandi juhtkonda olukorrast või probleemidest. **Tavad: proaktiivne** 4. tase keskendub reguleeritud salastamata teabe kaitsele ja hõlmab tõhustatud turbenõuete alamhulka. Need tavad suurendavad organisatsiooni suutlikkust avastada küberintsidente ja neile reageerida, käsitledes muutuvaid taktikaid, tehnikaid ja menetlusi ning kohanedes nendega.	**Protsessid: optimeerimine** 5. taseme saavutamiseks on vaja, et organisatsioon standardiks ja optimeeriks protsesside rakendamist kogu organisatsiooni ulatuses. **Tavad: edasijõudnud/progressiivne** 5. tase keskendub reguleeritud salastamata teabe kaitsele. Täiendavad tavad suurendavad küberturbesuutlikkuse ulatust ja keerukust.
Kogukondliku küberturvalisuse küpsusmudel (CCSMM)	**Turbeteadlikkus** Taseme tegevused on peamiselt seotud isikutele ja organisatsioonidele küberturbe ohtude, probleemide ja küsimuste teadvustamisega.	**Protsesside arendamine** Taseme eesmärk on aidata kogukondadel luua ja täiustada turbeprotsesse, mida on vaja küberturbeprobleemide tõhusaks lahendamiseks.	**Tõhus teabejagamine** Eesmärk on täiustada kogukonnasiseseid teabejagamise mehhanisme, et kogukond saaks tõhusalt seostada näiliselt eraldi teabeelemente.	**Taktika arendamine** Tasandi elemendid keskenduvad paremate ja proaktiivsemate meetodite väljatöötamisele, mille abil rünnakuid tuvastada ja neile reageerida. Sellel tasemel peaks enamik ennetusmeetodeid olema juba olemas.	**Täielik julgeolekualane operatiivsuutlikkus** Tase kajastab elemente, mis peavad olema kehtestatud, et organisatsioon oleks täielikult valmis käsitlema mis tahes liiki küberohte.
Avaliku sektori siseauditi suutlikkuse mudel (IA-CM)	**Esialgne** Puudub kestlik, korratav suutlikkus – sõltutakse üksiktoimingutest	**Taristu** Kestlikud ja korratavad tavad ja menetlused	**Lõimimine** Juhtimis- ja kutsetavasid kohaldatakse ühtselt	**Juhtimine** Teave lõimitakse kogu organisatsiooni ulatuses, et täiustada juhtimist ja riskijuhtimist	**Optimeerimine** Õppimine organisatsiooni sees ja mujalt, et saavutada pidev areng.

Tabel 7. Atribuutide/mõõtmete võrdlus

	Riikide küberturbesuutlikkuse küpsusmudel (CMM)	Küberturbesuutlikkuse küpsusmudel (C2M2)	Katari küberturbesuutlikkuse küpsusmudel (Q-C2M2)	Küberturbe küpsustaseme sertifitseerimismudel (CMMC)	Küberturbe küpsustaseme sertifitseerimismudel (CMMC)	NISTi küberturvalisuse raamistiku infoturbe küpsusmudel (ISMM)	Elutähtsa taristu küberturvalisuse täiustamise raamistik	Ülemaailmne küberturvalisuse indeks (GCI)	Kübervõimsuse indeks (CPI)
Tasemed	5 mõõdet, mis jagunevad mitmeks teguriks, mis omakorda hõlmavad mitut aspekti ja näitajaid (Joonis 4)	10 valdkonda, sealhulgas unikaalne halduseesmärk ja mitu lähenemisviisi eesmärki (Joonis 6)	5 valdkonda, mis jagunevad alamvaldkondadeks	17 valdkonda, mis jagunevad protsessideks ja üheks või mitmeks suutlikkuseks, mis omakorda jagunevad tavadeks (Joonis 9).	6 põhimõõdet	23 hinnatavat valdkonda	5 funktsiooni koos nende aluseks olevate põhiliste kategooriate ja alamkategooriatega (Joonis).	5 sammast koos mitme näitajaga	4 kategooriat koos mitme näitajaga
Atribuudid/ mõõtmed	i Küberturbepoliitika ja -strateegia väljatöötamine ii Vastutustundliku küberturbekultuuri edendamine ühiskonnas iii Küberturbeteadmiste arendamine iv Tõhusate õigus- ja regulatiivraamistike loomine v Riskide ohjamine standardite, organisatsioonide ja tehnoloogia abil	i Riskijuhtimine ii Varade, muutuste ja konfiguratsioonide haldamine iii Identiteedi ja juurdepääsu haldamine iv Ohtude ja haavatavuse haldamine v Olukorrateadlikkus vi Sündmustele ja intsidentidele reageerimine vii Tarneahela ja väliste sõltuvuste haldamine viii Personalihaldus ix Küberturbe arhitektuur x Küberturbekava juhtimine	i Mõistmine (küberjuhtimine, varad, riskid ja koolitused) ii Turvalisus (andmeturve, tehnoloogiaturve, juurdepääsukontrolli turve, sideturve ja töötajate julgeolek) iii Kokkupuude (seire, intsidentide haldamine, avastamine, analüüs ja teatamine) iv Reageerimine (reageerimise kavandamine, leevendamine ja reageerimisega seotud teabevahetus) v Kestlikkus (taaste kavandamine, järjepidevuse haldamine, täiustamine ja välissõltuvused)	i Juurdepääsukontroll ii Varahaldus iii Auditeerimine ja aruandekohustus iv Teadlikkus ja koolitused v Konfiguratsioonihaldus vi Tuvastamine ja autentimine vii Intsidentidele reageerimine viii Säilitamine ix Infokandjate kaitse x Töötajate julgeolek xi Füüsiline kaitse xii Taastamine xiii Riskijuhtimine xiv Turvalisuse hindamine xv Olukorrateadlikkus xvi Süsteemi ja side kaitse xvii Süsteemi- ja teabeterviklus	i Käsitletavad ohud ii Mõõdikud iii Teabe jagamine iv Tehnoloogia v Koolitused vi Testimine	i Varahaldus ii Tegevuskeskkond iii Juhtimine iv Riskihindamine v Riskijuhtimise strateegia vi Vastavushindamine vii Juurdepääsukontroll viii Teadlikkus ja koolitused ix Andmeturve x Infokaitseprotsessid ja -menetlused xi Säilitamine xii Kaitsetehnoloogia xiii Anomaaliad ja sündmused xiv Pidev turbeseire xv Avastamisprotsessid xvi Reageerimise kavandamine xvii Reageerimisega seotud teabevahetus xviii Reageerimise analüüs xix Reageerimisega seotud leevendamine xx Reageerimise täiustamine xxi Taaste kavandamine xxii Taastamise täiustamine xxiii Taastamisega seotud teabevahetus	i Tuvastamine ii Kaitsmine iii Avastamine iv Reageerimine v Taastamine	i Juriidiline ii Tehnoloogiline iii Organisatsiooniline iv Suutlikkuse suurendamine v Koostöö	i Õigus- ja regulatiivraamistik ii Majandus- ja sotsiaalkontekst iii Tehnoloogiataristu iv Tööstusrakendused

B LISA. DOKUMENTIDE ANALÜÜSI KIRJANDUSLOETELU

Almuhammadi, S. and Alsaleh, M. (2017) 'Information Security Maturity Model for Nist Cyber Security Framework', in Computer Science & Information Technology (CS & IT). Sixth International Conference on Information Technology Convergence and Services, Academy & Industry Research Collaboration Center (AIRCC).

Almuhammadi, S. and Alsaleh, M. (2017) 'Information Security Maturity Model for Nist Cyber Security Framework', in Computer Science & Information Technology (CS & IT). Avaldatud aadressil https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. et al. (2016) Stocktaking, analysis and recommendations on the protection of CIIs. Avaldatud aadressil http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:ET:HTML

Becker, J., Knackstedt, R. et al. (2009) Developing Maturity Models for IT Management – A Procedure Model and its Application. Avaldatud aadressil https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Belgia valitsus (2012). Küberturbestrateegia. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Bellasio, J. et al. (2018) Developing Cybersecurity Capacity: A proof-of-concept implementation guide. RAND Corporation. Avaldatud aadressil https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bourgue, R. (2012) 'Introduction to Return on Security Investment'.

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019) "Cybersecurity Capability Maturity Model (C2M2) Version 2.0. Avaldatud aadressil https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center for Security Studies (CSS), ETH Zürich (2019) National Cybersecurity Strategies in Comparison – Challenges for Switzerland. Avaldatud aadressil https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Council of Ministers (2019) Portuguese Official Journal, Series 1 — No. 108 - Resolution of the Council of Ministers No. 92/2019. Avaldatud aadressil https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Creese, S. (2016) Cybersecurity Capacity Maturity Model for Nations (CMM). University of Oxford.

CSIRT Maturity - Self-assessment Tool (dateerimata). Avaldatud aadressil https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Euroopa Nõukogu ja Euroopa Liidu projekt CyberCrime@IPA, Euroopa Nõukogu ja Euroopa Liidu küberkuritegevuse rakkerühma ülemaailmne projekt (2011). Küberkuritegevuse eriüksused – heade tavade uuring. Avaldatud aadressil https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (dateerimata). Avaldatud aadressil https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Darra, E. (2017) Public Private Partnerships (PPP).

Darra, E. (dateerimata) 'Welcome to the NCSS Training Tool'.

Dekker, M. A. C. (2014) Technical Guideline on Incident Reporting. Avaldatud aadressil https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C. (2014) Technical Guideline on Security Measures. Avaldatud aadressil https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Dekker, M. A. C. (2015) Guideline on Threats and Assets. Avaldatud aadressil https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Digital Slovenia (2016). Sloveenia küberturbestrateegia. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. *et al.* (2014) *Privacy and data protection by design - from policy to engineering.* Avaldatud aadressil http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:ET:HTML

Euroopa Komisjon (2012). Euroopa Parlamendi ja nõukogu määrus e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul. Avaldatud aadressil https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52012PC0238&from=ET

Euroopa Võrgu- ja Infoturbeamet (2012). NCSS: Practical Guide on Development and Execution. Heraklion: ENISA.

Euroopa Võrgu- ja Infoturbeamet (2012). NCSS: Setting the course for national efforts to strengthen security in cyberspace. Heraklion: ENISA.

Euroopa Võrgu- ja Infoturbeamet (2016). Guidelines for SMEs on the security of personal data processing.

Euroopa Võrgu- ja Infoturbeamet (2016). NCSS good practice guide: designing and implementing national cyber security strategies. Heraklion: ENISA.

Euroopa Liidu Võrgu- ja Infoturbeamet (2017). Handbook on security of personal data processing. Avaldatud aadressil http://dx.publications.europa.eu/10.2824/569768

Euroopa Liidu Võrgu- ja Infoturbeamet (2014). *ENISA CERT inventory inventory of CERT teams and activities in Europe*. Avaldatud aadressil http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Executive Office Of The President (2015) Memorandum for Heads of Executive Departments and Agencies. Avaldatud aadressil https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Austria Vabariigi liidukantselei (2013). Austria küberturbestrateegia. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-

security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Saksamaa föderaalne siseministeerium (2011). Saksamaa küberturbestrateegia. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en

Ferette, L. (2016) NIS Directive and national (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Avaldatud aadressil http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:ET:HTML

Ferette, L., Euroopa Liidu Võrgu- ja Infoturbeamet (2015). The 2015 report on national and international cyber security exercises: survey, analysis and recommendations. Avaldatud aadressil http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:ET:HTML

Prantsusmaa peaministri büroo (2014). Prantsusmaa riiklik digitaalse julgeoleku strateegia. Avaldatud aadressil https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Galan Manso, C. et al. (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Avaldatud aadressil http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:ET:HTML

Ghent University et al. (2017) 'Evaluating Business Process Maturity Models', Journal of the Association for Information Systems. Avaldatud aadressil https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Bulgaaria valitsus (2015). Riiklik küberturbestrateegia „Cyber-resistant Bulgaria 2020".

Horvaatia valitsus (2015). Horvaatia Vabariigi riiklik küberturbestrateegia. Avaldatud aadressil https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Kreeka valitsus (2017). Riiklik küberturbestrateegia. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Ungari valitsus (2018). Võrgu- ja infosüsteemide turvalisuse strateegia. Avaldatud aadressil https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

Iirimaa valitsus (2019). Riiklik küberturbestrateegia. Avaldatud aadressil https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Hispaania valitsus (2019). Riiklik küberturbestrateegia. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

Institute of Internal Auditors (ed.) (2009) Internal audit capability model (IA-CM) for the public sector: overview and application guide. Altamonte Springs, Fla: Institute of Internal Auditors, Research Foundation.

Rahvusvaheline Telekommunikatsiooni Liit (ITU) (2018). The Global Cybersecurity Index. Avaldatud aadressil https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Rahvusvaheline Telekommunikatsiooni Liit (ITU) (2018). Guide to developing a national cybersecurity strategy. Avaldatud aadressil https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

J.D., R. D. B. (2019) 'Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework', International Review of Law.

Läti valitsus (2014). Läti küberturbestrateegia. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Liveri, D. et al. (2014) An evaluation framework for national cyber security strategies. Heraklion: ENISA. Avaldatud aadressil http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:ET:HTML.

Mattioli, R. *et al.* (2014) *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks.* Avaldatud aadressil http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:ET:HTML

Konkurentsivõime ning digitaal-, merendus- ja teenusmajanduse ministeerium (2016). Malta küberturbestrateegia. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

Majandus- ja Kommunikatsiooniministeerium (2019). Eesti Vabariigi küberturvalisuse strateegia. Avaldatud aadressil https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Leedu Vabariigi kaitseministeerium (2018). Riiklik küberturbestrateegia.

Riiklik küberjulgeoleku keskus (2015). Tšehhi Vabariigi riiklik küberturbestrateegia. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Riiklike küberturbestrateegiate interaktiivne kaart (dateerimata). Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

Riiklike küberturbestrateegiate hindamisvahend (2018). Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

National Institute of Standards and Technology (2018). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. Avaldatud aadressil http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Object Management Group (2008) Business Process Maturity Model. Avaldatud aadressil https://www.omg.org/spec/BPMM/1.0/PDF

OECD, Euroopa Liit ja Teadusuuringute Ühiskeskus – Euroopa Komisjon (2008). Handbook on Constructing Composite Indicators: Methodology and User Guide. OECD. Avaldatud aadressil https://www.oecd.org/sdd/42495745.pdf.

Elektroonilise side ja postieeskirjade voliniku büroo (2012). Küprose Vabariigi küberturbestrateegia.

Euroopa Liidu Teataja (2008). NÕUKOGU 8. detsembri 2008 aasta DIREKTIIV 2008/114/EÜ Euroopa elutähtsate infrastruktuuride identifitseerimise ja määramise ning nende kaitse parandamise vajaduse hindamise kohta. Avaldatud aadressil https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32008L0114&from=ET

Organisation for Economic Co-operation and Development (OECD) (2012). Cybersecurity policy making at a turning point. Avaldatud aadressil http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E. (2012) 'National Cyber Security Strategies - Practical Guide on Development and Execution'.

Ouzounis, E. (2012) Good Practice Guide on National Exercises.

Portesi, S. (2017) Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects

Ministrite nõukogu eesistuja (2017). Itaalia küberturvalisuse tegevuskava. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

Ministrite nõukogu (2019). Poola küberturbestrateegia „Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej“. Avaldatud aadressil http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Rumeenia valitsus (2013). Rumeenia küberturbestrateegia. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Sarri, A., Kyranoudi, P. ja Euroopa Liidu Küberturvalisuse Amet (2019). Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies. Avaldatud aadressil https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Julgeolekukomitee sekretariaat (2019). Soome küberturbestrateegia 2019. Avaldatud aadressil https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Slovakkia valitsus (2015). Slovakkia Vabariigi küberturvalisuse kontseptsioon. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Smith, R. (2015) Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010

Smith, R. (2016) ‘Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010’, in Smith, R., Core EU Legislation. London: Macmillan Education. Avaldatud aadressil https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016L1148&from=ET.

Stavropoulos, V. (2017) European Cyber Security Month 2017.

Rootsi valitsus (2017). Rootsi riiklik küberturbestrateegia „Nationell strategi för samhällets informations- och cybersäkerhet“. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Taani valitsus – rahandusministeerium (2018). Taani küber- ja infoturbe strateegia. Avaldatud aadressil https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Šveitsi föderaalnõukogu (2018). Riiklik strateegia Šveitsi kaitsmiseks küberohtude eest.

Luksemburgi valitsuse nõukogu (2018). Riiklik küberturbestrateegia. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

Madalmaade valitsus (2018). Riiklik küberturvalisuse tegevuskava. Avaldatud aadressil https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

Valge Maja (2018). Ameerika Ühendriikide riiklik küberstrateegia. Avaldatud aadressil https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Trimintzios, P., et al. (2011) Cyber Europe Report. Avaldatud aadressil https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. ja Euroopa Liidu Võrgu- ja Infoturbeamet (2013). *National-level risk assessments: an analysis report.* Avaldatud aadressil http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:ET:HTML

Trimintzios, P., Gavrila, R., et al. (2015) Report on cyber-crisis cooperation and management. Avaldatud aadressil http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:ET:HTML

Trimintzios, P., Ogee, A., et al. (2015) Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises. Avaldatud aadressil http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:ET:HTML

Ühendkuningriigi riiklik küberturbestrateegia 2016–2021 (2016). Avaldatud aadressil https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

University of Innsbruck et al. (2009) Understanding Maturity Models.

Wamala, D. F. (2011) 'ITU National Cybersecurity Strategy Guide. Avaldatud aadressil https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. (2007) 'The Community Cyber Security Maturity Model', in 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)

C LISA. MUUD UURITUD EESMÄRGID

Järgmisi eesmärke uuriti dokumentide analüüsimise etapi ja ENISA korraldatud intervjuude raames. Eesmärgid ei kuulu riikide suutlikkuse hindamise raamistikku, kuid selgitavad käsitlemist väärivaid teemasid. Igas järgmises alapeatükis on selgitatud, miks konkreetne eesmärk kõrvale jäeti.

- Valdkonnaomaste küberturbestrateegiate arendamine
- Väärinfo levitamise kampaaniate vastane tegevus
- Turvalised tipptasemel tehnoloogiad (5G, tehisintellekt, kvantarvutus jt)
- Andmesuveräänsuse tagamine
- Küberkindlustusvaldkonna arendamise stiimulite pakkumine

Valdkonnaomaste küberturbestrateegiate arendamine

Sektorisisestele sekkumistele ja stiimulitele suunatud sektoripõhiste strateegiate kasutusele võtmine tooks kindlasti kaasa suurema detsentraliseeritud suutlikkuse. See sobib eriti hästi liikmesriikidele, kelle oluliste teenuste operaatorid peavad käsitlema mitmesuguseid raamistikke ja nõudeid, ning juhtudel, kus küberturvalisuse valdkonnaülese olemuse tõttu esineb arvukalt sõltuvusi. Mitmes liikmesriigis on tavaline, et on olemas kümneid riiklikke ametiasutusi ja reguleerivaid asutusi, kes tunnevad iga sektori eripära ja on volitatud jõustama iga sektori jaoks erinõudeid.

Näiteks Taanis võeti kasutusele kuus sihtstrateegiat, mis käsitlevad kõige olulisemate sektorite küber- ja infoturbetegevust, et arendada küber- ja infoturbe valdkonnas suuremat detsentraliseeritud suutlikkust. Iga sektoripõhine üksus aitab muu hulgas kaasa ohtude hindamisele sektori tasandil, seirele, valmisolekuõppustele, turbesüsteemide loomisele, teadmiste jagamisele ja juhiste andmisele. Sektoripõhised strateegiad hõlmavad järgmisi sektoreid:

- energeetika;
- tervishoid;
- transport;
- side;
- rahandus;
- merendus.

Ka teised liikmesriigid on väljendanud huvi valdkonnapõhiste küberturbestrateegiate kaalutlemise vastu, et need kajastaksid kõiki regulatiivnõudeid. Tuleb siiski märkida, et see eesmärk ei pruugi sobida kõigile liikmesriikidele, sest arvestada tuleb ka nende suurust, riiklikke poliitikaid ja küpsust. On väga raske tagada, et raamistik arvestab kõiki eripärasid, ja sel põhjusel ei lisanud ENISA seda eesmärki raamistikku.

Väärinfo levitamise kampaaniate vastane tegevus

Liikmesriikide küberturbestrateegiates on üks ülesannetest kaitsta aluspõhimõtteid, näiteks inimõigusi, läbipaistvust ja üldsuse usaldust. See on väga oluline eelkõige seoses väärinfoga, mida levitatakse tavapärase uudismeedia või ühismeediaplatvormide kaudu. Lisaks on küberturvalisus praegu üks suurimaid probleeme valimistel. Mitmes riigis on enne olulisi valimisi

täheldatud näiteks valeteabe levitamist või õõnestavat propagandat. See oht võib kahjustada ELi demokraatiaprotsessi. Euroopa tasandil on Euroopa Komisjon välja töötanud tegevuskava[32], et tõhustada tegevust väärteabe vastu Euroopas: kava keskendub neljale põhivaldkonnale (avastamine, koostöö, koostöö digiplatvormidega ja teadlikkus) ning selle eesmärk on suurendada ELi suutlikkust ja tugevdada liikmesriikide koostööd.

4 küsitletud riiki 19st on väljendanud kavatsust käsitleda oma riiklikus küberturbestrateegias ka väärinfo ja propaganda probleemi.

Näiteks märgitakse Prantsusmaa riiklikus küberturbestrateegias[33] järgmist: „riigi ülesanne on teavitada kodanikke internetis pahatahtlike osapoolte poolt kasutatavatest manipuleerimis- ja propagandatehnikatest. Pärast 2015. aasta jaanuaris toimunud terrorirünnakuid Prantsusmaa asutas valitsus teabeplatvormi ohtude kohta, mis on seotud islamistliku radikaliseerumisega elektrooniliste sidevõrkude kaudu: „Stop-djihadisme.gouv.fr“.“ Seda lähenemist saab laiendada, et reageerida ka muudele propaganda või destabiliseerimise ilmingutele.

Teine näide on Poola riiklik küberturbestrateegia aastateks 2019–2024[34], milles märgitakse: „Selliste manipuleerivate tegevuste suhtes nagu väärinfokampaaniad on vaja süsteemseid meetmeid, millega teadvustada kodanikele teabe autentsuse kontrollimist ja reageerimist teabe moonutamise katsetele.“

ENISA korraldatud küsitlustel teatasid mitu liikmesriiki siiski, et nad ei käsitle seda küsimust oma riikliku küberturbestrateegia osana kui küberohtu, vaid pigem laiemal ühiskondlikul tasandil, näiteks poliitikaalgatuste kaudu.

Turvalised tipptasemel tehnoloogiad (5G, tehisintellekt, kvantarvutus jt)

Et praegune küberohtude maastik üha laieneb, toob uute tehnoloogiate areng tõenäoliselt kaasa küberrünnete intensiivsuse ja arvu kasvu ning ohusubjektide kasutatavate meetodite, vahendite ja sihtmärkide mitmekesistumise. Seni on uutel tipptasemel tehnoloogilistel lahendustel potentsiaali, et nendest koosneb tulevikus Euroopa digitaalne turg. Et kaitsta liikmesriikide kasvavat digitaalset sõltuvust ja uute tehnoloogiate ilmudes tuleks luua stiimulid ja täiemahulised poliitikad, et toetada nende tehnoloogiate turvalist ja usaldusväärset arendamist ning kasutuselevõttu ELis.

Liikmesriikide küberturbestrateegiate analüüsimise etapis toodi välja järgmised tipptasemel tehnoloogiad, mis võiksid huvitada liikmesriike: 5G, tehisintellekt, kvantarvutus, krüptograafia, servtöötlus, andmesidega ja isejuhtivad sõidukid, suur- ja nutiandmed, plokiahel, robootika ja esemevõrk.

Eelkõige avaldas Euroopa Komisjon 2020. aasta alguses teatise, milles liikmesriike kutsuti üles tegema samme 5G-meetmepaketi järeldustes soovitatud meetmete rakendamiseks[35]. 5G meetmepakett järgneb komisjoni 2019. aastal vastu võetud soovitusele (EL) 2019/534 5G-võrkude küberturvalisuse kohta, milles kutsuti üles rakendama 5G-võrkude turvalisuse suhtes Euroopas ühtset lähenemisviisi[36].

ENISA korraldatud küsitlustel rõhutati, et see on pigem valdkonnaülene teema, mida käsitletakse riikliku küberturbestrateegia raames laiemalt, mitte otseselt eesmärk.

[32] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[35] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission
[36] https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32019H0534

Andmesuveräänsuse tagamine

Ühelt poolt võib küberruumi pidada tohutuks ülemaailmseks ühisruumiks, millele on lihtne juurdepääs, mis pakub suurt ühenduvust ja suurepäraseid võimalusi sotsiaal-majanduslikuks kasvuks. Teisalt iseloomustab küberruumi ka selle jurisdiktsiooni nõrkus, raskused tegevuste omistamisel, piiride puudumine ja vastastikku ühendatud süsteemid, mis võivad olla poorsed ja mille andmeid on võimalik varastada või millele võib olla juurdepääs isegi välisriikide valitsustel. Lisaks mõlemale mainitud aspektile iseloomustab digitaalset ökosüsteemi internetipõhiste teenuste platvormide ja taristu koondumine väga väheste sidusrühmade kätte. Kõik eespool nimetatud aspektid sunnivad liikmesriike edendama digitaalset suveräänsust. Digitaalse suveräänsuse saavutamine tähendab, et kodanikud ja ettevõtjad saavad parimal viisil kasutada usaldusväärseid digitaalseid teenuseid ja IKT-tooteid, ilma et peaksid kartma oma isikuandmete või digitaalsete varade, majandusliku sõltumatuse või poliitilise mõju pärast.

Liikmesriigid toetavad andmesuveräänsust või digitaalset suveräänsust riiklikul ja Euroopa tasandil. Kuigi näib, et liikmesriigid ei käsitle seda küsimust otseselt oma riiklikes küberturbestrateegiates konkreetse eesmärgina, käsitlevad nad seda kas valdkonnaülese põhimõttena või väljendavad oma kavatsust tagada digitaalne suveräänsus riiklikul tasandil sihtotstarbelistes väljaannetes, keskendudes peamistele tehnoloogiatele. Näiteks märgitakse Prantsusmaa 2018. aasta küberkaitse strateegilises ülevaates: „Digitaalse suveräänsuse tagamiseks on äärmiselt oluline hallata järgmisi tehnoloogiaid: side krüptimine, küberrünnete avastamine, professionaalne mobiilraadio, pilvandmetöötlus ja tehisintellekt.“[37]

Euroopa tasandil osalevad liikmesriigid aktiivselt Euroopa andmestrateegia (COM/2020/66 final) määratlemisel ning digitaalsete IKT-toodete, teenuste ja protsesside sertifitseerimise ELi raamistiku väljatöötamisel, mis on loodud ELi küberturvalisuse määrusega (2019/881), et tagada strateegiline digitaalne autonoomia Euroopa tasandil.

Liikmesriikide esindajate küsitlemisel selgus, et digitaalse suveräänsuse teemat peetakse sageli küberturbest laiemaks. Seega ei käsitle liikmesriigid seda teemat oma riiklikes küberturbestrateegiates. Need vähesed riigid, kes seda teevad, ei käsitle seda konkreetse eesmärgina.

Küberkindlustusvaldkonna arendamise stiimulite pakkumine

Küberkindlustussektori praegune olukord näitab, et ei ole kahtlust, et ülemaailmne turg on kasvanud. See on siiski alles arenemisjärgus, sest andmeid tuleb koguda ja paljud pretsedendid on veel loomata (nt passiivne kaitse, süsteemsed küberriskid jne). Lisaks oleks kogu maailmas toimuvate küberrünnete kahju hinnanguliselt mitu suurusjärku suurem kui küberkindlustussektori praegune kattevõime (IMFi töödokument – „Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment“, WP/18/143). Samas on küberkindlustussektori arendamisest kindlasti kasu ja see paneb aluse positiivsetele mehhanismidele. Eelkõige võivad küberkindlustusmehhanismid aidata

- teadvustada ettevõtetes küberturberiske;
- hinnata küberriskidega kokkupuudet kvantitatiivselt;
- täiustada küberturberiskide juhtimist;
- toetada küberrünnetes kannatanud organisatsioone;
- katta küberrünnetes tekkinud kahjusid (varalisi ja muid).

[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

Mõni liikmesriik on alustanud teema käsitlemist. Näited.

- Eesti võttis oma riiklikus küberturbestrateegias kasutusele äraootava seisukoha: „Erasektori küberriskide maandamiseks laiemalt analüüsitakse küberkindlustusteenuse nõudlust ja pakkumist Eestis, selle baasil lepitakse kokku seotud osapoolte koostööpõhimõtted mh. infojagamise, riskihinnangute koostamise jms. osas. Täna on küberkindlustusteenuse pakkujaid Eesti turul vähe ning vajalik on esmalt kaardistada, kes ja mida pakuvad. Kindlustuskaitse ulatuse keerukust peetakse sageli küberkindlustusturu arengu takistuseks.“
- Luksemburg toetab oma riiklikus küberturbestrateegias konkreetselt küberkindlustuse sektori arengut: „1. eesmärk: uute toodete ja teenuste loomine. Et koondada riske ja julgustada digitaalsetes küberintsidentides kannatanuid otsima abi ekspertidelt, et tulla toime intsidendiga ja taastada pahatahtlikust tegevusest mõjutatud süsteem, julgustatakse kindlustusandjaid looma konkreetseid tooteid küberkindlustuse valdkonnas.“

Küsitletute tagasiside oli selles küsimuses üsna mitmekesine: mõni liikmesriik märkis, et hiljuti on alanud arutelu küberkindlustuse teemal, kuid teised, et vaatamata teema paljulubavusele ei ole valdkond veel piisavalt küps. Palju küsitletuid teatas siiski, et teemat ei käsitleta riikliku küberturbestrateegia osana, sest seda peetakse liiga spetsiifiliseks või riikliku küberturbestrateegia kohaldamisalasse mittekuuluvaks.

TP-02-21-253-ET-N

Euroopa Liidu Küberturvalisuse Amet

Euroopa Liidu Küberturvalisuse Amet (ENISA) on Euroopa Liidu asutus, mille eesmärk on saavutada küberturvalisuse ühtlane kõrge tase kogu Euroopas. 2004. aastal asutatud ning ELi küberturvalisuse määrusega tugevdatud Euroopa Liidu Küberturvalisuse Amet osaleb ELi küberpoliitikas, suurendab IKT-toodete, -teenuste ja -protsesside usaldusväärsust küberturvalisuse sertifitseerimiskavade abil, teeb koostööd liikmesriikide ja ELi organitega ning aitab Euroopal valmistuda tuleviku küberprobleemideks. Jagades teadmisi ning suurendades suutlikkust ja teadlikkust teeb amet koostööd peamiste sidusrühmadega, et tugevdada usaldust sidusmajanduse vastu, edendada Euroopa Liidu taristu kerksust ning tagada kokkuvõttes Euroopa ühiskonna ja kodanike digitaalne turvalisus. Lisateave: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-479-4
DOI: 10.2824/307015