# KÜBERTURVALISUSE PROGRAMM AASTATEKS 2021-2024

| | |
|---|---|
| **Programmi koostaja ja vastutaja** | Riigi infosüsteemide osakond, side ja riigi infosüsteemide asekantsler |
| **Programmi eelnõu valmimise aeg** | märts 2020 |
| **Vormi sisu kasutamise selgitus** | Vorm on abiks riigi eelarvestrateegia (RES) protsessi sisendina koostatava programmi dokumendi eelnõu koostamiseks. Programmi eelnõu kohandatakse RES-ist ja RE-st lähtuvalt. Programmi kinnitab minister käskkirjaga |

## Sisukord



### 1. Programmi esileht

| | |
|---|---|
| **Tulemusvaldkond** | Infoühiskond |
| **Tulemusvaldkonna eesmärk** | Eestis on loodud hästi toimiv keskkond IKT laialdaseks kasutamiseks ja nutikate lahenduste loomiseks, mis on seeläbi tõstnud majanduse konkurentsivõimet, inimeste heaolu ja riigivalitsemise tõhusust |
| **Valdkonna arengukava** | Eesti infoühiskonna arengukava 2020[1] |
| | |
| **Programmi nimi** | Küberturvalisuse programm aastateks 2021-2024 |
| **Programmi eesmärk** | Eesti on kõige küberturvalisem digitaalne riik |
| **Programmi periood** | 2021–2024 |
| **Peavastutaja (ministeerium)** | Majandus- ja Kommunikatsiooniministeerium (MKM) |

[1] https://www.mkm.ee/sites/default/files/eesti_infouhiskonna_arengukava.pdf

| | |
|---|---|
| **Kaasvastutajad (oma valitsemisala asutused)** | Riigi Infosüsteemi Amet |
| **Kaasvastutaja ministeeriumi ja selle valitsemisala asutused** | Ei ole |

## 2. Sissejuhatus ehk programmi sisu lühikokkuvõte

Küberturvalisuse programm (edaspidi programm) on koostatud eesmärgiga viia ellu Eesti infoühiskonna arengukava 2020 alavaldkonna *Kübeturvalisuse tagamine* ning arengukava lisa *Küberturvalisuse strateegia (*edaspidi *KTS)* raames kavandatud tegevussuunad[2].

2017–2018. aastal toimunud küberturvalisuse strateegia koostamise protsessi kaudu kaardistas Majandus- ja Kommunikatsiooniministeerium (edaspidi MKM) olulisemad valdkondlikud probleemid ja prioriteedid. Nende põhjal on kujundatud programmi neli meedet, mis panustavad programmi eesmärkide täitmisele:

- jätkusuutlik digitaalne ühiskond;
- ettevõtlus ning teadus- ja arendustegevus;
- rahvusvahelised suhted;
- küberoskuslik ühiskond.

**Programmi eesmärk: Eesti on kõige küberturvalisem digitaalne riik**. Programmi ülesanne on tagada ühiskonna toimimise seisukohast oluliste funktsioonide (strateegilise taristu ja teenuste) vastupanuvõime küberohtude suhtes. Programm keskendub väljakutsete lahendamisele ennetuse, kaitse ja arenduse tegevuste kaudu. Näiteks ennetuse osas on Eesti riigil vaja tagada, et uued teenused ja andmekogud ehitatakse ülesse arvestades turvalisuse ja privaatsuse põhimõtet (*security and privacy by design*). Eesti info- ja võrguturbe riiklikul korraldamisel lähtutakse riskipõhisest lähenemisest ja parimatest rahvusvaheliselt tunnustatud standarditest ning praktikatest.

Kaitsetegevuse valdkonnas viiakse läbi küberturvalisuse võimete auditid ning vastavalt nende tulemustele ühendatakse riigi käsutuses olevad võimed ressursside paremaks kasutamiseks. Küberturvalisus lõimitakse riigikaitse planeerimisse ning regulaarselt viiakse läbi õppuseid.

Valdkonna arendamisel tagatakse spetsialistide järelkasv. Samuti toetatakse riigi, akadeemia ja erasektori võtmepartnerite koostööd, mh kübersektori majandusharu kasvu.

Eelnevast tulenevalt tagatakse programmi meetmetega Eesti riigi suutlikkus küberohtudega tõhusalt toime tulla ning tagada digitaalse ühiskonna turvaline ja tõrgeteta toimimine. Selleks toetutakse riigiasutuste ühisele võimekusele, teadlikule ja osalevale erasektorile ning väljapaistvale teaduskompetentsile. Eesti on küberturvalisuse valdkonnas rahvusvaheliselt hinnatud suunanäitaja, mis toetab riigi julgeolekut ja aitab kaasa valdkonnas tegutsevate ettevõtete globaalse konkurentsivõime kasvule. Ühiskond tervikuna tajub küberturvalisust ühise vastutusena, kus igaühel on täita oma roll.

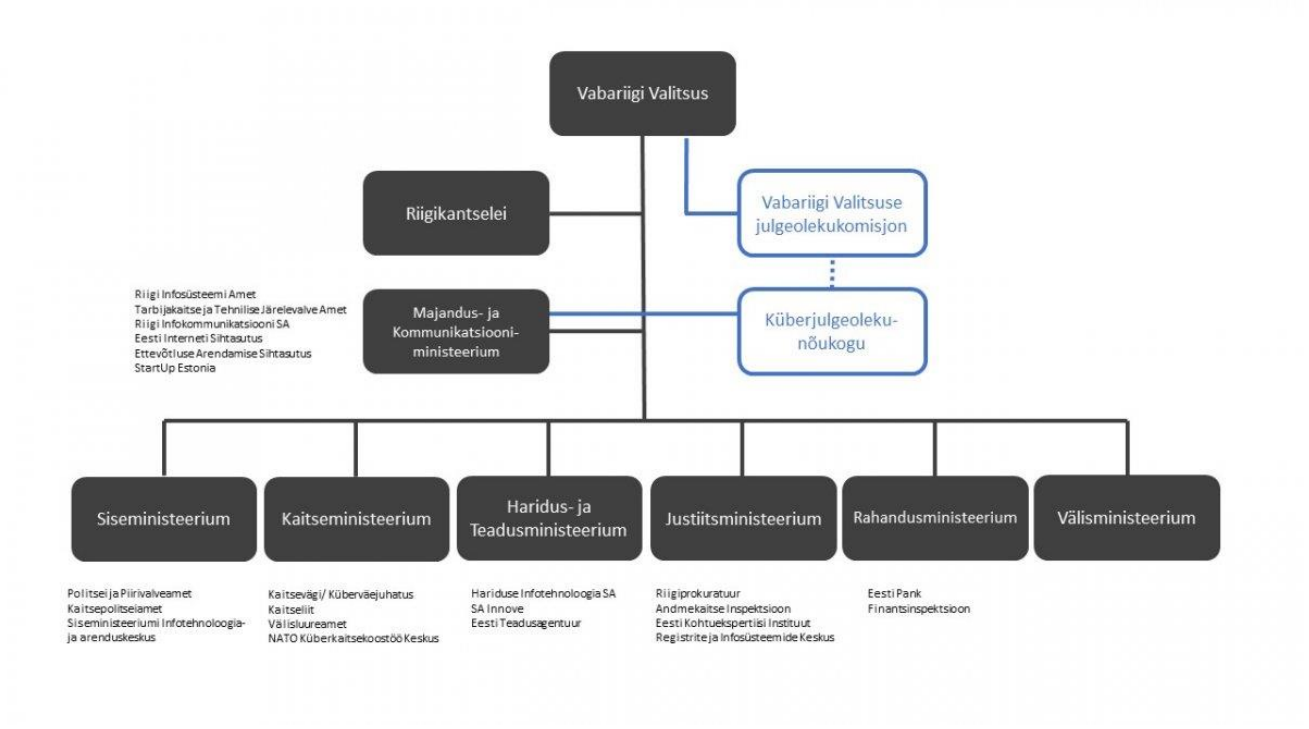
## 3. Programmi juhtimiskorraldus

### 3.1 Programmi koostamise ja juhtimise korraldus

Programmi koostas MKM-i riigi infosüsteemide osakond ning selle rakendamise eest vastutab side ja riigi infosüsteemide asekantsler. Programmi kaasvastutaja on Riigi Infosüsteemi Amet (edaspidi RIA). Terviklikkuse huvides on käesolevas programmis oluline välja tuua nii KTS-i kui programmi koostamisse

[2] Programmi dokument lähtub meetmete ja programmi tegevuste kirjeldamisel Eesti infoühiskonna arengukava 2020 lisast Küberturvalisuse strateegia, mis käsitleb strateegia eesmärke ja nende täitmiseks vajalikke tegevussuundi detailsemalt kui Infoühiskonna arengukava alamvaldkond küberturvalisuse tagamine.

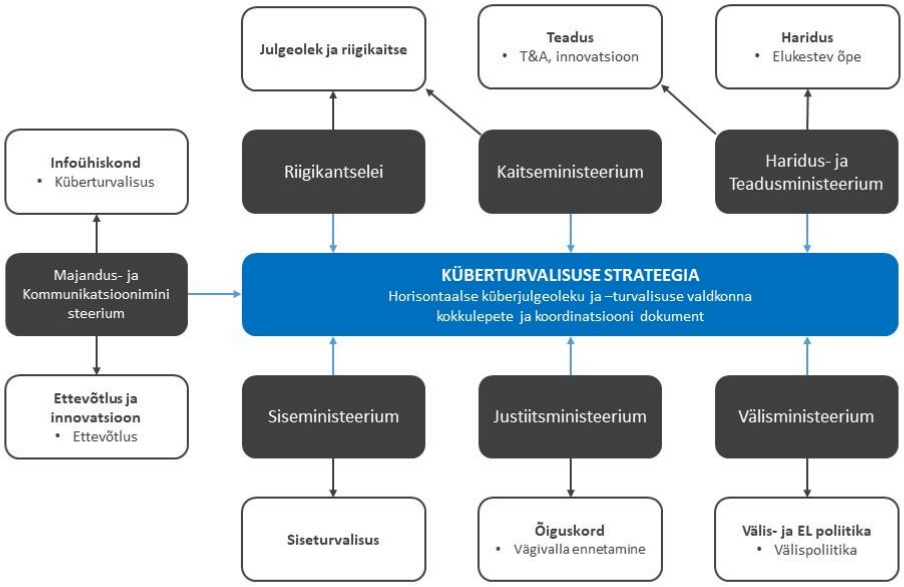
kaasatud osapooled (vt Joonis1). Lisaks küberturvalisuse valdkonna juhtimisega otseselt seotud osapooltele olid kaasatud akadeemia, valdkonna mõttekojad ning erasektori esindajad.




Joonis1. Küberturvalisuse valdkonna juhtimiskorraldus

## 3.2 Seos teiste tulemusvaldkondadega

Sarnaselt infoühiskonnale, on küberturvalisuse puhul tegemist strateegiliselt horisontaalse teemaga, mistõttu on KTS küberjulgeoleku ja –turvalisuse valdkonna kokkulepete ja koordinatsiooni dokument. KTS-s kokkulepitud eesmärkide saavutamiseks vajalikud meetmed, programmi tegevused ja rahastamiskava planeeritakse detailselt programmis ja teistes vastutavate ministeeriumite tulemusvaldkondadesse panustavates programmides. Seosed teiste tulemusvaldkondadega on toodud Joonisel 2.



Joonis2. Küberturvalisuse strateegia eesmärkide elluviimiseks vajalike tegevuste planeerimisega seotud tulemusvaldkonnad

### 3.4 Programmi seire

Programmi seire toimub ühtses ajakavas Eesti Infoühiskonna arengukava 2020 (edaspidi arengukava) ja selle lisa (KTS-i) eesmärkide täitmise seirega, mille tulemusel tekivad nii arengukava tulemusaruanne kui programmi aruanne. Arengukava lisa (KTS-s) puhul on eraldi kokkulepitud detailsem tegevuskava ja eesmärkide koordineeritud täitmiseks vaadatakse seda üle Küberjulgeoleku nõukogus vähemalt kaks korda aastas. Lisaks on KTS-i elluviimisesse otseselt panustavates ministeeriumites ja Riigikantseleis määratud vastutav ametnik, kes on enda haldusalas riikliku küberjulgeoleku- ja turvalisuse tagamist puudutavates küsimustes kontaktisikuks ning valmistab ette iga-aastase aruande küberjulgeoleku nõukogule[3]. Vastutavate ametnike jooksvat koostööd ja infovahetust korraldab MKM.

## 4. Programmi eesmärk, mõõdikud ja eelarve

### 4.1. Programmi eesmärk: Eesti on kõige küberturvalisem digitaalne riik

Eesti suudab küberohtudega tõhusalt toime tulles tagada digitaalse ühiskonna turvalise ja tõrgeteta toimimise, toetudes riigiasutuste ühisele võimekusele, teadlikule ja osalevale erasektorile ning väljapaistvale teaduskompetentsile. Eesti on küberturvalisuse valdkonnas rahvusvaheliselt hinnatud suunanäitaja, mis toetab riigi julgeolekut ja aitab kaasa valdkonnas tegutsevate ettevõtete globaalse konkurentsivõime kasvule. Ühiskond tervikuna tajub küberturvalisust ühise vastutusena, kus igaühel on täita oma roll.

### 4.2. Programmi mõõdikud

Tabel 1. Programmi mõõdikud

| **Mõõdik, sh allikas** | **Algtase (2018)** | **Sihttase (2021)** | **Sihttase (2022)** | **Sihttase (2023)** | **Sihttase (2024)** |
|---|---|---|---|---|---|
| Küberintsidentide arv, mis häirib olulisel määral ühiskonna sotsiaalset ja majanduslikku toimimist või sunnib loobuma harjumuspärastest digitaalsetest lahendustest[4]. Allikas: CERT.EE | 168 | 148 | 138 | 128 | 128 |
| **Mõõdik** Eesti elanikud tunnevad end internetis turvaliselt ning usaldavad e-riiki: | | | | | |
| Turvariski vältimise kaalutulustel avaliku sektori või teenusepakkujaga elektroonilisest suhtlemisest hoidunute osakaal.[5] Allikas: Statistikaamet | 3,1% (2015) | ≤ 3.1% | ≤ 3.1% | ≤ 3.1% | ≤ 3.1% |
| Turvalist elektroonilist identiteeti[6] kasutavate inimeste osakaal elektroonilist identiteeti omavatest elanikest. Allikas: SK ID Solutions AS | 57,6% (2017) | ≥ 65% | ≥ 65% | ≥ 65% | ≥ 65% |

[3] https://www.mkm.ee/et/tegevused-eesmargid/infouhiskond/kuberjulgeolek
[4] CERT.EE registreeritud kriitiliste küberturbe intsidentide arv aastas.
[5] Viimase 12 kuu jooksul turvariskide tõttu internetitegevusest hoidunud 16-74-aastased internetikasutajad: suhtlemine avaliku sektori asutuste või teenusepakkujatega. Allikas: Statistikaamet
[6] 2017. aasta andmete puhul loeti turvaliseks elektroonseks identiteediks riigi poolt väljastatavaid identiteete.

### 4.3. Programmi eelarve

Tabel 2. Programmi eelarve

| Eelarve jaotus[7] | 2021 | 2022 | 2023 | 2024 |
|---|---|---|---|---|
| Kulud | 3 426 831 | 3 424 774 | 3 425 360 | |
| sh välistoetused ja kaasrahastus | 42 897 | 41 272 | 41 272 | |
| investeeringud | 0 | 0 | 0 | |
| sh välistoetused ja kaasrahastus | 0 | 0 | 0 | |
| Mitterahalised kulud | 178 830 | 173 152 | 173 152 | |

## 5. Olukorra lühianalüüs

### 5.1 Seos infoühiskonna tulemusvaldkonnaga ja olulisemate näitajate kirjeldus

Programm panustab infoühiskonna tulemusvaldkonda (edaspidi TUV), mille eesmärk on luua Eestis hästi toimiv ning turvaline keskkond nutikate IKT-lahenduste laialdaseks kasutamise ja loomiseks.

Täpsed näitajad, millega TUV eesmärgi täitmist mõõdetakse, on toodud programmi punktis 4.2. Sisuliselt tagatakse Eesti riigi suutlikkus küberohtudega tõhusalt toime tulla ning tagada digitaalse ühiskonna turvaline ja tõrgeteta toimimine, toetudes riigiasutuste ühisele võimekusele, teadlikule ja osalevale erasektorile ning väljapaistvale teaduskompetentsile. Eesti on küberturvalisuse valdkonnas rahvusvaheliselt hinnatud suunanäitaja, mis toetab riigi julgeolekut ja aitab kaasa valdkonnas tegutsevate ettevõtete globaalse konkurentsivõime kasvule. Ühiskond tervikuna tajub küberturvalisust ühise vastutusena, kus igaühel on täita oma roll.

### 5.2 Olulisemad valdkondlikud väljakutsed ja riskid

Olulised väljakutsed Eesti küberjulgeoleku ja -turvalisuse tagamiseks ei erine oluliselt teiste võrreldavate riikide ees seisvatest probleemidest. Eesti on maailma üks kõige digisõltuvamatest riikidest, mistõttu on küberohtude võimalikud mõjud meie jaoks võrreldes paljude teiste riikidega oluliselt kaalukamad. Järgnevalt on välja toodud küberkogukonna poolt esile tõstetud seitse kõige prioriteetsemat probleemi ja väljakutset, mis takistavad valdkonna optimaalset toimimist ja arengut ning mida praeguseks rakendatud normatiivsed lahendused ei ole parandanud.

#### 5.2.1 Piiratud spetsialiseerumisvõime

Piiratud spetsialiseerumisvõime nii riigisektoris, eraettevõtetes kui ka teadusasutustes on Eesti kui väikese ja väheneva rahvastikuga ühiskonna alusprobleemiks. Kuigi väike ekspertide kogukond ja isiklikul tasemel hea läbisaamine tagab operatiivse kiiruse ja paindlikkuse esmaseks kriiside ja intsidentidega toimetulekuks, ei ole selles peituv tugevus jätkusuutlik olukorras, kus IT süsteemide ja ohtude keerukus järjest kasvab. Killustunud valdkondlik ekspertiis ei võimalda tipptasemel spetsialiseerumist. Sellega kaasneb omakorda oht tippspetsialistide Eestist ja eelkõige avalikust sektorist lahkumiseks.

#### 5.2.2 Puudulik tervikjuhtimine

Suureks väljakutseks on küberturvalisuse valdkonna strateegiline tervikjuhtimine ja ühtne koordinatsioon: valdkonna planeerimine toimub endiselt pigem asutuste vastutusalade summana ja igaühe enda prioriteete pidi.

[7] Kübeturvalisuse alavaldkonna tagamine eelarve on esitatud MKM-i riigi infosüsteemide osakonna küberturbe valdkonna tööjõukulu ning Riigi infosüsteemi ameti küberturvalisuse teenistuse eelarve baasil ning sisaldab tööjõukulusid, majandamiskulusid ja investeeringuid aastate 2019 – 2020 kohta. Arengukava eelarve kokku 2014-2020 ei sisalda küberturvalisuse tagamise alavaldkonna kulusid enne 2018. aastat.

Sellest lähtub ka ebapiisav asutusteülene olukorrateadlikkus ja teabevahetus ning killustunud, ebaühtlane ja raiskav infosüsteemide kaitse korraldus, vaatamata üldisele suunisele ressursside konsolideerimiseks.

### 5.2.3 Ebapiisav arusaam küberohtude ja –intsidentide mõjudest ja taristu (rist)sõltuvustest

Avar autonoomia IT-süsteemide arendamisel ja haldamisel toob kaasa olukorra, kus asutused korraldavad küberturberiskide haldamist sageli oma valikute laiemat mõju hindamata, vaatamata sellele, et ollakse seotud ühiskasutatava taristuga (riigivõrk). Ühtsete turbepõhimõtete ja standardite eiramine või puudumine seab ohtu Eesti hajusal arhitektuuril põhineva digiriigi toimimise. Endiselt puudub riigil süsteemne ülevaade süsteemide omavahelistest rist- ja piiriülestest sõltuvustest ja võimalikest mõjudest ning selge arusaam teenuste miinimumtaseme tagamisest, mis peab töötama ka kriisiolukorras.

### 5.2.4 Ebapiisav teadlikkus ja vähene omanikutunne

Küberturvalisuse alane teadlikkus on endiselt ebapiisav nii riigi ja erasektori juhtide hulgas kui ka ühiskonnas laiemalt, millega omakorda kaasneb vähene omanikutunne. Eelnevast tuleneb aga küberturbe alahindamine infosüsteemide ja teenuste arendamisel. Küberturvalisuse tagamist ei tajuta isikliku vastutusena ega organisatsiooni põhitegevuse riskina, vaid koheldakse valdavalt kui keerukat tehnilist teemat, millega keegi teine peab tegelema. Infoturbe tagamisse suunatud ressursside maht süsteemide arendamisel ja haldamisel on jäänud maha valdkonna arengust tulenevast vajadusest ning reguleerimiskoormuse kasvust – see on väljakutse, mida tehnoloogia pideva arenguga kaasnev kasvav keerukus üha süvendab.

### 5.2.5 Spetsialistide puudus ja ebapiisav juurdekasv

Kompetentse tööjõu vähesus nii avalikus kui ka erasektoris mõjutab kõigi strateegiliste eesmärkide täitmist. Küberturbe (töö)turg on globaalne ja toimub pidev konkurents parimate talentide pärast. Riigi kriitilisi funktsioone toetavaid tippspetsialiste tõmbavad aktiivselt nii Eesti kui ka välismaised ettevõtted. Riigisektori väljakutseks on pakkuda piisavalt mõtestatust, vabadust ning võimalusi uudseid ja unikaalseid lahendusi ellu viia. Samal ajal suureneb surve Eestist pärit spetsialistide värbamiseks erasektorisse ja rahvusvahelistesse ettevõtetesse koos Eesti tehnoloogiavaldkonna ja küberturbe rahvusvahelise mainega, mida riik ise aktiivselt võimendab.

Kehtivatel küberturbe õppekavadel ei ole seni piisaval määral arvestatud Eesti tööturu vajadustega, sest puudub selge tööjõuvajaduse kaardistus ja tellimus. Küberturbe õppekavade puudusena võib välja tuua ka paindlike ümberõppevõimaluste puudumise. Valdkonna kogukonna poolt tajutakse probleemina ka vajalike küberkompetentside omandamist IT-välistel õppekavadel ning riigi ja erasektori koostööd teadusasutustega, mis ei ole piisavalt süsteemne.

### 5.2.6 Vähene sektoris tegutsevate edukate ettevõtete hulk ja ebapiisav teadus- ja arendustegevuse maht

Oma küberturbetoodet või -teenust arendavate ja välisturgudel edukate Eesti ettevõtete hulk on endiselt väike, arvestades, et küberturbe- ja kaitsetööstusel on Eesti valdkondlike tugevusi arvestada tohutu ekspordipotentsiaal. Oluliseks arengut pärssivaks faktoriks on sealjuures spetsialistide puudus, mis pidurdab kasvu kogu IKT sektoris tervikuna.

Teisalt ei ole täna piisaval hulgal ressursse ka Eesti jaoks strateegiliselt olulistes teadusvaldkondades nagu krüptograafia või turvalised autentimislahendused. Üheks võtmeküsimuseks on sealjuures ebapiisav koostöö riigi ja teadusasutuste vahel, millest tuleneb vähene arusaam riigi praegustest ja tulevastest prioriteetidest ning väljakutsetest teadustegevuse planeerimisel. Samaväärselt on probleemiks ka ebapiisav sidusus teadustegevuse ja ettevõtluse vahel – probleemiks nii Eestis kui kogu Euroopas on teadustöö tulemuste kommertsialiseerimine: teaduspublikatsioone avaldatakse, kuid neist ei arene edasi reaalseid prototüüpe, tooteid ja patente.

Tugeval ja võimekal sektori ettevõtlusel ja seda võimaldaval teadus- ja arendustegevusel on lisaks panusele riigi arengusse (majanduskasv) ka väga vahetu mõju ühelt poolt riigile vajalike turbelahenduste pakkujana – Eesti kõrgelt digitaliseerinud riigihaldus tingib vajaduse innovaatiliste ja paindlike lahenduste järele, mida

välisettevõtetelt sageli ei saa – ning teisalt roll õhukese riigi kriisivaruna, tagades teadmuse ja talendi olemasolu, keda on võimalik vajadusel riigile appi kutsuda.[8]

### 5.2.7 Eesti kui usaldusväärse ja väärtusliku rahvusvahelise partneri maine hoidmine

Eesti koht küberturvalisuse tippriikide seas maailmas, mis toetab Eestile vajalikku teabe- ja teadmuse vahetust strateegiliste partneritega ning tugevdab Eesti häält rahvusvahelisel areenil, ei säili iseenesest – tegemist on kiirelt muutuva ja üha tiheneva konkurentsiga valdkonnaga, kus kiire areng on toimumas ka paljudes teistes riikides. Seega ei ole Eesti väljapaistev rahvusvaheline kuvand iseenesestmõistetav – kuigi on saanud meile harjumuspäraseks – ega säili inertsist, ilma täiendavate pingutuste ja ressursside suunamiseta.

## 5.3 Seniste tegevuste tulemuslikkus

Senise riikliku IKT-poliitika suurim tugevus on olnud riigi infosüsteemi süstemaatiline väljaarendamine, sealhulgas selle turvalisena rajamine. Selleks on rakendatud Eesti infopoliitika aluspõhimõtteid, nagu hajus teenusepõhine arhitektuur, andmete ja andmevahetuse turvalisus, sh infosüsteemide turvameetmete etalonsüsteem (ISKE[9]), veebipõhisus, orienteeritus e-teenustele ning tugevate autentimisvahendite kasutamine. Riigi infosüsteemi baasinfrastruktuur ehk teenustetaristu (X-tee, avaliku võtme infrastruktuur ja eID, dokumendivahetuskeskkond, teabevärav eesti.ee) on läbi aastate toetanud avalike teenuste arendamist kiirelt ja paindlikult valmivate IKT-lahendustega. Hajusalt ja samas üldiselt koosvõimelisena üles ehitatud riigi infosüsteem on loonud Eestile head eeldused tulla toime ning potentsiaalselt lõigata kasu trendist, kus üha enam seadmeid ja masinaid on ühendatud võrku.

Küberturvalisuse tagamisel on saavutatud elementaarne ja järeleproovitud küpsusaste, mille aluseks lisaks väljatoodule on keskne küberturbe intsidentide seire, lahendamise ja raporteerimise süsteem, toetav õigusruum ning toimivad koostööformaadid. Kahe kriisi kogemus (2007 küberründed ja 2017 toimetulek ID-kaardi turvanõrkuse lahendamisega) on andnud praktilise ja läbitestitud kindluse, et küberturvalisuse valdkonna arendamisel tehtud valikud on üldjoontes õiged ja tuleme oma digitaalse ühiskonna kaitsmisega toime. Asjaolust, et tegemist ei ole mainekujundusliku edu või üksikute innovaatiliste saavutuste tagajärjega, annab kinnitust ka 2016. aasta juunis avaldatud Rahvusvahelise Telekommunikatsiooni Liidu (ITU) indeks[10], mille põhjal on Eesti küberturvalisuse arengu poolest maailmas viiendal ja Euroopas esimesel kohal.

# 6. Meetmed ja tegevused

## 6.1 Meede: Jätkusuutlik digitaalne ühiskond

Tabel 3. Meetme „Jätkusuutlik digitaalne ühiskond“ eesmärk ja mõõdikud

| **Meetme eesmärk:** | Eesti on jätkusuutlik ja turvaline digitaalne ühiskond | | | | |
|---|---|---|---|---|---|
| **Mõõdik, sh. allikas** | Algtase (2018) | Sihttase (2021) | Sihttase (2022) | Sihttase (2023) | Sihttase (2024) |
| Riskidele avatud teenuste[11] koguarv riigivõrgus (CERT.EE seireandmete najal puudulikult konfigureeritud seadmeid riigivõrgus)[12] | 50 | 28 | 21 | 16 | 16 |

[8] Seda näitasid selgelt nii 2007 küberrünnetega toimetulek kui ka 2017 sügise ID-kaardi kriis.
[9] https://iske.ria.ee/
[10] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
[11] Avatud teenus on Eesti küberruumis pakutav teenus, mis on ligipääsetav kõigile interneti kasutajatele, kuid mis ei peaks olema ligipääsetav kõigile interneti kasutajatele (nt administreerimisliidesed, mis ei tohiks olla kättesaadavad)
[12] Telnet, POP3, NetBIOS, IMAP, LDAP, AD/SMB, MS-SQL, Oracle-DB, MySQL, RDP, UPnP, PostgreSQL, VNC, Redis, Memcached, MongoDB

| | | | | | |
|---|---|---|---|---|---|
| Allikas: Riigi Infosüsteemi Amet | | | | | |
| Riskidele avatud teenuste koguarv Eesti küberruumis (CERT.EE seireandmete najal puudulikult konfigureeritud seadmeid Eesti küberruumis)[14]<br><br>Allikas: Riigi Infosüsteemi Amet | 26 000 | 14 500 | 11 000 | 8000 | 8000 |

Antud meede keskendub ühelt poolt enim mõju omavate tänaste kitsaskohtade lahendamisele, teisalt paindliku valmisoleku tagamisele tulevikutrendidega toimetulekuks. Mõlema alus ja võimaldaja on riigiülene strateegiline tervikpilt, operatiivne koosvõime, toimiv kogukond ja kaasav planeerimine.

### 6.1.1 Programmi tegevus: Tehnoloogilise vastupanuvõime tõhustamine

Tabel 4. Programmi tegevuse eesmärk ja mõõdik

| **Tegevuse eesmärk:** | Tehnoloogilise vastupanuvõime tõhustamine | | | | |
|---|---|---|---|---|---|
| | Algtase (2018) | Sihttase (2021) | Sihttase (2022) | Sihttase (2023) | Sihttase (2024) |
| **Mõõdik:** Kõik uued riigi infosüsteemid ja e-teenused vastavad turvalise arhitektuuri põhimõtetele | Ajakohane turvalise arhitektuuri põhimõtete kirjeldus puudub | Turvalise arhitektuuri põhimõtete ja nõuete kirjelduse koostamine | Nõudeid rakendatakse uute süsteemide puhul | Nõudeid rakendatakse uute süsteemide puhul | Nõudeid rakendatakse uute süsteemide puhul |

Küberturvalisus hõlmab kogu infosüsteemi ja teenuse elutsüklit alates arhitektuurist, mis on teenuse orgaanilise osana. Et see põhimõte tegelikkuses rakenduks, tuleb riigi infosüsteemide ja digitaalsete teenuste arendamisel arvestada süsteemselt nii tehnilise kui ka protsessidisaini ja regulatiivsete nõuetega. Seejuures peab turbekompetents ja turvatestimine käima teenuse kujundamisega kaasas arendusprotsessi algusest peale.

2018. aastal jõustusid nii uus küberturvalisuse seadus, mis võtab Eesti seadusandlusesse üle Euroopa võrgu- ja infoturbe direktiivist tulenevad nõuded, kui ka isikuandmete kaitse üldmäärus. Vaatamata eraldiseisvatele regulatsioonidele ei ole rakendajate seisukohast andmekaitse ja infoturbe käsitlemine lahus distsipliinidena praeguseks enam ei mõistlik ega jõukohane. Seega lähtume edasiste tegevuste planeerimisel põhimõttest, et infoturbe ja andmekaitse nõuete rakendamist tuleb vaatamata eraldiseisvale regulatsioonile kohelda arendus- ja opereerimisprotsessi usaldusväärsust tagava tervikuna, püüeldes nende kooskõlalise ja holistilise rakendamise poole. See eeldab võimaldavat ja toetavat õigusruumi ning halduskorraldust.

Lisaks täna akuutsete riskide haldamisele tuleb arvestada ka pikaajalise vaatega. On alust arvata, et programmi lõpuks on olulisi arenguid läbinud suur osa Eesti e-riigi alustehnoloogiatest, sh kasutatavad krüptoalgoritmid. Krüptograafia arengutele ja nendest lähtuvatele ohtudele on Eesti digitaalne ökosüsteem eriti tundlik, kuna sellel põhineb riiklikult tagatud digitaalse identiteedi lahendus, peame andmeid kaitsma ja digitaalse allkirja kehtivuse tagama ka aastakümnete pikkuses perspektiivis. Strateegiliselt nõuab selleks valmisolek eelkõige kohanemis- ja reageerimisvõime tagamist, tehniliselt *no-legacy* põhimõtte järgimist ehk vananenud süsteemidest ja taaktarkvarast vabanemist.

### 6.1.2 Programmi tegevus: Intsidentide ja kriiside ennetamine, valmisolek ja haldamine

Tabel 5. Programmi tegevuse eesmärk ja mõõdik

| **Tegevuse eesmärk:** | Tagatud on valmisolek intsidentide ja kriiside ennetamiseks ja haldamiseks | | | | |
|---|---|---|---|---|---|
| | Algtase (2018) | Sihttase (2021) | Sihttase (2022) | Sihttase (2023) | Sihttase (2024) |
| **Mõõdik:** Loodud on avalikult kättesaadav *dashboard*[13], mis kajastab seireandmeid[14]: korrektselt konfigureeritud veebilehtede ja e-posti serverite osakaal (%) | *Dashboard puudub* | Korrektselt konfigureeritud veebilehti 35%<br><br>Korrektselt konfigureeritud E-posti servereid 35% | Korrektselt konfigureeritud veebilehti 40%<br><br>Korrektselt konfigureeritud E-posti servereid 40% | Korrektselt konfigureeritud veebilehti 40%<br><br>Korrektselt konfigureeritud E-posti servereid 40% | Korrektselt konfigureeritud veebilehti 40%<br><br>Korrektselt konfigureeritud E-posti servereid 40% |

Kahe KTS perioodi jooksul on riigi küberturvalisuse peamine rõhk olnud ühiskonna toimimiseks vajalike teenuste toimepidevuse tagamisel ning olulise mõjuga intsidentide ennetamisel. Viimase nelja aasta jooksul on üles ehitatud ööpäevaringselt toimiv üleriigiline seire- ja intsidentide lahendamise võimekus (CERT 24/7) ning olemas on küberintsidentide ennetamiseks ja reageerimiseks vajalik raamistik nii riigi kui erasektori oluliste teenuste osas – hädaolukorra seadus ja küberturvalisuse seadus loovad tõsisemate riskide haldamiseks piisava õigusliku raami.

Senini on aga probleemkohaks riskianalüüside ja teenuse toimepidevuse plaanide koostamine ning nende kõikuv kvaliteet. Programmi perioodi adresseeritud väljakutseks on riskide haldamises uuele tasemele jõudmine, tänaseks loodud õigusliku raamistiku praktiline rakendamine ning üleminek võimepõhisele küberkriiside lahendamisele, mis tähendab, et intsidentide ja kriiside lahendamisel kasutatakse koordineeritult erinevate asutuste spetsiifilisi võimeid, tagades sellega nii optimaalse reageerimisvõime kui riigi ressursside efektiivsema kasutamise.

### 6.1.3 Programmi tegevus: Valdkonna terviklik juhtimine ja sidusa kogukonna kujundamine

Tabel 6. Programmi tegevuse eesmärk ja mõõdik

| **Tegevuse eesmärk:** | Optimaalsel koostööl ja koosvõimel baseeruv, kaasav, dünaamiline ja tõhus küberturvalisuse tagamine | | | | |
|---|---|---|---|---|---|
| | Algtase (2018) | Sihttase (2021) | Sihttase (2022) | Sihttase (2023) | Sihttase (2024) |
| **Mõõdik:** Loodud on riigiülene küberturvalisuse keskus[15] | Keskus puudub | Analüüs teostatud ja õigusraamistik kujundatud | Keskus on mehitatud ja käivitatud | Keskus töötab | Keskus töötab |

Optimaalsel koostööl ja koosvõimel baseeruv, kaasav, dünaamiline ja tõhus küberturvalisuse tagamine on oluliseks eelduseks kogu KTS laiema visiooni saavutamisel, võimaldades maksimaalse tulemuslikkusega

[13] *Dashboard* ehk visualiseeritud töölaud, mis mõõdab Eesti küberruumi turvalisust

14 CERT.EE valimi põhjal ca 500 kriitilisemat Eesti asutuse domeeni ning e-posti serverit

kasutada Eesti piiratud ressursse. Koostöö ja koosvõime tagamisel olulisteks mõõtmeteks on terviklik juhtimine, kaasav planeerimine ning toimiv kogukond.

### 6.2 Meede: Ettevõtlus ning teadus- ja arendustegevus

Tabel 7. Meetme „Ettevõtlus ning teadus- ja arendustegevus“ eesmärk ja mõõdik

| **Meetme eesmärk:** | Eestis on teaduspõhine, innovaatiline ja globaalselt konkurentsivõimeline küberturbe sektori ettevõtlus, mis katab riigi jaoks olulised võtmekompetentsid | | | | |
|---|---|---|---|---|---|
| **Mõõdik, sh allikas** | Algtase (2018) | Sihttase (2021) | Sihttase (2022) | Sihttase (2023) | Sihttase (2024) |
| Küberturbe sektori ettevõtete ekspordi maht (mln eurot)[16]<br><br>Allikas: Kübervaldkonna tööjõuvajaduse uuring (Praxis 2018) | 15,86 | ≥ 15,86 | ≥ 15,86 | ≥ 15,86 | ≥ 15,86 |

Nii ülikoolides, eraettevõtetes kui ka avalikus sektoris on Eestil väljapaistvat kompetentsi erinevates küberturbe koolkondades, eelkõige turvalise digitaalse identiteedi, krüptograafia, andmete terviklikkuse, küberturbe oskuste, hariduse ja õppuste valdkondades. Rahvusvaheliselt eduka teadus- ja arendustegevuse ning sektori ettevõtluse arendamiseks tuleb Eestil selgelt keskenduda oma maailmas ainulaadsete tugevustele, milleks on eelkõige elektroonilisel identiteedil ja X-tee turvalisel arhitektuuril baseeruv ökosüsteem oma usaldusteenustega. Tugev valdkondlik kompetents erasektoris ja teadusasutustes tähendab Eesti jaoks nii potentsiaali majanduskasvuks läbi sektori edukuse kui ka valmisolekut kriisiolukorras hakkama saada, kuna kogu vajaliku kompetentsi avalikku sektorisse palkamine ei ole teostatav valik.

#### 6.2.1 Programmi tegevus: Küberturbe teadus- ja arendustegevuse ning teaduspõhise ettevõtluse toetamine ja edendamine

Tabel 8. Programmi tegevuse eesmärk ja mõõdik

| **Tegevuse eesmärk:** | Tagatud on riigi kui targa hankija edukas sisuline koostöö ettevõtete ning teadusasutustega. | | | | |
|---|---|---|---|---|---|
| **Mõõdik** | Algtase (2018) | Sihttase (2021) | Sihttase (2022) | Sihttase (2023) | Sihttase (2024) |
| Uute küberturvalisuse valdkonna iduettevõtete arv[17] | 22 | 37 | 42 | 47 | 47 |

Tegevuse eesmärgiks on luua tõhus koostöö ja parem sidusus teaduse, ettevõtluse ja riigi vahel, et parandada võimet viia ülikoolides toimuv arendus rakendusteni nii erasektoris kui riigi teenustes. Eesti väikest turgu võib näha inkubaatorifaasis eelisena, kus saab ühiskonna tasemel töötava toote kiirelt valmis. Strateegilise eesmärgi saavutamise kõige olulisemaks eelduseks on toimivate koostöömehhanismide tagamine akadeemia, eraettevõtete ja riigiasutuste vahel, mis kindlustab, et strateegilised prioriteedid suunavad teadus- ja arendustegevuse fookust nii akadeemias kui ka erasektoris, tagades sellega riigi jaoks oluliste kompetentside olemasolu.

### 6.3 Meede: Rahvusvahelised suhted

Tabel 9. Meetme „Rahvusvahelised suhted“ eesmärk ja mõõdikud

[16] „Küberturbe valdkonna tööjõuvajaduse ja hariduse uuring“, Praxis 2019.a
[17] https://www.startupestonia.ee/startups

| **Meetme eesmärk:** | Eesti on arvestatav partner rahvusvahelisel areenil ning rahvusvaheline suunanäitaja | | | | |
|---|---|---|---|---|---|
| **Mõõdik, sh allikas** | Algtase (2018) | Sihttase (2021) | Sihttase (2022) | Sihttase (2023) | Sihttase (2024) |
| Vastutavate asutuste[18] iga-aastane eksperthinnang Eesti rahvusvaheliste suhete sisulisele kvaliteedile ja fookusele<br><br>Allikas: Välisministeerium, MKM, RIA, Kaitseministeerium | Poliitiline ja strateegiline koostöö toimub läbi üksikute initsiatiivide ja ebaühtlaselt | Pareneb | Pareneb | Koostöö toimub mõtestatult ja süsteemselt, võttes aluseks Eest välispoliitilised prioriteedid | Koostöö toimub mõtestatult ja süsteemselt, võttes aluseks Eest välispoliitilised prioriteedid |

Eesti küber-kaubamärgi tugevus eeldab teadlikku ja terviklikku lähenemist rahvusvahelistele teemadele. Koostöö operatiivtasandil toimub süsteemselt, ent edasi arendamist vajab seda toetav poliitiline ja strateegiline koostöö. Poliitiline ja strateegiline koostöö küberturvalisuse valdkonnas rahvusvaheliste organisatsioonide ja teiste riikidega toimub läbi üksikute initsiatiivide, mis on üles ehitatud erinevate valdkondade ja institutsioonide kaudu ebaühtlaselt. Puudub terviklik ja süsteemne üldpilt koostöömehhanismidest, et kasutada ressursse vastavalt Eesti välispoliitilistest prioriteetidest.

Eesti küberteemaline välissuhtlus peab olema proaktiivne, et püsida üha tihenevas globaalses konkurentsis. Selles saab toetuda Eesti väljakujunenud tugevustele, samas tuleb pidevalt arendada edasi neid valdkondi, kus Eesti saaks olla juhtrollis ning jätkuvalt globaalselt nähtav. Hea näitena võimaldab NATO Küberkaitsekoostöö Keskus Tallinnas olla Eestil juhtrollis NATO küberkaitse küsimustes. Lisaks tuleks aktiivsemalt kaasuda Euroopa Liidu rahvusvahelistesse küberalgatustesse ning jätkata osalust ÜRO, Euroopa Nõukogu, OSCE ja teiste rahvusvaheliste organisatsioonide küberjulgeoleku alastes koostööformaatides.

Arvestades Eesti senist edukat kogemust küberekspertiisi edasiandmisel, tuleks tõhustada küberjulgeoleku alase arengukoostööga seotud tegevusi. Aktiivselt peaks kaasuma ka samameelsete riikide koostöösse küberheidutuse, rünnakute omistamise ja kollektiivsete vastumeetmete osas. Oluline on ka korrakaitseorganite omavaheline aktiivne koostöö rahvusvahelisel tasandil, mis on eelduseks küberkuritegude edukaks menetlemiseks ja tõhusama kaitse pakkumiseks. Koostööl strateegiliste välispartneritega peaks olema tugev praktiline mõõde ühisõppuste, tehnilise infovahetuse näol, mis tagab eduka intsidentide lahendamise.

### 6.3.1 Programmi tegevus: Koostöö tõhustamine strateegiliste välispartneritega

Tabel 10. Programmi tegevuse eesmärk ja mõõdikud

| **Tegevuse eesmärk:** | Stabiilsuse tagamine küberruumis läbi omapoolse osaluse kahe- ja mitmepoolses koostöös | | | | |
|---|---|---|---|---|---|
| **Mõõdik:** | Algtase (2018) | Sihttase (2021) | Sihttase (2022) | Sihttase (2023) | Sihttase (2024) |
| Operatiivtasandil on korraldatud rahvusvahelisele kogukonnale suunatud üritused ja õppused | 2 suuremat rahvusvahelist üritust ning 5 rahvusvahelist õppust aastas | 2 suuremat rahvusvahelist üritust ning 5 rahvusvahelist õppust aastas | 2 suuremat rahvusvahelist üritust ning 5 rahvusvahelist õppust aastas | 2 suuremat rahvusvahelist üritust ning 5 rahvusvahelist õppust aastas | 2 suuremat rahvusvahelist üritust ning 5 rahvusvahelist õppust aastas |

[18] Välisministeerium, MKM, RIA, Kaitseministeerium

| | | | | | |
|---|---|---|---|---|---|
| Eesti küberturvalisuse korraldusega tutvuvate välis-delegatsioonide arv | 80 delegatsiooni aastas | 80 delegatsiooni aastas | 80 delegatsiooni aastas | 80 delegatsiooni aastas | 80 delegatsiooni aastas |

Eesti peamine huvi rahvusvahelistes suhetes küberjulgeoleku valdkonnas on stabiilsuse tagamine küberruumis läbi omapoolse osaluse kahe- ja mitmepoolses koostöös. Selleks teeb Eesti tihendatud koostööd olulisemate liitlastega nii poliitilisel kui ka praktilisel tasandil, sh suuremate rahvusvaheliste organisatsioonide raames. Üheks näiteks Eesti senisest rahvusvahelisest koostööst on kübernormide, usaldusmeetmete ja rahvusvahelise õiguse valdkond, kus on oluline jätkata Eesti senist edukat osalust ÜRO, OSCE jt protsessides.

Süvendatud küberjulgeolekualase koostöö eelduseks lähemate partnerriikidega on vastavad koostööraamistikud ja protseduurid ning nende regulaarne rakendamine. Eestil on ka selles valdkonnas tänaseks kujunenud arvestatav ja globaalselt konkurentsivõimeline ekspertiis, mis väärib arendamist. Koostööformaatide konkurentsivõimelisena hoidmiseks tuleb tagada nende piisav rahastamine. Rahvusvaheline koostöö erinevate oluliste partneritega küberõppuste osas on kriitiline riigikaitse ning üldise küberturvalisuse jaoks. Eesti huvides on tagada ka küberrünnakute edukas lahendamine, mille jaoks on omakorda vaja hoida ja edendada piiriülest koostööd, sealjuures tagada menetlusteabe kiire ja tõhus kättesaamine teistest riikidest ning tugevdada üldist infovahetust ja koostööd.

Eesti kaasatuse küberjulgeolekuga seotud rahvusvahelistesse aruteludesse ja protsessidesse tagab suutlikkus pidada sisulist dialoogi oluliste partneritega. Sisulise dialoogi pidamiseks peab Eesti suutma panustada rahvusvahelisel areenil omapoolse teabe ja analüüsiga küberintsidentidest- ja rünnakutest.

Läbivalt oluline on rahvusvaheliste tegevuste riigisisene koordineerimine, mille tagamiseks hoitakse tugevat ja jätkupidevat koordinatsiooniformaati. See kindlustab, et Eesti rahvusvahelised sõnumid on ajakohased ja ühtsed ning kõik osapooled lähtuvad oma rahvusvahelistes tegevustes ühiselt kokkulepitud prioriteetidest.

### 6.4 Meede: Küberoskuslik ühiskond

Tabel 11. Meetme „Küberoskuslik ühiskond“ eesmärk ja mõõdikud

| **Meetme eesmärk:** | Eesti on ühiskonnana küberteadlik ning tagatud on valdkonna spetsialistide piisav järelkasv | | | | |
|---|---|---|---|---|---|
| **Mõõdik** | Algtase (2018) | Sihttase (2021) | Sihttase (2022) | Sihttase (2023) | Sihttase (2024) |
| Interneti kasutamisel turvaohuga kokku puutumise tulemusel kahjukannatanute osakaal (%)[19] | 27,7% (2015) | ≤ 20% | ≤ 20% | ≤ 20% | ≤ 20% |
| Ametlikult kinnitatud IKT turvapoliitika kasutamine ettevõtetes (%)[20] | 16.9% (2015) | ≥ 25% (2020) | ≥ 25% | ≥ 25% | ≥ 25% |
| **Mõõdik:** Küberkaitse erialade lõpetajate %, mis jõuab Eesti tööturule.[21] | 33 (2017) | >35 | >35 | >35 | >35 |

[19] Vähemalt ühe järgmise turvaohuga kokkupuutumine viimase 12 kuu jooksul 16-74.aastastest arvuti- ja internetikasutajatest: viiruse või muu pahavaraga nakatumine, mille tõttu läks kaotsi andmeid ja/või kulutasite aega; internetti sisestatud isikliku info kuritarvitamine või muu privaatsuse rikkumine; rahalise kahju saamine, järgides kuritahtliku e-kirja, libaveebilehe instruktsioone; kaardimaksepettuse ohvriks langemine; laste ligipääs ebasobivatele veebilehekülgedele.

[20] Valimis 10+ töötajaga ettevõtted

[21] „Küberturbe valdkonna tööjõuvajaduse ja hariduse uuring“, Praxis 2019.a

Laiemat ühiskonda silmas pidades, oli Eestis 2015.aastal turvaohuga kokku puutunud 30% internetikasutajatest[22]. Erasektori poolelt peegeldab üleüldist rünnetega toimetulekut madal teadlikkus turvapoliitikate rakendamisest, mida on 2015.a seisuga teinud 17% kõigist Eesti ettevõtetest[23].

Selleks, et ühiskonnaliikmed saaksid turvaliselt küberruumis tegutseda, on esmatähtis tagada spetsialistide järelkasv küberturvalisuse eest vastutavate organisatsioonide jaoks, pöörates tähelepanu talendiprogrammidele, taseme- ja täiendkoolitusele. Selge ootus spetsialistide järele avaldub kolmes grupis – avaliku sektori küberturbe eest vastutavad asutused, elutähtsaid teenuseid osutavad asutused ning kübersuunaline ettevõtlus.

Laiemale ühiskonnale on vaja järjepidevalt teadvustada valitsevaid riske, jagada nõuandeid riskide maandamiseks ja rõhutada, et küberturvalisuse alaste teadmiste ja oskuste arendamine on kõigi küberruumis tegutsejate ühine vastutus.

### 6.4.1 Programmi tegevus: Kodanike, riigi- ja erasektori küberteadlikkuse tõstmine

Tabel 12. Programmi tegevuse eesmärk ja mõõdik

| **Tegevuse eesmärk:** | Kõigil küberruumis tegutsejatel on vajalikul tasemel teadmised ohtudega toimetulekuks | | | | |
|---|---|---|---|---|---|
| | Algtase (2018) | Sihttase (2021) | Sihttase (2022) | Sihttase (2023) | Sihttase (2024) |
| **Mõõdik:** Küberteadlikkuse testimis- ja koolitusplatvormi kasutavad süsteemselt valitsusasutused, põhiseaduslikud institutsioonid ja KOVid [24] | 53% kõikidest valitsus-asutustest | 80% kõikidest valitsus-asutustest | 90% kõikidest valitsus-asutustest | Kõik valitsus-asutused | Kõik valitsus-asutused |

Kiirelt muutuv küberruum loob vajaduse tegeleda erinevate sihtrühmade teadmiste ja oskuste arendamisega järjepidevalt. Selle saavutamiseks on ühelt poolt vaja jooksvalt omada ülevaadet ohutrendidest ning teiselt poolt erinevate sihtrühmade teadmiste ja oskuste tasemetest. Küberturvalisus on märksõna, mis on muutnud oluliseks mitte ainult IT-valdkonna, vaid kõikides eluvaldkondades.

Erinevad osapooled rõhutavad üldharidustasemel omandatud digipädevuste[25] sh küberturvalisuse osaoskuste olulisust – mida paremate baasoskuste ja teadmistega noored sealt väljuvad, seda lihtsam on järgmistel haridustasemetel ja täiendkoolituste raames tegeleda spetsiifilisemate oskuste arendamisega. Varane kokkupuude IT õppega (nt programmeerimine, robootika jne) üldhariduses on aga tõendatult oluline positiivne mõjutegur IKT erialadel õpingutega jätkamiseks, sh küberturvalisuse suunal.

Tööturul on aasta-aastalt muutunud üha kriitilisemaks sihtrühmaks keskastme- ja tippjuhid, ühiskonnale oluliste teenuste osutajate ja riigiasutuste töötajad, mh omavalitustes. Jätkuvalt on riskigrupis eraettevõtted ja eeskätt väikeettevõtted, kellel puudub sageli võimekus ise küberintsidentidega toime tulla – igakuiselt pöördub RIA poole abi saamiseks ca kümmekond eraettevõtet.

Eelneva tulemusel koondatakse parema koordinatsiooni ja tervikpildi omamise eesmärgil küberteadlikkuse tõstmisega seotud tegevused ühisele platvormile ning pakutakse iseõppimisvõimalusi. Küberturvalisust käsitletakse haridussüsteemis digipädevuste arendamise raames läbivalt kõigil haridustasemetel.

### 6.4.2 Programmi tegevus: Riigi- ja erasektori nõudlusele vastava talendi arendamine

[22] Infotehnoloogia leibkonnas 2015.a www.stat.ee
[23] Infotehnoloogia ettevõttes 2016.a www.stat.ee
[24] Allikas: Riigi Infosüsteemi Amet
[25] Õppija digipädevuse mudel

Tabel 13. Programmi tegevuse eesmärk ja mõõdik

| **Tegevuse eesmärk:** | Tagatud on nii riigi kui avaliku sektori jaoks vajalik kübervaldkonna tööjõud | | | | |
|---|---|---|---|---|---|
| | Algtase (2018) | Sihttase (2021) | Sihttase (2022) | Sihttase (2023) | Sihttase (2024) |
| **Mõõdik:** Küberkaitse erialade lõpetajate %, mis jõuab Eesti tööturule.[26] | 33 (2017) | >35 | >35 | >35 | >35 |

2016. aastal läbi viidud OSKA info- ja kommunikatsioonitehnoloogia (IKT) valdkondlik tööjõuanalüüs[27] näitas, et aastas vajavad Eesti erinevad majandussektorid kokku ca 1,5 korda senisest enam IKT spetsialiste. Sama kinnitavad ka huvigruppidega peetud arutelud – kõrghariduse taseme lõpetanute kvantiteet ja kvaliteet ei vasta Eesti tööturu nõudlusele.

Puudub ka täpsem ülevaade küberturvalisuse valdkonna tööjõuvajadusest ja kompetentsidest. Viimane on eriti kriitilise tähtsusega ühiskonnale oluliste teenuste osutamisega tegelevate sektorite kontekstis – ettevõtetesse tööle asuvad spetsialistid peavad ideaalis erialased küberoskused saama tasemeõppest (nt energeetika ja sideinsenerid, tervishoiuspetsialistid jt). Samas puudub ülevaade ja arusaam prioriteetsete valdkondade spetsiifilistest vajadustest küberoskustele. Probleemiks on vastavate kompetentside kirjelduste puudumine (nt kutsestandardites) ning need ei ole lõimitud vastavatesse õppekavadesse.

Kuigi Eesti ametnike küberhügieen on hea, näitavad aga riigiasutuste intsidendid, et ainuüksi küberteadlikkuse tõstmisega turvalisust ei taga ning keskenduda tuleb turvalisele arhitektuurile, investeerida nõuete täitmisse ja tagada infoturbekompetentsi olemasolu asutustes[28]. Kokku tuleb leppida infoturbekompetentsis hõlmatud oskuste ja oskustasemete sisus ning vajaduse ulatuses asutuste lõikes. Seejärel on vajalik kaardistada vastavasisulise kõrghariduse ning täiendkoolituse pakkumist Eestis ja väliriikides ning luua vajaduspõhised toetusmeetmed. Eesmärk on tagada nii riigi kui avaliku sektori jaoks vajalik kübervaldkonna tööjõud, arendades selleks andekaid noori nii formaalhariduses kui koolivälise tegevuste kaudu ning koolitada tööturu nõudlustele vastavuses küberturvalisuse spetsialiste.

LISAD:

1. LISA 1 Rahastamiskava planeerimistasandite lõikes sh eesmärgid ja mõõdikud (SJIS)

[26] „Küberturbe valdkonna tööjõuvajaduse ja hariduse uuring“, Praxis 2019.a
[27] Tulevikuvaade tööjõu- ja oskuste vajadusele: Info- ja kommunikatsioonitehnoloogia 2016.a
[28] Riigi Infosüsteemi Amet Küberturvalisus 2018