Majandus- ja Kommunikatsiooniministeerium

KÜBERTURVALISUSE STRATEEGIA

2019-2022

Sisukord

Sissejuhatus 3
Strateegia visioon ja aluspõhimõtted 4
Prioriteetsed tegevused 5
1. Lähtekohad: küberturvalisuse olukord strateegia koostamisel 7
1.1. Küberturvalisuse tagamist mõjutavad arengusuundumused 7
1.2. Eesti tugevused 10
1.3. Eesti väljakutsed ja probleemid 11
2. Strateegia koordinatsioon ja elluviimine 14
2.1. Küberturvalisuse strateegia roll ja ulatus 14
2.2. Seosed teiste arengukavadega 14
2.3. Seosed teiste riikide ja rahvusvaheliste strateegiatega 16
2.4. Riikliku küberturvalisuse tagamise koordinatsioon ja juhtimiskorraldus 17
3. Strateegilised eesmärgid 20
JÄTKUSUUTLIK DIGITAALNE ÜHISKOND 22
Tegevussuund 1.1. Tehnoloogilise vastupanuvõime tõhustamine 22
Tegevussuund 1.2. Intsidentide ja kriiside ennetamine, valmisolek ja haldamine 25
Tegevussuund 1.3. Valdkonna terviklik juhtimine ja sidusa kogukonna kujundamine 26
ETTEVÕTLUS NING TEADUS- JA ARENDUSTEGEVUS 28
Tegevussuund 2.1. Küberturbe teadus- ja arendustegevuse ning teaduspõhise ettevõtluse toetamine ja edendamine 28
RAHVUSVAHELISED SUHTED 31
Tegevussuund 3.1. Koostöö tõhustamine strateegiliste välispartneritega 32
Tegevussuund 3.2. Jätkusuutliku kübervõime rahvusvaheline edendamine 33
KÜBEROSKUSLIK ÜHISKOND 35
Tegevussuund 4.1. Kodanike, riigi- ja erasektori küberteadlikkuse tõstmine 36
Tegevussuund 4.2. Riigi- ja erasektori nõudlusele vastava talendi arendamine 38
LISA 1: Kübervaldkonnaga seotud terminid ja definitsioonid 40

SISSEJUHATUS

„Küberturvalisuse strateegia“ on kolmas küberjulgeoleku ja -turvalisuse valdkonna strateegiadokument, mis määratleb valdkonna pikaajalisema visiooni, selle saavutamiseks vajalikud eesmärgid ja prioriteetsed tegevussuunad, rollid ja ülesanded ning on tegevuste ja ressursside planeerimise aluseks. Strateegia tugineb kahe eelneva perioodi (2008-2013 ja 2014-2017) kogemustele ning horisontaalse strateegiana kaasab see Eesti küberturvalisuse tagamisse panustavad osapooled: avaliku sektori (nii tsiviilvaldkond kui ka riigikaitse), ühiskonna toimimiseks oluliste teenuste osutajad, valdkonnas tegutsevad ettevõtjad ning ülikoolid ja teadusasutused. Dokumendi koostamise eesmärk on kokkulepete sõlmimine ja tingimuste loomine tervikliku, süsteemse ja kaasava valdkondliku poliitika elluviimiseks.

2008. aasta küberjulgeoleku strateegia[1] oli Eesti esimene riiklik strateegiadokument, mis tunnistas küberjulgeoleku ja -turvalisuse valdkondadeülesust ning vajadust koordineeritud tegevuse järele. Ühtlasi oli tegemist ühega esimestest horisontaalsetest kübervaldkonna strateegiatest maailmas – küberjulgeolekut ja -turvalisust hakati riigi julgeoleku ja turvalisuse aspektina tajuma alles pärast 2007. aastal toimunud Eesti-vastaseid küberrünnakuid.

Eesti strateegiale järgnes mõne aasta jooksul riiklike küberjulgeoleku strateegiate koostamise laine kogu maailmas. Tänaseks on küberjulgeoleku strateegia enam kui seitsmekümnel riigil[2] ning suur osa neist juhindub lähenemisest, mille Eesti esimeses strateegias defineeris. Euroopa Liidu 2013. aasta küberjulgeoleku strateegia[3] määratles ühtse küberturvalisuse miinimumpaketi (määrata riigi pädevad asutused, käivitada toimiv operatiivtasandi üksus küberintsidentidele reageerimiseks, kehtestada riiklik küberjulgeoleku strateegia); 2016. aastal vastu võetud Euroopa Liidu võrgu- ja infosüsteemide turbe direktiiv[4] tegi sellest õigusliku kohustuse. Teise põlvkonna küberjulgeoleku strateegia on praeguseks mõneteistkümnel riigil[5] - nende seas ka Eesti 2014. aasta küberjulgeoleku strateegia[6] - ja Euroopa Liidul. Kolmanda valdkondliku strateegiaga oleme maailmas esimeste riikide seas.

Küberjulgeolek ja -turvalisus on nüüdseks universaalselt leidnud aktsepteerimist nii riigi ja majanduse toimimise kui ka sise- ja välisjulgeoleku lahutamatu osana. Kiirenev, mitmekesistuv ja paljuski ennustamatu digitaliseerumine tähendab suuri väljakutseid võimalike riskide ja ohtude hindamisel. Kriitiliselt hinnates, ei ole selle kõrval, Eesti ühiskond täna valmis ka ammu teada küberohtudega toimetulekuks – riskid ja vajadused on nii era- kui avalikus sektoris paljus teadvustamata, seda ennekõike juhtimistasandil.

Digitaalsetel tehnoloogiatel on nüüdseks Eestis sedavõrd läbipõimunud roll mis tahes valdkonnas, et kõigi riskidega toimetulekut ei ole võimalik korraldada ühe planeerimisdokumendi kaudu. Küberturvalisuse põhimõtted on juba täna osaliselt integreeritud erinevatesse valdkondlikesse planeerimisprotsessidesse, kuid jätkusuutliku digitaalse keskkonna hoidmine ja arendamine eeldab lisaks küberohtude käsitlemisele integreeritud teemana ka valdkondadeülest fokusseeritud koostööd, mille elluviimisse on kaasatud kõik asjassepuutuvad osapooled era- ja avalikust sektorist. Seda saab tagada vaid tugeva ja ühtse valdkondliku strateegia läbi. Lisaks on strateegial ka oluline roll kommunikatsioonivahendina valdkonna arengusuundade teadvustamiseks poliitilisel otsustustasandil, avaliku- ja erasektori koostöö tõhustamisel ning Eesti rahvusvahelise kuvandi ja sõnumite kujundamisel.

Küberturvalisuse strateegia on koostatud ühtse protsessina koos „Infoühiskonna arengukavaga 2020“. Senised kogemused on viinud arusaamani, et eduka digiriigi loomiseks ja arendamiseks peavad infoühiskonna arendamine ja küberturvalisuse tagamine toimuma strateegiliselt ühtsena. Küberturvalisuse roll infoühiskonnas on tagada tingimused selleks, et IKT võimalusi saaks tõhusalt ja turvaliselt kasutada. Küberturvalisuse strateegia eesmärgid ja tulemusindikaatorid on üldreeglina (nagu kahel eelmisel strateegiaperioodil) planeeritud nelja-aastases perspektiivis, kuid kogu strateegiaperioodi lõpptähtaeg

[1] https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf
[2] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
[3] http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52017JC0450&from=EN
[4] http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[5] https://ccdcoe.org/cyber-security-strategy-documents.html
[6] https://www.mkm.ee/et/tegevused-eesmargid/infouhiskond/kuberjulgeolek

sünkroniseeritakse 2020. a. toimuva vaheülevaatuse ja strateegia ajakohastamise käigus Infoühiskonna arengukava järgmise perioodiga.
Küberturvalisuse strateegias kasutatud olulisemad terminid ja nende definitsioonid on toodud Lisas 1.

STRATEEGIA VISIOON JA ALUSPÕHIMÕTTED

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.

Visiooni elluviimiseks lähtub Eesti küberturvalisuse tagamisel järgmistest aluspõhimõtetest:

1. Peame põhiõiguste ja -vabaduste kaitset ja edendamist internetis sama oluliseks kui füüsilises keskkonnas.

2. Kohtleme küberturvalisust Eesti kiire digitaalse arengu võimaldaja ja võimendajana, mis on Eesti sotsiaalmajandusliku arengu aluseks. Turvalisus peab toetama innovatsiooni ja innovatsioon turvalisust.

3. Teadvustame, et krüptograafiliste lahenduste turvakindluse tagamine on Eesti jaoks unikaalselt oluline, kuna sellel tugineb kogu meie digiriigi ökosüsteem.

4. Digiriigi toimimise aluseks on läbipaistvus ja avalik usaldus. Selle hoidmiseks peame kinni riigipoolse avatud kommunikatsiooni põhimõttest.

Strateegia mõjuindikaatorid:

1. **Eestis ei toimu ühtegi küberintsidenti, mis häiriks olulisel määral ühiskonna sotsiaalset ja majanduslikku toimimist või sunniks loobuma harjumuspärastest digitaalsetest lahendustest**.

   Läbi aegade võib Eestis lugeda ainsaks infoühiskonna toimimise halvanud küberintsidendiks 2007. aasta küberründed. Reaktsioonina küberintsidendile ei ole Eesti seni kordagi loobunud kasutatavatest digitaalsetest lahendustest.

2. **Eesti elanikud tunnevad end internetis turvaliselt ning usaldavad e-riiki**.

Jälgitavad mõõdikud:

Mõõdik	**Algtase**	**Sihttase**	**Allikas**
Turvariski vältimise kaalutulustel avaliku sektori või teenusepakkujaga elektroonilisest suhtlemisest hoidunute osakaal[7]	3,1% (2015)	≤ 3.1%[8] (2020)	Statistikaamet

[7] Viimase 12 kuu jooksul turvariskide tõttu internetitegevusest hoidunud 16-74-aastased internetikasutajad: suhtlemine avaliku sektori asutuste või teenusepakkujatega. https://ec.europa.eu/eurostat/web/digital-economy-and-society/data/database
[8] Mõlema mõõdiku sihttase ajakohastatakse 2020 vaheülevaatuse käigus

Turvalist elektroonilist identiteeti[9] kasutavate inimeste osakaal elektroonilist identiteeti omavatest elanikest[10]	57,6% (2017)	≥ 65% (2020)	SK ID Solutions AS

PRIORITEETSED TEGEVUSED

Me **ennetame:**

- Uued teenused ja andmekogud ehitame ülesse arvestades turvalisuse ja privaatsuse põhimõtet (*security and privacy by design*) ning vabanetud on taakvarast ehk vananenud platvormidest (*no legacy* põhimõte). Selleks arendame välja keskse turvarhitektuuri nõustamise võimekuse.
- Eesti info- ja võrguturbe riiklikul korraldamisel lähtume riskipõhisest lähenemisest ja parimatest rahvusvaheliselt tunnustatud standarditest ning praktikatest. Toetame nende laiapindset rakendamist.
- Riik omab koostöös kõigi osapooltega terviklikku küberruumi olukorrapilti. Selleks süvendame riigivõrgu automaatseiret, võimaldame võrguseiret ka eravõrkudele.
- Meil on targad digitehnoloogia kasutajad. Selleks muudame küberteadmised ja -oskused üldhariduse läbivaks osaks ning viime süsteemselt ellu teavituskampaaniad ja täiendkoolitusi. Sealjuures tõstame teadlikkust nii ohtudest kui ka õiguspärasest ja õigusvastasest käitumisest.
- Tagatud on ühiskonnale oluliste teenuste digitaalne turvalisus. Selleks on tagatud süsteemne rist- ja piiriüleste sõltuvuste haldamine ning turvatestide läbiviimine kõige kriitilisemate teenuste andmekogudele ja infosüsteemidele.
- Küberturvalisuse tagamine on teadvustatud kõigi küberruumis tegutsejate ühise vastutusena.

Me **kaitseme:**

- Ühendame riigi käsutuses olevad võimed, et teha olemasoleva ressursiga enam. Selleks viime läbi küberturvalisuse võimete auditi ning käivitame riikliku küberturbe keskuse (NCSC).
- Hõlmame küberturvalisuse riigikaitse laia käsitusse. Selleks integreerime küberturvalisuse riigikaitse planeerimisdokumentidesse (riigikaitse arengukava ja riigi kaitsetegevuse kava) ning viime regulaarselt läbi ühiseid õppuseid ühiskondlikult oluliste teenuste osutajate, riigi poliitilise juhtkonna ning riigikaitseorganisatsioonidega.
- Hoiame aktiivset ja sidusat küberturvalisuse kogukonda. Selleks pakume tehnilist infovoogu, korraldame ühisõppuseid ning kaasame nii erasektori kui akadeemilise kompetentsi seadusloome ja strateegilise planeerimise protsessidesse.
- Arendame välja küberoperatsioonide võime. Selleks arendame edasi kaitseväe küberväejuhatust, töötame välja küberründe võime ning edendame küberajateenistust.
- Rakendame meetmeid küberkuritegevuse ohjeldamiseks. Selleks loome raamistiku ametkondadevaheliseks tõhusaks koostööks ja infovahetuseks, koolitame menetlejaid, edendame otsekontakte menetlejate ning rahvusvaheliste tippekspertide vahel ning suurendame õiguskaitseorganite võimekust.
- Tagame kriitiliste andmekogude ning riikliku andmeside turvalisuse. Selleks juurutame riigiside kontseptsiooni ning tagame kriitiliste andmekogude peegeldamise välisriikides asuvatesse andmesaatkondadesse[11].
- Tugevdame praktilist igapäevast koostööd oma rahvusvaheliste strateegiliste partnerite ja liitlastega.

[9] 2017. aasta andmete puhul loeti turvaliseks elektroonseks identiteediks riigi poolt väljastatavaid identiteete:
[10] Inimeste arv, kes on viimase aasta jooksul vähemalt ühe korra kasutanud eID teenust.
[11] Andmesaatkonna mõiste ja eesmärk on selgitatud dokumendis „Eesti Vabariigi ja Luksemburgi Suurhertsogiriigi vaheline andmete ja infosüsteemide majutamise kokkulepe“. https://www.riigiteataja.ee/akt/228032018002

Me **arendame:**

- Tagame spetsialistide järelkasvu. Selleks käsitleme küberturvalisust süvendatud IT-õppe osana üldharidustasemel ning esitame ootused ülikoolidele spetsialistide väljaõppeks.
- Toetame riigi, akadeemia ja erasektori võtmepartnerite tulemuslikku koostööd. Selleks käivitame nii siseriiklikku kui rahvusvahelist koostööd soodustava klastri.
- Võimendame küberturvalisuse kui majandussektori kasvu. Selleks toetame innovatsiooni ja tootearendust ning tugevdame diplomaatilist tuge turundustegevustele.
- Loome kübervaldkonna teadus- ja arendustegevuse kava ja koordinatsioonimehhanismi ülikoolide ja ettevõtete poolt läbiviidava teadus- ja arendustegevuse suunamiseks, ettevõtete toetusmeetmete sisustamiseks ning haridusprojektide ja stipendiumite rahastamiseks.
- Tulevikusuundumusi ja -riske analüüsides tagame võimekuse reageerida kiirelt uutele väljakutsetele ja ohtudele.
- Edendame konkurentsivõimelist ja jätkusuutlikku kübervõimet partnerriikides. Selleks jagame Eesti kogemusi kolmandatele riikidele läbi Euroopa Liidu ja ka rahvusvaheliste projektide.

Visioonini jõudmine vajab läbivalt:

- Piisava kompetentsi, inimressursi ja rahaliste vahendite olemasolu;
- Küberturvalisuse lõimimist kõikidesse valdkondadesse ja olulistesse planeerimisprotsessidesse;
- Protsesside keerukuse haldamist ja bürokraatlike tõkendite minimiseerimist riigi-, erasektori ja teadlaskonna jaoks nii õiguslike kui riigihalduslike vahenditega.

1. LÄHTEKOHAD: KÜBERTURVALISUSE OLUKORD STRATEEGIA KOOSTAMISEL

Digitaalne riik on ligi 20 aastat olnud ja on endiselt Eesti teadlik valik, mis loob ühiskonnale märkimisväärset lisaväärtust. Ainuüksi eID ökosüsteemi majanduslik kogumõju aastas jääb hinnanguliselt suurusjärku 800-1500 miljonit eurot ehk 4-7% SKPst.[12] Digiriigi teostuse ja paljude e-teenuste osas on Eesti rajaleidja kogu maailmas – see toob kaasa nii võimalusi kui ka riske. Tõsiseltvõetavat alternatiivi digiühiskonnale ei ole, mistõttu ei ole ka alternatiivi turvalisusesse investeerimisele. Küberturvalisus ei tähenda Eesti jaoks kitsalt tehnoloogiliste lahenduste kaitsmist, vaid ennekõike digitaalse ühiskonna ja eluviisi kaitsmist tervikuna.

Eesti strateegilisi valikuid mõjutab olulisel määral globaalne küberkeskkond ja selle nii soovitud kui soovimatud arengud, kuna küberohtudele on iseloomulik riigipiiride tähendusetus ja rünnete globaalne ulatus. Eesti küberruumi turvalisust mõjutavad olulisel määral erinevad siseriiklikud ja rahvusvahelised suundumused, mida on lähemalt käsitletud Riigi Infosüsteemi Ameti, Kaitsepolitseiameti ja Välisluureameti aastaraamatutes[13], akadeemilistes uuringutes[14] ning riskianalüüsides[15], ja küberkaitseõppuste järeldustes. Eriti väärtuslikud on vahetud õppetunnid nii enda kui välispartnerite kogemusest ja strateegia koostamise arutelude käigus saadud kogukonna tagasiside. Samuti on Eestil olnud ainulaadne võimalus läbida vajalikud õppetunnid maailmas ainulaadsete küberkriiside – näiteks 2007 küberrünnakud või 2017 ID-kaardi kriis – lahendamisel ning vahetult rakendada saadud kogemusi oma strateegiliste suundade valikul.

1.1. KÜBERTURVALISUSE TAGAMIST MÕJUTAVAD ARENGUSUUNDUMUSED

Küberturvalisust mõjutavad trendid kujundavad keskkonda, milles riigid toimetavad ja millest peab tegevuste kavandamisel lähtuma. Eestil on väga piiratud võimalused nende trendide muutmiseks, küll aga peame nende suundumustega arvestama.

Laienev tehnoloogiakasutus, kasvav digitaalne sõltuvus ja uute tehnoloogiate areng

Üleilmset digitaalset keskkonda tervikuna iseloomustavad mahtude intensiivne kasv, tehnoloogia kiire areng ja ühiskondade suurenev digitaalne sõltuvus. Ajavahemikus 2015-2019 hinnatakse internetikasutajate arvu kogu maailmas kasvavat miljardi, nutitelefonide hulk 2,6 miljardi ja internetti ühendatud erisuguste seadmete hulk 8,1 miljardi võrra. Globaalse andmesideliikluse maht kasvab oodatavalt rohkem kui kaks korda ja säilitatavate andmete maht viiekordistub.[16] Aastaks 2020 ennustatakse asjade interneti[17] seadmete hulga jõudmist 20-50 miljardile ning pilvandmetöötluse mahu kolmekordistumist võrreldes 2015. aastaga.[18] Samal ajal mõjutavad keskkonda masinõppe ja tehisintellekti areng, kiirelt kasvav robootika ja iseliikuvate objektide kasutuselevõtt, plokiahela tehnoloogia ning potentsiaalne kvantarvutite kasutuselevõtt lähitulevikus.

Uute tehnoloogiate areng toob kaasa nii küberründe vahendite, viiside ja sihtmärkide mitmekesistumise kui ka küberturvalisuse tagamise võimaluste muutumise. Kasvanud on nii riigi kui erasektori digitaalne sõltuvus,

---

[12] Arvestades digiallkirjastamisega keskmiselt säästetud aega, tööajapõhist kogukulu ning aastas antud digiallkirjade arvu. Lähteandmed: Tarmo Kalvet, Marek Tiits, Hille Hinsberg (toimetajad) (2013). E-teenuste kasutamise tulemuslikkus ja mõju. Tallinn: Balti Uuringute Instituut ja Poliitikauuringute Keskus Praxis (ajasääst); https://www.ria.ee/ee/pea-poole-miljoni-id-kaardi-sertifikaadid-vajavad-uuendamist.html (2016. aastal antud keskmine digiallkirjade ja tehtud autentimiste arv ning kasutatud digitaalsete isikut tõendavate dokumentide hulk); https://www.stat.ee/stat-skp-jooksevhindades (SKP jooksevhindades).

[13] https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturvalisus-2018.pdf, https://www.kapo.ee/et/content/aastaraamatu-v%c3%a4ljaandmise-traditsiooni-ajalugu-ja-eesm%c3%a4rk-0.html, https://www.valisluureamet.ee/pdf/raport-2018-EST-web.pdf

[14] „ID-kaardi kaasuse õppetunnid“, Tallinna Tehnikaülikool, 2018: https://www.ria.ee/public/PKI/ID-kaardi_oppetunnid.pdf

[15] „Küberintsident. Hädaolukorra riskianalüüs“, Riigi Infosüsteemi Amet, 2018 (juurdepääsupiiranguga AK)

[16] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-threats-predictions-2016.pdf

[17] internetiühendusega seadmete võrk, kus seadmed nii kasutaja kui ka üksteisega informatsiooni jagavad ja vahetavad. Asjade interneti seadmed võivad olla näiteks nutitelefonid, külmikud, pesumasinad, nutikellad, meditsiiniseadmed, hooned, lennukimootorid.

[18] Cloud and IoT Threats Predictions. McAfee Labs, Nov 2016. https://www.mcafee.com/hk/resources/misc/infographic-cloud-iot-predictions-2017.pdf

mis omakorda puudutab teenuseid kõigis eluvaldkondades, ka seni tehnoloogiaga üksnes kaudselt seotuid. 2016. aastal RIA tellimusel korraldatud elutähtsate teenuste toimepidevusuuringu järelduste kohaselt sõltuvad eranditult kõik Eesti elutähtsa teenuste osutajad oma tegevuses IKT-st ning ligi pooled loevad oma sõltuvust kriitiliseks.[19] ID-kaardi turvariski kaasus 2017. aasta sügisel näitas eluliselt, kuivõrd sõltuvad on digitaalse baastaristu toimimisest ja kättesaadavusest nii riigivõimu teostamine kui ka erasektor ehk ühiskonna tavapärane toimimine tervikuna.

Kasvav, muutuv ja teenuspõhine küberkuritegevus

Arvestades, et oluline osa inimeste tegevusest on liikunud küberruumi, pannakse ka järjest suurem osa süütegudest toime selle võimalusi kasutades. Teenusetõkestusrünnaku või lunavarakampaania korraldamiseks ei ole enam vaja kõrgeid tehnilisi oskusi või suuri ressursse. See lisab suure hulga võimalikke kurjategijaid, kellel on võimekus Eesti riiki ja inimesi interneti vahendusel rünnata. Europoli küberkuritegevuse ohuhinnangu kohaselt ületab mõnes Euroopa Liidu liikmesriikigis küberkuritegude arv traditsiooniliste kuritegude oma juba 2016. aastal.[20] Küberkuritegevusega tekitatud ülemaailmse majanduskahju suurus jääb maha vaid korruptsioonist ja narkokuritegevusest ning moodustab hinnanguliselt 0.8 protsenti maailma SKT-st.[21] IKT sektori arenguga tekivad uued küberrünnete toimepanemise vahendid ja meetodid. Endiselt pannakse enim küberkuritegusid toime kasutades lunavara, kuigi kasvu on märgata ka teenusetõkestusrünnete arvus, sealhulgas nende rünnete, mille käigus kasutatakse ära asjade interneti seadmete turvanõrkusi.[22] Küberkuritegevuse levikut mõjutavad mitmed tegurid nagu teenuste arhitektuuri turvalisus, elanikkonna teadlikkus ohtudest ja sellest, kuidas end nende eest kaitsta, kuriteo toimepanemiseks kuluv vaev, selle kasumlikkus ja tabamise tõenäosus.

Keerukas julgeolekuolukord

Eesti küberturvalisust mõjutab paratamatult ka keerukas julgeolekuolukord nii siinses regioonis kui kogu maailmas. Küberoperatsioonide kasutamine riikide soovitud strateegilise eesmärgi või mõju saavutamiseks on viimastel aastatel muutunud sagedamaks ja tõsisemaks: mõjutatakse nii demokraatlikke protsesse (valimised ja referendumid ning nendega seotud kampaaniad) kui ka rünnatakse elutähtsat taristut (eeskätt energia-, side- ja pangandussektoris).[23] Küberoperatsioonide laiemaks eesmärgiks võib olla poliitiline või majanduslik mõjuvõim ning vahendina kasutatakse rahvusvahelise kogemuse põhjal poliitilist (sh avaliku arvamuse) mõjutustegevust ja nt küberkuritegevuse toetamist või sihitud ründeid elutähtsate objektide vastu. Sealjuures võimaldab küberoperatsioonide läbiviimine kombata nõrkusi ja halle alasid, kus eesmärke on võimalik saavutada oluliselt madalama kuluga kui konventsionaalse sõjalise tegevuse korral (kuivõrd viimane kanaliseerib tugevuse rünnatava osapoole tugevuse vastu ning põhjustab rahvusvaheliselt kogukonnalt tugevamat vastuseisu).

Küberturvalisus on esmajoones tehnoloogilise ja institutsionaalse võimekuse olemasolu ning teadliku rakendamise küsimus, ent ühiskonna turvatunnet mõjutab olulisel määral ka kommunikatsiooniaspekt ehk küberturvalisuse tajumine. Erinevate avaliku arvamuse uuringute järgi hinnatakse küberrünnakute toimumise tõenäosust kas pigem madaks või keskmiseks[24]. Samas aasta varem, 2017. aasta märtsis tehtud uuringu kohaselt peab 67% eestlastest organiseeritud küberrünnaku toimumist kõige suurema tõenäosusega

---

[19] https://www.ria.ee/public/Kuberturvalisus/Elutahtsate-teenuste-osutamist-mojutavate-tegurite-uuringu-kokkuvote.pdf

[20] Internet Organised Crime Threat Assessment (IOCTA) 2016. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

[21] McAfee, Economic Impact of Cybercrime, 2018. https://www.mcafee.com/enterprise/en-us/solutions/lp/economics-cybercrime.html

[22] Iocta 2017. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

[23] nt WannaCry ja NotPetya. Pärast küberründeid elektrijaamade vastu Ukrainas 2015. ja 2016. aasta detsembris on energiasektori taristust saanud küberrünnete sagedane sihtmärk.

[24] 2018.a Siseturvalisuse avaliku arvamuse uuringus peetakse küberrünnakute toimepanemist infosüsteemide vastu tõenäoliseks 27% poolt vastanutest. Samas hinnatakse Eesti riigi / valitsuse tegevust küberkuritegevusega võitlemisel kõrgelt (64%).

ohuks Eestile.[25] Eeskätt ühiskonna stabiilsuse ja majanduskeskkonna toimimise seisukohast on hädavajalik, et riigi elanikud ja meie välispartnerid oleksid veendunud, et Eestil on olemas vajalik võimekus küberohtudega toimetulekuks.

Piiratud tehnoloogiline autonoomia

Eesti on osa ülemaailmsest digitaalsest keskkonnast ning tugineb suures osas välismaistele IT-lahendusele. Arvutite ja võrguseadmete riistvara on üldiselt pärit Aasiast, operatsioonisüsteemid, tarkvara ja teenused enamasti USA-st. See tingib, et meie küberturbe olukorda mõjutavad teiste riikide IT-lahenduste turvanõrkused ja nende vastu tehtud ründed.[26] Nii meie kui ka teiste Euroopa riikide käitumine on seetõttu paljus vältimatult passiivne ja keskendub laiatarbe-lahenduste turvavigadele reageerimisele või riskide ennetamisele. Eesti peamiste liitlasriikide praktika näitab, et ka riiklikes süsteemides kasutatav (küberkaitse-) tarkvara ja selle päritolu võib omada tähendust riiklikule julgeolekule (näiteks on USA ja Euroopa riigiasutused piiranud oma süsteemides Venemaa või Hiina päritolu toodete kasutamist). Nii Euroopa Liidu kui Eesti huvides on rahvusliku ja Euroopa kübertööstuse tugevdamise kaudu suurendada strateegilist autonoomiat.

Küberjulgeoleku debati globaliseerumine

Küberjulgeolek on saanud arenenud riikide jaoks oluliseks osaks riiklikust julgeolekust, tuues kaasa tähelepanu ja ressursside suurenemise. Viimase kümnendi jooksul on küberjulgeolek jõudnud rahvusvaheliste koostööformaatide prioriteetide hulka.

2010. aastal tunnistas **NATO** oma uues strateegilises kontseptsioonis esmakordselt, et küberründed kujutavad endast julgeolekuohtu.[27] NATO tunnustas 2014. aasta Walesi tippkohtumisel rahvusvahelise õiguse kehtivust küberruumis ning deklareeris, et kuivõrd küberründe mõju kaasaegsele ühiskonnale võib olla võrreldav konventsionaalse ründega, on küberkaitse osa NATO kollektiivkaitse mandaadist.[28] 2016. aasta Varssavi tippkohtumisel nimetas NATO küberruumi üheks sõjaliste operatsioonide domeeniks, kus alliansi kaitsevalmidust tagada.[29]

6. juulil 2016 võttis Euroopa Parlament **Euroopa Liidu** ühtse küberjulgeoleku taseme tõstmiseks vastu võrgu- ja infoturbe direktiivi,[30] mis sisaldab muu hulgas kõigile liikmesriikidele kohustust riikliku võrgu- ja infosüsteemide turvalisuse strateegia koostamiseks. Eesti eesistumise ajal 2017. aastal uuendati Euroopa Komisjoni küberjulgeolekupoliitikat nn. küberpaketi vastuvõtmisega[31], mis sisaldas endas ka Euroopa Liidu küberjulgeoleku strateegia uuendatud versiooni.

Üheks keerukamaks ja olulisemaks rahvusvaheliseks aruteluteemaks on osutunud rahvusvahelise õiguse kohaldumine küberruumile. **ÜRO** tasandil tajutud vajadusest suurema õigusselguse järele ning riikide põhimõttelisest valmisolekust seda selgust otsida ja luua annavad märku ÜRO Peaassamblee kokku kutsutud kübereksperte grupid (UN GGE). Nende 2013. ja 2015. aasta raportites tunnustatakse sõnaselgelt rahvusvahelise õiguse kohaldumist küberruumis. 2017. aasta grupp ei suutnud siiski lõppraportis kokku leppida ning riigid ei ole aastaks 2018 jõudnud lähemale konsensusele, kuidas rahvusvaheline õigus küberruumis kohaldub.

---

[25] „On kaks peamist ohtu, mille realiseerumist peavad enam kui pooled vastanuist lähemate aastate jooksul väga või küllaltki tõenäoliseks: 67 protsendi arvates võib toimuda organiseeritud rünnak Eesti riiklike infosüsteemide vastu (nn küberrünnak) ja 61 protsendi hinnangul võib mõni välisriik sekkuda Eesti poliitika või majanduse mõjutamiseks oma huvides." http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/avalik_arvamus_ja_riigikaitse_marts_2017.pdf

[26] 2017. suuremad küberintsidendid WannaCry ja Petya/NotPetya olid seotud Microsofti nõrkustega, kuid suure rahvusvahelise mõjuga vigu on leitud pea kõikide suurte IT-tootjate lahendustes.

[27] https://www.nato.int/cps/en/natohq/topics_82705.htm

[28] https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[29] https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

[30] http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32016L1148

[31] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=JOIN:2017:450:FIN&rid=3
https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

OSCE raames on 2013. ja 2016. aastal lepitud kokku küberruumi usaldusmeetmetes (*Confidence Building Measures*), mille abil läbi infovahetuse ja koostöö vähendada konfliktiohtu.[32]

Olulise akadeemilise panusena anti 2017. aasta veebruaris välja NATO Küberkaitsekoostöö Keskuse eestvedamisel koostatud küberoperatsioonidele kohalduva rahvusvahelise õiguse käsiraamat (Tallinn Manual 2.0),[33] mis käsitleb küberoperatsioone riikidevaheliste suhete osana rahvusvahelise õiguse kontekstis, andes riikidele praktilisi juhiseid.

Üha komplekssem õiguskeskkond turuosalistele

Digitaalse keskkonna kasvava tähtsuse ja suurenenud riskidega käib kaasas surve ja vajadus valdkonda senisest enam reguleerida nii Euroopa Liidu tasemel kui ka Eesti siseselt. Eesti võimalus on regulatsioonimahtu ohjata, sest protsessidele ja protseduuridele lisandub ka regulatsiooni summaarne keerukus: iga uus regulatsioon on täpsem ja põhjalikum kui eelmine. Riigi IT-lahenduste keerukus kasvab koos regulatsiooni mahuga ning samal ajal muutub olemuslikult keerukamaks ka IT ise. Ühest küljest peab regulatsioon aitama kaasa infoturbe sisulisele rakendamisele ning tagama ühiskonna turvalisuse vastavalt kaalule, mida digitaalne keskkond ühiskonna toimimises kannab. Samas on see väljakutseks valdkonnaülesele toetavale koostööle ning surve Eesti kiirusele ja paindlikkusele, muutes keerukamaks probleemide lahendamise uusi meetodeid ja enda reegleid kasutades, mis on mõneti olnud seniste edulugude eelduseks.

Internetivabaduse väljakutsed

Interneti kättesaadavus on üle maailma suurendanud inimeste juurdepääsu teabele ja toonud lisaks majanduskasule kaasa ka riigivalitsemise suurema läbipaistvuse, loonud võimaluse avalike teenuste paremaks ja odavamaks osutamiseks, kodanikuühiskonna osalemiseks otsustusprotsessides ning tõhustanud globaalset lävimist tervikuna. Viimased aastad on näidanud internetivabaduse tuge demokraatlikele protsessidele, aga ka autoritaarsete riikide kasvavat praktikat internetivabaduse piiramiseks. On riike ja huvigruppe, kes rõhutavad kasutajate ligipääsu piiramise positiivseid aspekte küberjulgeoleku ja turvalisuse vaatest: teenusepakkujate ja vastavate riiklike asutuste paindlikum ligipääs internetiliiklusele ja piirangute kehtestamine võimaldab nende hinnangul nii tõhusamat kaitset võrkudele ja kriitilisele taristule kui ka efektiivsemat võitlust kuritegevusega. Freedom House'i raportite põhjal on Eesti olnud aastast aastasse üks internetivabaduse juhtriikidest ja eeskujudest, kuid globaalsete trendide mõjutamine on suur väljakutse olukorras, kus ülemaailmne internetivabadus on olnud langustrendis viimased seitse aastat[34].

1.2. EESTI TUGEVUSED

Oma tugevustele toetumine võimaldab Eestil ellu viia strateegilisi eesmärke ja leida tõhusaid lahendusi väljakutsetele. Järgnevalt on välja toodud viis enim mõju ja potentsiaali omavat Eesti tugevust kübervaldkonnas.

Eesti digiriigi turvaline alusarhitektuur

Eesti digitaalne arhitektuur baseerub riigi tagatud turvalisel elektroonilisel identiteedil ja X-tee andmevahetuskeskkonnal, mis on olnud kiire digitaalse innovatsiooni võimaldaja ja võimendaja ning tagab, et turve on kodaniku jaoks mugavalt ja loomulikult korraldatud. X-tee võimaldab riigipoolsete teenuste ja andmevahetuse turvalist ülesehitamist ning koostööd ja ID-kaardi kui kohustuslikku isikut tõendava dokumendi näol jagab riik elanikele ühtaegu ka digitaalse identifitseerimistunnistuse (autentimis- ja allkirjastamisvahendi) ja krüpteerimisseadme, viies turvalise tehnoloogia massidesse. Enamgi kui tehnoloogia olemasolu, eristab Eestit teistest riikidest sealjuures suutlikkus tehnoloogiat rakendada.

---

[32] OSCE protsessi väärtus on, et see hõlmab vaadetelt väga erinevaid riike (sh EL riigid, USA ja Venemaa), kelle puhul küberruumis pingeid ja usaldamatust leevendavad praktilised meetmed globaalsele julgeolekule arvestatavat mõju avaldada.
[33] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press, 2017.
[34] https://freedomhouse.org/report/freedom-net/freedom-net-2017

Elementaarne ja järeleproovitud küpsusaste

Eesti praegust küberturvalisust kindlustavad toimiv digiriigi taristu, tugev digitaalne identiteet, riigiasutustele ja oluliste teenuste osutajatele rakendamiseks kohustuslik turvameetmete süsteem, keskne küberturbeintsidentide seire, lahendamise ja raporteerimise süsteem, toetav õigusruum ning toimivad koostööformaadid. Kahe kriisi kogemus (2007 ja 2017) 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 Rahvusvahelise Telekommunikatsiooni Liidu (ITU) indeks[35], mille põhjal Eesti on küberturvalisuse arengu poolest maailmas viiendal ja Euroopas esimesel kohal ning E-Riigi Akadeemia küberindeks[36], mille alusel Eesti on maailmas esimesel kohal.

Väikeriigile omane kiirus ja paindlikkus

Väike ja sidus küberturbe kogukond ning isiklikul tasemel hea läbisaamine on eelduseks efektiivselt aktuaalsetele probleemidele reageerida. Ka mitteformaalselt on teada, kes millega tegeleb, ning otsustusprotsesside subordinatsioon ei ole suur: vajadusel saab suhelda otse tippjuhtide ja poliitikutega. Usalduslikku ja efektiivset koostööd turuosalistega toetab riigipoolne avatus kui põhimõte.

Eesti rahvusvaheline kaal

Kõrge rahvusvaheline maine on tingitud asjaolust, et oleme viimase kümne aasta jooksul hoidnud rahvusvahelist juhtrolli, olnud innovaator – uudsete küberturvalisuse kontseptsioonide tutvustaja ja esmarakendaja – ning seeläbi rahvusvaheline suunanäitaja. See on toonud kaasa rahvusvahelise huvi Eesti kui küberturvalisuse tippvõimekusega riigi vastu. Eestit loetakse usaldusväärseks partneriks ning Eesti häälel on arvestatav mõju rahvusvahelistes aruteludes. Lisaks kübervaldkonnale tugevdab see Eesti positsiooni nii julgeoleku- kui ka majandusküsimustes laiemalt.

Lõppkasutajate kõrge usaldus

Kodanike usaldus digitaalse riigi ja teenuste vastu ning baastasemel ühiskondlik arusaam küberturvalisuse olulisusest on saanud olulisel määral mõjutatutd 2007. aasta küberrünnakutega toimetulekust ja 2017. aasta ID-kaardi turvanõrkuse ilmnemisega toimetulekust, mis andsid laiemale ühiskonnale kogemuse digitaalse keskkonna mõjust igapäevasele elule ning tõid kaasa praktilise kogemuse, et turvalisuse tagamine nõuab lõppkasutaja aktiivsust (tarkvara uuendamist, alternatiivlahenduse soetamist). Usaldust digitaalse identiteedi ja teenuste vastu näitab ka 2017. aasta sügisel ID-kaardiga tehtud toimingute arv[37], mis jäi kriisieelsega võrreldes tavapärasele tasemele.

1.3. EESTI VÄLJAKUTSED JA PROBLEEMID

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 kogukonna poolt strateegia koostamise käigus esile toodud seitse kõige prioriteetsemat probleemi ja väljakutset, mis takistavad valdkonna optimaalset toimimist ja arengut ning mida praeguseks rakendatud normatiivsed lahendused ei ole parandanud.

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

[35] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf (2016.a)
[36] https://ncsi.ega.ee/ncsi-index/ (2018.a)
[37] 2017.a tehti 108 mln autentimistehingut ja anti 123 mln digiallkirja ID-kaardi ning Mobiil-ID kasutajate poolt (RIA 2018.a)

valdkondlik ekspertiis ei võimalda tipptasemel spetsialiseerumist. Sellega kaasneb omakorda oht tippspetsialistide Eestist ja eelkõige avalikust sektorist lahkumiseks.

Puudulik tervikjuhtimine

Suureks väljakutseks on küberturvalisuse valdkonna strateegiline tervikjuhtimine ja ühtne koordinatsioon: valdkonna planeerimine toimub endiselt pigem asutuste vastutusalade summana, igaühe enda prioriteete pidi. Sellest lähtub ka ebapiisav asutusteülene olukorrateadlikkus ja teabevahetus ning killustunud, ebaühtlane ja raiskav infosüsteemide kaitse korraldus, vaatamata üldisele suunisele ressursside konsolideerimiseks.

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.

Ebapiisav teadlikkus ja vähene omanikutunne

Küberturvalisuse alane teadlikkus on endiselt ebapiisav niiriigi 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.

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. Valdkondliku kogukonna poolt tajutakse probleemina ka vajalike küberkompetentside omandamist IT-välistel õppekavadel ning riigi ja erasektori koostööd teadusasutustega, mis ei ole piisavalt süsteemne.

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 julgeolekutööstusel on Eesti valdkondlikke tugevusi arvestada suur 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 identimislahendused. Üheks võtmeküsimuseks on sealjuures ebapiisav koostöö riigi ja teadusasutuste vahel, mistuleneb vähesest arusaamast 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.[38]

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.

[38] Seda näitasis selgelt nii 2007 küberrünnetega toimetulek kui ka 2017 sügise ID-kaardi kriis.

2. STRATEEGIA KOORDINATSIOON JA ELLUVIIMINE

2.1. KÜBERTURVALISUSE STRATEEGIA ROLL JA ULATUS

Küberturvalisuse strateegia on horisontaalne küberjulgeoleku ja –turvalisuse valdkonna kokkulepete ja koordinatsiooni dokument, mille koostamisse ja elluviimisse on kaasatud kõik olulisemad Eesti küberjulgeoleku- ja turvalisuse tagamisse panustavad osapooled: riigiasutused, akadeemia ja mõttekojad ning erasektor. Strateegia ei kata detailselt kõiki küberturvalisuse tagamiseks vajalikke tegevusi, millest oluline osa on juba saanud erinevate valdkondlike planeerimisprotsesside loomulikuks osaks. Küberturvalisuse strateegia ülesandeks on luua tervikpilt, koordineerida kõigi osapoolte tegevust, vältida dubleerimist ning kindlustada, et strateegia koostamise raames kokkulepitud põhimõtted ja eesmärgid saaksid kõigi osapoolte ning protsesside koostoimes ellu viidud.
Strateegia fookuses on riigi- ja ühiskonnalaiused probleemid, mille lahendus peitub erinevate osapoolte vahelises koostöös. Strateegia rolliks on kindlustada küberturvalisuse tagamise raamistik, mis võimaldab ja võimendab tulemuslikku dialoogi teaduse ja tehnoloogia, eraettevõtluse ning riigivalitsemise vahel, toetades sellega laiemalt nii hästi toimiva majanduskeskkonna kui ka riikliku julgeoleku tagamist.

2.2. SEOSED TEISTE ARENGUKAVADEGA

Eesti küberjulgeoleku ja –turvalisuse valdkonna eesmärgid lähtuvad kõige üldisemal tasemel **Eesti julgeolekupoliitika alustes** markeeritud kokkulepetest.

„**Infoühiskonna arengukava 2020“** käsitleb e-riigi arengu, andmeside tagamise ja üldiste IKT oskustega seotud eesmärke ning selle sisu planeeritakse ühtse protsessina Küberturvalisuse strateegiaga. Ainult digitaalse keskkonna arengu ja infoturbe tagamise ühtse planeerimisega on võimalik tagada *„security by design“* põhimõtte praktiline rakendamine, mis eeldab, et turvanõrkuste otsimine ja vältimine on nii võrgu, teenuste kui baastaristu arendamise lahutamatu osa ja teenuse omaniku isiklik vastutus. Turvalisuse eraldiseisev käsitlemine ja hilisem lisamine ei ole tulemuslik. Järgnevalt on välja toodud riigi üldise küberjulgeoleku ja -turvalisuse tagamise seisukohast olulised teemad, mis on sisustatud Infoühiskonna arengukavas, lähtudes e-riigi arendamise holistilisest vaatest, mitte kitsalt infoturbe tagamise aspektist:

- **Elektroonilise identiteedi turvalisus ja elektroonilise isikutuvastamise võime areng**[39], mis on oma olemuselt Eesti küberturvalisuse tagamise baasvõimekus. Lisaks tugineb sellele avalike teenuste toimimine, millest tulenevalt on tegemist laiema ühiskonna turvalisuse küsimusega.
- **„No-legacy“ põhimõtte järgmine –** avalikus sektoris ei tohi olla aegunud olulise tähtsusega IKT teenuseid ja lahendusi. Avalike IKT lahenduste ja teenuste ajakohasus tagab süsteemide turvalisuse taseme vastavuse ühtsetele kvaliteedinõuetele.
- **Riigipilve lahenduse väljatöötamine ja laialdane kasutuselevõtt,** mis maandab infotehnoloogiast tulenevaid taristuriske, võimaldades hoida infosüsteeme turvalises keskkonnas ja tagades turvalisuse ajakohasuse.
- **Turvalised e-valimised –** igasugune valimistehnoloogia peab olema testitud, auditeeritud, turvaline ja vastama valimistele esitatavatele seaduslikele nõuetele. Valimised ja laiemalt demokraatia toimimine on küberruumi kontekstis viimaste aastate jooksul muutunud kriitilise infrastruktuuri kõrval teiseks riigi julgeoleku vaates olulisemaks ründeobjektiks.

Riigikaitse arengukava 2017–2026 on riigikaitse keskne võimeplaneerimise dokument, mille eesmärk on lähtudes olemasolevatest ohustsenaariumitest tuvastada järgmise kümne aasta vajalikud ning riigi võimalustega kooskõlas olevad mittesõjalised ja sõjalised võimearendused.[40] Riigikaitse arengukavas on

[39] Täpne sisu lähtub riigiasutuste ja erasektori koostöös valmivast identiteedihalduse ja isikut tõendavate dokumentide valgest raamatust, mis sisaldab elektroonilise identiteedi ja selle kandja laiapõhjalisi tulevikustsenaariume ja strateegilisi valikuid.
[40] https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/rkak_2017_2026_avalik_osa.pdf

peamisteks kübervaldkonna prioriteetideks tervikpildi loomine küberruumis toimuva jälgimiseks reaalajas ning küberväejuhatuse ja küberajateenistuse arendamine.

Küberkuritegevuse vastase võitluse võimekuse arendamise ning riigi sisejulgeolekut ohustavate rünnete tuvastamisega seotud tegevuste elluviimise planeerimist käsitlevad „**Siseturvalisuse arengukava 2015-2020“** kooskõlaliselt „Küberjulgeoleku strateegia 2014-2017“ eesmärkidega ning planeerimisjärgus **„Siseturvalisuse arengukavaga 2021-2030“**, milles Eesti ühiskonna küberturvalisuse tagamise vaates on peamisteks olulisteks tegevussuundadeks: IKT sektori arengut arvestav küberkuritegude avastamise ja menetlemise võimekuse edendamine; valmisoleku tagamine küberkuritegevuse ja –julgeolekuga seotud tulevikuohtudeks ja väljakutseteks; nii riigisisese kui rahvusvahelise praktilise koostöö ning infovahetuse edendamine partnerasutuste vahel; teavitustöö; asjakohase info kogumine ja analüüs, saavutamaks võimalikult täielik ülevaade küberkuritegude olukorrast; ebaseaduslike kaupade ja teenuste müügi tõkestamine internetis; e-residentsuse ja digitaalse identiteediga seotud riskide analüüsimine ning maandamine.

Kriminaalpoliitika arengusuundades aastani 2030[41] määratakse kriminaalpoliitika pikaajalised eesmärgid, mille fookusteemade hulgas pööratakse tähelepanu ka küberiusamise vähendamisele. Samuti kriminaalmenetluse valdkonnas küberkuritegevusega toimetulekule.
„Vägivalla ennetamise strateegia aastateks 2015-2020“[42] keskendub eeskätt laste ja noorte turvalise meediatarbimise ja keskkonna tagamisele, et kaitsta lapsi netiohtude, sh küberkiusamise, eest, planeerides tegevusi interneti vahendusel toime pandud laste vägivallajuhtumite ennetamiseks. Strateegiat toetab ka „**Laste ja perede arengukava 2012-2020“**[43], mille raames tegeletakse internetiturvalisuse alase nõustamise, sealhulgas lapsevanemate oskuste arendamisega ning illegaalse sisu ja tegevuse tõkestamiseks vihjeliini toimise tagamisega.

Eesti kuvandi ühe kindla osana küberturvalisuse tagamise ning küberohtude vastase kiire reageerimisvõime ja tegevuste arendamise sätestab „**Välispoliitika arengukava 2030“** koostamise ettepanek[44]. Arengukava käsitleb rahvusvahelise õiguse temaatika teadvustamist kübervaldkonnas, tegeleb arengukoostöö edendamisega, näeb ette Eesti aktiivset osalemist Euroopa Liidu küberabivõrgustiku loomisse ning rõhutab vajadust tagada ühiskonna usaldus küberruumi vastu. Eesti soovi toetada IKT ja e-riigi lahenduste mitmekülgset kasutuselevõttu arenguriikides sätestab „**Arengukoostöö ja humanitaarabi arengukava 2016-2020“**[45]**.** Eesti eesmärgiks on teadvustada laiemalt IKT ja e-riigi kui arengu edendajate potentsiaali EL arengupoliitikas, tagades IKT ja e-riigi toimimise seisukohalt oluliste funktsioonide vastupanuvõime ka küberohtude suhtes.

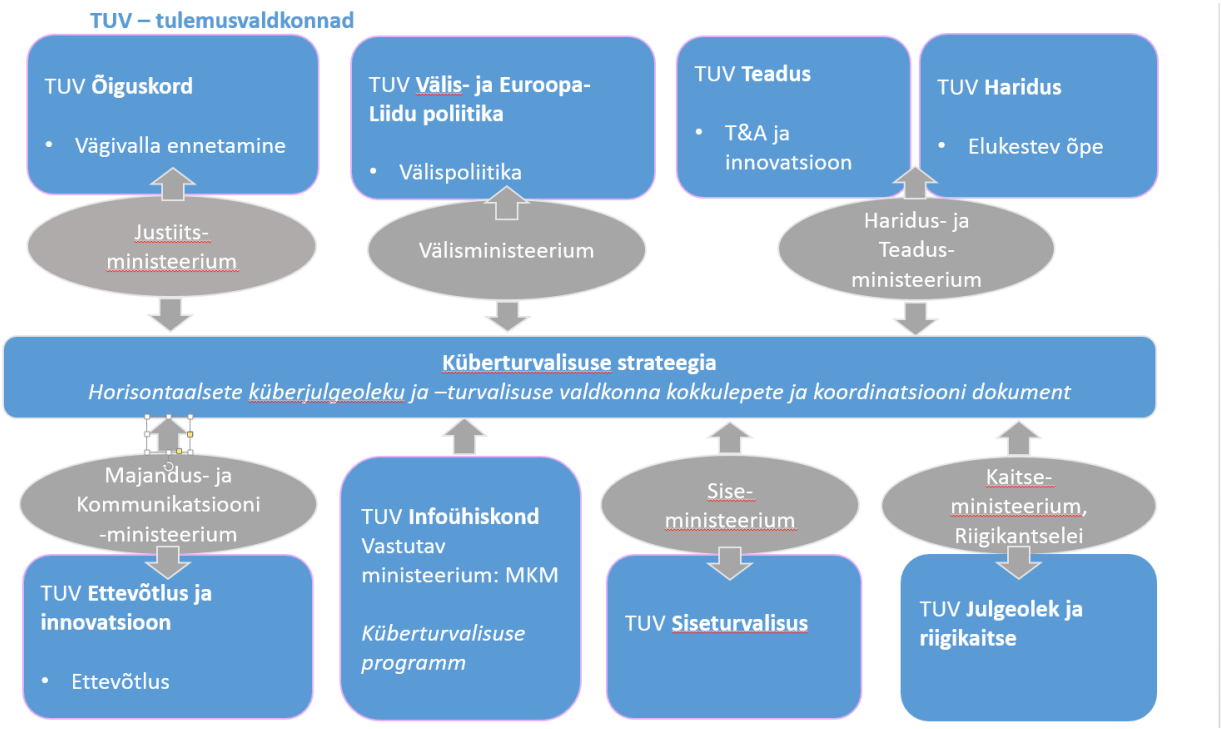
„Elukestva õppe strateegia 2014-2020“[46] elluviimise raames tagatakse, et digioskuseid puudutavad kompetentsid sisaldavad ka küberturvalisust ning õppekavadesse integreeritakse lisaks digitehnoloogiale ka küberturvalisusega seonduvaid elementaarseid teadmisi. Elukestva õppe strateegia digipöörde programmi eesmärk on digivõimaluste teadlik ning tark integreerimine õppeprotsessi ja selle kaudu digipädevuse arendamise (mh turvalisusega seotud kompetentside) tagamine üldhariduse valdkonnas.

Innovaatilise ja konkurentsivõimelise küberturbe sektori ettevõtluse ning teadus- ja arendustegevuse saavutamiseks on olulised koostöökohad „**Eesti teadus- ja arendustegevuse ning innovatsiooni strateegia**

[41] https://www.just.ee/et/kriminaalpoliitika-arengusuunad
[42] https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/vagivalla_ennetamise_strateegia_2015-2020_kodulehele.pdf
[43] https://www.sm.ee/sites/default/files/content-editors/Lapsed_ja_pered/laste_ja_perede_arengukava_2012_-_2020.pdf
[44] https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/valispoliitika_arengukava_koostamise_ettepanek_kodulehele.pdf
[45] https://vm.ee/sites/default/files/content-editors/development-cooperation/2016_2020_arengukava_tekst.pdf
[46] https://www.hm.ee/sites/default/files/strateegia2020.pdf

2014-2020“[47] ja „**Eesti ettevõtluse kasvustrateegiaga 2014-2020“**[48]. Strateegia huvides on tagada riigi kui TA ja innovatsiooni tellija ja algatajana edukas sisuline koostöö ettevõtete ja teadusasutustega, mis võimaldaksid suurendada innovaatiliste toodete teket.

Vabariigi Valitsus on seadnud eesmärgiks võtta kasutusele tegevuspõhine eelarve aastaks 2020, et lähtuda tulemusjuhtimisest, sidudes strateegia juhtimise finantsarvestusega. Sellest planeerimise loogikast lähtub ka Küberturvalisuse strateegia elluviimise raamistik: küberturvalisuse strateegias kokkulepitud prioriteetide saavutamiseks vajalikud meetmed, tegevused ja rahastamiskava planeeritakse detailselt küberturvalisuse programmis ja teistes vastutavate ministeeriumite tulemusvaldkondadesse kuuluvate arengukavade programmides. Küberturvalisuse strateegia seoseid teiste valdkondlike planeerimisprotsessidega illustreerib Joonis 2.



Joonis 2: Küberturvalisuse strateegia eesmärkide elluviimiseks vajalike tegevuste planeerimisega seotud tulemusvaldkonnad

2.3. SEOSED TEISTE RIIKIDE JA RAHVUSVAHELISTE STRATEEGIATEGA

Eesti küberturvalisuse strateegiline planeerimine lähtub rahvusvahelisest olukorrast, võttes arvesse teiste Eesti jaoks oluliste riikide strateegilisi kavatsusi ning toetades laiemalt Euroopa Liidu ja NATO küberjulgeolekupoliitika strateegilisi eesmärke. See tähendab, et Eesti küberturvalisusega seotud otsused kattuvad Euroopa Liidu 2017. aasta küberpaketis väljendatud ühiste seisukohtadega ning strateegia prioriteetide hulka kuuluvad elutähtsate teenuste toimepidevus ning operatiivne koostöö teiste liikmesriikidega intsidentide ennetamisel ja lahendamisel. Olles ühinenud Cyber Defence Pledge[49] leppega, on Eesti koos teiste liitlastega kinnitanud, et pühendub riikliku infrastruktuuri ja võrkude kaitsele, edendades seeläbi ühtlasi NATO küberjulgeolekut tervikuna.

[47] https://www.hm.ee/sites/default/files/tai_strateegia.pdf
[48] http://kasvustrateegia.mkm.ee/
[49] https://www.nato.int/cps/su/natohq/official_texts_133177.htm

2.4. RIIKLIKU KÜBERTURVALISUSE TAGAMISE KOORDINATSIOON JA JUHTIMISKORRALDUS

Küberjulgeoleku poliitika kujundamist ja strateegia elluviimist koordineerib ning vastavat riigiasutuste ja laiema kogukonna koostööd korraldab Majandus- ja Kommunikatsiooniministeerium. Strateegilisel tasandil toimub koordinatsioon läbi Majandus- ja Kommunikatsiooniministeeriumi juhitud **Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu,** mis tagab küberturvalisuse strateegia eesmärkide elluviimise vastutavate riigiasutuste planeerimisdokumentide, programmide ja tööplaanide kaudu. Küberturvalisuse strateegias kokkulepitud riigiülese kübervaldkonna poliitika elluviimise eest vastutavad esmaselt küberjulgeoleku nõukogu töösse panustavad valitsusasutused. Erinevate asutuste vastutusvaldkonnad on kirjeldatud alltoodud loetelus ja küberturvalisuse strateegia juhtimiskorraldus on illustreeritud Joonisel 1.

- **Majandus- ja Kommunikatsiooniministeerium** juhib ja koordineerib küberturvalisuse strateegia koostamist ja elluviimist osana infoühiskonna arengukava tervikpildist ning koostöös **Riigi Infosüsteemi Amet**iga (RIA) omab keskset rolli tehnoloogilise vastupanuvõime, kriiside ja intsidentide halduse ning küberturbe sektori ettevõtluse arendamise ning teadus- ja arendustegevuse suunamisega seotud tegevustes. Sealjuures on Riigi Infosüsteemi Ameti ülesanded küberturvalisuse valdkonnas laiapindsed, hõlmates kõikide riigi toimimiseks oluliste võrgu- ja infosüsteemide turvalisuse tagamist seadusest tulenevate eranditega.

  Majandus- ja Kommunikatsiooniministeeriumi haldusala asutustest on Eesti küberturvalisuse tagamisse ja strateegilisse planeerimisse panustajateks veel **Tehnilise Järelevalve Amet** (TJA), mille ülesandeks IKT-valdkonnas on elektroonilise kommunikatsiooni seadmete turvalisuse ja usaldusväärsuse edendamine ning sertifitseerimisteenuste pakkujate ja ajatempliteenuste kontrollimine; **Eesti Interneti Sihtasutus** (EIS), mis on Eesti internetikogukonda esindav ja Eesti maatunnusega domeeninimesid haldav organisatsioon; **Riigi Infokommunikatsiooni Sihtasutus** (RIKS), mille ülesandeks on tagada riigile toimepidevad, kõrgkvaliteetsed, turvalised ja kulutõhusad infokommunikatsiooni- ning taristuteenused (näiteks riigipilv ja riigiside kontseptsioon); **Ettevõtluse Arendamise Sihtasutus** (EAS) ja **Startup Estonia** (SUE)**,** mis panustavad sektori ettevõtluse ja innovatsiooni arengu toetamisse.

- **Haridus- ja Teadusministeerium** arvestab küberturvalisuse strateegia eesmärkides kokku lepitud prioriteetidega elukestva õppe strateegia tegevuste planeerimises, toetades kõigi haridustasemete lõpetajatele baasteadmiste omandamist küberohtudega toimetulekuks.
  Haridus- ja Teadusministeeriumi haldusalas toetab küberturvalisuse strateegia eesmärkide täitmist **Hariduse Infotehnoloogia Sihtasutus** (HITSA), mis aitab kaasa valdkonna spetsialistide ettevalmistamisele nii Targalt Interentis programmi kui IT Akadeemia programmi koordineerimise kaudu.
- **Justiitsministeerium** panustab koostöös **Riigiprokuratuuriga**, mis juhib kohtueelset kriminaalmenetlust, läbivalt kübervaldkonna õigus- ja kriminaalpoliitika planeerimisse ning vägivalla ennetamise strateegia tegevuste kaudu kavandab valdkondlikku ennetustegevust.
  Küberturvalisuse valdkonna vaatest oluliste asutustena kuuluvad Justiitsministeeriumi haldusalasse **Andmekaitse Inspektsioon** (AKI), mis teostab järelevalvet isikuandmete kaitse alaste õiguste ja kohustuste üle; **Eesti Kohtuekspertiisi Instituut** (EKEI), mis tegeleb mh infotehnoloogiaalase ekspertiisiga, ning **Registrite ja Infosüsteemide Keskus** (RIK), mis arendab ja haldab olulisi registreid ja infosüsteeme.

- **Kaitseministeerium** tagab koostöös **Kaitseväe**, **Kaitseliidu** ja **Välisluureametiga** riigikaitse arengukava sõjalise kaitse osa kübervaldkonnaga seotud tegevuste elluviimise ning panustab läbivalt valdkonnaüleste koostöö- ja koordinatsioonimehhanismide ning ühtse olukorrapildi loomisse.

- **Siseministeerium** tagab koostöös **Politsei- ja Piirivalveameti** ja **Kaitsepolitseiametiga** küberkuritegude ennetamise, tõkestamise ja avastamise, menetlemise ja küberjulgeolekut ohustavate süütegude ennetamise ja tõkestamise ning küberturvalisuse strateegia prioriteetide elluviimise siseturvalisuse

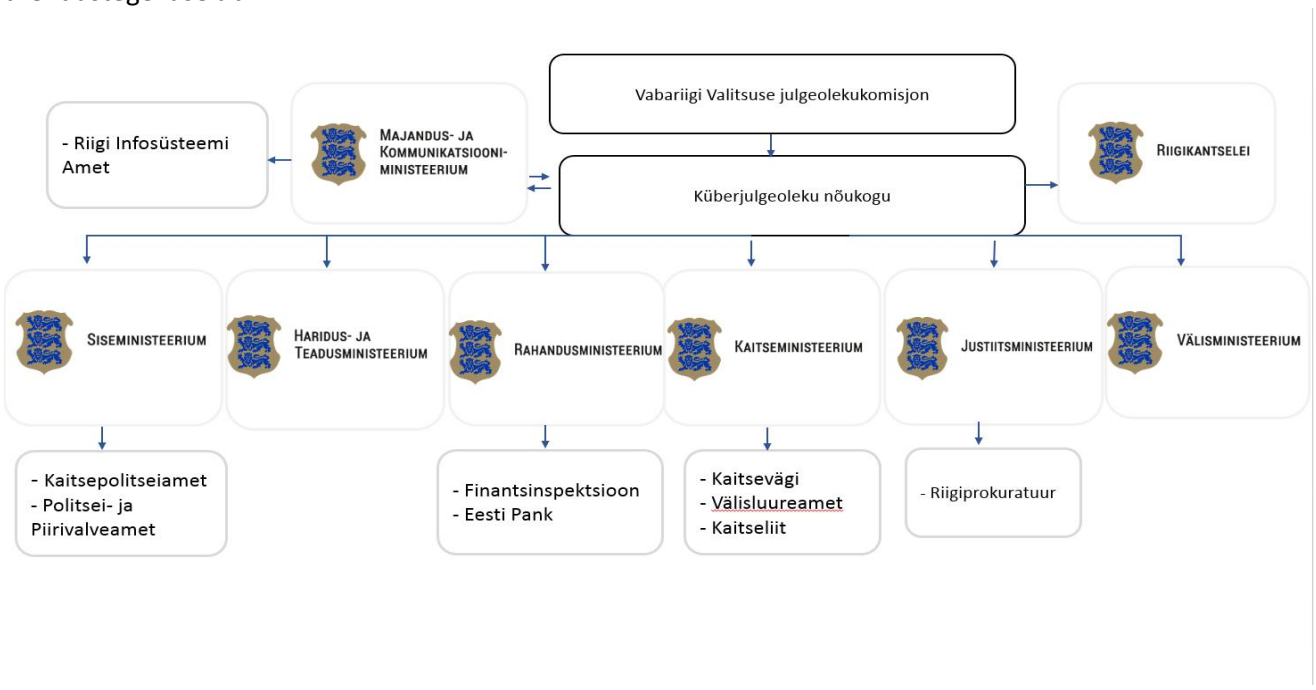
arengukava ja seotud programmide tegevustega ning panustab valdkonnaüleste koostöö- ja koordinatsioonimehhanismide ning ühtse olukorrapildi loomisse.
Oluline roll on ka **Siseministeeriumi Infotehnoloogia- ja Arenduskeskusel** (SMIT), mis tagab siseturvalisusega seotud infosüsteemide halduse ja arenduse.

- **Välisministeerium** suunab ja koordineerib strateegia rahvusvahelise koostöö tegevusi.

- **Rahandusministeerium** osaleb läbivalt strateegia erinevate osade sisustamisel, sealhulgas jätkusuutlikkuse tagamisel ning integreerituse tagamisel teiste strateegilise planeerimise protsessidega. Lisaks tagab finantssektori kaasatuse. Küberturvalisuse temaatikaga omavad puutumust ka **Finantsinspektsioon**, mis teostab järelvalvet finantsasutuste üle ja **Eesti Pank** läbi Euroopa keskpankade süsteemi kehtestatud nõuete.

- **Riigikantselei** tagab küberturvalisuse integreerimise riigikaitse planeerimisdokumentidesse (riigikaitse arengukava ja riigi kaitsetegevuse kava).

Nii strateegia planeerimisel ja elluviimisel kui laiemalt Eesti riigi küberturvalisuse tagamisel on äärmiselt oluline tihe koostöö valdkonnas teadmust ja võimekust omavate kompetentsikeskuste ja mõttekodade, ülikoolide ja teadusasutuste ning erasektori partneritega. Riik kasutab mõttekodade kui strateegiliste partnerite võimekust Eesti valdkondliku kompetentsi ja rahvusvahelise koostöö arendamisel. **NATO Küberkaitsekoostöö Keskuse** võõrustaja- ja raamriigina on Eesti strateegiline huvi edendada keskuse kui rahvusvahelise samameelsete riikide organisatsiooni arengut, kasutades aktiivselt keskuse pakutavaid küberkaitseõppusi, rahvusvahelisi arutelufoorumeid ja teadusuuringuid. **E-riigi Akadeemia** (EGA) infoühiskonna nõustamis- ja mõttekeskusena toetab muuhulgas Eesti digitaalsete (sh. küberturbe) lahenduste rahvusvahelist kasutuselevõttu. **Rahvusvaheline Kaitseuuringite Keskus (RKK)** on juhtiv välispoliitika, julgeoleku ja riigikaitsega seotud teemale spetsialiseeruv mõttekoda Eestis. Eesti ekspertide küberkaitsealase kompetentsi sihipärase kaasamisega toetatakse mh laiapindse riigikaitse arendamist. **TalTech Küberkriminalistika ja küberjulgeoleku keskus** koondab peamised avaliku sektori kübervaldkonna eest vastutavad asutused ning koostöös on seatud keskuse eesmärgiks Eesti küberjulgeoleku kompetentsi ja võimekuse tõstmine hariduse-, teaduse- ja arendustegevuse abil.



Joonis 1: Küberturvalisuse valdkonna juhtimiskorraldus

Küberturvalisuse strateegias kokkulepitud eesmärkide koordineeritud elluviimiseks määratakse oma planeerimisdokumentide kaudu strateegia elluviimisse otseselt panustavates ministeeriumites[50] ja Riigikantseleis vastutav ametnik, kes on enda haldusalas riikliku küberjulgeoleku- ja turvalisuse tagamist puudutavates küsimustes kontaktisikuks ning tagab küberturvalisuse strateegias kokkulepitud prioriteetide elluviimise enda ministeeriumi ja selle valitsemisala planeerimisdokumentide kaudu, valmistades selle põhjal ette iga-aastase aruande küberjulgeoleku nõukogule. Vastutavate ametnike jooksvat koostööd ja infovahetust korraldab Majandus- ja Kommunikatsiooniministeerium.

Kord aastas kinnitab küberjulgeoleku ja –turvalisuse valdkonna tegevuste koondaruande Vabariigi Valitsuse julgeolekukomisjon ning infoühiskonna arengukava elluviimise aruande koosseisus antakse tegevuste elluviimisest ülevaade kogu Vabariigi Valitsusele.

[50] Haridus- ja Teadusministeerium, Justiitsministeerium, Kaitseministeerium, Majandus- ja Kommunikatsiooniministeerium, Siseministeerium, Välisministeerium.

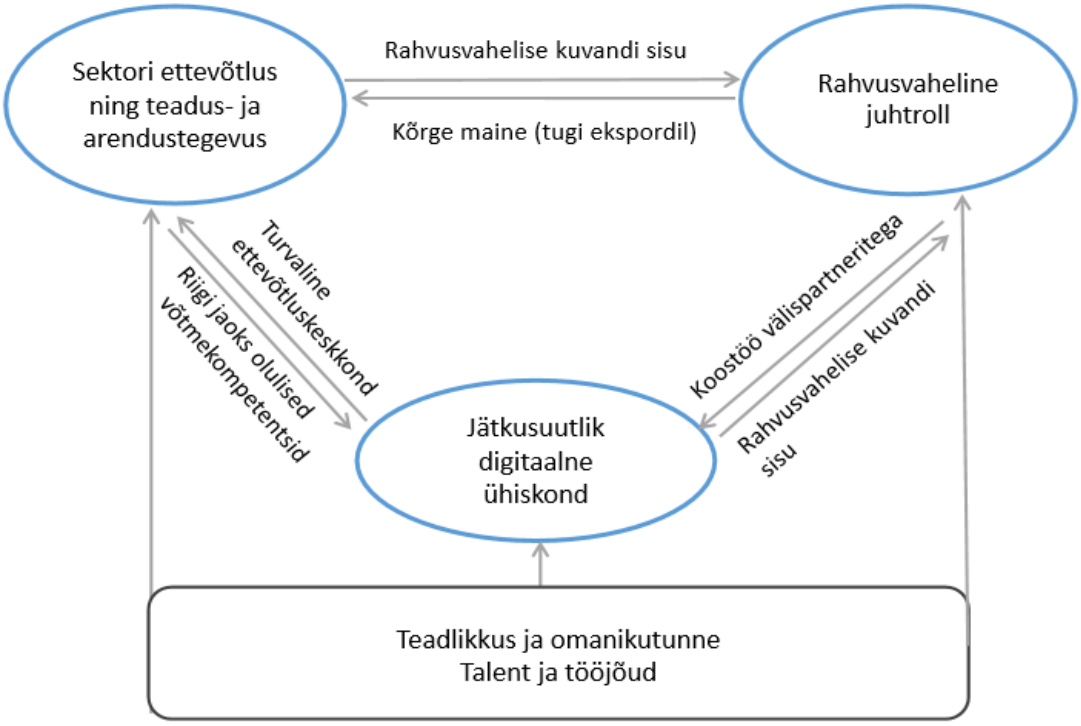
3. STRATEEGILISED EESMÄRGID

Visiooni elluviimiseks keskendub strateegia neljale strateegilisele eesmärgile, millega seotud tegevussuunad katavad ära kõik strateegia koostamisel prioriteetsetena kaardistatud fookusprobleemid (täpsem kirjeldus alapeatükis 1.3.). Eesmärkide elluviimist mõjutavad üldised trendid (kirjeldatud alapeatükis 1.1.) ning võimaldavad Eesti tugevused (kirjeldatud alapeatükis 1.2.).

Probleem (2018)	**Eesmärk (2022)**	**Tegevussuunad**
- Nõrk strateegiline tervikjuhtimine, ebapiisav asutusteülene olukorrateadlikkus, killustunud infosüsteemide kaitse korraldus - Küberturbe alahindamine infosüsteemide ja teenuste arendamisel - Ebapiisav arusaam küberohtude ja –intsidentide mõjudest ja taristu (rist)sõltuvustest	Eesti on jätkusuutlik digitaalne ühiskond, millel on tugev tehnoloogiline vastupanuvõime ja valmisolek kriisidega toimetulekuks.	- Tehnoloogilise vastupanuvõime tõhustamine - Intsidentide ja kriiside ennetamine, valmisolek ja Lahendamine - Valdkonna terviklik juhtimine ja sidusa kogukonna kujundamine
Oma küberturbetoodet või –teenust arendavate ja välisturgudel edukate Eesti ettevõtete vähesus ning ebapiisav teadus- ja arendustegevuse maht.	Eestis on tugev, innovaatiline, teaduspõhine ja globaalselt konkurentsivõimeline küberturbe sektori ettevõtlus ning teadus- ja arendustegevus, mis katab riigi jaoks olulised võtmekompetentsid.	Küberturbe teadus- ja arendustegevuse ning teaduspõhise ettevõtluse toetamine ja edendamine.
Eesti kui rahvusvahelise partneri kõrge usaldusväärsuse hoidmine	Eesti on arvestatav ja tugev partner rahvusvahelisel areenil	- Koostöö tõhustamine strateegiliste välispartneritega - Jätkusuutliku kübervõime rahvusvaheline edendamine.
- Vähene küberteadlikkus ning isiklik omanikutunne küberturvalisuse riskide eest vastutamiseks - Spetsialistide puudus ja ebapiisav juurdekasv	Eesti on ühiskonnana küberteadlik ning tagatud on valdkonna spetsialistide järelkasv.	- Kodanike, riigi- ja erasektori küberteadlikkuse tõstmine - Riigi- ja erasektori nõudlusele vastava talendi arendamine

Lisaks on läbivaks alusprobleemiks Eesti kui väikese rahvastikuga ühiskonna piiratud spetsialiseerumisvõime nii avalikus sektoris, ettevõtetes kui riigiasutustes. Probleemi adresseerivad strateegias läbiva prioriteedina käsitletud koostöö- ja kommunikatsioonimehhanisminde tõhustamine, konsolideerimine ning ekspertiisi killustamise vähendamine, mis võimaldavad piiratud ressursse optimaalselt kasutada.

Strateegiliste eesmärkide omavahelisi seoseid illustreerib joonis 3. Keskseks eesmärgiks on jätkusuutliku ja turvalise e-riigi toimimise tagamine, mis loob ühtlasi aluse nii teadus- ja arendustegevuse ning ettevõtluskeskkonna võimendamiseks kui ka jätkusuutlikuks rahvusvaheliseks juhtrolliks. Eelnev toetab oma kompetentsiga riigi sisemist tugevust ja võimekust, koostööd välispartneritega ja rahvusvahelise juhtrolli sisustamist. Sisulisele kompetentsile tuginev rahvusvaheline juhtroll tagab omakorda tulemusliku koostöö rahvusvaheliste partneritega küberintsidentide ja –kriiside lahendamisel ning laiemalt tugevate partnerlussuhete loomisse ja hoidmisse panustades. Strateegia visiooni saavutamine ei ole võimalik ilma läbivalt kõrge teadlikkuseta küberohtudega arvestamise olulisusest ja kompetentse tööjõu olemasoluta.



Joonis 3: Küberturvalisuse strateegia eesmärgid ja nendevahelised seosed

JÄTKUSUUTLIK DIGITAALNE ÜHISKOND

Eesmärk 1: Eesti on jätkusuutlik digitaalne ühiskond, millel on tugev tehnoloogiline vastupanuvõime ja valmisolek kriisidega toimetulekuks.

Strateegia esmane ülesanne on tagada ühiskonna toimimise seisukohast oluliste funktsioonide (strateegilise taristu ja teenuste) vastupanuvõime küberohtude suhtes. Eesmärk 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.

Sellest lähtuvalt sisustavad eesmärgi kolm tegevussuunda:

1. Tehnoloogiline vastupanuvõime
2. Kriiside, rünnete ja intsidentide haldamine ning valmisolek
3. Valdkonna terviklik juhtimine ja sidus kogukond

Tulemusindikaatorid:

Mõõdik[51]	**Algtase**	**Sihttase**	**Allikas**
Avatud teenuste[52] koguarv riigivõrgus	*/täpsustub 2018.a. lõpuks/*	0	Riigi Infosüsteemi Amet
Avatud teenuste koguarv Eesti küberruumis	/täpsustub 2018.a. lõpuks/	On kolmandiku võrra vähenenud *(täpsustub)*	Riigi Infosüsteemi Amet

Tegevussuund 1.1. Tehnoloogilise vastupanuvõime tõhustamine

Toimiv küberturvalisus hõlmab kogu infosüsteemi ja teenuse elutsüklit alates **arhitektuur**ist, mis on teenuse orgaanilise osa. 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 ja halduskorraldust.

Lisaks täna akuutsete riskide haldamisele tuleb **arvestada pikaajalise vaatega**. On alust arvata, et strateegiaperioodi 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

[51] Mõõdikud lähtuvad RAPID7 National Exposure Indexist https://www.rapid7.com /
[52] 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).

valmisolek eelkõige adaptiivsuse ja reageerimisvõime tagamist, tehniliselt *no-legacy* põhimõtte järgimist ehk vananenud süsteemidest ja taaktarkvarast vabanemist.

Infoturbe ja andmekaitse põhimõtete järgimine riigi infosüsteemide arhitektuuris

Riigi infosüsteeme ja digitaalseid teenuseid tuleb arendada algusest peale turvaliselt, arvestades nii tehnoloogilisi kui ka organisatsioonilisi nõudeid, põhimõtteid ja standardeid. See tagab, et uued teenused ja andmekogud oleksid üles ehitatud arvestades turvalisuse ja privaatsuse põhimõtet (*security and privacy by design)*. Enamiku avaliku sektori IT-lahenduste kasutuselevõtul arvestatakse turvalisuse aspektiga, ent vastutus on detsentraliseeritud ning keskne tugi ei ole piisavalt süsteemne. Turvalisust ja privaatsust toetava arhitektuuri põhimõtte senisest tõhusamaks ja süsteemsemaks rakendamiseks on planeerimisel juhendmaterjalide süsteemi loomine arendusprotsesside kvaliteedi tagamiseks koos tagasiside- ja kontrollmehhanismiga. See annab vajalikud suunised ja toe, järgides samas põhimõtet, et turbe tagamine on iga teenuseomaniku isiklik vastutus.

Baasturbenõuete laiapindne rakendamine

Riigi küberturvalisuse tagamiseks on võtmetähtsusega, et osapooled järgiksid infoturbestandarditest lähtuvaid baasturbenõudeid vähemalt seadusega ettenähtud tasemel. Avaliku sektori asutuste infoturbe tagamise aluseks on baasturbenõuete järgimine lähtuvalt infosüsteemide kolmeastmelisest etalonturbe süsteemist ISKE[53], mis kehtib alates 2003. aastast. Täna on endiselt probleemiks ISKE keerukus ning selle rakendamist hindavad eriti väiksemad kohuslased, sh kohalikud omavalitsused, ülejõukäivaks, eeskätt administratiivselt. Lisaks valitsusasutustele vajavad suuniseid ja tuge küberriskide haldamisel ning andmekaitse- ja infoturbenõuete täitmisel ka väikeettevõtjad, vabakond ja üksikisikud. Vajalikus ulatuses baasturbenõuete rakendatavuse tagamiseks on vaja riigi täiendavalt tuge, et süsteemselt tagada lihtsa tööriista, juhendmaterjalide ja koolituste kättesaadavus. Sihiks on luua ajakohane, süsteemne ja laialt kasutusel olev baasturbenõuete süsteem, mis hõlmab nii infoturbe kui andmekaitse miinimumnõudeid. Sellega pakutakse tuge nii ISKE või sellega samaväärse infoturbestandardi kohuslastele[54] kui ka väiksematele teenusepakkujatele ja ettevõtetele. Lisaks tuleb arvestada, et baasturbestandardist tulenevad infoturbenõuded ei jää staatiliseks, vaid neid tuleb süsteemselt ajakohasena hoida. Eesti info- ja võrguturbe korraldus peab lähtuma parimatest rahvusvahelistest standarditest, mis on eestindatud ning kohandatud meie vajadustele. 2018. aastal on uuendamisel kogu ISKE aluseks olev BSI IT-Grundschutz, mis sellest lähtuvalt reformiks ka Eesti ISKE, minnes muuhulgas üle riskianalüüsipõhisele infoturbe korraldusele: see tähendab, et infoturbe tagamise osana hakkavad riskianalüüse koostama kõik riigiasutused ja ühiskonnale olulise teenuse osutajad. Baasturbenõuete süsteemi ajakohastamisega kooskõlaliselt vaadatakse üle ka andmeid töötlevate infosüsteemide turvalisuse tagamist puudutav seadusandlus, et vähendada erinevatest regulatsioonidest tulenevat halduskoormust ning juurutada terviklik andmehaldus. Kindlustamaks piiratud võimekusega asutuste toimetulek turbenõuete järgimisega, süstematiseeritakse ka keskselt pakutavad infoturbe teenused, et muuta nende sisse-ostmine lihtsalt kättesaadavaks alternatiiviks.

Riigiasutuste vahelise turvalise andmevahetuse tagamine

Riigile on kriitiliselt oluline tagada turvaline ja toimiv side ja andmevahetus erinevatele haldusaladele ja ametitele mõeldud süsteemide vahel (sh telefoniside ja internetiühendus). Selleks on kavas esmakordselt välja töötada terviknägemus ehk riigiside kontseptsioon, millega kaardistatakse ettevaatavalt sidevajadus tavaolukorras ja kriisiolukorras. Sellest lähtuvalt saab kaardistada arendusvajadused,kavandada tegevused ning panna paika tööjaotus ja -korraldus eri osapoolte vahel. Lisaks on plaanis jätkata riigi andmesidevõrgu laiendamist ja arendamist ning krüpteeritud e-kirjavahetusele ja andmesidele üleminekut riigiasutuste vahelise turvalise kommunikatsiooni tagamiseks.

---

[53] väljatöötamisel ja arendamisel on aluseks võetud Saksamaa BSI (saksa k. *Bundesamt für Sicherheit in der Informationstechnik*, inglise k. *Federal Office for Information Security*) avaldatav infoturbe standard – IT Baseline Protection Manual (saksa k. *IT-Grundschutz*).

[54] riigiasutused ja teenuseosutajad küberturvalisuse seaduse mõistes, sh digitaalsete teenuste osutajad

Eesti riigi toimimiseks vajalike kriitiliste andmekogude turvalisuse tagamine

Eesti omariikluse säilitamine tähendab Eesti territooriumi kaitsmise kõrval riigi jaoks üha enam digitaalsete varade hoidmist. Kõige enam kaitset vajavad digitaalsed varad on riigi käes olevad põhiandmed kodanike, riigi territooriumi ja õigusloome kohta ehk kriitilise tähtsusega andmekogud[55]. Kui riigile esmavajalikke andmeid ilma volitusteta muudetakse või need hävinevad on oht, et riik ei tule enam oma põhiülesannete täitmisega toime. Kriitiliste andmekogude turvalisuse tagamiseks ei ole jõukohane tagada ühtselt kõrgel tasemel andmekeksuste olemasolu kõigis riigiasutustes, kuna see eeldab suuri investeeringuid. Kuluefektiivsema lahendusena standardiseeritud infoturbe taseme tagamiseks on väljatöötamisel kava kriitiliste andmekogude ja olulisemate Eesti e-teenuste kolimiseks riigipilve[56]. Väljaspool Eesti territooriumi rajatakse andmesaatkondade võrgutik, kus oleks võimalik vajadusel rakendusi koos andmekogudega tööle panna[57]. Nii riigipilve kui andmesaatkonna lahenduse puhul tagatakse kõrge käideldavus põhimõttel, et hoiustatud andmeid on võimalik kasutada ja teenuseid opereerida reaalajas. See tähendab, et kui Eesti andmekeskused mistahes põhjusel hävib, saab riik kriitilisi teenuseid osutada eemalt andmesaatkonna tehnilise lahenduse toel. Jätkusuutlikkuse tagamiseks on vaja järgmisena välja töötada ka süsteemne reeglistik kriitiliste andmekogude nimekirja ja neile rakenduvate turva- ja varundamisnõuete regulaarseks ajakohastamiseks ning luua õiguslik raamistik kriitiliste andmekogude pidamisega seotud osapoolte ja nende rollide kindlaksmääramiseks.

Uue põlvkonna tehnoloogiatega seotud riskide süsteemne hindamine ja haldamine

Kuigi tulevikuriskid on suurel määral ennustamatud, tuleb Eestil kujundada kindlad põhimõtted ja poliitilised pidepunktid tulevikutehnoloogiaid puudutavates olulistes küsimustes. Tulevikuriskidega toimetulek eeldab esmalt sisulise ühiskondliku diskussiooni loomist: selleks tuleb keerukat infot ja tehnilisi sõnumeid edastada arusaadavalt, vältides samas liigset lihtsustamist ning oluliste detailide eiramist. Sellise lähenemisega kindlustatakse, et suudetakse ka suure määramatusega riske adresseeritada kompetentsi ja teadmiste, mitte reaktiivselt ja hirmude põhiselt. Eesmärgi saavutamiseks tuleb toetuda teaduskompetentsile ning Eesti riigi jaoks prioriteetsetes valdkondades (nagu krüptograafia, plokiahela tehnoloogia, tehisintellekt ja turvaline identiteedihaldus) tagada, et Eesti ühiskonna toimimiseks kriitiliste võimekuste arendamine ja kompetents on esindatud nii fundamentaal- kui ka rakendusteaduste tasemel.

Tehnoloogiliste riskide praktiliseks maandamiseks näeme ette eelkõige IT-lahenduste ajakohasena hoidmist, tagades arhitektuursed lahendused, mis võimaldavad vajadusel paindlikult muudatusi sisse viia ning alternatiivlahenduste olemasolu. Lisaks küberohtude ennetamisele on uute tehnoloogiate ja arengutega kaasas käimine oluline võitluses küberkuritegevusega ning võimalike hübriidohtudega[58].

Rahvusvahelises pildis oleme üha enam seotud globaalsete arengutega ning lahutamatuks osaks Euroopa IT-maastikust – et see areng mahutaks Eesti huvid ja vajadused, tuleb suuta rahvusvahelistes formaatides kaasa rääkida. Riigina oleme vältimatult seotud erasektori ja suurte tootjate teenustega (Google, Apple, Microsoft jne) – selliste sõltuvuste võimalikku mõju illustreeris ilmekalt ID-kaardi kiibi turvanõrkuse ilmnemine 2017. aasta sügisel. Selliste riskidega ja sõltuvustega toimetulekuks peame arendama välja kompetentsikeskuse, mis suudab hinnata tehnoloogiate ja teenuste turvakindlustmab keskset ülevaadet peamistest riskidest, nõustab

---

[55] Kriitilised andmekogude hulka kuuluvad näiteks kinnistusraamat, äriregister ja rahvastikuregister. Nimekirja ajakohastamine toimub regulaarselt küberjulgeoleku nõukogu ja arhitektuurinõukogu koostöös.

[56] Riigipilv on Riigi Infokommunikatsiooni Sihtasutuse hallatav pilvekeskkond, mis võimaldab riigi institutsioonidele ja elutähtsa teenuse osutajatele mugavaid ja turvalisi pilvelahendusi (https://riigipilv.ee/).

[57] 2018 seisuga on käivitatud üks andmesaatkond Luksemburgi riiklikus andmekeskuses. Teiste andmesaatkondade loomise võimalust analüüsitakse Luksemburgi projekti kogemuse põhjal.

[58] Hübriidohuks loetakse konventsionaalseid ja mittekonventsionaalseid meetodeid ühendavate tegevuste kooslust, mida riigid või muud jõud saavad koordineeritud viisil kasutada ametlikku sõjategevust alustamata. Eesmärk on lisaks otsesele kahjustamisele ja haavatavuste ärakasutamisele ka ühiskonda destabiliseerida ja tekitada otsustusprotsesse takistavat ebakindlust.

nii avaliku- kui erasektori asutusi tuleviku tehnoloogiatega seonduvate riskide teemal ning kaasub rahvusvahelistesse formaatidesse.

Tegevussuund 1.2. Intsidentide ja kriiside ennetamine, valmisolek ja haldamine

Kahe strateegiaperioodi 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 riigi ja 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. Käesoleval strateegiaperioodil 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.

Võimekuse tugevdamine küberohtude varajaseks avastamiseks ja ennetuseks

Eestil on küberruumi arengutest ja küberturbe olukorrast täna eelkõige kvalitatiivne ülevaade, kuid puudub järjepidevalt koostatav, ajas võrreldav ja selgetel indikaatoritel põhinev kvantitatiivne pilt, mille abil saaks objektiivsetel alustel küberruumi tervist hinnata ja sellest tulenevaid juhtimisotsuseid teha. Riik seirab pidevalt enda võrku ja ründepinda, mõõtes konkreetseid intsidente, sündmusi, tehnilisi andmeid ja nende dünaamikat. Järgmise sammuna arendatakse tehniliste seireandmete süsteemseks analüüsimiseks välja olukorrateadlikkuse tööriistad ning luuakse automatiseeritult reaalaja-lähedane pilt, mis mõõdab tehnilist küberturbe taset, võimaldades teha järeldusi Eesti üldise küberkeskkonna ja asutuste küberturbe alase küpsuse kohta, tagades ajalise võrdluse arengu illustreerimiseks ning võrdlusbaasi teiste riikidega[59].

Riskide hindamiseks, juhtimiseks ja vastutuse määramiseks ettevõtte tasandil annab aluse küberturvalisuse seaduse sisuline rakendamine. Tagamaks ühiskonnale olulise teenuse osutajate[60] infosüsteemide turvalisus, ajakohane ja terviklik arusaam ohusuundumustest ja rünnete varane avastamine, kindlustatakse süsteemne ning pidev ülevaade teenusepakkujate võrkude arhitektuursest turvalisusest, võrguliiklusest ning rist- ja piiriülestest sõltuvustest. Selleks arendatakse välja võrguseiresüsteem, millest strateegiaperioodi alguseks on olemas toimiv prototüüp[61], mille rakendamist laiendatakse eravõrkudesse ja suurendatakse analüüsivõimekust läbi seire automatiseerimise ja lahenduste edasiarendamise. Olulisemates avaliku sektori andmekogudes ja infosüsteemides toimunust tagasiulatuva ülevaate saamiseks rakendatakse keskne kohustus pidada kriitilisi logisid.[62] Turvalisuse testimiseks viiakse senisest oluliselt suuremas mahus läbi praktilisi ründekatseid ehk läbistusteste, mis näitavad kas ja kuidas on potentsiaalsel ründajal võimalik saavutada ligipääs testitava asutuse kriitilistele juhtimis-, side- või IT-süsteemidele, millele järgneb konkreetsete soovituste andmine ning regulaarne kontrollmehhanism.
Elutähtsa teenuse osutajate rist- ja piiriüleste sõltuvuste välja selgitamiseks viidi 2016. aastal läbi esmane uuring. Järgmine ambitsioon on töötada välja kontseptsioon rist- ja piiriüleste sõltuvuste süsteemseks käsitlemiseks. Selgitatakse välja ühiskondlikult oluliste teenuste osutamiseks ja riigi toimimise tagamiseks kasutatavate kriitiliste võrgu- ja infosüsteemide omavahelised sõltuvused ning kavandatakse vajalikud

---

[59] Eelkõige on olulised meiega võrreldavad Põhjala ja Balti riigid

[60] Ühiskonnale oluliste teenustena on mõeldud teenuseid küberturvalisuse seaduse mõttes, kus definitsioon lähtub võrgu- ja infoturbe direktiivi olulise teenuse osutaja mõistest. Tegemist on laiema ringiga kui hädaolukorra seaduse elutähtsa teenuse osutajate nimekiri.

[61] 2018. aasta lõpuks valminud prototüübi raames on loodud liidestused projekti kaasatud valitsus- ja riigiasutuste ning erasektori teenusepakkujatega info ja andmevoo vahetuseks ja lisaks vahendid andmete analüüsiks.

[62] Kriitiliste logide kogum sisaldab kõikide rakenduste autentimistegevuste detailseid jälgi ja internetist kõigi avalikult ligipääsetavate teenuste sissetulevate päringute detailseid jälgi.

arendustegevused. Eesmärgiks on omada süsteemset ülevaadet olulisematest rist- ja piiriülestest sõltuvustest ning suunata asutusi võtma meetmeid riskide maandamiseks.
Paremaks ülevaateks riigivõrkude ja infosüsteemide olukorrast ühendatakse riigiasutused ja kohalikud omavalitsused võimalikult suures ulatuses riigivõrku. Parema võrguturbe tagamiseks viiakse läbi pilootprojekt riigivõrgu keskse sissetungi tõkestamise süsteemi rakendamiseks.

Erasektori küberriskide maandamiseks laiemalt analüüsitakse küberkindlustusteenuse[63] 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.

Küberturvalisuse integreerimine riigikaitse planeerimisse ja valmisolekusse kriisidega toime tulla

Eesmärgiks on esmalt hõlmata küberturvalisus riigikaitse planeerimisse ja läbiharjutamisse, millega tagatakse küberturvalisuse tegevuste ja võimete planeerimine vastavalt riigikaitse planeerimise aluseks olevatele ohustsenaariumitele. Selle kaudu tõstetakse riigi suutlikkust toimida küberruumis julgeolekuohtude tõrjumisel ja riigikaitseliste kriiside lahendamisel. Teiseks jätkatakse küberturvalisuse integreerimist riigiasutuste ja oluliste teenuste pakkujate valmisolekut tagavatesse plaanidesse ning riskihinnangutesse. Antud tegevuse kaudu suureneb võime ennetada küberriskide realiseerumist Eestis ja eskaleerumist kriisideks. Samuti paranebvalmisolek küberohtudest või -intsidentidest tingitud kriise lahendada ja piirata neist tulenevat negatiivset mõju. Võimearendusena arendatakse reaalajas tekkivat ühist olukorrapilti Eesti küberruumi kohta ning selle jagamist kõigi oluliste osapoolte vahel. Praktilise valmisoleku tagamiseks kriisidega toimetulekul viiakse regulaarselt läbi ühiseid koostööõppuseid riigi poliitilise juhtkonna, ühiskonnale oluliste teenuseosutajate ning sõjalist kaitset tagavate struktuuridega. Avalikus sektoris rakendatakse küberkriiside võimepõhist lahendamist, et kasutada optimaalselt ära erinevate asutuste kompetentsi.

Tegevussuund 1.3. Valdkonna terviklik juhtimine ja sidusa kogukonna kujundamine

Optimaalsel koostööl ja koosvõimel baseeruv, kaasav, dünaamiline ja tõhus küberturvalisuse tagamine on oluliseks eelduseks kogu strateegia visiooni saavutamisel, võimaldades maksimaalse tulemuslikkusega kasutada Eesti piiratud ressursse. Koostöö ja koosvõime tagamisel olulisteks mõõtmeteks on terviklik juhtimine,kaasavplaneerimine ning toimiv kogukond.

Küberturvalisuse valdkonna terviklik juhtimine ja võimete konsolideerimine

Riigiülese küberjulgeoleku ja –turvalisuse tagamise aluseks on vajalike võimete süsteemne planeerimine, hästi toimiv koostöö ja koosvõime ning kübervaldkonna juhtimine ühe tervikuna, mitte valitsemisalade põhiselt. Selleks, et planeerida ressursse ja tegevusi riigi laiuselt ning suurendada sellega efektiivsust teha olemasolevate ressurssidega enam, kaardistatakse esimese sammuna erinevate ministeeriumite valitsemisalade küberturbega seonduvad võimed, nende kattuvused ja puudujäägid valdkondliku võimeauditi käigus. Võimeauditi tulemustele tuginedes konsolideeritakse riiklikku olukorrapilti ja riigivõrkude turbe korralduse juhtimist. Selle tegevuse eelsammuna käivitatakse riigiülese küberturvalisuse keskus (NCSC) Riigi Infosüsteemi Ameti küberturvalisuse teenistuse baasil, mida võimeauditi järeldustest lähtuvalt edasi arendatakse. Riigiülese küberturvalisuse poliitika ühtseks juhtimiseks ja asutusteüleseks planeerimiseks tagab Majandus- ja Kommunikatsiooniministeerium koostöös teiste ministeeriumitega ning küberjulgeoleku nõukogu ning Vabariigi Valitsuse julgeolekukomisjoni toel küberturvalisuse strateegia koordineeritud elluviimise ja ajakohasena hoidmise.

[63] OECD, Enhancing the Role of Insurance in Cyber Risk Management. https://read.oecd-ilibrary.org/finance-and-investment/enhancing-the-role-of-insurance-in-cyber-risk-management_9789264282148-en#page

Ühtse küberjulgeoleku kogukonna kujundamine ja järjepidevalt kaasava planeerimisprotsessi tagamine

Valdkonna ühtse toimimise aluseks on toimiv infoliikumine, tugevad partnerlussuhted ning isiklik kontakt erinevate valdkonna ekspertide seas ja vahel, mis hõlmab nii riigiasutusi, erasektorit kui ka akadeemiat.

Tugev, sidus ja kogukonnakultuuril põhinev igapäevane koostöö on olnud aluseks Eesti senisele edule küberturbe tagamisel ja laialdaste tagajärgedega intsidentide ärahoidmisel - seda praktikat jätkatakse ja tugevdatakse ka uuel strateegiaperioodil. Laiema kogukonna kaasamiseks tugevdatakse riigiasutuste ja ühiskonnale olulise teenuse osutajate infoturbejuhtide ning juhtkondade koostööformaate, mh strateegilise planeerimise protsessidesse. Tõhus siseriiklik koostöö erinevate ametiasutuste vahel on eelduseks nii küberturvalisuse tagamisel, rahvusvahelise koostöö prioriteetide saavutamisel kui ka küberkuritegevuse ohjamisel. Selleks tagatakse riigisisesed koostööformaadid, jõustatakse vajalikud asutustevahelised koostöökokkulepped tulemusliku koostöö tagamiseks ning soodustatakse asutustevaheliste rotatsioonide toimumist kompetentsi vahetuks jagamiseks.

ETTEVÕTLUS NING TEADUS- JA ARENDUSTEGEVUS

Eesmärk 2: Eestis on tugev, innovaatiline, teaduspõhine ja globaalselt konkurentsivõimeline küberturbe sektori ettevõtlus ning teadus- ja arendustegevus, mis katab riigi jaoks olulised võtmekompetentsid.

Nii ülikoolides, eraettevõtetes kui ka avalikus sektoris on Eestil väljapaistvat kompetentsi erinevates küberturbe koolkondades, eelkõige turvalise digitaalse identiteedi, krüptograafia, andmete terviklikuse, 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.

Tulemusindikaatorid:

Mõõdik	**Algtase**	**Sihttase**	**Allikas**
Sektori ettevõtete ekspordi maht[64]	*/täpsustub 2018.a. jooksul/*	*/kahe-kordistumine/*	Kübervaldkonna tööjõuvajaduse uuring[65] ja Kasvualade edendamise uuring[66]
Uute küberturvalisuse valdkonna iduettevõtete arv	*/täpsustub 2018.a. jooksul/*	*/täpsustub 2018.a. jooksul/*	Startu-up Estonia
Küberturvalisuse valdkonnas kaitstud doktoritööde arv	1.7 doktorit aastas (perioodil 2014-2017)	2.5 doktorit aastas (2019-2022)	TalTech, Tartu Ülikool

Tegevussuund 2.1. Küberturbe teadus- ja arendustegevuse ning teaduspõhise ettevõtluse toetamine ja edendamine

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.

Erasektori, riigi ja akadeemia vahelise tulemusliku koostöö võimendamine

Tulemusliku koostöö võimaldamiseks on tänaseks loodud erasektori, akadeemia ja riigi koostööd toetav info- ja küberturbe klaster Eesti Infoturbe Assotsiatsioon (*Estonain Information Security Association - EISA*). Järgmiseks väljakutseks on uue koostööformaadi optimaalne käivitamine, et luua võimalus kompetentside kohtumiseks ning tagada administratiivse tugimehhanism sektoriüleseks ühtseks kandideerimiseks rahvusvahelistel hangetel, võistlustel ja konkurssidel, tagades sellega eeldused ekspordi võimendamiseks ja

[64] Väljakutseks on küberturbe kui sektori defineerimine, mida ei ole võimalik teha äriregistri andmete baasil automaatselt. Vajalik on kasutada erialaorganisatsioonide tuge ning regulaarseid uuringuid.
[65] Praxis (2018)
[66] TÜ, TalTech, Technopolis Group Eesti OÜ (2018)

teadusrahastuse kaasamiseks. Samal ajal panustatakse kaitsetööstuse arendamiseks võimaluste loomisse osalemaks Euroopa Liidu kaitsealastes algatustes nagu European Defence Fund ja European Defence Industrial Development Programme.

Riigiülese küberturbe valdkonna teadus- ja arendustegevuse kava koostamine, mis defineerib riigi jaoks prioriteetsed fookusvaldkonnad

Eestis puudub ühtne, infoühiskonda ja küberturvalisust ning nende tehnilisi lahendusi käsitlev teadus- ja arendustegevuse kava. Vabariigi Valitsuse algatatud IKT valdkonna arenguprogramm[67] hõlmab vähesel määral vastavaid meetmeid ning nimetab ära esmased küberturvalisuse teadussuunad. IKT valdkonna teadusele annab lisaks tõuke 2018.a IT Akadeemia programmi rammes käivitatud teadusmeede. Järgmiseks sammuks on laiemat strateegilist plaani arvestades luua koordinatsioonimehhanism ning defineerida küberturbe valdkonna teadus- ja arendustegevuse fookusvaldkonnad. Nendele vastavatest riigile prioriteetsetest uurimisküsimustest lähtuvalt saab edaspidi anda suunised ülikoolide ja ettevõtete poolt läbiviidavaks teadus- ja arendustegevuseks, ettevõtete toetusmeetmete sisustamiseks ning haridusprojektideks ja stipendiumiteks.

Innovatsiooniloome ja ekspordipotentsiaali toetamine

Sektori globaalse konkurentsivõime parandamiseks tuleb soodustada innovatsiooni loomet ja tootestamise mahu tõstmist. Selleks süstematiseeritakse küberturvalisuse valdkonnale suunatud innovatsiooni toetusmeetmed ning toetatakse nende aktiivset kasutuselevõttu. Ekspordipotentsiaali võimendamiseks süstematiseeritakse riigi poolt küberturbega tegelevate (väike)ettevõtete parem kaasamine äridiplomaatia visiitidel ja delegatsioonide külastusel.

Sektori ettevõtete arengut ja innovatsiooniloomet toetavat potentsiaali omab ka Eesti Kaitseväe poolt opereeritav NATO küberharjutusväljak ehk virtuaalne keskkond, mis võimaldab üles ehitada info- ja kommunikatsioonisüsteeme ning harjutada läbi olukordi, mida ei saa teha igapäevaselt kasutatavates võrkudes. Küberharjutusväljaku esmaseks eesmärgiks on koondada rahvusvaheline küberkaitseõppuste ning väljaõppe kogemus, kuid kasutusvõimalusi saab laiendada. Arendades näiteks edasi avatud küberharjutusväljaku (Open Cyber Range) platvormi, mis võimaldab pakkuda valdkondlikele (idu)ettevõtetele ja ülikoolidele lahendusi teadus- ja arendustegevuse läbiviimiseks, toodete testimiseks ja katsetamiseks ning väljaõppeks.

Avaliku- ja erasektori tõhusa koostöö võimaldamiseks riigi tellimusel loodud uudsete lahenduste tootestamiseks vajab ajakohastamist ka intellektuaalse omandi käitlemist puudutav regulatsioon[68], mis täna keskendub toodetele ja teenustele füüsilises ruumis, arvestamata digitaalse keskkonna olemuslikke erisusi. Esimeses faasis on plaanis detailsemalt kaardistada tänane olukord ja probleemistik, võttes arvesse asutuste tänast hanke- ja litsentsipraktikat, teiste riikide parimaid praktikaid ja regulatsioone ning küberturbelahendusi puudutavaid erisusi. Teostatud analüüsi alusel saab töötada välja tervikliku riigi tarkvara intellektuaalse omandi õiguste strateegia, mis toetaks Eesti tarkvaraettevõtete arengut ja konkurentsivõimet maailmas ning sisse viia selle saavutamiseks vajalikud seadusemuudatused. Eesmärgiks on luua võimalus paindlikult ning ettevõtluse arengut soodustavalt kommertsialiseerida riigi tellimusel loodud tarkvara nii, et tarkvara intellektuaalse omandi õigused võivad kuuluda ka tarkvara arendanud eraettevõtetele ja riik kasutab neid litsentsi alusel, kuid samal ajal on riigile tagatud võimalus tarkvara parandada ja edasi arendada oma tarbeks.

Iduettevõtete tekkeks ja arenguks toetava keskkonna tagamine

Riigi eesmärgiks on tagada optimaalne keskkond kübertehnoloogiaid arendavate ettevõtete tekkeks ja kasvuks – see tähendab ka valdkondliku iduettevõtluse kogukonnale suunatud toetustegevusi. Iduettevõtete toetamisel on tänaseks läbitud kaheaastane pilootfaas Startup Estonia ja Kaitseministeeriumi koostöös, mille

[67] IKT valdkonna arenguprogrammi kontseptsioon
[68] Reguleerib riigivaraseadus

käigus ehitati üles toimivad koostööformaadid ja võrgustik ning tekkinud on väike hulk potentsiaalseid iduettevõtete meeskondi. Uuel strateegiaperioodil jätkab Startup Estonia kogukonna edendamist koostöös Majandus- ja Kommunikatsiooniministeeriumiga, et toetada initsiatiive regulaarsete seminaride ja ürituste korraldamiseks, käivitada süsteemsed mentorlusprogrammid ning liikuda piisava arengutaseme saavutamisel edasi kübervaldkonna ettevõtete kiirendi loomise suunas, et pakkuda väärtust ka esmase arengufaasi läbinud ettevõtetele globaalseks kasvuks.

RAHVUSVAHELISED SUHTED

Eesmärk 3: Eesti on arvestatav ja tugev partner rahvusvahelisel areenil

Eesti küber-kaubamärgi tugevus eeldab teadlikku ja terviklikku lähenemist rahvusvahelistele teemadele. 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 lahendamiseks ja tõhusama kaitse pakkumiseks.
Eesmärgi saavutamiseks on kaks tegevussuunda:

- Koostöö tõhustamine strateegiliste välispartneritega
- Jätkusuutliku kübervõime rahvusvaheline edendamine

Tulemusindikaator:

Mõõdik	**Algtase**	**Sihttase**	**Allikas**
Välisministeeriumi ja teiste vastutavate asutuste[69] iga-aastane eksperthinnang Eesti rahvusvaheliste suhete sisulisele kvaliteedile ja fookusele.	Koostöö rahvusvaheliste organisatsioonide ja teiste riikidega toimub läbi üksikute initsiatiivide, mis on üles ehitatud erinevate valdkondade ja institutsioonide kaudu ebaühtlaselt. Puudub tervikliku ja süsteemse üldpildi omamine koostöömehhanismidest, et kasutada ressursse vastavalt Eesti välispoliitilistest prioriteetidest.	- Välisministeeriumi eestvedamisel ning teiste vastutavate asutuste kaasamisel koordineeritakse koostööd erinevate rahvusvaheliste organisatsioonidega ja teiste riikidega mõtestatult ja süsteemselt. - Süsteemse lähenemise loomisel on aluseks Eesti välispoliitilised prioriteedid. - Koostöös strateegiliste välispartneritega on tugev praktiline mõõde ühisõppuste, tehnilise infovahetuse näol, mis tagab eduka intsidentide lahendamise. - Eesti on tõstnud oma nähtavust läbi arengukoostöö suurendamise. - Välisministeerium on keskne institutsioon, mille kaudu toimub infovahetus rahvusvahelistes organisatsioonides	Välis-ministeerium

[69] Välisministeerium, Majandus- ja Kommunikatsiooniministeerium, Riigi Infosüsteemi Amet, Kaitseministeerium

		küberdiplomaatia ekspertide roteerumise osas.	

Tegevussuund 3.1. Koostöö tõhustamine strateegiliste välispartneritega

Eesti peamine huvi rahvusvahelistes suhetes küberjulgeoleku valdkonnas on stabiilsuse tagamine küberruumis läbi omapoolse osaluse kahe- ja mitmepoolses koostöös. Üheks 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.

Tagatakse Eesti piisav esindatus ning kompetents küberteemadel Eesti välisesindustes ning Euroopa Liidu, NATO ja ÜRO juures

Tegevuse eesmärk on nähtav Eesti jalajälg Euroopa Liidu ja NATO küberkoostöös ning jätkuv osalus ÜRO küberprotsessides. Eesmärgi saavutamise eelduseks on sisukad sõnumid ja ekspertiis välispoliitiliste eesmärkide seadmisel.

Eduka rahvusvahelise koostöö eeldus on, et Eesti diplomaadid ja teised Eestit esindavad ametnikud oskaksid edastada ühtseid riigisiseselt koordineeritud sõnumeid Eesti rahvusvahelise küberturvalisuse valdkonna poliitika kohta. Eesti aktiivne osalemine Euroopa Liidu, NATO, ÜRO jt rahvusvaheliste organisatsioonide protsessides võimaldab paremini seista riigi huvide ja prioriteetide eest. Ajakohase küberkompetentsi hoidmiseks tuleb soodustada diplomaatide ja ametnike asutusteülest rotatsiooni ning teadmiste ja oskuste jagamist. Küberturbe valdkonna ekspertide kaasamine välisteenistusse võimaldab viia mitmekesisemaid ja ka tehnilisi teadmisi poliitikakujundamise protsessidesse, mis omakorda aitavad kaasa kvaliteetsemate otsuste langetamisele rahvusvahelisel tasandil.

Siinkohal on tugev roll just Välisministeeriumil, kelle ülesandeks on koolitada välja diplomaate küberjulgeoleku- ja turvalisuse teemadel ning tagada nende piisav küberkompetents, samuti välja töötada kübereksperdide rotatsioonisüsteem rahvusvahelistesse organisatsioonidesse.

Eesti panustab rahvusvahelise õiguse kujundamise protsessidesse läbi oma seisukohtade esitamise

Eesti aktiivse panustamise toel suureneb rahvusvahelise õiguse kehtivust küberruumis tunnistavate ja selle nimel aktiivselt töötavate riikide hulk. Olulise globaalse protsessina küberjulgeolekupoliitikas on kübernormide, usaldusmeetmete ja rahvusvahelise õiguse valdkond, kus on oluline jätkata Eesti senist edukat

osalust ÜRO jt protsessides. Kaalutakse ka mõne spetsiifilise valdkonna väljaarendamist, näiteks on oluline arendada seni lünklikult kaetud rahvusvahelise õiguse kehtimise analüüsi kompetentsi. *Tallinn Manual*ide väljaandmine NATO CCDCOE poolt on olnud edulugu, mida tuleks kinnistada osana Eesti kuvandist. Eesti seisukohti tuleb nähtavalt esitada erinevates koostöövormides ning tagada, et nende mõju on tuvastatav rahvusvaheliselt kokkulepitud seisukohtades.

Eesti arendab kahepoolseid koostööformaate võtmepartneritega ning korraldab regulaarseid ühisõppusi

Tegevuse eesmärk on sisulise koostöö arendamine võtmepartneritega, sh analüüside, tehnilise informatsiooni ning praktiliste teadmiste ja kogemuste vastastikune jagamine. Eesti riigi küberteadlikkust, valmisolekut ja suutlikkust tuvastada ning tegeleda uute ohtudega ja ka usaldusväärsust tõstetakse läbi partneritega aktiivse koostöö tegemise ja regulaarsete õppuste korraldamise. Eesti jaoks on oluline süsteemne kahepoolne küberkoostöö erinevate võtmeriikide ja neis paiknevates küberagentuuridega, mis koosneks poliitilisest dialoogist, regulaarsest analüüside jagamisest, koostööüritustest ja teistest koostööformaatidest.

Eesti osaleb rahvusvahelises kaitsealases koostöös ja panustab küberstabiilsuse suurendamisse

Tegevuse eesmärk on tagada Eesti tugev kuvand kui tunnustatud vastutustundlik koostööpartner rahvusvahelises kaitsealases koostöös ja panustaja rahvusvahelise küberstabiilsuse suurendamisel. Oluline on kindlaks määrata vajalikud prioriteedid, luua regulaarseid dialooge erinevate strateegiliste partneritega nii kahepoolses koostöös kui ka rahvusvaheliste organisatsioonidega (eriti EL, NATO, OSCE ja ÜRO). Kollektiivsete vastumeetemete arendamine küberrünnakutele lähtub kahe- ja mitmepoolsest rahvusvahelisest koostööst. Tähtsal kohal on aktiivne tegevus suuremate organisatsioonide suunal, seda eriti EL ja NATO heidutushoiaku tugevdamisel. Eesti aktiivset rolli küberjulgeoleku valdkonnas aitab kinnistada ka seniste suuremahuliste õppuste toimumine Eestis (nagu *Locked Shields* või *Cyber Coalition*).

Eesti huvides on sidusus liitlaste sõjalise kohaloluga *(*NATO eFP *ehk enhanced Forward Presence*) ka küberkaitse valdkonnas. See tähendab uute koostöömehhanismide ja –protseduuride väljatöötamist ühise küber ohu-ja olupildi loomiseks, mis aitavad kaasa ka NATO üldise heidutushoiaku tugevnemisele regioonis. Eestil on vajalik sõlmida vastavad küberkaitsealased koostööraamistikud ning korraldada regulaarseid ühisõppusi.

Eesmärgiks on arendada välja toimiv küberrünnakute omistamise protseduur Eestis nii poliitilisel, õiguslikul kui tehnilisel tasandil ning osaleda aktiivselt samameelsete riikide heidutus- ja omistamisalastes koostööformaatides.

Tegevussuund 3.2. Jätkusuutliku kübervõime rahvusvaheline edendamine

Turvaline, usaldusväärne ja stabiilne küberruum on eelduseks toimivate ja tõhusate digitaalsete lahenduste kasutamiseks ja seetõttu oluline valdkond paljude riikide jaoks oma digitaalvaldkondade arendamisel. Eestil on tänaseks välja kujunenud potentsiaal kujuneda oluliseks kübervõime edendajaks üle maailma ja osaleda suuremates ELi ning teistes rahvusvahelistes projektides. Eesti aktiivne osalemine Euroopa Liidu küberabivõrgustiku loomisel ning jätkusuutliku ja konkurentsivõimelise kübervõime edendamisel aitab Eestil jätkuvalt kuuluda juhtivate küberriikide hulka ning tooks ka lisaressursse välisprojektide näol.

Eestil on olemas kompetents riikliku küberkoordinatsioonimudeli loomisel ja ülesehitamisel, mida oleks võimalik jagada teiste riikidega. Küberjulgeoleku-alase abi osutamine on alles algusjärgus ning hetkel puuduvad organisatsioonid rahvusvahelisel tasandil, mis suudaks koordineerida doonorriikide koostööd ja pakkuda kübervõime arendamist sihtriikides. Euroopa Liit on otsustanud luua võrgustiku, mis hakkaks tegelema küberkompetentsi koondamise ja edasiarendamisega uute abiprojektide tarbeks. Eesti saaks täita mitmeid eesmärke eelnimetatud kübervõimete arendamise alastes tegevustes, mis on praegu katmata.

Eesti annab juhtiva panuse konkurentsivõimelise ja jätkusuutliku kübervõime tagamisse partnerriikides ning osaleb Euroopa Liidu küberabivõrgustiku loomises

Tegevuse eesmärk on tagada, et Eesti oleks vajadusel võimeline edendama konkurentsivõimelist ja jätkusuutlikku kübervõimet partnerriikides. Eesti saab teistele riikidele pakkuda oma kogemuste jagamist, osaledes ELi, NATO ja teistes rahvusvahelistes projektides. Lisaks peab defineerima rahvusvahelises digitaal- ja küberkoostöös konkreetsed Eestile jõukohased ja vajalikud valdkonnad, näiteks küberturvalisuse valdkonna poliitika ja strateegiate kujundamine, e-valitsemine, teatud geograafiline fookus, riigid mujal regioonides jmt. Koostöös RIA, TalTech`i ja teiste asutustega tuleks välja arendada vastav väljaõppesüsteem, mille lisaväärtus oleks ka Eesti IT-turvalisuse ja küberkaitsetööstuse kaasamine koostööprojektidesse ning nende tutvustamine. Olulisel kohal on kaasuda ka rahvusvahelistesse standardimise ja sertifitseerimise protsessidesse.

Samuti on Eesti jaoks oluline süsteemselt toetada kübervõimete arendamist väljaspool EL ja NATOt ja selleks tuleb näiteks osaleda Euroopa Liidu küberabivõrgustiku loomises, arendamaks välja konkurentsivõimelist ja jätkusuutlikku küberabi osutamise võimet, mis omakorda kinnistaks Eesti kuulumist juhtivate küberriikide hulka ning tooks Eestile täiendavaid ressursse.

KÜBEROSKUSLIK ÜHISKOND

Eesmärk 4: Eesti on ühiskonnana küberteadlik ning tagatud on valdkonna spetsialistide järelkasv.

Laiemat ühiskonda silmas pidades, oli Eestis 2015.aastal turvaohuga kokku puutunud 30% internetikasutajatest[70]. Erasektori poolelt peegeldab üleüldist rünnetega toimetulekut madal teadlikkus turvapoliitikate rakendamisest, mida on 2015.a seisuga teinud 17% kõigist Eesti ettevõtetest[71].

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.

Eesmärgi saavutamiseks viiakse tegevused ellu kahe tegevussuuna abil:

- Kodanike, riigi- ja erasektori küberteadlikkuse tõstmine
- Riigi- ja erasektori nõudlusele vastava talendi arendamine

Tulemusindikaatorid:

Mõõdik	**Algtase**	**Sihttase**	**Allikas**
Interneti kasutamisel turvaohuga kokku puutumise tulemusel kahjukannatanute osakaal (%)[72]	44,8% (2010) 27,7% (2015)	≤ 20% (2022)	Statistikaamet
Ametlikult kinnitatud IKT turvapoliitika kasutamine ettevõtetes (%)[73]	16.9% (2015)	≥ 25% (2022)	Statistikaamet
Valitsusasutuste ja kohalike omavalitsuste töötajata küberteadlikkuse ja –oskuste tase, mõõdetuna praktiliste oskuste testi põhjal.	N/A (2018)[74]	≥ 75% tase rahuldav (2022)	Riigi Infosüsteemi Amet
Hinnanguline tööjõu puudujääk[75]	/täsustub/	/täpsustub/	Kübervaldkonna tööjõuvajaduse uuring: Praxis 2018

[70] Infotehnoloogia leibkonnas 2015.a www.stat.ee
[71] Infotehnoloogia ettevõttes 2016.a www.stat.ee
[72] 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.
[73] Valimis 10+ töötajaga ettevõtted.
[74] Algtase selgitatakse välja 2018.a lõpu seisuga testi sooritanud sihtrühma tulemuse järgi.
[75] 2018.a viidi MKM-i tellimusel esimest korda läbi kübertööjõu uuring, mis kaardistas kübeturbe spetsialistide ametiprofiilid ning selle alusel hinnati tööjõuvajadust täna ja viie aasta pärast. Hinnang tööjõu kättesaadavusele anti valimis olnud ettevõtete poolt subjektiivse hinnanguna ning sellega fikseeriti ära 2018.a seis. Erinevate meetmetedukal rakendumisel ei ole tööjõu puudujääk / hinnang puudujäägile strateegia perioodi lõpuks kasvanud.

Tegevussuund 4.1. Kodanike, riigi- ja erasektori küberteadlikkuse tõstmine

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[76] sh küberturvalisuse osaoskuste olulisust 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.

Viiakse läbi laiemale avalikkusele suunatud teadlikkuse tõstmise tegevusi

Aastate jooksul on Eesti riigi siseselt välja kujunenud selgete rollidega ja vastutusega asutused, kes küberturvalisuse tagamise eest hea seisavad, mh tegelevad ka laiema ühiskonna vastavasisulise teavitusega. Samas on see ajapikku kaasa toonud informatsiooni killustatuse ja osaliselt tegevuste dubleerimise - info küberturvalisusest on jaotunud mitmete (projektipõhiste) keskkondade vahel (nt. RIA blogi[77], Politsei- ja Piirivalveameti veebilehekülg[78], Targalt Internetis projektilehekülg) ja puudub kodanike teavitamiseks keskne kanal. Samuti on Eestis kasutamata potentsiaal, pakkuda kohalikku konteksti sisaldavaid e-kursuseid (MOOC´e) ja iseõppimisvõimalusi.

Ootuspäraselt tuuakse RIA 2018. a aastaraamatus välja, et lõviosa 2017.aasta küberjuhtumitest puudutas erasektorit, kes kasutajaskonnalt on kõige arvukam. Siia kuuluvad nii suur- ja väikeettevõtjad, vabaühendused kui ka üksikisikuist arvutikasutajad, kelle digitaalne sõltuvus ning küberturvalisuse alane teadlikkus erinevad väga palju. Samas on tõsi ka see, et digitaalsete lahenduste toimimise tähtsust kiputakse alahindama ning riskide ennetamise asemel pööratakse turvalisusele tähelepanu alles pärast intsidenti.

Eelnevast tulenevalt on tegevuse eesmärgiks saavutada olukord, kus eri ametkondade koostöös tagatakse laiema avalikkuse teadlikkus küberohtudest nii oskus ohtude eest end kaitsta kui ka teadmised, kuidsas küberründe järgselt käituda. RIA võtab küberturvalisuse seaduse jõustumise järel keskse rolli küberhügieeni, riiklike ennetustegevuste ning ühiskondliku teadlikkuse kasvatamisel. Sarnaselt PPAle ning Päästeametile käivitatakse laiamahulised ennetus- ja teadlikkusekampaaniad küberohtude teadvustamiseks erinevatele sihtrühmadele, sealjuures ettevõtjatele. Luuaks formaat teadlikkuse kasvatamisega seonduvate tegevuste koordineerimiseks Eestis ning koondatakse ennetustegevusi puudutav info arusaadaval ja avalikkusele kättesaadaval kujul ühte kohta. Riigiasutuste küberhügieeni taseme tõstmiseks muudetakse kohustuslikuks riigiasutuste ja KOVide töötajatele küberturvalisust puudutavate testide läbiviimine. Jätkatakse sihtrühmade koolituste ning teavitustegevustega.

---

[76] Õppija digipädevuse mudel
[77] https://blog.ria.ee/
[78] Politsei- ja Piirivalveamet

Õpilaste ja õpetajate küberturvalisuse alaseid teadmisi ja oskusi mõõdetakse süsteemselt ning tagatakse üldharidus- ja kutsekoolide õpetajatele küberturvalisuse alaste koolituste pakkumine.

Oluliseks eelduseks ja sisendiks küberturvalisuse koolituste planeerimisel on teadmiste ning oskuste taseme fikseerimine, mis käesoleval hetkel on lünklik[79]. Turvalisust käsitletakse põgusalt 2018.a esimest korda toimunud digipädevuse riikliku tasemetöö ja suuresti akadeemilistel eesmärkidel läbi viidava KüberPähkli uuring-võistluse raames[80]. Samas puuduvad süsteemsed võrreldavad mõõtmistulemused nii õpilaste kui õpetajate osas.

Üks oluline lahendus küberturbealase teadlikkuse tõstmisel on teema käsitlus üld- ja kutsehariduses. Eestis on olemas kokkulepe, millised teadmised ja oskused peaksid noored üldhariduse tasemel küberturvalisusest saama ning see on kirjeldatud riiklikes õppekavades digipädevuse raames.[81] Valminud on nii põhikooli ja gümnaasiumi[82] valikainete kavad ja neile vastavad materjalid, mis sisaldavad metoodilisi materjale ja on heaks aluseks koolituste läbi viimisel. Samas napib üle riigi motiveeritud ja kompetentseid õpetajaid, kes vastavaid teadmisi õpilastes võiks lõimitult teiste õppekavaliste teemadega edasi anda – küberturvalisuse teema käsitlemist ei nähta sageli kooli ja õpetaja kaasvastutusena. Siiani on põhjalikumad ja ainult küberturvalisust käsitlevad koolitused olnud enamasti projektipõhised (nt Targalt Internetis[83] programmis, Küberkaitseliidu ja TalTech`ga koostöös).

Seetõttu on oluline hoida õpilaste ja õpetajate kübeturvalisusega seotud osaoskused digipädevuste mudelites ajakohased ning süsteemselt tegeleda pädevuste mõõtmisega. Tegevuse tulemusel on olemas erinevate sihtrühmade kohta algtasemed, mis on ajas võrreldavad ning annavad sisendi temaatilistesse koolitustesse, õppekavaarenduseks ja - materjalide arenduseks.

Arendatakse välja süsteemne riigiülene küberteadlikkuse tõstmise platvorm riigiasutustele ja kohalikele omavalitsustele

2018.a maist kehtima hakanud Küberturvalisuse seadus (edaspidi KÜTS)[84] paneb RIA-le küberintsidentide ennetamise ja lahendamise koordineerija rolli, mis tähendab, et esimest korda on seadusega fikseeritud RIA kohustused, mida on asutus täitnud aastaid. Koordineerija rolli paremaks täitmiseks võetakse ühe töövahendina kasutusele keskne küberteadmiste mõõtmis- ja koolitusplatvorm, mis sisaldab riigiasutustele, KOV-dele ja ühiskonnale oluliste teenuste osutajatele keskseid tööriistu teadmiste ja oskuste taseme mõõtmiseks, analüüsiks ning teavitus-/koolitustegevuseks. Tegevuse tulemusel on küberteadlikkuse testimist kasutama hakanud kõik valitsusasutused (mh rakendatakse kohustuslikku testimist avalikku teenistusse esmakordselt tööle asujate puhul) ning KOV-d, vabatahtlikult saavad seda kasutada ka oluliste teenuste osutajad.

Tugevdatakse riigi keskastme- ja tippjuhtide küberturvalisuse alaseid teadmisi ja oskuseid

Küberturvalisuse tähtsustamine asutuses sõltub otseselt juhtide hoiakutest ja teadlikkusest. Samas ei sisalda Riigikantselei poolt loodud riigi tippjuhtide kompetentsimudel[85] digioskuseid puudutavaid kompetentse (mh küberturvalisus) ning sellest tulenevalt ei tegeleta ka süsteemselt vastavate oskuste arendamisega. Nii riigi- kui kohalike omavalitsuse asutuste tegevust analüüsides võib järeldada, et infoturve on suuresti juhtimis- ja alles seejärel ressursiküsimus. Pahatihti on küberturvalisusalane teadmatus tingitud huvipuudusest ja vastupidi. Teadmiste puudumisel kiputakse ressursinappust takistusena üle tähtsustama. Organisatsioonide IT-personali teadmised ennetamise ja kahjude minimeerimise vallas on küll tõusnud, kuid endiselt teeb muret

[79] Eestis on vaja viia läbi enam teaduslikke uuringuid, luua erinevaid mõõteriistu, mille abil paremini leida lahendused, kuidas ühiskonna küberkaitse alast teadlikkust (küberhügieeni) kasvatada. Küberpähkli uuringu ülevaatest tulenevad soovitused 2018.a

[80] www.kyberpahkel.ee

[81] Digipädevus õppekavades

[82] Valmib 2019.a

[83] http://www.targaltinternetis.ee/

[84] Küberturvalisuse seadus

[85] https://riigikantselei.ee/et/tippjuhtide-kompetentsimudel

korduvate intsidentide muster. Ühetaoliste intsidentide kordumine viitab, et organisatsiooni juhtkond ei teadvusta piisavalt töötajate tegevuses rutiinselt ette tulevaid riske ning nende tegelikku mõju organisatsiooni osutatavatele teenustele.

Juhtide teadmiste ja oskuste parandamiseks kaardistatakse teadmiste tase, viiakse läbi koolitusi (mh riskiteadlikkuse ja –halduse teemal) ning õppuseid ja kõrgemaid küberkaitsekursuseid. Tegevuste tulemusel on küberturvalisuse teema lõimitud riigi keskastme- ja tippjuhtide koolitusprogrammidesse ja loonud laiemas pildis eeldused kriisisituatsioonides paremini toime tulla.

Tegevussuund 4.2. Riigi- ja erasektori nõudlusele vastava talendi arendamine

2016.aastal läbi viidud OSKA info- ja kommunikatsioonitehnoloogia (IKT) valdkondlik tööjõuanalüüs[86] 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 tööjõuvajaduse ja kompetentside osas. 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 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[87]. 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.

Arendatakse küberkaitselist õpet üldhariduskoolides ja tegeletakse andekate noorte potentsiaali tõstmisega

2018.a seisuga on riigikaitseõpetus sisse viidud 127 gümnaasiumisse ja 22 kutsekooli[88]. Riigikaitseõppe loomuliku osana käsitletakse ka küber- ja siseturvalisust, kuid teemade edasi andmiseks kavandatud tundide maht ei ole siiski piisav süvitsi minekuks. Sellest tulenevalt on oluline lõimida küberturvalisus informaatika ainekavasse ning toetada küberkaitse süvaõppe jõudmist võimalikult paljudesse gümnaasiumidesse ja luua nii eeldused küberspetsialistide järelkasvuks formaalharidussüsteemi kaudu.

Kui IKT valdkonna vastu laiemalt huvi tundvad noored saavad Eestis ennast proovile panna robootika ja programmeerimisringides, siis küberturvalisuse suunaline huvitegevus on praktiliselt olematu. Hetkel puudub Eestis ka selge ootus ning arusaam, kuidas ja millises sisus noorte hulgas kübervaldkonna vastu huvi tekitada ja läbi selle järelkasvu luua. Kasutamata on kohustusliku ajateenistuse formaat kübervaldkonna tööjõu sihtotstarbelise arendusvõimalusena. Samas saaks KaM valitsemisala ja muu riigisektori ühisel panustamisel küberajateenistust kasutada esmase värbamisplatvormina.
Kirjeldatud võimaluste realiseerimiseks luuakse KüberNaaskli[89] (võistlus-)mudeli baasil andekatele ja kübetruvalisusest huvitatud noortele koolivälise tegevuse programm. See omakorda loob kasvulava

[86] Tulevikuvaade tööjõu- ja oskuste vajadusele: Info- ja kommunikatsioonitehnoloogia 2016.a
[87] Riigi Infosüsteemi Amet Küberturvalisus 2018
[88] Allikas: Kaitseministeerium
[89] www.kybernaaskel.ee

küberajateenistusse siirdujate leidmiseks ning ajateenistusest kujuneks küberkaitse alase haridustee osa ja riigi värbamisplatvorm.

Tagatakse süsteemne ülevaade küberkaitsespetsialistide tööjõuvajadusest.

Eelnevalt viidatud OSKA raport kirjeldab küll küberkompetentside vajadust IKT põhikutsealade sees, kuid kaardistamata on küberturbespetsialistide tööjõuvajadus nii riigi- kui erasektori tellimusena. Tegemist on olulise lüliga õppekohtade planeerimise, suurema potentsiaaliga õppesuundade välja selgitamise ja tippspetsialistide täiendkoolituse vajaduse vahel mh väliskoolitused kui ka tööstusdoktorantuur. Edasiselt tagatakse süsteemsete uuringutega ülevaade küberturvalisuse valdkonna spetsialistide tööjõuvajadusest, mis seotakse poliitikasoovitustega. Uuringud on aluseks talendiarenduse alase koostöö tugevdamiseks ettevõtete ja ülikoolide vahel, mis tagab õppekavade ajakohasuse ja ülikoolilõpetajate vajaliku kompetentsi.

Tagatakse küberkaitse ja siseturvalisuse valdkondade spetsialistide taseme- ning täiendõppe kvaliteet.

Küberkaitselise õppe arendamisel on Eestis siiani lähtutud avaliku ja erasektori vajadustest, püüdes sisustada vastavad õppekavad võimalikult laia teadmiste spektriga. TalTech`i ja Tartu Ülikooli küberkaitse magistriprogramm on tunnustatud rahvusvaheliste tudengite poolt. Samas on vajalik analüüsida nii õppe- kui teadussuundade potentsiaali, et suurendada seeläbi nende rahastust ja kvaliteeti.

Kui küberkaitselise kõrghariduse arendamist saab hinnata süsteemseks, sest olemas on TTÜ juures tegutsev Küberkriminalistika ja küberjulgeoleku keskus[90], kaasates kõiki strateegilisi partnereid, siis riigisektoris töötavate küberspetsialistide (täiend-) koolitusel puudub ühtne lähenemine ja planeeritud ressurss, mida saab käsitleda riskina laiemas küberkaitse juhtimise kontekstis. Lahenduseks on asutuste ülese tehniliste koolituste süsteemi loomine, et toetada tehnoloogiaga seotud uuenduste ja riskide tundmist, et seeläbi vähendada turvaintsidentide arvu ja maandada turvariske olulisemates ametiasutustes.

Näiteks tuleb tagada, et siseturvalisuse- ja julgeoleku eest vastutavatele spetsialistidele on tagatud vastavasisuline õpe. Täna käsitletakse küberturvalisust vaid Sisekaitseakadeemia sisejulgeoleku magistriprogrammi valikkursuse raames. Samuti on vaja tasemeõppe kõrvale luua täiendõppe võimalused juba valdkonnas tegutsevatele spetsialistidele.

. Selle kõrval vajavad lisaks kaardistamist ühiskonnale oluliste teenuste pakkumisega tegelevate spetsialistide erialaspetsiifilised küberoskused ning need on vaja lõimida vastavatesse õppekavadesse.

Eesti rahvusvahelise küberõiguse kompetentsi arendamine.

2016.aastal käivitus Tartu Ülikoolis IT-õiguse koolitus- ja teadusprogramm, mille eesmärk on valmistada ette kõrgelt kvalifitseeritud juristid IKT ja küberjulgeoleku valdkonnas tarbeks. TalTechis tegutseb viimased kaheksa aastat tehnoloogiaõiguse õppetool. Selliste akadeemiliste üksuste olemasolu on heaks eelduseks rahvusvahelise küberõiguse keskuse loomiseks, mis tagaks Eestile piisava ekspertiisi, et aktiivselt panustada rahvusvahelise õiguse teemalistesse rahvusvahelistesse projektidesse ja panustada temaatilistesse debattidesse koos Euroopa Liidu ja NATO juhtriikidega. NATO Küberkaitse Koostöökeskus Tallinnas on oluline kompetentsikeskus rahvusvahelise õiguse küsimustes, kuid hetkel puudub kogu Euroopa Liidus organisatsioon teema sisuliseks edasiviimiseks rahvusvahelise õiguse tsiviilpoolel. Edasiste tegevuste planeerimiseks viiakse esmalt läbi analüüs rakendusliku suunaga rahvsvahelise küberõiguse keskuse loomise võimaluste kaardistamiseks. Eesmärgiks on liita Eestis hästi väljaarenenud akadeemilise kompetentsi välispoliitika kujundamisega kübervaldkonnas, luua võimalused õigusekspertide järelkasvu tekkeks ja kinnistada Eesti küberõiguse alane kompetents läbi osaluse rahvusvahelistes projektides.

[90] http://cybercentre.cs.ttu.ee/haridus/

KÜBERVALDKONNAGA SEOTUD TERMINID JA DEFINITSIOONID

1. Terminite ja definitsioonide koostamise alus[91]

Mõiste — arusaam, käsitlus; abstraktse mõtlemise vorm, mis peegeldab esemeid ja nähtusi nende oluliste tunnuste, seoste ja suhete kaudu.

Definitsioon — mõiste oluliste tunnuste lühike täpne esitus, määratlus

Termin — täpselt piiritletud tähendusega sõna või sõnaühend, oskussõna

Terminid saadakse siis, kui mõisted defineeritakse valdkonna spetsiifikale vastavalt.
Definitsioonide koostamisel on lähtutud järgmistest põhimõtetest:

- Definitsioonid peavad olema **arusaadavad tavalugejale**
- Definitsioonid peavad olema nii **lühikese**d, kui võimalik
- Definitsioonid peavad **baseeruma ühtsel loogikal**

Definitsioonide koostamise loogika
Küber- on eesliide erinevatele sõnadele, mille abil eraldatakse üldisest mõistest väiksem ja spetsiifilisem osa. Näiteks:

- ruum > küberruum
- turvalisus > küberturvalisus
- intsident > küberintsident

Erinevates valdkondades on defineeritud üldised mõisted (ruum, turvalisus, intsident, jne) erinevalt ning seetõttu peab arvestama, et praktikas hakatakse kasutama ka ***küber-*** eesliitega mõisteid erinevates valdkondades natuke erinevalt.

Oluline on defineerida täpselt eesliide ***küber-*** , mida oleks hea rakendada hiljem erinevates dokumentides sama loogika alusel.

Terminid ja definitsioonid

Nr.	Termin	Definitsioon	Kommentaar
Põhimõisted			
1.	**Küber-**	Eesliide, mis tähistab võrgu- ja infosüsteeme.	Näiteks küberturvalisuse seaduse mõistes on võrgu- ja infosüsteem elektroonilise side võrk, seade või omavahel ühendatud või seotud seadmete rühm, millest vähemalt ühes toimub digitaalsete andmete töötlemine.
2.	**Küberturvalisus**	Seisund, kus võrgu- ja infosüsteemid on kaitstud ohtude realiseerumise eest.	Inglise keeles defineeritakse antud terminit (cybersecurity) samuti turvalisuse tagamisena. Eesti keeles kasutatakse sellises kontekstis terminit „küberturve“.

[91] Ettepaneku koostajad: Raul Rikk, Agu Kivimägi (E-riigi Akadeemia); koostöös: Siim Alatalu, Kadri Kaska (NATO CCDCOE), Liis Rebane (MKM); arvesse on võetud esmane tagasiside osapooltelt. Selliste definitsioonidega on strateegia koostamisel lähtutud – aga need definitsioonid on ajas edasiarenevad ja uuendatakse vajadusel edaspidise rakendamise käigus.

3.	**Küberturve**	Võrgu- ja infosüsteemide turvalisuse tagamine.	Teiste sõnadega on küberturve meetmete rakendamine küberturvalisuse saavutamiseks.
4.	**Küberjulgeolek**	Seisund, kus riigi julgeolek[92] on kaitstud võrgu- ja infosüsteemide kaudu tekkivate ohtude eest.	Eesti keeles on kasutusel kaks mõistet – turvalisus ja julgeolek. Inglise keeles sellist vahet ei tehta (security). Seetõttu võiks „küberjulgeoleku“ tõlge olla inglise keeles „National Cybersecurity“.
Olulisemad küber- eesliite abil moodustatud mõisted			
5.	**Küberhügieen**	Üksikisiku või organisatsiooni elementaarsed toimingud vältimaks võrgu- ja infosüsteemide kaudu tekkivate ohtude realiseerumist.	
6.	**Küberintsident**	Võrgu- ja infosüsteemis toimuv ootamatu sündmus, mis ohustab või kahjustab süsteemi turvalisust.	Baseerub küberturvalisuse seaduse terminil.
7.	**Küberkaitse**	Meetmete rakendamine küberrünnakute ennetamiseks ja tõrjumiseks.	Üldjuhul on mõiste kasutusel riigikaitse valdkonnas.
8.	**Küberkriis**	Küberintsidendist põhjustatud hädaolukord või hädaolukorra oht.	Hädaolukord ja hädaolukorra oht on defineeritud hädaolukorra seaduses.
9.	**Küberkuritegu**	Kuritegu, mis on toime pandud arvutisüsteemi, või arvutiandmete vastu kasutades IKT vahendeid.	Budapesti konventsioon: *Offences against the CIA of computer data and systems.*
10.	**Küberoht**	Võrgu- ja infosüsteemi kaudu tekkiv sündmus või asjaolu, mis võib põhjustada kahju.	
11.	**Küber-operatsioon**	Võrgu- ja infosüsteemide keskkonnas kindlal eesmärgil toimuv küberturvalisust mõjutav tegevus.	Tavaliselt räägitakse operatsioonidest riigi julgeoleku kontekstis.
12.	**Küberruum**	Võrgu- ja infosüsteemide ühendamisel tekkiv keskkond.	Näiteks on internet globaalne küberruum.
13.	**Küberrünnak**	Tahtlik tegevus võrgu- ja infosüsteemide kaudu kahju tekitamise eesmärgil.	
Muud küberturvalisuse strateegia kontekstis läbivad mõisted			
14.	**Asjade internet**	Võrgustatud seadmete kogum, kus seadmed iseseisvalt üksteisega informatsiooni jagavad ja vahetavad.	Asjade interneti seadmed võivad olla näiteks nutitelefonid, kodumasinad,

[92] Definitsioon: põhiseadus § 129 lg 2 kommentaar http://www.pohiseadus.ee/index.php?sid=1&ptid=2526&p=129#c2

			nutikellad, meditsiiniseadmed või hooned.
15.	**Haavatavus**	Võrgu- ja infosüsteemi turvanõrkus, mida on võimalik ära kasutada kahju tekitamiseks.	Küberturvalisuse seaduse alusel välja antud määruse **§ 2 p-s 4 on defineeritud "nõrkus", mis on haavatusega samatähenduslik järgmiselt:** süsteemide või süsteemidega seotud ressursside turvalisuse puudus, mis muudab süsteemid või süsteemidega seotud ressursid ohule vastuvõtlikuks.
16.	**Krüptograafia**	Põhimõtted, vahendid ja meetodid andmete salastamiseks ja/või nende märkamatu muutmise vältimiseks.	Lähtub ITU definitsioonist
17.	**Plokiahel**	Plokiahel (inglise keeles blockchain) on hajutatud andmebaas, mis baseerub järjestikustest andmeplokkidest koosneval andmestruktuuril. Sellises andmebaasis toimub andmete uuendamine ainult läbi matemaatilise konsensuse saavutamise, tagades sellega andmete tervikluse.	
18.	**Ühiskonnale oluline teenus**	Teenus küberturvalisuse seaduse mõttes – hõlmab peamiselt elutähtsad teenused (hädaolukorra seadus) ning olulised teenused (EL võrgu- ja infoturbe direktiiv).	Küberturvalisuse seaduse teenuse mõiste on olulistest teenustest ja elutähtsatest teenustest pisut laiem, hõlmates ka tervishoiu teenuse osutajad laiemalt vältimatust abi osutamisest ja rahvusringhäälingu.