2014–2017

Küberjulgeoleku strateegia

Majandus- ja Kommunikatsiooniministeerium

2014

SISUKORD

Sissejuhatus 2

1. Hetkeolukorra analüüs 2

1.1. Valdkondlikud edusammud 2

1.2. Suundumused 4

1.3. Väljakutsed 5

2. Küberjulgeoleku tagamise põhimõtted 6

3. Strateegia üldeesmärk 2017 7

4. Alaeesmärgid 7

5. Strateegiaga seotud osapooled 12

SISSEJUHATUS

„Küberjulgeoleku strateegia 2014–2017“ on Eesti küberjulgeoleku planeerimise alusdokument ning osa Eesti laiapindsest julgeolekustrateegiast. Strateegias tuuakse välja olulisemad arengud, hinnatakse ohte Eesti küberjulgeolekule ning esitatakse meetmed ohtude maandamiseks. Käesolev strateegia jätkab mitmete „Küberjulgeoleku strateegia 2008–2013“ seatud eesmärkide ellu viimist, kuid on lisandunud ka uusi ohte ning vajadusi, mida eelmises strateegias ei kajastatud.

1. HETKEOLUKORRA ANALÜÜS

1.1. Valdkondlikud edusammud

2009. aastal asutati Vabariigi Valitsuse julgeolekukomisjoni juurde küberjulgeoleku nõukogu, mille peamised ülesanded on toetada strateegilisel tasandil ametkondade vahelist koostööd ning teostada järelevalvet küberjulgeoleku strateegia eesmärkide elluviimise üle.

2010. aastal anti Vabariigi Valitsuse otsusega Riigi Infosüsteemide Arenduskeskusele valitsusasutuse staatus. Uue nimega Riigi Infosüsteemi Amet (edaspidi *RIA*) sai täiendavad volitused ja vahendid riigi info- ja kommunikatsioonitehnoloogia (edaspidi *IKT*) infrastruktuuri kaitse korraldamiseks ning infosüsteemide turvalisuse üle järelevalve teostamiseks. RIA kooseisu moodustati osakond kriitilise informatsiooni infrastruktuuri kaitse (edaspidi *KIIK*) korraldamiseks. 2010. aasta alguses käivitas RIA kriitilise informatsiooni infrastruktuuri (edaspidi *KII*) kaardistamise projekti, mille käigus tuvastati elutähtsate teenuste sõltuvused infosüsteemidest. Kaardistuse põhjal töötati välja turvanõuded riigi toimimiseks vajalikele elutähtsatele infosüsteemidele. 2011. a moodustati riigi- ja erasektori koostöö arendamiseks KIIKi komisjon. Elutähtsaid teenuseid osutavate asutuste küberturbe- ja IT-juhte koondava komisjoni tegevuse eesmärk on vahetada operatiivselt teavet, tuvastada probleeme ning teha ettepanekuid riigi elutähtsa infrastruktuuri küberjulgeoleku parandamiseks.

2012. aastal koondati Politsei- ja Piirivalveameti (edaspidi *PPA*) küberkuritegude uurimise võimekus ühte talitusse. Lisaks asutati 2013. aastal prefektuurides küberkuritegude ja

digitaaltõendite teenistused, kuhu koondati prefektuuride erinevates üksustes paiknenud küberkuritegude menetluse ja digitaaltõendite haldamisega tegelevad ametnikud. Samuti tegeleb PPA küberkuritegevuse ohtude teadlikkuse tõstmisega, mille käigus on muu hulgas loodud veebikonstaabli ametikohad. Veebikonstaabli ülesanne on tõsta inimeste teadlikkust Interneti turvalisusest ning kaitsta lapsi ja noori Internetis. Kaitsepolitseiamet tugevdas riigi julgeolekut ohustavate küberrünnakute ja -luure takistamiseks oma uurimisvõimekust.

Riigikaitse tagamisel on olnud oluline Kaitseliidu küberkaitseüksuse (edaspidi *KKÜ*) loomine, mis toimus avaliku, era- ja kolmanda sektori koostööna. KKÜ vabatahtlike teadmisi rakendatakse õppustel, lahenduste testimisel, koolitustel jms koordineeritud abi kaudu Eesti riigiasutustes ning ettevõtetes küberturvalisuse parandamiseks. Loodud on võimalused KKÜ kasutamiseks kriisiolukorras, kus üksust on võimalik rakendada tsiviilstruktuuride toetuseks ja kriitilise infrastruktuuri kaitseks. Oluline roll küberjulgeoleku võimekuste arendamisel ja hindamisel on olnud riigisisestel ja rahvusvahelistel küberkaitseõppustel. 2012. aastal toimusid Vabariigi Valitsuse küberkaitse staabiharjutus "Küberpalavik" ning NATO kriisireguleerimisõppus „CMX 2012. Igal aastal toimub Eestis NATO Küberkaitse Koostöökeskuse (*NATO CCD COE*) õppus Locked Shields ja alates 2013. aastast NATO küberkaitseõppus Cyber Coalition. Küberkaitsealase väljaõppe toetamiseks on Kaitseväe koosseisu loodud Küberlabor, mida kasutatakse eelnimetatud küberõppuste läbiviimiseks, riigisiseste harjutuste korraldamiseks ja kõrgkoolide õppetöös.

Küberturvalisuse valdkonna peamine koolitaja ja teadlikkuse tõstja on Hariduse Infotehnoloogia Sihtasutus (edaspidi *HITSA*), endise nimega Tiigrihüppe Sihtasutus. Kaasates õpetajaid ja lapsevanemaid, toimuvad HITSA koolitused juba eelkooliealistele ja ka vanematele lastele. 2013. aastal käivitati riigi ja erasektori koostöös projekt nutiseadmete kasutajate, arendajate ja müüjate oskuste ning turvateadlikkuse tõstmiseks. 2009. aastal avati Tallinna Tehnikaülikooli (edaspidi *TTÜ*) ja Tartu Ülikooli koostöös rahvusvaheline küberkaitse magistriõppekava, kuhu võetakse igal aastal vastu 50 tudengit. TTÜ avab koostöös 2CENTRE Eesti keskusega 2014. aastal küberkriminalistika magistriõppekava. Eesti 2CENTRE küberkriminalistika keskus on osa Euroopa Liidu 2CENTRE kompetentsikeskustest, kus õpetatakse välja küberkuritegevuse vastase võitlusega seotud spetsialiste ning korraldatakse neile jätkukoolitusi.

Eesti on edukalt teinud küberjulgeolekualast koostööd teiste arenenud IKT-riikide ja rahvusvaheliste organisatsioonidega. Aktiivne roll küberjulgeolekupoliitika kujundamisel tõi kaasa NATO Küberkaitse Koostöökeskuse rajamise Eestisse. Küberjulgeolek on Eesti kaasabil saanud osaks NATO ja Euroopa Liidu poliitikast ning märkimisväärselt on kasvanud riikide huvi Eesti küberturbe kogemuse vastu. Edukalt toimib regionaalne küberjulgeolekualane koostöö Põhjala ja Baltimaadega, samuti teiste strateegiliste partnerite ja samameelsete riikidega. Tekkinud on uusi Eesti osalusel toimuvaid koostöö formaate – Internetivabaduse koalitsioon, Ühinenud Rahvaste Organisatsiooni valitsusekspertide rühm, küberruumis usaldusmeetmete väljatöötamise töörühm OSCEs, eesistuja sõprade grupp Euroopa Liidus jt.

1.2. Suundumused

Info- ja kommunikatsioonitehnoloogiate jätkuv kiire areng, üleilmastumine, andmemahtude drastiline suurenemine ja andmesidevõrkudesse ühendatud eritüübiliste seadmete kasvav hulk omavad mõju nii igapäevaelu, majanduse kui ka riigi toimimisele. Ühest küljest toob IKT selline areng kaasa teenuste parema kättesaadavuse ja kasutusmugavuse, parandab riigi toimimise läbipaistvust ja kodanike osalemisvõimalust ning kärbib nii avaliku kui erasektori kulusid. Teisalt kaasneb tehnoloogia suureneva osatähtsusega ühiskonna, majanduse ja riigi kasvav sõltuvus juba harjumuspärastest e-lahendustest ning kinnistub ootus tehnoloogia tõrgeteta toimimisele. Lisaks muutub Internet üha kättesaadavamaks, suureneb selle kasutajate arv ning uute tehnoloogiliste lahenduste ja teenuste – nagu „asjade Internet“ ja pilvandmetöötlus – kaudu ka võimalike ründevektorite arv ja võimalike rünnete keerukus.

Sotsiaalsed protsessid sõltuvad samuti üha rohkem infotehnoloogilistest vahenditest ning edaspidi tuleb tähelepanu suunata sellele, et ühiskonnal laiemalt ja igal isikul kitsamalt säiliks kontroll vastavate protsesside üle. Vastasel juhul võivad protsessid muutuda isereguleeruvaiks, kui infotehnoloogia võimalused pisendavad inimese osatähtsust protsessiotsuste tegemisel (tehnoloogiline singulaarsus).

Peamine ohuallikas on küberkuritegevus, mille kasv peegeldub küberkurjategijate oskuste olulises arengus ja organiseeritud rünnete toimepanemise võimekuse tõusus. Kuritegude menetlemise üks lahutamatu osa on digitaalsete asitõendite kogumine ja käitlemine, mis seab uued väljakutsed politsei menetlus- ja küberkriminalistika võimekusele.

Riigi küberjulgeolekut mõjutavad arvukad küberruumis erinevate oskuste, sihtmärkidega ja motivatsiooniga toimijad. Sageli on keeruline toimijaid üksteisest eristada või määrata kindlaks nende seotust riikide või rahvusvaheliste organisatsioonidega. Kasvab riiklike toimijate hulk küberruumis, kes on seotud nii Internetiga ühendatud kui ka suletud arvutivõrke sihtiva küberspionaažiga, mille eesmärgiks on koguda teavet nii riigi julgeoleku- kui ka majandushuvide kohta. Suureneb küberründevõimekust omavate riikide hulk ja aktiivsus.

Lisaks riiklike toimijate aktiviseerumisele kasvab poliitiliselt motiveeritud üksikisikute ja ühenduste suutlikkus panna väheste vahenditega toime teenusetõkestus- jm ründeid, samuti oma tegevust sotsiaalvõrgustikes organiseerida.

Nii riigi küberjulgeoleku korralduse ülesehitamisel kui ka küberintsidentide ennetamisel ja lahendamisel muutub järjest möödapääsmatumaks avaliku ja erasektori sisuline ja tõhus koostöö. Riigikaitse ja sisejulgeolek sõltuvad erasektori taristust ja vahenditest, samas vajavad elutähtsate teenuste osutajad ja kriitilise informatsiooni infrastruktuuri tagajad riigi tuge erinevate huvide koordineerija ja tasakaalustajana.

1.3. Väljakutsed

Peamised küberjulgeolekuohud tulenevad Eesti riigi, majanduse ja elanikkonna ulatuslikust ning kasvavast sõltuvusest IKT taristust ja e-teenustest. Seetõttu keskendub küberjulgeoleku strateegia peamiste valdkondadena elutähtsate teenuste tagamisele, küberkuritegevusvastase võitluse tõhustamisele ja riigikaitseliste võimete arendamisele. Täiendavalt nähakse ette neid valdkondi toetavad tegevused: õigusliku raamistiku kujundamine, rahvusvahelise koostöö ja suhtluse edendamine, teadlikkuse tõstmine ja küberjulgeolekut tagavate spetsialistide pealekasvu kindlustamine ja lahenduste tagamine.

Elutähtsate teenuste puhul on tekkinud infotehnoloogilised ristsõltuvused selliste teenuste vahel, mille tagamine ei sõltu vaid Eestis paiknevatest osapooltest, vaid mille tagamine ületab ka riigipiire. Teenuste või nende osade üle, mida osutatakse väljaspool Eesti Vabariiki, puudub Eesti riigil efektiivne järelvalvevõimalus. Tuleb kindlustada, et kõik elutähtsad teenused ja nende sõltuvused on kaardistatud, välja töötatud on alternatiivid ning ollakse valmis neid operatiivselt kasutusele võtma. Ühiskonna toimimise seisukohalt oluliste andmete

ja infosüsteemide säilimine tuleb tagada nii avalikus kui erasektoris. Peab olema tagatud riiki, ühiskonda ja isikut ohustavate küberohtude õigeaegne märkamine ja neile reageerimine.

Küberkuritegevus kahjustab majandusruumi toimimist, vähendab usaldust digitaalsete teenuste vastu ja võib halvimal juhul viia inimohvritega intsidentideni. Tuleb tagada küberkuritegevuse ennetamine, avastamine ja menetlemine; selleks on vajalik pädev personal ja kaasaegsed tehnilised vahendid. Üha olulisemaks muutub küberkuritegevusalase teabe operatiivne vahetamine riikide vahel.

Riigikaitseliste võimete tagamiseks peavad riigi käsutuses olevad tsiviil-, sõjalisel ja rahvusvahelisel koostööl põhinevad ressursid toimima ka küberruumis ning moodustama terviku riigi tsiviilstruktuuride juhtimisel toimiva küberruumi kaitsega. Riigikaitse planeerimisel tuleb järjest enam lisaks konventsionaalsetele sõjalistele keskkondadele arvestada ka küberruumiga.

Tuleviku julgeolekuohtude ennetamiseks ja tõrjumiseks on vaja pidevalt arendada küberjulgeolekualast oskusteavet ja investeerida tehnoloogiasse. Usaldusväärsete ja konkurentsivõimeliste küberlahenduste tagamiseks tuleb tagada riigi tark tellimus ja lahenduste eksport, saadud teadmised ja vahendid tuleb aga uuesti innovaatilistesse lahendustesse investeerida.

Toetava tegevusena on ülalloetletud väljakutsete terviklikuks lahendamiseks vaja tagada ajakohane õiguslik raamistik. Rahvusvahelises plaanis tuleb seista vaba ja turvalise küberruumi säilimise eest ning tagada Eesti keskne roll ja suunav osalemine rahvusvahelise küberjulgeolekupoliitika edendamisel nii rahvusvahelistes organisatsioonides kui ka samameelsetes kooslustes.

2. KÜBERJULGEOLEKU TAGAMISE PÕHIMÕTTED

1. Küberjulgeolek on riikliku julgeoleku lahutamatu osa, see toetab riigi ja ühiskonna toimimist, majanduse konkurentsivõimet ja innovatsiooni.
2. Küberjulgeolek on tagatud põhiõigusi ja vabadusi järgides ning isikuvabadusi, isikuandmeid ja identiteeti kaitstes.
3. Küberjulgeoleku tagamisel lähtutakse proportsionaalsuse põhimõttest, arvestades sealjuures olemasolevate ning võimalike riskide ja ressurssidega.

4. Küberjulgeolek on tagatud koordineeritult avaliku, era- ja kolmanda sektori koostöös, võttes arvesse küberuumis olevate taristute ja teenuste omavahelist seotust ning sõltuvust.

5. Küberjulgeoleku tagamine algab individuaalsest vastutusest IKT vahendite turvalisel kasutamisel.

6. Küberjulgeoleku tagamisel on esmatähtis võimalikke ohte ennetada ja tõkestada ning realiseerunud ohtudele tõhusalt reageerida.

7. Küberjulgeoleku tagamist toetab intensiivne ja rahvusvaheliselt konkurentsivõimeline teadus- ja arendustegevus.

8. Küberjulgeolekut tagatakse rahvusvahelises koostöös liitlaste ja partneritega. Koostöö kaudu edendab Eesti ülemaailmset küberjulgeolekut ja suurendab enda kompetentsi.

3. STRATEEGIA ÜLDEESMÄRK 2017

Visioon:

Eesti suudab tagada riigi küberjulgeoleku ning toetada avatud, kaasava ja turvalise infoühiskonna toimimist.

Üldeesmärk:

Küberjulgeoleku strateegia nelja aasta eesmärk on suurendada küberturvalisuse alast võimekust ja inimeste teadlikkust küberohtudest, tagamaks jätkuvat usaldust küberruumi vastu.

4. ALAEESMÄRGID

Alaeesmärk 1: Oluliste teenuste infosüsteemide kaitse tagamine

Eesti riigi ja ühiskonna toimimine, iga inimese majanduslik ja sotsiaalne heaolu, elu ning tervis sõltuvad üha enam kasutatavate infosüsteemide ja teenuste turvalisusest. Strateegia üks põhieesmärk on kirjeldada meetmeid elutähtsate teenuste katkematuks toimimiseks ja vastupidavuseks ning kriitilise informatsiooni infrastruktuuri kaitseks küberohtude eest.

1.1. Oluliste teenuste alternatiivlahenduste tagamine

Riigi, majanduse ja elanikkonna sõltuvus IKT infrastruktuurist ning e-teenustest on pidevalt ajakohaselt kaardistatud ja hallatud. Määratletud on alternatiivlahendused, mis võetakse kasutusele juhul, kui IKT infrastruktuuri ja e-teenuste tavapärane toimimine on häiritud.

1.2. Oluliste teenuste vaheliste ristsõltuvuste haldamine

Oluliste teenuste vaheliste ristsõltuvuste kaardistust hoitakse ajakohasena, ristsõltuvuste mõju ulatus teenuste toimimisele on ajakohaselt hinnatud ning seonduvad riskid süstemaatiliselt maandatud. Kaardistust, mis kirjeldab oluliste teenuste sõltuvust väljaspool Eesti Vabariiki osutavatest teenustest, hoitakse ajakohasena, nende mõju ulatus teenuste toimimisele on ajakohaselt hinnatud ning seonduvad riskid süstemaatiliselt maandatud.

1.3. IKT infrastruktuuri ja teenuste turvalisuse tagamine

Info- ja kommunikatsioonitehnoloogia infrastruktuur on kaitstud kaasaegsete ohtude eest. Kriitilisi andmeid hoitakse ning töödeldakse kõrgturvalistes andmekeskustes, muu hulgas kasutatakse andmete varundamist väljaspool Eestit. Riigi ja elutähtsate teenuste toimimiseks vajalikke infosüsteeme arendatakse ja hallatakse turvariske arvestades, nähes ette vahendid ja meetmed riskide maandamiseks.

1.4. Avaliku ja erasektori küberriskide haldamine

Avaliku ja erasektori tegevuse riskide juhtimisel suudetakse hinnata ja mõõta infotehnoloogilisi riske, selleks on olemas vajalike oskustega personal, metoodika, koolitusvõimalused ja muud vajalikud ressursid. Kaardistatakse valdkonnad, millele ei ole seni küberkaitsealaselt piisavalt tähelepanu pööratud, ja luuakse vastavad teadlikkuse tõstmise programmid.

1.5. Riikliku küberjulgeoleku seiresüsteemi juurutamine

Riiki, ühiskonda ja isikut ohustavate küberohtude õigeaegseks märkamiseks ja nendele reageerimiseks võetakse kasutusele riiklik terviklik seire-, analüüsi- ja raporteerimissüsteem.

1.6. Riigi digitaalse järjepidevuse tagamine

Riigi digitaalseks järjepidevuseks hädavajalikud e-teenused, protsessid ja infosüsteemid (sh täisdigitaalsed tõestusväärtusega registrid) on pidevalt ajakohaselt kaardistatud, neile on loodud peegeldus- ja varundusalternatiivid. Virtuaalsaatkondade abil tagatakse riigi toimimine, olenemata Eesti territoriaalsest terviklikkusest.

1.7. Kriitilise informatsiooni infrastruktuuri kaitse rahvusvahelise koostöö edendamine

Kriitilise informatsiooni infrastruktuuri kaitset tõhustatakse rahvusvaheliste organisatsioonide

töös osalemise, partnerite ja liitlaste huvigruppides esindatuse ja tippspetsialistide professionaalsesse arengusse panustamise abil.

Alaeesmärk 2: Küberkuritegevusvastase võitluse tõhustamine

Küberkuritegevusest tulenev majanduslik kahju vähendab usaldust digitaalsete teenuste vastu ja võib halvimal juhul tuua kaasa inimohvreid. Laiema üldsuse kõrgem teadlikkus küberjulgeolekuriskidest aitab ennetada küberkuritegevust. Suurem teadlikkus saavutatakse, käsitledes küberteemasid kõikidel haridustasemetel ning teavitades inimesi turvakäitumisuuringutel ja -analüüsidel rajaneva teabega.

2.1. Küberkuritegude avastamise tõhustamine

Küberkuritegude avastamise ja menetlemise tõhustamiseks korrastatakse senist korrakaitsestruktuuri ja töökorraldust, suurendatakse küberkuritegevusega seotud isikkoosseisu ning tõstetakse menetlejate digitaalsete andmekandjate käitlemise võimekust. Võimekuse arendamiseks tehakse koostööd ülikoolide ja rahvusvaheliste kompetentsikeskustega.

2.2. Avalikkuse teadlikkuse tõstmine küberohtudest

Küberruumis tegutsevate osaliste teadlikkuse tõstmiseks pööratakse tähelepanu küberohte ennetavate tegevuste tutvustamisele, intsidentide äratundmiseks vajalike teadmiste andmisele ja intsidentidele targalt reageerimise teadvustamisele. E-teenuste tarbijad suunatakse kasutama turvalisemaid lahendusi ning teavitatakse neid uutest tehnoloogiatest ning lahenduste turvalisest kasutamisest.

2.3. Rahvusvahelise küberkuritegevuse vastase koostöö edendamine

Rahvusvahelise mõõtmega küberkuritegude efektiivsemaks ja kiiremaks menetlemiseks parandatakse riikidevahelist suhtlust. Osaletakse aktiivselt rahvusvahelise küberkuritegevuse vastase võitluse initsiatiivides ja projektides.

Alaeesmärk 3: Riigikaitseliste võimete arendamine küberkaitse valdkonnas

Riigi käsutuses olevad tsiviil-, sõjalisel ja rahvusvahelisel koostööl põhinevad ressursid peavad suutma toimida adekvaatselt ka küberruumis – nii eelhoiatuse ja heidutuse kui ka aktiivse kaitse funktsioonis. Ühtlasi peavad riigikaitselised ressursid moodustama terviku riigi

tsiviilstruktuuride juhtimisel toimiva küberruumi kaitsega.

3.1.Sõjalise planeerimise ning tsiviilhädaolukordadeks valmistumise sünkroniseerimine

Laiapindse riigikaitse tagamiseks vajalike elutähtsate teenuste osutajate toimepidavusplaanid viiakse kooskõlla riigikaitse ohustsenaariumitega.

3.2. Küberkollektiivkaitse ja rahvusvahelise koostöö arendamine

Kollektiivkaitse tagamiseks rahvusvahelises keskkonnas tõhustatakse infovahetust ja koostööd NATO ning Euroopa Liidu küberinstantside ja muude partneritega. Panustatakse NATO ühiste küberjulgeolekualaste võimete, standardite, väljaõppe- ja treeningvõimaluste loomisse ning arendamisse.

3.3. Sõjalise kaitse kübervõimete arendamine

Sõjalise kaitse kübervõimete arendamisega saavutatakse olukord, kus küberkaitse on üks osa laiapindsest kollektiivkaitsest, mille tagamiseks rakendatakse lisaks Kaitseväe ning Kaitseliidu spetsialistidele teisi avaliku ning erasektori spetsialiste.

3.4. Riigikaitse valdkonna küberjulgeolekualase kõrge teadlikkuse tagamine

Riigikaitse valdkonna küberjulgeoleku riskide teadlikkuse tõstmiseks ning selle seostamiseks teiste sõjaliste domeenidega korraldatakse valdkonna personalile täiendavaid koolitusi.

Alaeesmärk 4: Eesti maandab kujunevaid küberjulgeolekuohte

Küberjulgeolekuvõimekuse säilitamiseks ja tõstmiseks võtab Eesti kasutusele sõltumatud küberturbelahendused, mida toetavad küberturbealane väljaõpe ja treeningvõimalused, teadus- ja arendustegevus ning ettevõtlus. Lahenduste jätkusuutlikkuse tagamiseks toimib riik „targa tellijana“ ning toetab küberturbelahenduste eksporti.

4.1. Küberjulgeoleku spetsialistide järelkasvu tagamine

Küberjulgeoleku spetsialistide järelkasvu tagamiseks luuakse täiendavaid rahvusvahelisel tasemel kõrgharidust ning täienduskoolitust pakkuvaid õppevorme. Toetatakse küberjulgeoleku eriala magistrikraadiga lõpetanud üliõpilaste ning küberjulgeolekuteemaliste doktoritööde arvu kasvu. Õppetöösse kaasatakse senisest enam välisõppejõude ja -eksperte.

4.2. Küberjulgeoleku lahenduste targa tellimuse arendamine

Turvaliste lahenduste loomiseks panustatakse riigi toel küberjulgeolekualasesse teadus- ja arendustegevusse. Luuakse vastavat tegevust koordineeriv ning riigikaitset, julgeolekut, majandusarengut ja akadeemilist ringkonda koondav nõukogu.

4.3. Küberturbe- ja -julgeolekulahendusi pakkuvate ettevõtete arengu toetamine

Turvaliste lahenduste jätkusuutlikkuse toetamiseks panustatakse riigi toel küberturbe- ja küberjulgeolekulahenduste eksporti ja nende rahvusvahelise kasutamise suurendamisse.

4.4. Uute lahenduste turvariskide ennetamine

Uute tehnoloogiate arendamisel ja juurutamisel uuritakse ning hinnatakse põhjalikult tehnoloogilisi riske, et vältida ulatuslike küberintsidentide teket. Heatasemelise ning teadmispõhise riskiteadlikkuse abil saavutatakse eeliseid riigi, ühiskonna ja majanduse arendamisel.

Alaeesmärk 5: Eesti arendab valdkonnaüleseid tegevusi

Küberohtudevastaseks kaitseks vajalike võimekuste tõstmiseks on vaja saavutada mitmed eesmärgid, mille meetmed on valdkondadeülesed. Õigusliku raamistiku ja välispoliitilise ruumi kujundamine on olulised nii elutähtsate teenuste kaitsel, küberkuritegevusega võitlemisel kui ka riigikaitse kujundamisel küberruumis.

5.1. Küberjulgeolekut toetava õigusliku raamistiku kujundamine

Turvalisemat küberruumi tagavate meetmete rakendamiseks ajakohastatakse küberjulgeolekuga seotud õiguslikku raamistikku.

5.2. Rahvusvahelise küberjulgeolekupoliitika edendamine

Rahvusvahelistes organisatsioonides keskendutakse Eesti küberjulgeolekualaste välispoliitiliste seisukohtade ja visiooni esitlemisele ja kaitsmisele, rahvusvahelise õiguse normide ja usaldusmeetmete küberruumis kohaldamise ühiste arusaamade kujundamises kaasarääkimisele. Erilist tähelepanu pööratakse põhiõiguste ja -vabaduste kaitse ning Interneti haldamise temaatikale. Samuti aidatakse abikäepoliitika ja turvaliste e-lahenduste kaudu kaasa vaba ja turvalise küberruumi tekkele riikides, kus vabakonnal puudub tegutsemisvabadus ja vajaminev tehniline baas.

5.3. Liitlaste ning partneritega koostöö tihendamine

Liitlas- ja partnerlussuhete tugevdamiseks tihendatakse koostööd lähinaabritega ja laiendatakse koostööformaati samameelsete riikidega, oluliselt panustatakse küberjulgeolekualase oskusteabe ja kogemuste jagamisele.

5.4. Euroopa Liidu tegutsemisvõime tugevdamine

Euroopa Liidu ühtse küberjulgeoleku ja selle poliitika edendamiseks tehakse koostööd, et tõsta liikmesriikide küberteadlikkust ning parandada valmisolekut uuteks ohtudeks ja suutlikkust nendega tegeleda.

5. STRATEEGIAGA SEOTUD OSAPOOLED

Küberjulgeolekupoliitikat juhib ja strateegia elluviimist koordineerib Majandus- ja Kommunikatsiooniministeerium. Strateegia elluviimisel osalevad kõik ministeeriumid ja valitsusasutused, eelkõige Kaitseministeerium, Riigi Infosüsteemi Amet, Justiitsministeerium, Politsei- ja Piirivalveamet, Riigikantselei, Välisministeerium, Siseministeerium ning Haridus- ja Teadusministeerium. Strateegia elluviimisel ja hindamisel tehakse koostööd vabaühenduste, ettevõtlusorganisatsioonide, omavalitsuste ja haridusasutustega.

Strateegia täitmisega seotud asutused esitavad Majandus- ja Kommunikatsiooniministeeriumi taotlusel kirjalikult ülevaate meetmete ja tegevuste täitmise kohta igal aastal hiljemalt 31. jaanuaril. Majandus- ja Kommunikatsiooniministeerium koostab ülevaadete põhjal meetmete ja tegevuste elluviimise aruande ning hindab strateegia elluviimise tulemuslikkust hiljemalt iga aasta 31. maiks. Lühiaruanne strateegia täitmise kohta, mis sisaldab ülevaadet tegevustest, rakendusprobleemidest ja kuludest, esitatakse igal aastal hiljemalt 30. juunil Vabariigi Valitsusele. Strateegia täitmise lõpparuande esitab Majandus- ja Kommunikatsiooniministeerium Vabariigi Valitsusele hiljemalt 31.05.2018.

Strateegia tegevused koos vastutajate ja eelarvega esitatakse rakendusplaanis. Strateegia nelja aasta maksumus on ligi 16 miljonit eurot. Rakendusplaani täiendamise ettepanekud esitatakse Vabariigi Valitsusele koos arengukava täitmise aruandega. Rakendusplaani tegevused kajastatakse ministeeriumide ja teiste valitsusasutuste tööplaanis.

Strateegia ei muuda küberjulgeoleku eest vastutavate ametkondade pädevusi.

Strateegia koostamisel osalenute ja seda nõustanute nimekiri on strateegia Lisas 1 „Küberjulgeoleku strateegia 2014–2017 koostamises osalenute nimekiri“[1].

Lisad:

Lisa 1 Küberjulgeoleku strateegia 2014–2017 koostamisse kaasatud osapooled

Lisa 2 Valdkondlik metoodika

[1] Strateegia koostas majandus- ja kommunikatsiooniministeeriumi riigi infosüsteemide osakonna küberturbe valdkonna juht Sander Retel.