TALLINNA TEHNIKAÜLIKOOL
Majandusteaduskond
Ragnar Nurkse innovatsiooni ja valitsemise instituut

Liis Mesi, Hans Christian Ende

KÜBERTURVALISUSE TAGAMISE JUUHTUMIANALÜÜS EESTI KÜBERSTRATEEGIA JA -TEGEVUSKAVA PÕHJAL

Juhtumianalüüs 2023
Avaliku sektori juhtimine ja innovatsioon

Koordineerimine ja koostöö keeruliste poliitikaprobleemide lahendamisel
Õppejõud: Külli Sarapuu

Tallinn 2023

SISUKORD

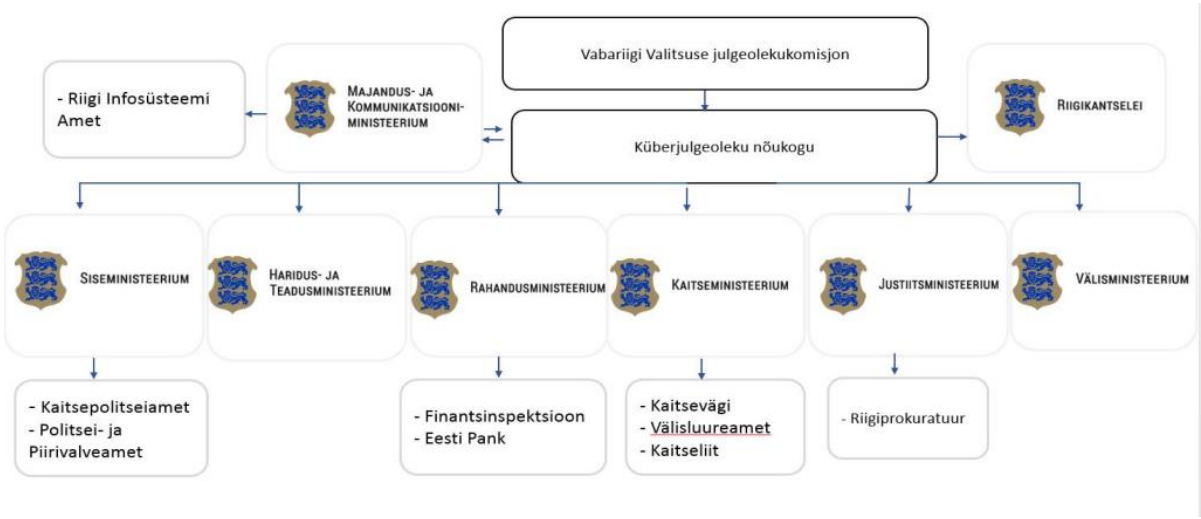
SISSEJUHATUS:

Töö eesmärgiks on analüüsida küberturvalisuse tagamist Eestis ning selle juhtimisskeemi analüüs läbi Riikliku küberturvalisuse strateegia 2019-2022 vaate. Probleemi on oluline kuna Euroopa Komisjoni avaldatava digitaalmajanduse ja -ühiskonna indeksi (DESI) 2022. aasta Eesti riigi aruande kohaselt on Eesti avalike teenuste digitaliseerimise üleilmne liider, kus nii ettevõtted kui üksikisikud on harjunud tegema haldustoiminguid veebi vahendusel (DESI 2022) ning ligi 99% (e-Estonia 2023) Eesti digiriigi teenustest pakub riik veebi vahendusel. Lisaks omab Statistikaameti 2022. aasta teise kvartali uuringu andmetel 92,4% Eesti leibkondadest kodust internetiühendust (Statistikaamet 2022), mis näitab et suurem osa ühiskonnas kasutab internetis pakutavaid teenuseid peaaegu igapäevaselt. Samas ei saa digitaliseerimisest rääkida ilma küberjulgeolekuta. Küberjulgeolek on digitaliseerimise võimaldaja, mis tõttu on küberjulgeolgeolek ja digitaliseerimine sama mündi kaks erinevalt poolt. Ukrainas on kineetilise sõja taustal käimas maailma esimene kübersõda, millega seoses on märgata ka küberrünnakute arvu tõusu ka mh. NATO liikmeriikide ning sealhulgas Eesti vastu. Riigi Infosüsteemi Ameti (RIA) sõnul 2022. aastal laekus RIA intsidentide käsitlemise osakonda CERT-EE 27 115 pöördumist ehk 74 pöördumist päevas, millest 2672 olid mõjuga intsidendid, mille tõttu olid häiritud teabe või süsteemide konfidentsiaalsus, terviklus või kättesaadavus (RIA 2023). Ainuüksi septembris registreeris CERT-EE 299 mõjuga intsidenti (Olukord küberruumis 2023). Kui geograafiliselt oleme kaitstud kaugemate riikide eest, siis küber puuduvad selged piirid ja küberründeid on võimalik läbi viia koheselt ükskõik kust. Küberründed aga ei mõjuta ainult veebis pakutavad teenuseid, vaid tänapäeval on võimalik läbi rünnete halvata ka elektrivõrke ja riigile kriitilist infrastruktuuri. Juhul kui küberkaitse võimesse ei panustata võivad inimesed jääda ilma elektrist, veest ja muust eluks vajalikust. RIA sõnul „oht, et Eestit tabab suure mõjuga lunavararünnak, on eelmainitud põhjustel kasvamas. Samuti võib prognoosida, et järgnevate aastate jooksul muutuvad tehnoloogia – nt tehisintellekti – arenguga juba mitu aastat Eestiski probleeme tekitanud õngitsusrünnakud usutavamaks, sihitumaks ja seeläbi raskemini avastatavaks“ (RIA 2023). Kui riik ei panusta süsteemselt küberkaitsevõimekuse tõstmisesse ja küberekpsrtide järelkasvule ei suuda me tehnoloogia arenguga kaasa käia, mistõttu muutuvad kõigi kodanike andmed ja info haavatavaks ning halvata Eesti riigi toimimist ning küberkurjategijatel on võimalik läbi lunavararünnkute tekitada meeletult kahju riigile, ettevõtjatele ja/või kodanikele. Töö keskendub eelkõige küberturvalisuse strateegia ja selles välja toodud koordinatsioonisüsteemi ja valdkonna juhtimiskorralduse analüüsile, kuna Majandus- ja Kommunikatsiooniministeeriumi (MKM) on küberturvalisuse strateegias välja toonud, et „suureks väljakutseks on küberturvalisuse

valdkonna strateegiline tervikjuhtimine ja ühtne koordinatsioon: valdkonna planeerimine toimub endiselt pigem asutuste vastutusalade summana, igaühe enda prioriteete pidi“ (MKM 2019, lk 12).

OSAPOOLED:

Kuna küberturvalisus puudutab kõiki ühiskonna kihte ja valdkondi nii era- kui ka avalikus sektoris pole antud töö raames võimalik täielikku kaardistust läbi viia, mistõttu keskendutakse antud juhtumianalüüsis eelkõige küberturvalisuse strateegias mainitud osapooltele, mis jagunevad ametlikeks ja mitteametlikeks osapoolteks. Ametlikud osapooled on MKM, RIA, Tarbijakaitse ja Tehnilise Järelevalve Amet (TTJA), Haridus- ja Teadusministeerium, Justiitsministeerium, Riigiprokuratuuriga, Andmekaitse Inspektsioon, Eesti Kohtuekspertiisi Instituut, Registrite ja Infosüsteemide Keskus, Kaitseministeerium, Siseministeerium, Välisministeerium, Rahandusministeerium, Riigikantselei ning nende asutuste allasutused (vt. joonis 1). Mitteametlikeks osapoolteks on erinevad rahvusvahelised organisatsioonid nagu ÜRO ja Euroopa Liit ning erinevad mõttekojad NATO Küberkaitsekoostöö Keskus (CCDCOE), e-Riigi akadeemia (eGA), Rahvusvaheline kaitseuuringute Keskus (RKK) ja TalTech Küberkriminalistika ja küberjulgeoleku keskus. Lisaks kuuluvad mitteametlike osapoolte hulka ka erinevad IT ettevõtted ja suurfirmad nagu, Microsoft, Mandiant, Google ja teised kellel on mastaabist tulenevalt suurem pilt kübermaailmas olevatest ohtudest.



Joonis 1. Ametlikud osapooled (MKM 2019)

Küberturvalisuse valdkonna sisuline komplekssus tuleneb eelkõige sellest, et küberruum on seoses uute tehnoloogiatega aina kiiremini arenev keskkond, kus uute digitaalsete teenuste lisandudes suureneb ka kaitsvate süsteemide hulk, mistõttu pole ühtainsat õiget viisi kuidas probleemi

lahendada. Kuigi küberturvalisuse strateegia määrab ära üldised suunad mille poole liikuda, ei ole välja Seetõttu „osapooled kujundavad oma käitumist lähtuvalt nende tajutud keskkonnast ja selles keskkonnas esinevatest probleemidest“ (Klijn, et al 2016, lk 49). Sellest tulenevalt on ka erinevatel asutustel erinev küberkaitse korraldus, mis tihtipeale duplitseerib ressursse. Detsentraliseeritusest tulenevalt on kõigil asutustel oma nägemus sellest, milliseid küberohte nad prioriteetseks peavad ning kui palju nad ressursse nad erinevatesse IT süsteemidesse panustavad. Kõik IT majad arendavad oma lahendusi ning arvestavad nende juures ainult asutuse siseseid ohukohti jättes tihtipeale suurema mõjuhinnangu tegemata, kuigi kõik asutused on seotud ühtse taristuga ehk riigivõrguga (MKM 2023). Kuna küberturvalisuse eest üldise vastutajana vaadatakse MKMi suunas ja eeldatakse, et nad tegelevad laiapindse läbiva küberturvalisuse tagamisega, puudub erinevatel asutustel ka omanikutunne.

Kuna MKMi pädevuses on küberturvalisuse strateegia koostamise ja elluviimist (MKM 2019, lk 17) läbi Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu loob eelkõige teadmist probleemi suurema tervikpildi osas, sh ka läbi oma allasutuste. MKMi haldusalasse kuuluv RIA „kujundab ja kindlustab Eesti digiühiskonna alustalasid: arendab ja haldab digiriigi keskseid tehnoloogilisi platvorme ning tagab riigi küberturvalisuse“ (Ameti ülesanded ja struktuur 2023) ning koostab igakuiseid ja aastaseid ülevaated küberruumi ohupildist, mistõttu RIA toob eelkõige tehnilist teadmist erinevate küberintisentide ja küberünnete trendide osas. Haridus- ja Teadusministeeriumi toetab teadmustega erinevatest küberi alastest õppeprogrammidest ja lõpetanud IT spetsialistide statistikast ning seeläbi ka teadmuse võimalikust inimressursist. Justiitsministeerium koostöös Riigiprokuratuuriga toob teadmisi kübervaldkonna kriminaalmenetluse, õigus- ja kriminaalpoliitika planeerimise osas, ning läbi oma allasutust infotehnoloogiaalase ekspertiisiga (MKM 2023). Kaitseministeerium koostöös Kaitseväe, Kaitseliidu ja Välisluureametiga panustavad koostöös eelkõige riigikaitse arengukava sõjalise kaitse osa kübervaldkonnaga seotud tegevuste elluviimise ning panustab läbivalt valdkonnaüleste koostöö- ja koordinatsioonimehhanismide ning ühtse olukorrapildi loomisse (*ebit*), mistõttu nemad toovad teadmust sõjaliste süsteemide ja ohupildi kohta. Siseministeerium koostöös Politsei- ja Piirivalveametiga ning Kaitsepolitseiga omab teadmust küberkuritegude ennetamise, tõkestamise ja avastamise, menetlemise ja küberjulgeolekut ohustavate süütegude ennetamise ja tõkestamise ning küberturvalisuse strateegia prioriteetide elluviimise siseturvalisuse arengukava ja seotud programmide tegevustega(*ebit*). Välisministeerium suunab ja koordineerib strateegia rahvusvahelise koostöö tegevusi (MKM 2023) ning osaleb erinevate rahvusvaheliste koostööformaatides ning tegeleb välis- ja julgeolekupoliitiliste riskidega. Välisministeerium toob

eelkõige teadmust rahvusvaheliste trendide osas. Rahastusministeerium tegeleb jätkusuutlikkuse tagamisega läbi eelarveliste vahendite ning seetõttu toob teadmust rahaliste ressursside osas. Riigikantselei tagab küberturvalisuse integreerimise riigikaitse planeerimisdokumentidesse (*ebit*). Mitteametlike osapoolte tehakse koostööd erinevate mõttekodade, kompetentsikeskuste, ülikoolidega, IT ettevõtetega, kes omavad praktilisi teadmisi ja saavad pakkuda teaduspõhiseid lahendusi.

Nagu varasemalt mainitud tuleneb strateegiline komplekssus sellest, et Küberturvalise strateegia seab üldised strateegilised suunad, kuid puudu on konkreetsetest sammudes, mis erinevatele asutustele ette seatakse. Lisaks on Eesti riigiasutuste detsentraliseeritusest tulenevalt puudus ka strateegilisest tervikjuhtimisest ning koordinatsioonist. Igal ministeeriumil on oma vastutusala, prioriteedid ja kompetentsid, mistõttu kübermaastik on killustanud (MKM 2019, lk 12). Seetõttu on iga asutus võtnud endale asutusesisesed prioriteetteemad millega tegeleda või milliseid digilahendusi arendada ning milliseid turvalisuse meetmeid rakendatakse. Kuigi üldises pildis on suund sama, ajavad erinevad asutused endiselt enda asutustele tähtsat teemat. Kuna aga „puudub riigil süsteemne ülevaade süsteemide omavahelistest rist- ja piiriülestest sõltuvustest ja võimalikest mõjudest ning selge arusaam teenuste miinimumtaseme tagamisest, mis peab töötama ka kriisiolukorras“ (*ebit*), ei ole palju formaalseid võimalusi peale Küberjulgeoleku nõukogu MKMi poolt suuna korrigeerimiseks. Kuid kuna Eesti on väike riik toimub infovahetust palju läbi informaalsete kanalite ja isiklike suhete, mistõttu on võimalik vajadusel probleeme ka läbi teiste kanalite lahendada. Kõige suurem strateegiline komplekssus avaldub ametlike ja mitteametlike osapoolte vahel. Kui ametlike osapoolte fookuses on riigi küberkaitsevõimekuse tõstmine, siis eraettevõtted soovivad eelkõige edendada enda huvisid ja teha lobitööd enda toodet ja teenuste edendamiseks, kuigi Eesti kogemus üldiselt on olnud selles osas positiivne.

Eesti kontekstis on küberturvalisuse tagamiseks esmatähtis koostöö era- ja avaliku sektori vahel on toiminud ning paljud Eesti digi- ja küberlahendused on välja töötatud omavahelises koostöös. Üldine arusaam on, et küberturvalisus saab tagatud olla vaid koostöö kaudu ning kõikidel tasanditel – riiklikul, erasektori ja individuaalsel – on vajalik ühine panus (Invest in Estonia 2017). Kõige suuremaks murekohaks väikeriigi puhul on inimressursi puudus mis tähendab, et Eestis on kübereksperti iside kogukond väike ja ekspertiis on killustunud erinevate asutuste vahel, mistõttu on peaaegu kõigis asutustes puudus teadmistest (knowledge)ehk inimeste puudusest tulenevalt pole võimalik kõigi uute tehnoloogiate ja kübervaldkonna trendidega kaasas käia, mistõttu sõltuvad ametlikud osapooled väga suuresti mõttekodade, ülikoolide ning era sektori teadmistest.

Ilma era- ja avaliku sektori koostööta ei oleks võimalik kaardistada küberruumi ohupilti ega tehnoloogia arenguga. Probleemi lahendamises põhiroll on MKMil, kuna MKM juhib Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu ning koostab ja jälgib küberturvalisuse strateegia rakendamist. Lisaks saab MKM otseinfot RIAlt küberruumi hetkesisu kohta ning saab antud informatsiooni jagades koordineerida teiste ministeeriumite tegevusi. Kuid vaatamata sellele, et ametiasutused konsulteerivad suures osas paljudes küsimustes ka erasektoriga puudub regulaarne formaalne formaat kus mõttekodade ja IT-ettevõtetega. MKMil on siinkohal võimalus luua formaat, kus kõik asutused saaksid jagada teadmisi erinevate küberohtude ja trendide kohta ning tõstatada mõlema poolseid murekohti.

Osapooled	Roll	Arusaam / Vaade	Teadmus	Ressursid
Majandus- ja Kommunikatsiooni- ministeerium	Valdkonna eest vastutav ministeerium	Vajalik luua tervikpilt, koordineerida kõigi osapoolte tegevust, vältida dubleerimist. Vajadus küberekspertide järgi ning luua parem ühendus erasektori ettevõtetega	Arusaam ja ülevaade õigusaktidest ja regulatsioonidest	Kompetents, Legitiimsus, Teadmine
Riigi Infosüsteemi Amet	Arendab ja haldab digiriigi keskseid tehnoloogilisi platvorme ning tagab riigi küberturvalisuse	Vajalik suurendada küberekspertide arvu	Tehniline ekspertiis	Kompetents, Legitiimsus, Teadmine
Haridus- ja Teadusministeerium	Haridus ja õppprogrammide loomine, IT	Vajadus suurendada IT - tudengite arvu	Teadlikkuse tõstmise meetodid	Kompetents, Teadmine

	spetsialistide harimine			
Justiitsministeerium	Toob teadmisi kübervaldkonna kriminaalmenetluse, õigus- ja kriminaalpoliitika planeerimise osas	Vajadus küberi alase ekspertiisi järgi	Õigusalane pädevus ja tervikvaade regulatsioonidest	Legitiimsus, Kompetents, Teadmine
Kaitseministeerium	Sõjalise taristu kaitse	Vaja suurendada sõjalise taristu kaitset	Riigikaitseline vaade	Legitiimsus Kompetents Teadmine
Siseministeerium	Küberkuritegude ennetamise, tõkestamise ja avastamise, menetlemise ja küberjulgeolekut ohustavate süütegude ennetamise ja tõkestamise	Vajadus koolitada PPA ametnikke küberi alal	Ekspertiis küberkuritegevuse osas	Legitiimsus Kompetents Teadmine
Välisministeerium	Suunab ja koordineerib strateegia rahvusvahelise koostöö tegevusi	Vajadus Eesti efektiivseks esindamiseks koolitada küberdiplomaate	Ekspertiis rahvusvaheliste protsesside ja trendide osas	Legitiimsus Kompetents Teadmine
Rahandus-ministeerium	Jätkusuutlikkuse tagamine läbi eelarveliste vahendite	Vajalik iga-aastaselt panustada küberkaitse valdkonda	Ekspertiis eelarvepoliitika osas	Kompetents, Teadmine, Legitiimsus, Finants
Riigikantselei	Tagab küberturvalisuse integreerimise	Tervikpilt	Strateegiline ekspertiis	Legitiimsus, Kompetents

	riigikaitse planeerimisdokumentidesse			
Mõttekojad	Praktilised teadmised	Vajalik panustada akadeemiliste teadmistega.	Akadeemiline teadmine küberturvalisusele	Teadmine, Kompetents
IT ettevõtted	Praktilised teadmised	Vajalik reklaamida oma tooteid ja pakkuda teenust	Konkreetne tehniline informatsioon.	Teadmine, Kompetents

VÕRGUSTIKU JUHTIMINE:

Nagu eespool mainitud on peamiseks poliitikakujundajaks ja valdkonna eestvedajaks küberturvalisuse teemal MKM, kes juhib ja koordineerib küberjulgeoleku strateegia väljatöötamist ja rakendamist, ühtlasi juhib küberjulgeoleku nõukogu tegevust Vabariigi Valitsuse julgeolekukomisjoni raames ning tagab strateegilisel tasemel koordinatsiooni ning küberturvalisuse eesmärkide saavutamise erinevate planeerimisdokumentide, programmide ja tööplaanidega (Majandus- ja kommunikatsiooniministeerium 2019, lk 17).

Küberturvalisuse strateegia juhtimise aluseks on hierarhia, turu ja võrgustiku mehhanismide kombinatsioon (Peters, 2003, lk 21), mis hõlmab eesmärkide seadmist ja reeglite kehtestamist, era ja avalikusektori koostöö tagamist tehnoloogiate ja it-arendusteks, teadlikkuse ja kompetentsi tõstmise stiimulite loomist, ning ühiste teadmiste ja strateegiate arendamist turvalisuse tagamiseks (Majandus- ja kommunikatsiooniministeerium 2019, lk 14).

Võrgustikupõhist juhtimist iseloomustab erinevate sektorite nagu avaliku, akadeemilise, mõttekodade ja erasektori kaasamist, eesmärgiga saada erinevate tasandite ja pädevuse teadmus millega arvestada ja leppida kokku eesmärgid ja tegevuskava ning toob välja iga osapoole rolli ja vastutuse. Küberturvalisuse strateegias on välja toodud: “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.“ (Majandus- ja kommunikatsiooniministeerium 2019, lk 14). Vertikaalsed instrumendid ilmnevad selgelt hierarhiliste struktuuride ja kontrollimehhanismide kaudu, samas kui horisontaalsed instrumendid ilmnevad koostöö ja kooskõlastamise kaudu erinevate organisatsioonide ja sektorite vahel. Eesti on küberturvalisuse valdkonnas maailma esi viisikus (Postimees, 2023) millest saab järeldada, et olemasolevad juhtimis ja koordineerimis meetodid on olnud seni tõhusad. Hea juhtimise ja koordineerimise tunnuseks peavad autorid ka seda, et strateegia väljatöötamise raames on välja toodud erinevate valdkondade ja tasemete riskid, mis võivad ohustada täna toimivat ja tõhusat küberturvalisuse valdkonda. Väljakutsed on seotud nii inimressursside, organisatsioonilise juhtimise, teadlikkuse kui ka koostööga era- ja avaliku sektori vahel. Selleks, et tugevdada küberturvalisuse võrgustikku ja kasutada ära kogu olemasolevat potentsiaali, on hädavajalik kaasata laiem ring osapooli, eriti neid, kes omavad vajalikke teadmisi ja ressursse, kuid pole veel otseselt kaasatud. Eestis, nagu ka mujal maailmas, seisab küberturvalisuse valdkond silmitsi kiiresti arenevate ohtudega, mis nõuavad kiiret reageerimist ja head koostööd kõikide osapoolte vahel. Selleks, et tõhusalt vastu seista nendele väljakutsetele, on hädavajalik suurendada koostööd erasektori ja avaliku sektori vahel. Oluline on tõsta teadlikkust küberturvalisuse ohtudest, et inimesed ja organisatsioonid mõistaksid potentsiaalseid riske ja oskaksid neid ennetada. Selle saavutamiseks tuleb kokku leppida selged reeglid ja luua ühtne raamistik IT tehnoloogiate ja platvormide kasutamiseks, mis aitaks tagada küberhügieeni ja süsteemide vastupanuvõimet ohtudele. See hõlmab standardite kehtestamist andmekaitseks, küberhügieeni parimate praktikate jagamist ja turvalisuse auditeid, mis aitavad tuvastada ja kõrvaldada nõrkusi meie digitaalses infrastruktuuris. Samuti on oluline tõsta ühiskonna teadlikkust läbi sihipäraste kampaaniate, hariduslike seminaride ja lihtsasti mõistetavate infoampsude, mis selgitavad küberohtude olemust ja õpetavad, kuidas igaüks saab end kaitsta. See hõlmab küberturvalisuse alaseid koolitusi koolides, töökohal toimuvaid koolitusi ning kampaaniaid, mis suunavad tähelepanu paroolide turvalisusele, tarkvara uuendamise tähtsusele ning petuskeemide äratundmisele.

Sisulise komplekssuse vähendamisel on oluline kaasatud osapoolte mõistmine ja erinevate tasandite nagu avaliku, akadeemilise, mõttekodade ja erasektori sisendi väärtustamine ja arvestamine. Nii tegevuskavade, riskide hindamisel ja maandamismeetodite väljatöötamisel on oluline roll osapoolte omavahelisel usaldusel ja erinevate vaadete lõimumisel (Klijn, et al, 2016, lk 64). See toob kaasa suurema edu seatud eesmärkide ellurakendamisel kuna takistused ja tõrked

on välja toodud ja nendega on arvestatud. MKM, olles valdkonna eestvedaja peaks eriarvamuste ja vastuolude lahendamise protsessis kindlustama usalduse ja koostöö hoidmise ning vajadusel esitama võimalikke alternatiivseid lähenemisi või selgitama piiranguid, miks eriarvamusi ei pruugita arvesse võtta.

Strateegilise komplekssuse vähendamine eeldab kokkulepitud eesmärkida saavutamiseks kindlate tegevuste, rollide, vastutuse ja ressursi plaani. Strateegiad ja tegevuskavad ei rakendu kui nende täitmiseks ei ole tagatud ressursse või ei ole lepitud kokku milliste vahenditega tegevusi ellu viiakse. Rolliselgus, ressursiplaan ja tegevuste elluviimine aga on edukas kui on tehtud sisulist koostööd, arvestades erinevate osapoolte hinnangu, ressursivajaduse ja muude vajadustega mis tagavad eesmärkide täitmise olles samal ajal teadlik oportunistlikust käitumisest. See nõuab sisulist lähenemist, kus lähtepunktiks ei ole valdkondliku eestvedaja kinnisidee, vaid pigem toimub pidev kohanemine ja paindlikkus (Klijn, et al 2016, lk 97). Suurendamaks era-ja avalikusektori koostööd IT- tehnoloogia ja julgeoleku valdkonnas tagamaks tehnoloogilise taristu jätkusuutlikuse kui ka teadlikkuse tõstmise programmi on vaja tänasest paindlikumat ja koostööd soodustava halduspraktikat ja õiguslik ruum ja koostöö kokkuleppeid.

Institutsionaalset keerukust loob mitmetasandiline valitsemine, kus erinevate tasandite osalejad tegutsevad kohalikul, regionaalsel, riiklikul või rahvusvahelisel tasandil. Küberturvalisuse strateegias on välja toodud mh: „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.“ (Majandus- ja kommunikatsiooniministeerium 2019, lk 14) Küberturvalisuse tegevusprogrammis on ühe tegevusena toodud välja riigiülese küberturvalisuse keskuse loomine kuid selle loomine ei lahenda tänast IT taristu tehnilise mahajäämuse ja kompetentsi puudumise probleemi mis on üheks väljatoodud küberturvalisuse riskiks. Institutsionaalse komplekssuse vaates tegevusprogrammis toodud küberturvalisuse keskuse loomine, tänaste IT keskuste tsentraliseerimise näol vähendab juhtimis ja koordineerimiskeerukust, kuid see võib lõhkuda loodud usaldust kui selle eesmärgid ei ole piisavalt põhjendatud ja argumenteeritud ning ei ole näidatud selget kasu lõppeesmärgi saavutamiseks.

MKMil on täna kõige suurem puudus infost ehk millist pädevust, teadmust ja andmeid IT asutused omavad. Läbi teadlikkuse tõstmise saame luua aluse laiapõhjaliseks kaasamiseks. Kaasates IT ettevõtted ja erinevad teadusasutused, kellel on asjakohane tehnoloogiline pädevus ja võimekus, saaksid panustada riikliku küberturvaisuse tagamisse. Viies läbi seminare, töötubasid ja konverentse saab MKM selgitada ohte ja näidata, kuidas iga organisatsiooni tegevus aitab kaasa ühisele küberturvalisusele. Sørensen ja Trofing on toonud oma raamatus välja: „Soodsate tingimuste loomine tulevaseks koostööks kognitiivse, strateegilise ja institutsionaalse õppimise kaudu, mis konstrueerivad ühiseid raamistikke, ergutavad sõltuvuse arengut ja loovad vastastikuse usalduse.“ (Sørensen, Torfing 2009). Ühisprojektid ja ühised uurimis- ja arendustegevused, võivad viia uute turvatehnoloogiate väljatöötamiseni, mis aitaksid tõsta riikliku küberturvalisuse taset. Suuremal määral erasektori kaasamine avaliku sektori eesmärkide täitmisesse eeldab kindlate reeglite ja koostööeesmärkide kokkuleppimist. Et tagada võrgustikus välja töötatud lahenduste legitiimsus, tuleb võtta arvesse mitmeid tegureid, sealhulgas osapoolte kaasamist, läbipaistvust, arutelu ja demokraatlikke põhimõtteid. Ainult siis, kui need tegurid on tasakaalus, saab võrgustiku lahendusi pidada tõeliselt legitiimseteks (Klijn, et al 2016, lk 300).

Hea valitsemine ja efektiivne koordineerimine eeldab tugevat juhtimist, diplomaatilisi oskusi ja võimet osapooli kokku tuua, samuti uute korralduste ja reguleerimiste sisseviimist, mis kaitsevad avalikke huvisid ja leevendavad negatiivseid mõjusid (Klijn, et al 2016, pt 4). MKM küberjulgeoleku valdkonna eestvedajana on kaasanud strateegia ja tegevusprogrammi elluviimiseks erineval tasemel eelpoolnimetatud osapooli. Hinnatud on riske ja ohte ja välja on töötatud tegevuskava nende elluviimiseks. Ettepanekud on tehtud suuremaks riigireformiks, kus erinevate riigiasutuste IT keskused tsenraliseeritakse üheks keskseks IT keskuseks vähendamaks juhtimiskeerukust, ühtlustamaks reegleid, standardeid, tehnoloogilist võimekust ja taristut.

POLIITIKASOOVITUSED:

Vaatamata killustatud kübermaastikule on Eestis küberturvalisus võrdlemisi hästi koordineeritud ja juhitud. Kuigi MKMil puudub tervikjuhtimine ja asutuste üleseks ametlikuks koordineerimiseks on ainult üks formaat, toimib asutuste vaheline koostöö väga heal tasemel. See tuleneb eelkõige küberkogukonna väiksusest ja isiklikest suhetest erinevate asutuste ametnike vahel. Kaardistatud on kõik riigisektori osapooled ning mainitud on ka erinevad kompetentsikeskused ning kõigil neil on oma kindel roll ja nägemus, mis suures pildis ühtib strateegia suunaga. Murekohaks on aga

täpne olukorra kaardistus ja ebaühtlane küberkaitsevõime erinevate asutuste vahel. Lisaks on veel probleemiks järelkasvu puudus, mis tekitab muret olukorras koos digi ja küberruum on eksponentsiaalselt paisumas. Haridus ja Teadusministeerium võiks siinkohal võtta suurema rolli. Et aga paremini tegeleda pidavalt muutuva kübermaastikuga tuleks rohkem tähelepanu pöörata võrgustiku juhtimise lähenemisele ning sealjuures luua platvormid, mis võimaldavad läbi kõiki sidusrühmi kaasava lähenemise võimaldada riigil omandada laiem pilt nii küberohtudest kui ka uutest tehnoloogiatest, mida oleks võimalik küberkaitse eesmärkidel ära kasutada.

Töös käsitletud probleemi leevandamiseks on pakutud järgmised poliitikasoovitused:

1. **Kaardistada riigiasutuste IT keskuste küberturvalisuse võimekus ja viia läbi IT keskuste konsolideerimise mõjuanalüüs.** Peamiseks eesmärgiks oleks kaardistada asutuste küberturvalisuse võimekus eesmärgiga luua tervikpilt asutuste digisüsteemidest ja küberkaitsevõimekustest, et vähendada ametkondade vahelist killustatust ja vältida ressursside dubleerimist. Tulemusena valmib mõjuanalüüs IT keskuste konsolideerimise osas.

2. **Luua lisaks Küberjulgeolekunõukogule platvorm avaliku- ja erasektori vaheliste partnerluste tugevdamiseks.** Platvorm annaks aluse avaliku- ja erasektori vahelise koostöö edendamiseks, kontaktide ja võrgustike loomiseks ning erinevate teadmiste, ressursside ja oskuste ühendamiseks ning ühisprojektide läbiviimiseks. Läbi antud platvormi oleks võimalik korraldada regulaarsedi koolitusi, seminare ja töötubasid, kus avaliku- ja era sektori esindajad saavad arutatleda konkreetsete kübervaldkonna probleemide ja lahenduste üle. Seejuures aitaks platvorm luua riigi ja erasektori seas küberprojektide suhtes omanikutunnet ja süvendada isiklikku vastutust.

3. **Luua vastastikused kohustused ja stiimulid, mis motiveerivad ettevõtteid kaasa aitama küberturvalisuse tugevdamisele**. Näiteks võiks MKM pakkuda erinevaid maksusoodustusi või muid hüvesid nagu valitsuse toetused ja/või subsiidiumid ning madala intressimääraga laenude pakkumine neile ettevõtetele, kes investeerivad küberturvalisusesse või vastavad teatud turvastandarditele, nagu E-ITS.

4. **Võimestada koostööprojektide läbiviimist kaasates kriisiõppustesse erasektor**, et paremini mõista riikliku küberturvalisuse süsteemi toimimist ning osaleda tõhusalt selle

kaitsmisel ja tugevdamisel. Erasektori kriisiõppustel aitaks luua sünergiaid avaliku sektoriga ning aitavad kaaasa tõhusamale teabe jagamisele ja koordineerimisele.

5. **Julgustata kandideerimist IT alasele õppele läbi erinevate riigi poolsete stipendiumite pakkumise.** Stipendiumid IT alasel õppel julgustavad õpilasi kandideerima IT suunitlusega õppeprogrammidele. Sealjuures suurendada koostöös Haridus- ja Teadusministeeriumiga IT alaste õppeprogrammide õppekohti, mis süsteemselt arvestaks Eesti tööturu vajadustega.

KASUTATUD KIRJANDUS:

e-Estonia. (2023). Facts and Figures. Kasutatud 06. november 2023 https://e-estonia.com/facts-and-figures/

Euroopa Komisjon. (2022). Digitaalmajanduse ja -ühiskonna indeks (DESI) 2022. Kasutatud 06. november 2023 https://digital-strategy.ec.europa.eu/en/policies/desi

Invest in Estonia. (2017). How Estonia became a global heavyweight in cyber security. Kasutatud 07. november 2023 https://investinestonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

Klijn, E. H., and J. Koppenjan. 2016. Governance Networks in the Public Sector. Abingdon: Routledge. Kasutatud 07. november 2023 https://ebookcentral.proquest.com/lib/tuee/detail.action?docID=4054052

Majandus- ja Kommunikatsiooniministeerium. (2019). Küberturvalisuse stragteegia 2019-2022. Kasutatud 07. november 2023 https://www.mkm.ee/media/700/download

Peters, B. G. 2003. "The Capacity to Coordinate" Paper presented at the Workshop on Policy Capacity, Hongkong, October 3

Postimees. (2023), Uuring: Eesti küberturvalisus on maailma tipus. Kättesaadav 07. november 2023 https://tehnika.postimees.ee/7718942/uuring-eesti-kuberturvalisus-on-maailma-tipus

Riigi Infosüsteemi Amet. (2023). Küberturvalisuse aastaraamat. Kasutatud 06. november 2023 https://www.ria.ee/media/2653/download

Riigi Infosüsteemi Amet. (2023). Ameti ülesanded ja struktuur. Kasutatud 07. november 2023 https://www.ria.ee/amet-uudised-ja-kontakt/amet-ja-juhtkond/ameti-ulesanded-ja-struktuur

Riigi Infosüsteemi Amet. (2023). Olukord küberruumis september 2023. Kasutatud 06.

november 2023 https://www.ria.ee/media/3213/download

R, Liive. (2021). Kaimar Karu sõnul võivad taakvara ja tehnoloogiline võlg e-riigi põhja viia. Kasutatud 07. november 2023 https://digipro.geenius.ee/eksklusiiv/kaimar-karu-sonul-voivad-taakvara-ja-tehnoloogiline-volg-e-riigi-pohja-viia/

Sørensen, E. and J. Torfing. 2009. "Making Governance Networks Effective and Democratic through Metagovernance." Public Administration, 87(2): 234-258