TALLINNA TEHNIKAÜLIKOOL
Majandusteaduskond
Ragnar Nurkse innovatsiooni ja valitsemise instituut

Toomas Vaks

KÜBERJULGEOLEKU STRATEEGIA MÕJU KÜBERTURVALISUSE ARENGULE EESTIS 2008-2018

Magistritöö
Õppekava HAHM, peaeriala haldusjuhtimine

Juhendaja:
Maarja Toots, MA

Tallinn 2018

Deklareerin, et olen koostanud töö iseseisvalt ja olen viidanud kõikidele töö koostamisel kasutatud teiste autorite töödele, olulistele seisukohtadele ja andmetele, ning ei ole esitanud sama tööd varasemalt ainepunktide saamiseks.
Töö pikkuseks on 13 046 sõna sissejuhatusest kuni kokkuvõtte lõpuni.

Toomas Vaks .....

(allkiri, kuupäev)

Üliõpilase kood: 107304 HAHM
Üliõpilase e-posti aadress: toomas.vaks@icloud.com

Juhendaja: Maarja Toots, MA:

Töö vastab kehtivatele nõuetele

.....

(allkiri, kuupäev)

Kaitsmiskomisjoni esimees: Erkki Karo, PhD

Lubatud kaitsmisele

.....

(nimi, allkiri, kuupäev)

Tänan kõiki oma suurepäraseid kolleege, kelleta poleks Eesti küberjulgeolekut.

Eraldi tänu kuulub Liis Rebasele, Piret Pernikule ja Lauri Luhtile, kelleta poleks seda tööd saanud kirjutada.

SISUKORD

LÜHIKOKKUVÕTE

Käesolevas töös uuritakse avaliku halduse strateegilise planeerimise probleeme riiklike küberjulgeolekustrateegiate koostamisel ja rakendamisel ning hinnanguid selle mõjule küberjulgeoleku olukorrale, jälgides Eesti arengut selles valdkonnas 10 aasta jooksul.

Peamiseks eesmärgiks on uurida Eesti küberjulgeoleku strateegiate koostamise näitel küberjulgeoleku strateegilise planeerimise probleeme avaliku halduse strateegilise planeerimise teoreetilise raamistiku taustal, mõistmaks selle valdkonnale omaseid probleeme ja eripärasid. Teiseks eesmärgiks on analüüsida ja hinnata Eesti küberjulgeoleku strateegiate koostamise ja rakendamise protsessi tunnetatud mõju nii Eesti küberjulgeoleku üldisele arengule kui ka seda toetavate valdkondade (teadus- ja haridusvaldkond, riigikaitse jms) arengule.

Töös jõutakse järeldusele, et küberjulgeoleku strateegiline planeerimine strateegiate koostamise kaudu aastail 2008-2018 on avaldanud olulist mõju nii Eesti küberjulgeoleku olukorrale kui ka Eesti rahvusvahelise maine ning konkurentsivõime kujunemisele. Samuti ei leitud, et küberjulgeoleku valdkonna strateegilise planeerimise probleemid erineksid oluliselt teistest avaliku halduse strateegiate loomisele ja elluviimisele omastest probleemidest. Nende lahendamiseks tuleb leida võimalused valdkonna riigiülese koordinatsiooni ja juhtimise, teiste arengukavade seostatuse ja eelarve planeerimisega seotud probleemide lahendamiseks.

Märksõnad: küberjulgeolek, küberturvalisus, küberjulgeoleku strateegia, arengukava

SISSEJUHATUS

2007. aasta aprillis toimunud nn Pronksiööle järgnenud küberrünnakud Eesti ettevõtete ja valitsusasutuste vastu pälvisid maailmas suurt tähelepanu ning järgneva 10 aasta jooksul on märksõna *cyber* saanud Eesti riigi rahvusvahelise imago lahutamatuks osaks. Küberrünnakutele järgnenud tähelepanupuhangus valdkonna vastu töötati välja Eesti esimene küberjulgeolekustrateegia 2008-2013 (edaspidi KJS 2008), mis viis Eesti tol ajal väga väheste riikide sekka, kellel selline riiklik arengukava olemas oli. 2013. aastal töötati välja strateegia uus versioon 2014-2017 (edaspidi KJS 2014) ning 2017. aastal alustati juba uue, järjekorras kolmanda strateegia väljatöötamist mis valitsuse poolt ka novembris 2018 heaks kiideti (KTS 2018).

Küberjulgeoleku valdkonnas (siin töös on küberturvalisust ja küberjulgeolekut kasutatud sünonüümidena lähtuvalt asjaolust, et mõlemad tähendavad inglise keeles *cybersecurity*) on Eestil saavutatud küllalt suur rahvusvaheline tuntus, mis on andnud võimaluse rakendada seda edukalt ka riigi rahvusvahelise maine ja tuntuse edendamisel. NATO kübervaldkonna oivakeskuse (CCDCOE) rajamine Eestisse, iga-aastased Tallinnas toimuvad kõrgetasemelised küberjulgeoleku konverentsid CyCon ning muidugi ka prominentne küberjulgeoleku valdkonna rahvusvahelise õiguse loomise protsess Tallinn Manual on kinnistanud Eesti kui eduka „küberriigi“ mainet. 2017. aastal avaldatud ÜRO Rahvusvahelise Telekommunikatsiooniliidu (ITU) globaalses indeksis pälvis Eesti Euroopas esikoha ja maailmas viienda koha (ITU 2017).

Siseriiklikud hinnangud Eesti küberjulgeolekule on aga kriitilisemad. 2017. aasta uuringu andmetel peab 67% küsitletud Eesti elanikest kõige tõenäolisemaks julgeolekuohuks küberrünnakut Eesti infosüsteemide vastu (Kivirähk 2017). Osaliselt on see seletatav Eesti ühiskonna kõrge teadlikkusega sõltuvusest infotehnoloogilistest (IT) teenustest nii era- kui avaliku sektori toimimisel, kuid eksisteerib ka võimalus, et valdkonna strateegiline planeerimine ja -juhtimine pole andnud soovitud tulemusi. Autor on pidanud olema tunnistajaks paljudele diskussioonidele nii ekspertide kokkusaamistel kui isegi sotsiaalmeedias, kus prominentsed kübervaldkonna eksperdid ja ka avalikkuse esindajad on väljendanud arvamust, et riiklike ressursside planeerimine küberjulgeoleku tagamisel pole olnud piisavalt efektiivne, mistõttu on teenuste turvaprobleemide tõttu ohtu sattunud ka Eesti e-riigi usaldusväärsus ja hea kuvand.

Tallinna Tehnikaülikooli (TTÜ) uurijate rühm tõdes oma kokkuvõttes 2017. aasta nn ID kaardi kriisi kohta: „Süstemaatiline, sihipärane ning identiteedihalduse aspekte terviklikult käsitlev strateegia peaks kaasama kõiki seotud ministeeriume ning asutusi" (TTÜ... 2018). Tõdemus strateegia puudumisest on osa laiemast probleemist- kuigi ID kaart (e-identiteet) liigitatakse tinglikult e-riigi toimimiseks vajaliku nn baastaristu alla (MKM... 2014), pole e-riigi toimimiseks vajaliku baastaristu turvalisuse aspekte strateegiates käsitletud. Võiks eeldada, et valdkondliku, mitmeid ministeeriume ja asutusi kaasava strateegiaprotsessi käigus tekib plaan ka ühe Eesti e-riigi olulisema nurgakivi, elektroonilise identiteedihalduse turvalisuse tagamiseks, kuid see eeldus osutus valeks. Turvalise identiteedihalduse küsimusi on mingil kujul käsitletud kõigi küberjulgeolekustrateegiate koostamise käigus, kuid dokumentidesse on see jõudnud vaid väga üldsõnaliselt (KJS 2008;KJS 2014). Kuigi Majandus- ja Kommunikatsiooniministeeriumi (MKM) poolt koostatavas Infoühiskonna Arengukavas (MKM...2014) käsitletakse baastaristu arendamist ja haldamist, pole turvalisusprobleeme eraldi adresseeritud. Seega on arusaadav, et valdkonna arendamisel ja strateegia rakendamisel osalevatel ekspertidel võib tekkida küsimusi nii kõrge abstraktsusastmega dokumentide vajalikkusest.

Nii Eestis kui ka rahvusvaheliselt on kahtluse alla seatud ka riikide *versus* erasektori tegelik mõju küberjulgeoleku tagamisel. Riikide traditsioonilise võimumonopoli kehtivus küberkeskkonnas on olnud diskussiooniteemaks juba alates interneti laiema leviku algusest 1990. aastate keskel. Üldisemaid küsimärke küberjulgeoleku valdkonna riikliku strateegilise planeerimise kasulikkuse kohta ilmestavad ka valdkonna ekspertide arvamused, mille kohaselt on riikide võimekus tehnoloogia valdkonnas toimuvaid arenguid ja ohte ette näha pigem vähene ning seega pole mõtet loota, et strateegiline planeerimine aitaks olukorda sisuliselt oluliselt parandada, kuna vastav taristu ja selle arendamine on täielikult erasektori kontrolli all. Küberturvalisuse ekspert Kaur Virunurm näeb riikide võimekust mustades värvides: „Maailm on väheste suurfirmade käes pantvangis. Igas IT valdkonnas – kiibid, operatsioonisüsteemid, telefonid, teenused – domineerib paar-kolm suuremat tootjat, kel on oma tehnoloogilises kihis pea täielik ülemvõim, ning see monopol on globaalne, st sama elektroonikat ja tarkvara kasutavad nii USA, Venemaa kui Eesti. Ka kodanike ja kasutajate andmed on suurte ühisteenuste (Google, Facebook) käes koos. Sisuliselt on tekkinud monokultuur. Apple ja Microsoft, AMD ja Intel, Google ja Amazon on monopolid, kellest sõltub kogu maailma töö." (RIA...2018)

Arenenud ühiskondade sõltuvus IT- st, majanduse üldine digitaliseerumine, globaliseerumine ning robootika areng on näited avaliku halduse ees seisvatest väljakutsetest, mis kõik nõuavad tähelepanu ka julgeoleku seisukohast. Küberjulgeoleku roll tuleviku ühiskonnas ilmselt suurem kui me täna arvame - info globaalne piirideta ja viivituseta liikumine mõjutab selgelt ühiskonna arengut tervikuna. Püüd selle valdkonna tegevusi ja arengut strateegiliselt planeerida on seega mõistetav ja vajalik, kuna selle tulemuslikkusest sõltub ka paljude teiste valdkondade areng: küberjulgeoleku riskid omavad täna tähtsust meditsiiniteenuste osutamisest kuni demokraatlike valimiste korraldamiseni.

Antud uurimistööl on kaks eesmärki. Esmaseks eesmärgiks on uurida Eesti küberjulgeoleku strateegiate koostamise näitel küberjulgeoleku strateegilise planeerimise probleeme avaliku halduse strateegilise planeerimise teoreetilises raamistikus, et kaardistada valdkonnale omased probleemid ja eripärad. Teiseks eesmärgiks on analüüsida ja hinnata Eesti küberjulgeoleku strateegiate koostamise ja rakendamise protsessi tajutavat mõju nii Eesti küberjulgeoleku üldisele arengule kui ka seda toetavate valdkondade arengule. Antud töös on vaatluse all küberjulgeolekustrateegiate mõju majandusele, teadus- ja haridusvaldkonnale, riigikaitse valdkonnale ja rahvusvahelistele suhetele.

1. TEOREETILINE RAAMISTIK

1.1 Strateegia mõiste

Mõiste pärineb sõjandusest, kreekakeelsest sõnast στρατηγία (*stratēgia*), mille algupärane tähendus oli "väejuhi oskus". Sõjalises tõlgenduses õpetab strateegia, kuidas pidada sõda või kuidas relvajõudusid kasutades saavutada poliitilisi eesmärke (Osinga 2006,22).

Strateegiat on määratletud mitmel viisil, kuid enamasti peetakse selle all silmas teadlikke valikuid ja nendest kujunevat tegevusmustrit, mis määrab tulevikus tehtavaid otsuseid (Mintzberg 1978a, 1994b) ning tegevuskava eesmärgi saavutamiseks koos mõõdikute süsteemiga selle saavutamiseks (Osinga 2006). Strateegiat avalikus sektoris saab kirjeldada ka kui eesmärkide, poliitikate, programmide, tegevuste, otsuste või ressursside struktuuri, mis aitab tegeleda oluliste põhiteemadega ning mis peab ühtima organisatsiooni üldise filosoofia ja põhiväärtustega (Bryson 2004). Avaliku sektoris strateegiat on defineeritud ka kui „avalike ressursside ja võimu süstemaatilist kasutamist avaliku sektori asutuste poolt avalikes huvides - avalike eesmärkide täitmiseks" (Mulgan 2009) .

Ärivaldkonnas on üheks populaarsemaks strateegia käsitluseks näha seda kui organisatsiooni positsioneerimist konkurentsieelise saavutamiseks. See peab sisaldama valikuid, millistes tööstusharudes osaleda, milliseid tooteid ja teenuseid pakkuda ja kuidas paigutada organisatsiooni ressursid. Üldistatult võib organisatsiooni strateegiat pidada kõikehõlmavaks pikaajaliseks tegevusplaaniks organisatsiooni eesmärkide saavutamiseks (Alas 2005).

Strateegia peamise eesmärgina nähakse osanikele ja teistele (soodustatud) isikutele tulu tekitamist kliendile väärtuse loomise kaudu (de Kluyver, Pearce 2010). Seega ei ole ärivaldkonna ja sõjanduse vaated strateegiale tegelikult sugugi erinevad vaid baseeruvad vastase (konkurendi) suhtes eelise loomiseks loodavate vahendite leidmisel ja tegevuste kirjeldamisel.

Antud töös pole selgelt eristatud ühe avaliku organisatsiooni ja mitmete organisatsioonide (valdkondlike) strateegiate loomist ning strateegilist planeerimist, kuna vastavad protsessid on sisuliselt sarnased, erinedes peamiselt vaid planeerimisprotsessi kaasatavate isikute hulga osas. Avaliku sektori valdkondlikud strateegiad kinnitatakse tavaliselt protsessiga haaratud

organisatsioonide üle võimu omava organi, näiteks valitsuskabineti või parlamendi poolt. Seega on organisatsiooni mõiste teoreetilises osas laiem kui üks organisatsioon, hõlmates tinglikult ka mingi valdkonna tegevuse planeerimist, milles osalevad mitmed avaliku sektori organisatsioonid, ning käsitledes organisatsiooni mõistes avalikku haldust tervikuna.

Strateegiale omistatakse tavaliselt järgmisi omadusi (Coker 2004):

- Strateegia puudutab nii organisatsiooni kui ka seda ümbritsevat keskkonda- organisatsioon kasutab strateegiat muutuva keskkonnaga toimetulemiseks;
- Strateegia mõjutab kogu organisatsiooni käekäiku - strateegilisi otsuseid peetakse piisavalt tähtsateks, et nad mõjutaksid organisatsiooni üleüldist heaolu;
- Strateegia hõlmab nii sisu kui ka protsessi- õpetus strateegiast sisaldab nii elluviidavate tegevuste kirjeldust ehk strateegia sisu kui ka protsesside kirjeldust, mille käigus tegevused otsustatakse ja ellu viiakse;
- Strateegiad erinevad eri tasanditel - ettevõtetel on nii korporatiivne strateegia (*millist äri me ajame*) kui ka äristrateegia (*kuidas me võistleme selles äris*)
- Strateegia hõlmab erinevaid mõtteprotsesse, see hõlmab nii kontseptuaalseid kui ka analüütilisi harjutusi.

Kokkuvõttes võib strateegiat defineeridagi kui pikaajaliste eesmärkide saavutamiseks vajalike tegevuste ja tegevuspõhimõtete kogumit, mis loob kontseptsiooni organisatsiooni(de) arengu ja tegevuse juhtimiseks ning edu tagamiseks.

1.2 Strateegiline planeerimine ja strateegiline juhtimine

Strateegia koostamist võib üldistatult pidada strateegilise planeerimise osaks ja põhiinstrumendiks, mis loob ka aluse strateegilise juhtimise kasutamiseks. Organisatsioonide tegevuse planeerimise vajadus lähtub peamiselt vajadusest tegevusi koordineerida, valmistuda tulevikus toimuvateks sündmusteks, olla ratsionaalne ja säilitada kontrolli (Mintzberg 1994). Strateegilist planeerimist on defineeritud kui strateegilise juhtimise olulist, kuid samal ajal mitte möödapääsmatut elementi, mis sisaldab ressursside juhtimist, rakendamist ja selle kontrollimist ning hindamist (Poister,Streib 1999,310).

Tegevuse planeerimist saab lugeda strateegiliseks juhul kui osalistel on selge arusaam sellest, mis korrastamist vajab, ja tahe seda teha - olles seejuures eesmärkide, poliitikate, strateegia ja

protsesside osas vajalikul määral paindlik. Viimane on oluline selleks, et jätta ruumi olukorra keerukusega arvestamiseks, kasutada ära protsessi kestel ilmnevaid võimalusi, suurendada vastupanuvõimet ja olla jätkusuutlik ka tuleviku muutuvates oludes (Bryson *et al* 2018,321).

Avaliku sektori strateegilist planeerimist on kokkuvõtlikult defineeritud ka kui nõustavat, korrastatud lähenemist oluliste otsuste ja tegevuste elluviimiseks, mis kujundavad ja mõtestavad organisatsiooni, tema tegevust ja tegevuse põhjuseid (Bryson 2011,7). Strateegiline juhtimine peab lähtuma ka huvist strateegia efektiivse rakendamise vastu, julgustades pidevat strateegiakeskset õppimist, mõtlemist ja tegutsemist. (Poister 2010,247-249). Strateegiline juhtimine peab seega olema pidev, tulevikku suunatud protsess, strateegia muutmine peab toimuma tervikliku protsessi käigus.

Strateegilise juhtimise defineerimisel tuuakse olulise aspektina välja ka selle tulevikku suunatust: „(*Strateegiline planeerimine kui...*) Suure pildi lähenemine, kus segatakse futuristlik mõtlemine, objektiivne analüüs ja subjektiivsed hinnangud väärtustele, eesmärkidele ja prioriteetidele, kaardistamaks tulevikusihid ja tegevussuunad tagamaks organisatsiooni elujõulisus, efektiivsus ja võimekus toota väärtust“ (Poister 2010).

Küberjulgeoleku valdkonna ning ka IT valdkonna strateegilise planeerimise üheks suuremaks väljakutseks on paarist aastast pikema tulevikuperspektiivi nägemine. Probleemiks pole niivõrd tehnoloogia kiire areng ise, kuivõrd selle mõju ja suundade hindamine. Siiski pole tegemist võimatu ülesandega, tähtis on vaid tagada võimalike stsenaariumite arutelu strateegia koostamise ajal ning kõigi võimalike mõjude analüüs. Liigne paindlikkuse taotlus kätkeb aga ka ohtu, et põhimõtete „paindlik“ muutmine sarnaneb pigem igapäevase juhtimisega, mitte strateegilise juhtimisega (Mintzberg 1994).

Ühe olulise aspektina ongi vajalik eristada strateegiat, strateegilist planeerimist ja - juhtimist igapäevasest (taktikalisest) planeerimisest ja juhtimisest. Kui viimane on üldreeglina keskendunud asjade tegemisele paremini või efektiivsemalt (väiksemate kuludega), siis strateegia peab näitama, kuidas teha asju teist moodi (de Kluyver, Pearce 2010). Seetõttu peaks strateegilise planeerimise tagajärjel tekkima ka tavapärasest selgelt eristuvad eesmärgid ja vahendid.

Viimase 25 aasta jooksul on strateegiate koostamine saanud avalikus sektoris tavapäraseks praktikaks, kuid samas on korduvalt kahtluse alla seatud nende koostamine ilma strateegilise

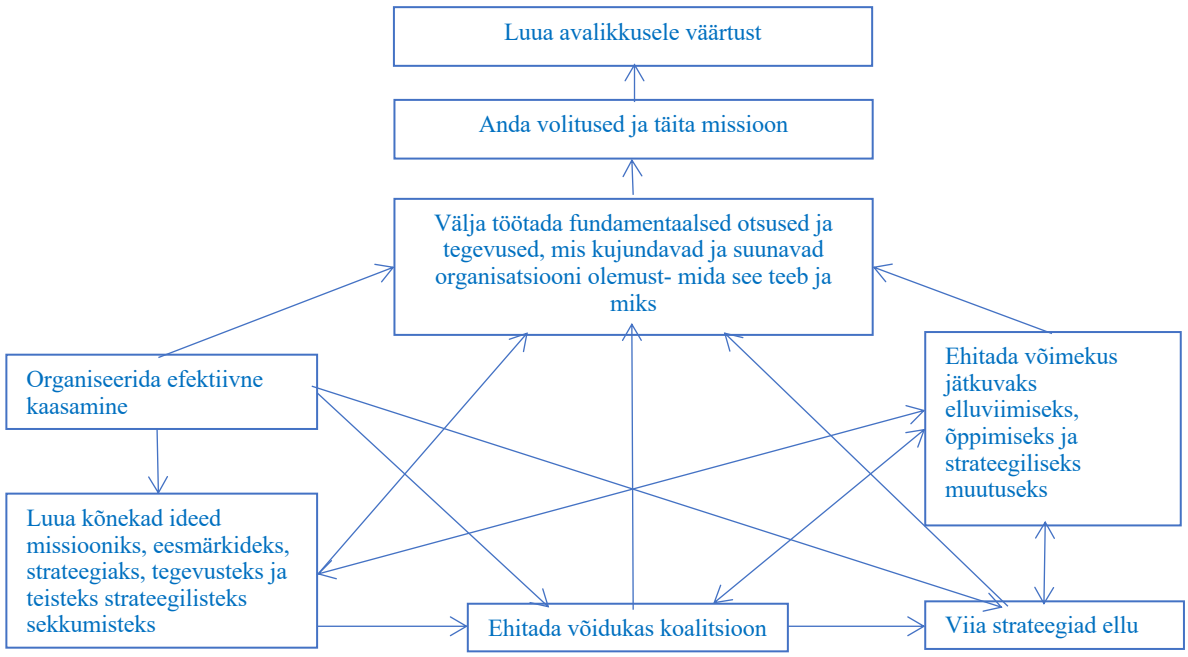
juhtimise põhimõtete kasutamiseta (Poister 2010). Ühe ohuna avaliku sektori strateegilise planeerimisele tuuakse välja võimalust, et planeerimist tehakse „planeerimise pärast“, mistõttu kaob võimekus midagi tegelikult ära teha (Mintzberg 1993).Samuti osutatakse, et paljud organisatsioonid küll tegelevad planeerimisega, kuid mitmed neist ei suuda efektiivseid plaane koostada või puudub seos planeerimise ja tegeliku elluviimise vahel (Kaplan *et al* 2005) . Seega on äärmiselt oluline pöörata tähelepanu ka planeerimise protsessile, viisile kuidas planeerimisprotsess toimub ja kuidas toimub plaanide elluviimine.

Vahel seostatakse riiklike strateegiaid üldsõnalisuse ja deklaratiivsusega. Sajandivahetuse paiku alanud strateegiate koostamine USA, Vene Föderatsiooni ja ka OSCE, NATO ja Euroopa Liidu poolt on tootnud hulga dokumente, mis kannavad strateegia nimetust ning ka sarnanevad strateegiatega, olles nende organisatsioonide poolt vastu võetud mingi küsimuse kohta, omades kindlat otstarvet ja olles pigem poliitiliselt kui seaduslikult siduvad. Olemuslikult on tegemist nö kavatsuste deklaratsiooniga (*statement of intent*), mille sisuks on eelkõige seisukohtade avalik väljendamine. Samas ei saa väita, et tegu poleks tegelikult strateegiatega (strateegilise planeerimise mõttes). Näiteks Bailes on asunud seisukohale, et riiklikke strateegiaid saabki jagada deklaratiivseteks ja sügavateks strateegiateks, mis kirjeldavad strateegilisi plaane (Bailes 2009). Samuti tõdeb ta, et sügava- ja deklaratiivse strateegia eristamine võib küllalt hästi kirjeldada tüüpilist väikeriigi stsenaariumit, kus enesesäilitamise sügavat vajadust saab saavutada ainult läbi poliitiliste valikute, mis on deklaratiivsed ja ei pruugi olla vahetult seotud riigi enda (rahvuslike) traditsioonidega (*ibid*).

Eeltoodust lähtuvalt võib järeldada, et teatud deklaratiivsus ja eesmärkide mõningane üldsõnalisus on strateegilisel planeerimisel väikeriikide puhul täiesti mõistetav, kuna tehtavad valikud eeldavad strateegia sidumist väliste (nt rahvusvaheliste) faktoritega, mis ei pruugi olla koheselt seostatavad praktiliste tegevuste või siseriiklike sammudega. Näiteks kuulumine rahvusvahelistesse organisatsioonidesse ja koalitsioonidesse ning nende väärtuste ja eesmärkide tsiteerimine strateegiates. Kaudselt võib deklaratiivsus olla seotud ka vajadusega tagada sõnumite kõnekus ja kiiduväärsus huvigruppide ja avalikkuse silmis, mis omab strateegia loomise protsessis olulist tähendust (Allison,Kaye 2005, Bryson 2011).

1.3 Strateegilise planeerimise protsess

Bryson on kirjeldanud strateegilise planeerimise ja juhtimise funktsioonid ja eesmärgid avalikus halduses järgneval joonisel:



Joonis 1: Strateegilise planeerimise ja juhtimise funktsioonid (Bryson 2011)

Eduka strateegilise planeerimise ja strateegia(te) koostamise oluliseks komponent on kaasamine. Esmalt on eduka strateegilise planeerimise jaoks vajalik organisatsiooni juhtide aktiivne osalus (Bryson 2011). Juhtide ja ka teiste organisatsiooni(de) töötajate teadlikkust protsessi toimumisest ja võimalust selles kaasa rääkida peetakse üldiselt vajalikuks, kuid praktikas on selle rakendamine tihti komplitseeritud, kuna suure hulga inimeste kaasamine muudab protsessi aeglasemaks ja kallimaks. Üldine soovituseks saab pidada, et inimesi tuleb kaasata siis, kui neil on infot, mida ei ole võimalik muudmoodi teada saada või kui nende kaasamine on oluline, et tagada strateegilise plaani omaksvõtt ja elluviimine (Thomas 1995, viidatud *ibid*). Oluliseks peetakse ka organisatsiooni(de) töötajate kaasatust protsessis, tagamaks, et nad tunnevad, et nende arvamus on oluline (Allison,Kaye 2005).

Üht organisatsiooni puudutava strateegia koostamisel on kaasatavate juhtide ja töötajate määratlemine üldiselt lihtsam kui mitmeid organisatsioone haaravate valdkondlike strateegiate puhul. Valdkondlike, mastaapsete arengukavade ja strateegiate koostamisel on aga kaasatavate ringi määratlemine keerukam, samuti on tihti probleeme vajalike teadmistega isikute tööaja

ning pühendumise pälvimisega. Oluline on ka võimalikult täpselt määratleda strateegia seisukohalt olulised huvigrupid. Huvigrupid (*stakeholders*) on lihtsustatult isikud, grupid ja teised organisatsioonid, kellel on mingisugune huvi valdkonna või organisatsiooni vastu. Need võivad olla nii need, kes strateegilist plaani rakendavad, need, kes selle rakendamisel on kasusaajad kui ka need, kes võivad olulisel määral kaasa aidata või takistada selle elluviimist (Allison, Kaye 2005). Enamasti ei ole aga strateegia koostamise algatamise ajal siiski täielikku ülevaadet kõigist huvigruppidest ning tuleb arvestada võimalusega, et strateegia koostamise käigus tuleb protsessi kaasata ka täiendavaid huvigruppe. Kaasatutest peaks ideaalis tekkima ühtne koalitsioon, mis aitab strateegiat rakendada ja ellu viia (Bryson 2011).

Üheks levinuimaks mudeliks avaliku ja mittetulundussektori strateegilise planeerimise vallas on selle protsessi jagamine järgnevalt toodud 10 etapiks (*ibid*):

1. Strateegiaprotsessi algatamine ja kokku leppimine
2. Volituste kindlaksmääramine õigusaktidest ja regulatsioonidest tulenevalt.
3. Missiooni ja väärtuste selgitamine
4. Välise ja sisemise keskkonna hindamine, tugevuste, nõrkuste, võimaluste ja ohtude väljaselgitamine (SWOT analüüs)
5. Eesseisvate strateegiliste väljakutsete väljaselgitamine
6. Väljakutsetega toimetulekuks vajalike strateegiate kujundamine
7. Strateegiate ja strateegilise plaani ülevaatamine ja vastuvõtmine
8. Efektiivse organisatsioonivisiooni loomine
9. Kujundada efektiivne rakendamisprotsess
10. Hinnata uuesti kasutusel strateegiaid ja strateegilise planeerimise protsessi.

Strateegilise planeerimise lahutamatu osa on arusaam hetkel valitsevast olukorrast nii organisatsioonis endas kui ka seda ümbritsevas väliskeskkonnas. Strateegiliseks planeerimiseks vajalik analüüs peaks sisaldama nii sise- kui väliskeskkonna põhjalikku analüüsi, hõlmates ka olemasolevaid strateegiad ja programme, mis tooks välja nii väliskeskkonna võimalused ja ohud kui ka organisatsiooni tugevused ning nõrkused (Bryson 2011; Allison, Kaye 2005).

Oluline etapp on ka organisatsiooni missiooni, väärtushinnangute ja visiooni sõnastamine. Missiooni saab käsitleda kui organisatsiooni olemusliku eesmärgi sõnastamist: miks teeme, mida teeme ja kellele teeme. Organisatsiooni väärtushinnanguteks on seal kehtivad tõekspidamised, põhimõtted, hoiakud või suhtumised, mis mõjuvad otseselt eesmärkidele

jõudmise viisi (kuidas tehakse?). Visiooniks peetakse tavapäraselt üldist kujutlust sellest, millisesse olukorda peaks organisatsioon (plaanist lähtudes) tulevikus jõudma. (Allison,Kaye 2005)

Strateegiliste eesmärkidena määratletakse olukord, mida soovitakse planeerimise tagajärjel tegelikult saavutada. Seda sammu on kirjeldatud ka kui prioriteetide leidmist ja kokku leppimist. Selles etapis tuleb arvesse võtta nii varasemates etappides kogutud teavet kui ka lähtuda kokkulepitud missioonist, visioonist ja väärtushinnangutest, tagamaks strateegiliste eesmärkide süsteemse kooskõla eeltooduga. Selle etapi käigus toimub tavapäraselt ka strateegia sisuline arutelu ja loomine. Antud etapp võib võtta palju aega, kuna selle tulemused kujunevad eri arusaamu omavate osapoolte diskussioonide kaudu, mille käigus tuleb leida lahendus ka tekkivatele konfliktidele. (Bryson 2011; Allison, Kaye 2005)

Peale strateegia kirjaliku versiooni valmimise järgneb tavaliselt strateegia tutvustamise ja ülevaatamise protsess, millele võib järgneda ka kokkuvõtete tegemine planeerimisprotsessist, nö protsessi seire (Bryson 2011). Riiklike strateegiate puhul on viimasteks sammudeks rakenduskava koostamine ning strateegia heakskiitmine selleks pädevust omava organi poolt.

Strateegia loomeprotsessi ja samuti ka strateegia tulemuste hindamisel on oluline hinnata ka strateegia rakendamise kulgu. Tuleb jälgida strateegia seostatust eelarve koostamisega, tulemuste mõõtmist ja tulemuste juhtimist mandaadis ettenähtu (volituste ulatuse) saavutamisel. Kokkulepitud missiooni, eesmärkide ja strateegiate elluviimise edukuse jälgimine ning saavutatu hindamine (*ibid*) on peamiseks võimaluseks hinnata ka valitud strateegiaprotsessi edukust.

1.4 Küberjulgeoleku valdkonna strateegiline planeerimine

Küberjulgeoleku strateegilise planeerimine on olnud vahetult seotud riikliku (*national*) julgeoleku strateegilise planeerimise ja strateegiate loomisega. Enamikes riikides hakati selle valdkonnaga tegelema 90ndate aastate alguses ja 2000. aastate alguses. Valdkonna teerajajaks saab lugeda USAd, kes formuleeris riikliku julgeoleku kontseptsiooni ja poliitika põhimõtted riikliku strateegiana juba 1947 aastal, kui kirjutati alla Riikliku Julgeoleku Seadus (*National Security Act*). Üldiste strateegiliste dokumentidena sisaldavad riikliku julgeoleku strateegiad tavaliselt poliitilist, sisejulgeoleku, välispoliitika, riigikaitse struktuuri ja majanduslikku

mõõdet ning kajastavad rahvusliku julgeoleku strateegia strateegilisi eesmärke, mis on kooskõlas riiklike huvide ja väärtushinnangutega. (Lindström ,Luiijf 2012,45-46)

Eelduseks, mis võimaldab näha küberjulgeolekut riikliku julgeoleku komponendina, võib pidada laiemat vaadet riigikaitse probleemidele. Võib väita, et kuni 1990. aastate alguseni olid riikliku julgeoleku strateegiad ja arengukavad eelkõige keskendunud riikide sõjalisele kaitsevõimele. Alles siis hakkas tekkima arusaam riikliku julgeoleku laiemast olemusest. OSCE kontseptsioon laiapõhjalisest julgeolekust nägi riikliku julgeoleku oluliste faktoritena ka elanikkonna kaitset ja ühiskonna turvalisust tervikuna, mis oli erinev seni kehtinud arusaamast näha riikliku julgeoleku peamiste probleemidena territoriaalse puutumatusega seotut ning esitas väljakutse riigi-kesksele lähenemisele riigikaitses (OSCE 2009). Küsimus inimeste julgeolekust (arenenud peamiselt ÜRO egiidi all) seadis otseselt küsimärgi alla „ riigi-keskse“ lähenemise julgeolekule ja seadis esikohale indiviidi huvid (Lindstrom, Luiijf 2012,45). Seetõttu kerkisid üles ka küsimused, mis on seotud kriitilise infrastruktuuri kaitsega ning elutähtsate teenuste tagamisega. On selge, et olukorras, kus võõrriik on huvitatud oma mõju suurendamisest teise riigi territooriumil ning on selleks valmis astuma radikaalseid samme, on üheks võimalikuks tegevusliiniks ka riigi elanike survestamine elutähtsate teenuste ja kriitilise infrastruktuuri toimimise häirimise kaudu.

Küberjulgeoleku, tol ajal eelkõige IT süsteemide turvalisuse mõjust riikide julgeolekule ning sõjalisele riigikaitsele hakati rääkima juba 1990. aastate alguses. USA Teaduste Akadeemia raport arvutite turvalisuse kohta algas sõnadega: „ Oleme ohus. Ameerika sõltub järjest rohkem arvutitest/.../ Homsed terroristid on võimelised tegema rohkem kahju klaviatuuri kui pommi kasutades“ (NAS 1990). Võib oletada, et julgeolekuspetsialistide hulgas pöörati teemale juba siis tähelepanu, kuid laiema avalikkuse jaoks kerkis probleem esile tunduvalt hiljem. 1997. aasta detsembris kasutas maailmas internetti vaid 70 miljonit inimest (1,7% maailma rahvastikust), 2007. aastal aga juba 1,3 miljardit (20% maailma rahvastikust). 2017. aasta detsembri andmetel oleme jõudnud 4,1 miljardi kasutajani ehk 54,4% maailma rahvastikust omab internetile juurdepääsu ja kasutab seda (Internetstat 2018). 2000. aastate alguseks oli IT roll igapäevaelus piisavalt tajutav, et järjest rohkem kerkisid esile ka mured valdkonna turvalisuse pärast ja eriti mure selle võimaliku mõju pärast riiklikule julgeolekule.

2003. aastal võeti USAs vastu esimene küberjulgeoleku strateegia *The National Strategy to Secure CyberSpace* mis kuulus 2001 aasta terrorirünnakutele järgnenud sisejulgeoleku tugevdamise paketi hulka. Strateegia nägi kolme põhieesmärgina ette USA kriitilise

infrastruktuuri vastaste küberrünnakute ärahoidmist, riikliku küberründe haavatavuse vähendamist ja rünnakute põhjustatud kahju ning taastumisaja vähendamist. Seega näitab, et juba selleks ajaks oli vähemalt osades riikides arusaam küberjulgeoleku rollist riigi julgeolekus olemas.

Küberjulgeoleku kui mõiste kohta on valdkonnas siiani käibel mõnevõrra erinevaid definitsioone, esmajoones sõltuvalt defineerijate vaatepunktist: poliitiline või tehnoloogiline. 2008. aastal defineeris Rahvusvaheline Telekommunikatsiooni Liit (ITU) küberjulgeolekut kui: „kogumit vahenditest, poliitikatest, turvalisuse kontseptsioonidest, riskijuhtimise lähenemistest, tegevustest, väljaõppest, parimatest praktikatest, kindlustavatest vahenditest ja tehnoloogiatest, mida kasutatakse küberkeskkonna, organisatsiooni ja kasutaja vara kaitseks./.../“ Hollandi riiklik küberjulgeoleku strateegia aastast 2011 defineerib küberjulgeolekut aga kui :“Infotehnoloogiliste süsteemide katkemisest, hävimisest või väärkasutusest tekkiva ohu ja kahju puudumist./.../“ (Klimburg *et al* 2012,12). Üldiselt saab siiski väita, et küberjulgeoleku definitsioonid erinevate riikide ja rahvusvaheliste organisatsioonide käsitluses hõlmavad ootust infotehnoloogiste süsteemide turvalisele ja eesmärgipärasele toimimisele riikliku julgeoleku ning ühiskondliku turvalisuse kontekstis.

Küberjulgeoleku kontseptsiooni on põhjalikumalt uuritud ka Kopenhaageni julgeolekuuuringute koolkonna[1] poolt. Klassikalise, kompleksse julgeoleku teooria ehk julgeoleku kompleksi teooria (*classical security complex theory*) autorite, näiteks Barry Buzani järgi on kõik riigid omavahel julgeoleku valdkonnas seotud ja riik on ka peamine üksus, mis suhtleb sama tasandi teiste üksustega (Buzan *et al* 1998,10-11).

Klassikalist julgeoleku kompleksi teooria mõistet vaadeldakse referentsobjektide alusel kahe kompleksi liigina, lähtudes kelle vahel julgeolekualaseid diskussioone peetakse ja otsuseid vastu võetakse (*ibid*):

1. Homogeensed (*homogeneous complexes*) – põhineb lähenemisel, kus julgeolek keskendub spetsiifilistele sektoritele ja sarnaste üksuste omavahelisele suhtlusele;

[1] Kopenhaageni koolkonna mõiste tõi kasutusele Bill McSweeney (McSweeney 1996), viidates peamiselt Kopenhaageni Rahuuuringute Institutuudi (COPRI) juures 1988 aastast tegutsevale teadlaste grupile, mille rajajateks loetakse Barry Buzani ja Ole Wæverit.

2. Heterogeensed (*heterogeneous complexes*) – loobutud on ideest, kus julgeolek on kindlate sektorite vaheline aruteluteema vaid põhineb erinevate sektorite vaheliste osalejate koostööl (nt riik ja erasektor, riik ja rahvas).

Ülaltoodud käsitluse raames tuleks küberjulgeolekut käsitleda heterogeense kompleksina, kuna küberjulgeoleku tagamiseks on vajalik riigi ja erasektori vaheline mitmetasemeline koostöö, mida on ka vajalik strateegia koostamisel silmas pidada.

Küberjulgeoleku valdkonda käsitles Kopenhaageni koolkond 1990. aastatel peamiselt kui näidet julgeolekustamise (*securitization*) kohta ning isegi aastal 2009 nenditakse veel, et küberjulgeoleku valdkond on uus julgeoleku liik, mis pole konkreetset definitsiooni veel leidnud (Hansen, Nissenbaum 2009). Kopenhaageni koolkond käsitleb julgeolekustamisena olukorda, kus üks või mitu teemat nimetatakse ajalooliste näidete põhjal ohuks riigi julgeolekule ning ühiskonna püsimajäämisele ning näidatakse nende kohese kaitsmise vajalikkust (Buzan *et al* 1998). Küberjulgeolekut tuuakse näitena olukorrast kus näiteks Pentagon üritab (põhjendamatult) julgeolekustada kriitilise infrastruktuuri häkkimist – „seda olukorras, kus see on välistatud, kuna sel puudub kaskaadmõju teistele julgeolekuküsimustele“ (Buzan *et al* 1998,25 *via* Hansen, Nissenbaum). Järgmistel aastatel toimunu näitas selle järelduse ekslikkust, kuid siinkohal tasub silmas pidada, et 1990. aastatel ei tajutud riikide kriitilise taristu ning ka sõjalise riigikaitse sõltuvust infotehnoloogilistest lahendustest eriti märkimisväärsena.

Avalikkuse huvi tekkimine küberjulgeoleku probleemide vastu on üheks faktoriks, mis on aidanud probleemi tähendust mõista nii poliitilisel tasandil kui ka akadeemilistel ringkondadel. Vastavasuunaliste uurimustööde arvu kasvus on küllalt suur roll Eestit 2007. aastal tabanud küberrünnakutel, mis tõstatasid küberkomponendi rolli riiklikus julgeolekus praktiliselt tajutavate näidete varal.

Eesti „kübersõja“ näitel pakutakse küberjulgeoleku kontseptsiooni üheks analüütiliseks raamistikuks välja küberjulgeoleku valdkonnale omast kolme eristatavat mõõdet: hüperjulgeolekustamist, igapäevaseid julgeolekupraktikaid ning nn tehnifikatsioone (*hypersecurityzations, everyday security practices and technifications*) (Hansen,Nissenbaum 2009). Toodud kolme mõõtme sisu saab interpreteerida järgnevalt:

- Hüperjulgeolekustamine on kokkuvõtlikult kaldumine teatud liialdustesse ohtude kirjeldamisel, mis on tingitud ennekõike küberohtude abstraktsusest, konstrueeritusest

ning ebamäärasusest mõju hindamisel, teatud esoteerilisusest (Klimburg 2012). Selle peamiseks põhjuseks võib käesoleva kirjutise autori hinnangul lugeda mitte ainult toimunud ja uuritavate juhtumite vähesust, vaid ka IT süsteemide väga keerulisi koosmõjusid- nn ristsõltuvusi, mis teevad tegelike mõjude ennustamise väga komplitseerituks.

- Igapäevaseid julgeoleku(turva)praktikad on viisid, kuidas tavainimesed ja organisatsioonid igapäevaselt IT vahendeid kasutavad ning milliseid turvapraktikaid rakendavad. Sellised praktikad annavad konteksti riigi küberjulgeoleku olukorra hindamiseks ning aitavad tasakaalustada esimeses mõõtmes kirjeldatud ebatäpseid hinnanguid.
- Küberjulgeoleku valdkonnas väga tugevat mõju omav tehniline aspekt on vahetult seotud nii esimese kui teise mõõtmega. (*ibid*) Ilma põhjalike teadmisteta IT-valdkonna kohta on võimatu täpselt hinnata tehnoloogilisi nõrkusi ja nende ärakasutamise võimalusi. Seetõttu satutakse küberjulgeoleku valdkonnas tihtipeale olukorda, kus pole selge, kas rünnak on tehniliselt üldse võimalik, milliseid ressursse see nõuab ja kui tõenäoline see on.

Küberjulgeoleku valdkonna strateegilise planeerimise uurimisel saab hinnata, millises ulatuses on neile strateegia eesmärke kajastavatele mõõtmetele tähelepanu pööratud ning milline on nende mõõtmete omavaheline mõju.

Lisaks on võimalik hinnata kolme põhilist mõõdet, kus soovitakse mõju saavutada, eristades valitsuse-, rahvusvahelist- ja (üle)riiklikku mõõdet järgnevalt:

- Valitsuse mõõdet võib esmajoones kirjeldada kui vajadust koordineerida eri valitsusasutuste (kes omavad küberjulgeolekuga puutumust) vahelist koostööd, saavutamaks võimalikult valitsusülest (*Whole of Government*) lähenemist, mille saavutamine on küberjulgeolekus isegi raskem kui teiste julgeolekudistsipliinide puhul (Klimburg *et al* 2012, 29-31).
- Rahvusvaheline mõõde tuleneb küberjulgeoleku olemusest- internet on rahvusvaheline ja riigipiiridest põhimõtteliselt sõltumatu.
- Riiklik mõõde- väljendab vajadust leida üleriigiline (*Whole of Nation*) lähenemisviis, mis haaraks küberjulgeoleku tagamisse peale riiklike institutsioonide ka erasektori (*ibid*).

2. UURIMISRAAMISTIK

Antud uurimistöö peamiseks eesmärgiks on uurida Eesti küberjulgeoleku strateegiate koostamise näitel küberjulgeoleku strateegilise planeerimise probleeme avaliku halduse strateegilise planeerimise teoreetilise raamistiku taustal, mõistmaks selle valdkonnale omaseid probleeme ja eripärasid. Teiseks eesmärgiks on analüüsida ja hinnata Eesti küberjulgeoleku strateegiate koostamise ja rakendamise protsessi tajutud mõju nii Eesti küberjulgeoleku üldisele arengule kui ka seda toetavate valdkondade (teadus- ja haridusvaldkond, riigikaitse jms) arengule. Töö tulemusi on võimalik kasutada ka teiste riikide küberjulgeoleku valdkonna strateegilise juhtimise probleemide uurimisel.

Tuli tõmmata selge piir kasutatavate teoreetiliste lähtekohtade poolt võimaldatava uurimisraamistiku ja sellest väljapoole jääva vahel. Antud töö eesmärgiks pole pakkuda küberjulgeoleku strateegiate rakendamise ammendavat mõjuhinnangut ega põhjalikku uurimust küberjulgeoleku strateegia koostamise teoreetilistele lähtekohtadele riigiõiguse ja avaliku halduse õigusliku reguleerimise taustal. Samuti pole eesmärk hinnata strateegiate koostamise vajadust üldiselt, kuna just väikeriikide jaoks peetakse strateegilist planeerimist ja strateegiate koostamist oluliseks (Bailes 2009).

Uurimise läbiviimisel lähtus autor järgnevatest, tinglikult kolme plokki jaotatud faktoritest, mis iseloomustavad strateegiate loomist, strateegilist planeerimist ja strateegilist juhtimist, ning koostas nende alusel uurimisküsimused lisas 1.

Strateegiate hindamisel saab arvesse võtta planeerimise ulatust iseloomustavaid faktoreid (toetudes peamiselt Klimburg 2012;Bryson 2011; Hansen,Nissenbaum 2009):

- Kas küberjulgeoleku tagamist ja selle strateegilist planeerimist käsitletakse kui üleriigilist, heterogeensete osalistega protsessi? Kas võetakse arvesse vajadust kaasata erasektorit ja teisi partnereid?
- Kas küberjulgeoleku strateegilisel planeerimisel lähtutakse vajalikul määral vajadusest valitsusasutuste vahelise koostöö ja koordinatsiooni järele? Kas nähakse vajadust läheneda küberjulgeoleku valdkonnale valitsusüleselt?
- Kas küberjulgeoleku strateegilisel planeerimisel on käsitletud selle rahvusvahelist mõõdet? Kas saadakse aru vajadusest teha rahvusvahelist koostööd?

Küberjulgeoleku strateegia koostamise ja küberjulgeoleku strateegilise planeerimise protsessi probleemide hindamisel avaliku halduse strateegilise planeerimise teooria kontekstis keskendutakse protsessi põhiliselt iseloomustavatele faktoritele, milleks on (Bryson 2011, Allison, Kaye 2005 järgi):

- Strateegia koostamise juhtimine ja probleemid (nt organisatsioonide juhtide ja vajalike huvigruppide kaasatus ning juhtgrupi tegevus)
- Strateegia põhieesmärkide seadmise ja sõnastamise edukus (põhieesmärgi arusaadavus, sõnumite selgus, ühiste eesmärkide kokkuleppimine)
- Seostatus teiste strateegiatega ja arengukavadega ning eelarvete koostamisega;
- Küberjulgeoleku strateegia koostamine poliitika planeerimise ja rakendamise osana ning protsessi elluviimine ja selle seire;

Kuivõrd töö eesmärgiks on hinnata nii strateegiate koostamise protsessi kui ka selle mõju, uuritakse töös järgmisi probleeme (peamiselt Klimburg *et al* 2012, Hansen,Nissenbaum 2009, Brangetto, Kert-Saint Aubyn 2015, ITU... 2018):

- Strateegia põhieesmärkide elluviimisele ja Eesti saavutatud üldisele olukorrale küberjulgeoleku tagamisel;
- Strateegia ja selle koostamise protsessi mõju küberjulgeoleku kui probleemi teadvustamisele riigi julgeoleku probleemina;
- Strateegia ja selle koostamise mõjule küberjulgeoleku valdkonnas olulist rolli omavate valitud (järgnevalt loetletud) valdkondade arengule.

Küberjulgeoleku strateegia ja selle koostamise mõju hindamisel pidas autor otstarbekaks käsitleda valdkonnas olulist tähtsust omavate valdkondadena riigi majandust üldiselt, julgeoleku- ja riigikaitse valdkonda, haridus- ja teadusvaldkonda ning rahvusvaheliste suhete valdkonda.

CCDCOE poolt 2015 aastal läbi viidud projekti tulemused näitasid, et kuigi e-teenuste toimimise, digitaalse majanduse ja kogu infotehnoloogiast sõltuva majanduse toimimise eelduseks on turvalisuse olemasolu ning valdkonna strateegiatel on selge majanduslik mõju, pole küberjulgeoleku majanduslike mõjude uurimisega eriti tegeletud (Brangetto,Kert-Saint Aubyn 2015).

Hariduse- ja teadusvaldkonna areng on küberjulgeoleku tagamisel määrava tähtsusega nii lühikeses kui ka pikas perspektiivis. Haridus- ja teadusvaldkonna arengut peetakse oluliseks enamike riikide küberjulgeoleku strateegiates, seda nii üldise teadlikkuse kui ka tehnilise valmisoleku arendamise seisukohalt (Lujif *et al* 2013). Eesti on küberjulgeoleku valdkonnas hariduse ja teadusega seotud probleeme käsitlenud kõigis kolmes strateegias (KJS 2008,KJS 2014, KJS 2018)

Küberjulgeoleku valdkonna arengu mõju riigikaitse valdkonnale on käesolevas töös hinnatud eelkõige lähtuvalt eelkirjeldatud arenguprotsessist, kus küberjulgeoleku valdkonna riiklik strateegiline planeerimine (ka Eestis) sai alguse arusaamast, et tegemist on riigi julgeoleku valdkonda mõjutava aspektiga. Küberjulgeoleku strateegiad käsitlevad riigikaitse probleeme (Klimburg *et al* 2012) , samuti on küberjulgeolek tänapäeval kindlasti ka oluline riigikaitse osa. Eesti KTS 2018 koostamine Infoühiskonna arengukava osana jätab aga mulje sellest kontseptsioonist kaugenemisena, mistõttu on huvipakkuv jälgida protsessi, mis sellise arenguni viis.

Rahvusvaheliste suhete arengule avaldatud mõju on huvitav ennekõike Eesti rahvusvahelise kuvandi kontekstis. Ühelt poolt on põhjuseks Eesti tuntus riigina, kus 2007. aastal toimus „esimene kübersõda.“ Teisalt on Eesti seadnud oma eesmärgiks panustada Põhjala-Balti regiooni muutumisse IT turvalisuse ja e-riigi kompetentsikeskuseks (Areng 2014) ning on oma positiivset, juhtiva digiriigi rolli selles ka rahvusvahelises suhtluses rõhutanud. Kolmas aspekt on küberjulgeoleku valdkonna probleemide piiriülesus ja globaalsus, mis seab rahvusvahelisel suhtlemisel strateegilisi väljakutseid nii väike- kui suurriikidele.

Loetletud valdkondades strateegia mõju hindamine ekspertide poolt võrrelduna strateegia rakendamise kokkuvõtete ja hindamisraportitega annab autori hinnangul ülevaate küberjulgeoleku strateegia tervikprotsessi tajutud mõjust ülaltoodud olulistele valdkondadele, mida on võrreldes küberkuritegevuse või kriitilise taristu valdkonnaga oluliselt vähem uuritud.

2.1 Meetodi valik

Strateegilise planeerimise ja selle tulemuste uurimiseks on kasutatud mitmeid meetodeid. Üks levinumaid käsitlusi (Poole *et al* 2000) eristab erinevustele ja protsessile keskenduvaid uuringuid (*variance* vs *process*) ning üldiselt arvatakse, et otstarbekas on kasutada mõlemaid. Esimesel juhul on avaliku sektori strateegiline planeerimine käsitletud kui fikseeritud, eraldi objektina esinev rutiin või tavapärane praktika, mitte kui genereeriv süsteem, mis koosneb paljudest vahetatavatest ja üksteisega suhtlevatest osadest (Bryson *et al* 2017). Teisel juhul, protsessiuuringutes, eeldatakse, et strateegilise planeerimise efektiivsuse (või siis ka võimaliku mitteefektiivsuse) peamiseks võtmeks on selle käsitlemine kompleksse, suunatud protsessina, mille eesmärgiks on arusaamine ja tegutsemine (Mintzberg 2007; Ferlie, Ongaro 2015 *via* Bryson *et al* 2017).

Eesti küberjulgeoleku strateegiaid on mitmesugustes teaduslikes väljaannetes ja konverentsidel avaldatud töödes käsitletud peamiselt keskendunult a)strateegia varasele adopteerimisele Eestis või b)strateegia(te) struktuurile. Seega on ilmne, et koostamise protsessi ja tulemuste hindamisel tuleb ametlike kokkuvõtete ning uurijate ja rahvusvaheliste organisatsioonide koostatud hinnangute kõrval paljuski lähtuda protsessis endas või strateegia elluviimisel osalenud ekspertide hinnangutest.

Kvantifitseeritavate arvandmete vähesus või puudumine ja uurimisküsimuste iseloom tingib kvalitatiivse uurimismetoodika eelistamise. Kvalitatiivset uuringut saab pidada lähenemiseks, kus uuritakse individuaalset või grupi mõju sotsiaalsele või inimlikule probleemile ning mille uurimisprotsess hõlmab esilekerkivaid küsimusi ja protseduure, osalise poolt kogutud andmeid ning nende andmete nii induktiivset kui ka deduktiivset analüüsi (Creswell 2014, 32). Võimaldamaks toetumist nii kvalitatiivsetele kui ka kvantitatiivsetele andmetele on otstarbekas kasutada juhtumiuuringu (*case study*) metoodikat, mis võimaldab uurida sündmusi viisil, mis säilitab selle tervikliku konteksti ja olulised tunnusjooned (Yin 2003a, 13-14; 2011,307; 2003b,4). Juhtumiuuringu kasutamine võimaldab andmete kogumisel ja nende analüüsil toetuda ka valdkonna teoreetilistele alustele (Meyer 2001; Yin 2009). Juhtumiuuringu eesmärgiks on siin üldistamist vältiv juhtumi põhjalik ning sügavuti uurimine (Creswell 2003; Simons 2009), ja kasutatava metoodika eelisena näeb autor ka võimalust saada põhjalik arusaam käsitletavast spetsiifilisest valdkonnast ja anda selle kaudu sisend edasisteks tegevusteks poliitika kujundamisel (Simons 2009).

Kuivõrd juhtumiuuringu puhul ei käsitleta andmete valimit, vaid analüüsiüksust, siis antud uuringu puhul on tegemist ühe juhtumiga, milleks on küberjulgeoleku valdkonna strateegiate loomine. Juhtumiuuringu raames on eristatud, analüüsitud ja võrreldud kahte analüüsiüksust: protsessi osaliste ja huvigruppide hinnangut strateegiatele ja nende koostamise protsessile ning uuringutes ja ametlikes kokkuvõtetes saadud hinnanguid. Käesolev juhtumiuuring on seega on kahe alamanalüüsiüksusega ühe juhtumi uuring, ehk hõlmava disainiga uuring (Yin 2009). Kuna juhtumiuuringu käigus kogutud andmete analüüsiks pole üldjuhul võimalik kasutada kvantitatiivset andmeanalüüsi, tuleb leida juhtumile sobiv ja võimalikult objektiivne viis andmete hindamiseks kvalitatiivselt. (Laherand 2008; Simons 2009; Yin 2009)

Uurimismeetodiks valiti avalikult kättesaadavate dokumentide analüüs, võrdlus valdkonna rahvusvahelise praktikaga ja ekspertintervjuude läbiviimine strateegiat koostanud ja rakendanud ekspertidega. Teoreetiline ja empiiriline osa on seotud teoreetilisest osast lähtuvate hinnangute kaudu empiirilises osas kogutud infole.

Intervjuudega kogutud andmete analüüsiks sobis tavapärase sisuanalüüsi meetod (Laherand 2008) mis võimaldab kirjeldada uurimisobjekti lähtuvalt kogutud andmetest, vältides liigset sõltumist teoreetilisest raamistikust. Lähtutakse antud töös ju ühelt poolt nii strateegilise planeerimise ja -juhtimise piisavalt läbi uuritud ja ulatuslikust teoreetilisest raamistikust, kui ka tunduvalt vähem uuritud küberjulgeoleku strateegilise planeerimise temaatikast kitsamalt.

2.2 Andmete kogumine

Saavutamaks juhtumi nägemist erinevatest vaatepunktidest, kasutati erinevaid, kuid üksteist täiendavaid andmete kogumise viise (Baxter, Jack 2008; Yin 2009) – selline andmete triangulatsiooniks nimetatud meetod võimaldab suurendada uuringu üldist usaldusväärsust (Yin 2009).

Uuringu peamise meetodina kasutati strateegiate loomise protsessis osalenud, sellega puutumuses olnud või muul viisil küberjulgeoleku valdkonna arenguga kursis olevate ekspertide intervjueerimist. Selleks viidi peale uurimistöö põhiküsimuste sõnastamist läbi struktureeritud kirjalikud intervjuud, mida vajadusel täiendati täpsustavate suuliste küsimustega.

Intervjueeritavad valiti välja ettekavatsetud valimina (*purposive sample*) (Palys 2008) lähtudes töö autori poolt valdkonnas töötades omandatud teadmistest isikute rolli kohta Eesti küberjulgeoleku valdkonna arendamisel. Valimisse koondati 25 Eesti küberjulgeoleku arendamises vahetult osalenud poliitikakujundajat, riigi tippjuhti ja tippeksperti, eesmärgiga saada hinnangud võimalikult suurelt osalt Eesti küberjulgeoleku valdkonna kujundamisel ja otsuste tegemisel osalenud inimestelt, kellest 23 leidis ka võimaluse uuringus osaleda.

Intervjueeritutest 15 on vahetult osalenud strateegiate väljatöötamises, 11 osalevad või on osalenud poliitika kujundamisel ministeeriumite või ametkondade tippametnikena, neist kuus on osalenud Küberjulgeoleku nõukogu töös; 16 on vahetult osalenud strateegiate rakendamisel ning 13 leidis, et tal on olnud roll strateegia tulemuste hindamisel: 12 vastanut pidas võimalikuks nende vastustele nimelist viitamist, 8 soovisid jääda anonüümseks.

Intervjuud viidi läbi 28. juulist 2018 – 15. oktoobrini 2018, kirjaliku intervjuu vormis, milleks edastati osalejatele küsimustik (Lisa 3) ja osalemise kutse. Juhtumiuuringu eetilisuse tagamiseks oli intervjuu küsimustikus eraldi küsimus intervjueeritava nõusoleku kohta temale nimeliseks viitamiseks. Samuti olid kõik intervjueeritavad teadlikud uurimistöö läbiviimise eesmärgist ja nendepoolsete vastuste kajastamisest nagu selliste uurimuste hea praktika ette näeb (Gillham 2009). Allikate nimistus ja viidetes kasutatakse intervjuudele viitamisel terminit „intervjueeritav“ või „ekspert“, viimast juhul kui on vaja rõhutada intervjueeritava rolli küberjulgeoleku valdkonna sisueksperdina. Juhul kui intervjueeritav andis selgesõnalise nõusoleku nimeliseks viitamiseks, on seda tehtud juhul, kui see on vajalik vastusele konteksti andmiseks.

Intervjuudega kogutud teave sisestati MS Excelisse ja jaotati olemasoleva teoreetilise raamistiku ja uurimisküsimuste põhjal tinglikku kodeerimisraamistikku (Hsieh,Shannon 2005). Teabe analüüsil lähtuti kolmest peamisest põhimõttest:

- Tekstimahukate vastuste hindamisel kasutati märksõnade kogumist valimi vastuste koondist ja nende kordumise (esinemissageduse) hindamist (näiteks : millised olid küberjulgeoleku strateegia koostamise põhilised probleemid).
- Küsimuse puhul, mis eeldas hinnangu andmist, jaotati vastused negatiivse denotatsiooniga ja/või konnotatsiooniga (näiteks: pigem arvan et mitte, ei arvestatud jne) ja positiivse denotatsiooni ja/või konnotatsiooniga (näiteks: teatud määral oli ikka, oli oluline mõju jne) vastusteks ja summeeriti tulemused.

- Intervjueeritava rolli iseloomustavate küsimuste (näiteks: kas osalesite /.../ strateegia koostamisel?) vastuseid kasutati vaid intervjuu tsiteerimisel vajaliku konteksti andmiseks.

Lisaks intervjuudele koguti ja analüüsiti lisaks dokumente, mis võimaldasid saada objektiivset informatsiooni küberjulgeoleku strateegiate protsessile ja tulemustele antud hinnangute kohta, et hinnata Eesti objektiivset olukorda küberjulgeoleku tagamisel. Kahel juhul ei olnud tegemist avalikult kättesaadavate dokumentidega, mis olid algselt mõeldud asutusesiseseks kasutamiseks. Kuna tegemist oli ülevaadetega, mis vaid osaliselt käsitlesid Avaliku teabe seaduse mõttes asutusesiseseks kasutamiseks mõeldud teavet, andis teabe valdaja ühel juhul loa teabe kasutamiseks ning teisel juhul möödus uurimistöö kirjutamise ajaks dokumendi asutusesiseseks teabeks tunnistanud märke kehtivusaeg. Kasutatud dokumentide loetelu asub töö lõpus kasutatud kirjanduse loetelus.

Läbivalt oli võimalik kasutada töö autori enda vahetut kogemust, kes on olnud küberturvalisuse tagamisega seotud alates 1998 aastast, töötades valdkonnaga seotud ametikohtadel nii riigi- kui erasektoris. 2011- 2017 töötas ta Riigi Infosüsteemi Ameti (RIA) peadirektori asetäitjana küberturvalisuse valdkonnas ning juhtis RIA küberturvalisuse teenistust, mille ülesannete hulka kuulus kriitilise informatsiooni infrastruktuuri ja riigi infosüsteemide kaitse korraldamine, küberintsidentide lahendamine jne. Autor on osalenud nii teise kui kolmanda küberjulgeoleku strateegia loomisel ning nii esimese kui ka teise strateegia rakendamisel. Vahetu kokkupuude uuritud protsessidega võimaldas sündmuste ja protsesside vaatlemist loomulikus keskkonnas (Yin 2009) ning nende kohta hinnangu andmist. Sisuliselt on töö koostajal olnud võimalus olla osalusvaatleja, mis annab hea võimaluse uurimuse osaliste vaatenurkade mõistmiseks (Laherand 2008). Kuna aga sündmuste vaatlemisel ei jälgitud metoodikat (tehtud märkmeid jne), taandub autori isikliku kogemuse roll pigem kontekstuaalsete seoste nägemisele ja mõistmisele ning võimalusele hinnata mõnda olukorda ka isiklikele kogemustele toetudes.

3. KÜBERJULGEOLEKU STRATEEGIAD EESTIS

3.1 Küberjulgeoleku strateegia 2008-2013 (KJS 2008) koostamine

Eesti oli esimene Euroopa Liidu liikmesriik, kes koostas küberjulgeoleku arendamiseks laiaulatusliku strateegia. Küberjulgeoleku strateegia koostamise peamiseks ajendiks oli 2007. aasta aprillis ja mais toimunud küberrünnakud, mis tekitasid vajaduse parandada riigi võimet tulla toime kriitilise informatsiooni infrastruktuuri (KII) vastu suunatud küberrünnetega (Pernik 2013).

Küberjulgeolekuga tegeleti Eestis ka enne esimese strateegia koostamist. 2006. aastal loodi riiklik küberintsidentidele reageerimise üksus CERT-EE[2], mis paiknes tollase Riigi Infosüsteemide Arenduskeskuse, Majandus- ja Kommunikatsiooniministeeriumi (MKM) poolt hallatava asutuse juures. CERT-EE oli 2007. aastaks juba rahvusvahelise võrgustiku osa ning tegi aktiivset rahvusvahelist koostööd partnerasutustega. Samuti oli autori isikliku kogemuse põhjal hästi arenenud ka CERT-EE mitteformaalne koostöö Eesti pangandussektori ja telekommunikatsioonisettevõtete küberturvalisuse ekspertidega ja Eesti politsei küberkuritegude vastu võitleval üksusel oli tänu nende efektiivsele tööle keerukate rahvusvaheliste küberkuritegude lahendamisel väga hea maine. Teabeameti (praeguse Välisluureameti) poolt korraldati riigisaladust ja/või salastatud välisteavet sisaldava info kaitset infosüsteemides.

2007. aasta nn aprillirahutustele järgnenud küberrünnakud ja eelkõige nende ootamatult suur mõju olid siiski üllatuseks nii poliitilise tasandile kui ka laiemale avalikkusele nii Eestis kui välismaal. Kuigi nende rünnete hilisemal analüüsil pole ekspertidel nende tegeliku mõju osas siiani üksmeelt, oli üldise arvamuse kohaselt tegemist sündmustega, mis muutsid radikaalselt rahvusvahelise üldsuse vaadet küberjulgeoleku probleemidele ning tõi need teravdatud tähelepanu alla (O'Neill 2016). Eestis, kus küberrünnakuid tajuti otsese välisriigist lähtuva agressioonina, mis tänu internetipanganduse ja muude e-teenuste laiale levikule, põhjustasid koheselt elava diskussiooni küberjulgeoleku arendamise vajaduse üle. 2007. aasta rünnakute rolli kirjeldatakse strateegia (KJS 2008) tekstis järgnevalt: „Küberohtude teadvustamine jõudis 2007. aastal rahvusvahelise julgeoleku seisukohalt uuele tasandile mitte ainult esimese koordineeritud küberrünnaku toimepanemise tõttu Eesti kui riigi vastu, vaid ka paljude teiste

[2] CERT- *Computer Emergency Response Team* on Carnegie Mellon University poolt patenteeritud kaubamärk mida kasutavad rahvusvahelisse võrgustikku kuuluvad, valdavalt riiklikud või akadeemiliste asutuste küberturvalisuse üksused Carnegie Mellon University loal.

riikide era ja avaliku sektori oluliste infosüsteemide vastu suunatud ulatuslike küberrünnakute tõttu. Sagenenud küberrünnakud annavad tunnistust uue ajajärgu saabumisest, kus küberruum on saavutamas globaalset julgeolekumõõdet ning kriitilise tähendusega infosüsteemide kaitset käsitletakse sama olulisena kui riikide traditsioonilist kaitsevõimet ja julgeoleku tagamist."

Peale ründeid Vabariigi Valitsuse julgeolekukomisjoni poolt mais 2007 tellitud raportis tehti ettepanek muuta küberkaitse arendamine riigi üheks prioriteetseks valdkonnaks ja töötada välja küberjulgeoleku strateegia (Pernik 2013). 19 novembril 2007 kiitis Vabariigi Valitsus heaks strateegia koostamise ettepaneku ja määras küberjulgeoleku strateegia 2008–2013 (KJS 2008) koostamise eest vastutavaks ministeeriumiks Kaitseministeeriumi ning strateegia väljatöötamisel osalevateks ministeeriumideks Haridus- ja Teadusministeeriumi, Justiitsministeeriumi, Majandus- ja Kommunikatsiooniministeeriumi, Siseministeeriumi ja Välisministeeriumi. Kaitseminister moodustas seejärel strateegia koostamiseks kaitseministeeriumi (KM) juhitava ametkondadevahelise komisjoni, mis asus strateegiat välja töötama. KJS 2008 kiideti Vabariigi Valitsuse poolt heaks 8. mail 2008.

Strateegia kui valitsuse arengukava koostamisel lähtuti Vabariigi Valitsuse määrusega nr 302 „Strateegiliste arengukavade liigid ning nende koostamise, täiendamise, elluviimise, hindamise ja aruandluse kord" kehtestatud strateegilise arengukava koostamise, elluviimise, aruandluse, täiendamise ja lõpetamise alustest. Samuti oli Rahandusministeerium 2006 aastal koostanud Strateegilise planeerimise käsiraamatu (Rahandusministeerium... 2006), mis andis juhised strateegiliseks planeerimiseks ja arengukavade koostamiseks.

Strateegia koostamiseks loodud organ oli küll nimeliselt ametkondadevaheline komisjon, mis aga ei tähenda, et strateegia koostamisel oleksid osalenud ainult riiklike ametkondade esindajad. Kaasatud, enamasti küll mitteformaalselt, olid ka paljud eraettevõtete küberturvalisuse eksperdid ning akadeemilise ringkonna esindajad. Käesoleva töö raames intervjueeritutest osales strateegia väljatöötamisel seitse intervjueeritavat ja neist kaks erasektoris töötanud eksperti pidas vajalikuks intervjuus täpsustada, et nende roll oli mitteametlik. Ekspertide kaasamisele viidatakse ka strateegia (KJS 2008) tekstis endas: „Ametkondadevaheline komisjon strateegia koostamiseks kaasas ka Eesti ettevõtete infoturbeeksperte". Erasektori ja teiste huvigruppide kaasamisele aitasid autori hinnangul kaasa ka eelnevalt mainitud küberturvalisuse ekspertide mitteformaalse koostöövõrgustiku olemasolu, mistõttu oli strateegia koostamist juhtinud ametnikel ülevaade valdkonna ekspertidest Eestis. Samuti oli ekspertide kaasamisel oma roll ka küberrünnakute käigus saadud koostöö kogemus erasektori ja riigiasutuste vahel. Võib nõustuda RKK teaduri Piret Perniku

tõdemusega, et KJS 2008 üks olulisemaid saavutusi oli koostamise protsess ise, mis tõi kokku palju riigiasutusi ning parandas riigi koostööd eraettevõtete ja haridusasutustega (Pernik 2013).

Strateegiaprotsessi ühe olulise osana käsitletavat olemasoleva olukorra kaardistamist kirjeldas üks ekspert intervjuul isegi selle küberjulgeoleku strateegia põhieesmärgina, mis tema arvamust mööda ka täideti. Strateegia tekstis kirjeldatakse ja analüüsitakse hetkeolukorda tõepoolest väga põhjalikult: 11. leheküljel kirjeldatakse nii üldiseid küberohte kui esitatakse põhjalik analüüs kokku seitsmes kategoorias: Eesti infoühiskonna ja informatsiooni infrastruktuur, infosüsteemide turvalisuse, infoturbealane väljaõpe ja täienduskoolitus, rahvusvaheline koostöö ning õigusruum küberjulgeoleku tagamisel nii rahvusvahelise õiguse kui ka riigisisese õigusruumi vaates.

Strateegia väljatöötamisel osalenud intervjueeritavatest mainisid intervjuude käigus pea kõik peamise probleemina teema uudsust nii koostajate kui ka sihtrühmade jaoks, mis tingis vajaduse alustada sisuliselt nullist, kuna eeskuju polnud kuskilt võtta. Üks intervjueeritav rõhutas, et: "Väga palju oli vaidlusi skoobi ning terminoloogia asjus (mida strateegia katab ja mida tähendavad strateegias kasutatavad mõisted), kuna teema oli enamikule uus." Strateegia loomise käigus leidis terminoloogia probleem põhjalikku käsitlemist, valminud strateegia lisa sisaldas kasutatud mõistete nimistut ja definitsioone, millest enamik olid uudsed.

Strateegia seostatuse osas teiste riiklike arengukavadega olid intervjueeritavad valdavalt (10 vastanut 17st arvamuse avaldajast) arvamusel, et strateegia ei mõjutanud teisi riiklikke arengukavasid ega olnud nendega seotud.

KJS kohta toodi analüüsis (Pernik 2013) puudustena välja:

1) Eesmärgid ja meetmed ei ole piisavalt seotud eelarvestamise ja ressurssidega;
2) Vähene sidusus ministeeriumite strateegiliste dokumentide ja asutuste tegeliku; tegevusega;
3) Vähene sidusus riigi alusdokumentidega ja valitsuse arengukavadega;
4) Teiste arengukavade dubleerimine.

Antud hinnangut kinnitavad ka käesoleva uurimistöö raames intervjueeritavate poolt antud hinnangud strateegiaga seotud põhiprobleemide kohta: „Vähene seos ressursside planeerimisega – tunnistatakse teema prioriteetsust, aga sellega ei võeta vastutust ressursside eraldamiseks.", „Vähene seos teiste planeerimisdokumentidega – küberstrateegia oli esialgu

mõneti isoleeritud dokument ja erinevad ministeeriumid ei teadvustanud oma vastutust ja rolli küberjulgeoleku poliitika kui prioriteetse suuna elluviimise eest.“, „ Strateegia ei olnud minu hinnangul reaalselt kaetud elluviimiseks vajalike ressurssidega“. Üks tol ajal tippametniku rollis olnud intervjueeritav on ka arvamusel, et küberjulgeoleku strateegia koostamisel tekkinud probleemid olid omased kõigile tolle aja strateegiatele: „Probleemiks oli ka ametkondade vaheline rivaalitsemine, kriitilise informatsiooni infrastruktuuri ettevõtete kohatine tõrksus, vähene seotus eelarveplaneerimisega./…/ Samas iseloomustasid sellised väljakutseid kõiki tolleaegseid strateegiate väljatöötamisi.“

Strateegia vormi leidmise probleemina leidis mitmel korral mainimist ka koostamisel osalenute erinevad vaated strateegia struktuurile ja koostamise põhimõtetele. Näiteks toodi välja:“ Strateegia töögruppides osalevatel inimestel oli erinev taust ja sellest tulenevalt võttis aega „ühise keele“ leidmine. Probleemiks oli ka erinev eelnev ettekujutus strateegiast.“ Probleemina toodi välja ka seatud ajaraamist tingitud kiirustamist ja koostajate ebapiisavat ettevalmistust: „Strateegia oli ehk liiga akadeemiliselt ambitsioonikas, samas (aja survel) kiiresti koostatud. Kirjutajatel oli ebapiisavalt valdkonnapõhist praktilist kogemust.“ Ajalist survet iseloomustab asjaolu, et kui valitsus kiitis strateegia koostamise heaks 19 novembril, siis esialgne plaan oli strateegia koostamisega toime saada kõigest poolteise kuuga: „Kaitseministeerium esitab strateegia valitsusele kinnitamiseks hiljemalt jaanuaris.“ (BNS 2007).

Strateegiat tajusid mingil määral poliitika planeerimise instrumendina valdav enamik intervjueeritavatest: 15 vastajat 22st vastanust. Neli vastajat sellise hinnanguga pigem ei nõustunud ning kolm vastajat ei osanud sellele küsimusele selget hinnangut anda. Samas jääb enamik intervjueeritavatest oma hinnangutes strateegia koostamise käsitlemisel poliitika planeerimise vahendina siiski küllalt ettevaatlikuks- kasutatakse väljendeid:“ teatud määral“, „pigem“, „üldiselt jah“ jne. Enamik intervjueeritavatest iseloomustas strateegiat siiski otseselt poliitikat mõjutanud dokumendina, millega määrati kindlaks nii üldised tegevussuunad kui ka selle saavutamise vahendid, rollide jaotus jne. Hoolimata sellest, et strateegia lisas on küllalt detailselt kirjeldatud strateegia rakendamiseks vajalikke ressursse (kogusummas 302,3 miljonit krooni), leidis vaid üks vastanutest, et tema hinnangul arvestati strateegiaga ka eelarvete koostamisel. 2008. aastal kavandati KJS 2008 elluviimiseks 170 miljonit krooni riigieelarvest, millele lisaks pidi eraldatama 132,8 miljonit krooni. Teada on, et lisaraha ei eraldatud, kuid samas ei teata ka seda, kui palju riigieelarvest kulutati. (Pernik 2013)

Kaitseministeeriumi tollane kantsler ja strateegia koostamise protsessi algataja Lauri Allman kirjeldab strateegia koostamise eesmärke: „Esimese küberjulgeoleku strateegia eesmärk oli astuda otsustav samm küberjulgeoleku temaatika sõnastamiseks. Peamine esimese küberjulgeoleku strateegia funktsioon oli selles mõttes entsüklopeediline. Julge katse ühtse sõnavara, mõistete ja mõistmise kokkuleppimiseks riiklikul tasemel. See eesmärk täideti ja see omas suurt mõju edasise seadusandluse, praktiliste koostöömehhanismide aga ka rahvusvahelise koostöö seisukohalt.“ (Allman 2018) Valdav enamik intervjueeritavatest pidaski strateegia peamiseks ülesandeks raamistiku, vundamendi loomist küberjulgeoleku tagamiseks. Samuti toonitati strateegia eesmärgina teadlikkuse tõstmist küberjulgeoleku tagamise vajadusest, seda just eriti poliitilise juhtkonna seas.

Strateegias endas on eesmärgid sõnastatud järgmiselt (KJS 2008):

- Eestis on laiaulatuslikult rakendatud astmeline turvameetmete süsteem, mis tagab Eesti riigi küberjulgeoleku eesmärkide saavutamise;
- Eesti on väga kõrge infoturbealase kompetentsuse ja teadlikkusega riik;
- infosüsteemide turvalist ja laialdast kasutamist toetab proportsionaalne regulatsioon;
- Eesti on üks juhtivaid riike rahvusvahelises koostöös küberjulgeoleku tagamisel.

Strateegia põhieesmärgina nähti (Eesti) riigi kui terviku küberruumi haavatavuse vähendamist. Alameesmärkide sõnastus on küllalt üldine ja eesmärgiks seatu saavutamist on kasutatud sõnastuse põhjal raske hinnata kuna määratlused nagu „laiaulatuslikult“ ja „väga kõrge“ on ebamäärased ja laialt tõlgendatavad. Siiski kirjeldatakse strateegias eesmärkide täitmise indikaatoreid, mis seavad juba konkreetsed eesmärgid: näiteks infoturbealase kompetentsuse suurendamise eesmärki loetakse täidetuks juhul kui aastaks 2013 on küberjulgeoleku valdkonna magistriõppe läbinud vähemalt 200 õppurit ja infoturbe kursuste osakaal suureneb bakalaureuseõppes 50%.

Eesti esimene strateegia käsitleb küberjulgeoleku planeerimist tunduvalt kitsamalt kui see teiste riikide hilisemates strateegiates tavaks on. Tavapäraselt käsitletakse riiklikes küberjulgeoleku strateegiates nii küberjulgeoleku riigikaitse, küberkuritegevuse, luure, vastuluure, kriisireguleerimise, kriitilise infrastruktuuri kaitse, kübervaldkonna diplomaatilise suhtluse ja muude rahvusvaheliste suhete valdkonda kuuluvate praktiliste teemadega (nt internetihalduse) seotud küsimusi (Klimburg 2012). Eesti strateegia keskendus aga eeltoodust sisuliselt vaid kahele – kriitilise infrastruktuuri kaitse ja rahvusvaheline koostöö. Näiteks küberkuritegevuse vastast võitlemist oli käsitletud vaid seadusandluse ning rahvusvahelise

koostöö võtmes, põhjendades seda valdkonna käsitlemisega Siseministeeriumi ja Justiitsministeeriumi poolt koostatavates arengukavades. Riigikaitse osas viidatakse valmivale sõjalise riigikaitse arengukavale, mis pidi käsitlema ka sõjalise otstarbega infosüsteemide turvalisust. (KJS 2008) Arvestades, et strateegia koostamist juhtis Kaitseministeerium, on riigikaitse aspektide alaesindatus mõnevõrra ebatavaline.

Kokkuvõttes võib väita, et Eesti esimese küberjulgeoleku strateegia loomise protsessi iseloomustavad pingeline ajaraam, teema uudsusest tingitud raskused eesmärkide seadmisel ja sõnastamisel ning ühine arusaam, et tehakse midagi täiesti uut ja süsteemi loovat. Protsessi iseloomustas eri ametkondade, huvigruppide ja ekspertide laialdane kaasatus ning selge ambitsioon teha võimalikult laiapõhjalist strateegilist plaani, millel oleks valdkondadeülene mõju. Samuti iseloomustas strateegiat laiemate julgeoleku- ja riigikaitse aspektide alaesindatus.

3.2 Kokkuvõte hinnangutest KJS 2008 koostamise ja rakendamise mõjudele

Käesolevas töö osas on uuritud ekspertide hinnanguid strateegia mõjude kohta majandusele, julgeoleku- ja riigikaitse valdkonnale, haridus- ja teadusvaldkonnale ning rahvusvahelisele suhtlusele. Kokkuvõttes oli strateegia koostamine ekspertide hinnangul positiivse mõjuga ning eriti väljendus see nö teisese, ehk siis planeerimata kaudse mõjuna julgeoleku ja riigikaitse valdkonnale ning Eesti positiivse rahvusvahelise kuvandi kujunemisele.

3.2.1 KJS 2008 mõju majandusele

KJS 2008 strateegias tõdetakse, et.“ tänapäeva maailmas on majanduslikku edu ning kõrget elukvaliteeti suutnud tagada vaid need riigid, kus tähtsustatakse teadmiste ja informatsiooni efektiivset käsitlemist ning rakendatakse seda ühiskonna hüvanguks.“ Strateegia koostajad on ka seisukohal, et Eesti kriitilise informatsiooni infrastruktuuri töökindlus on esmatähtis Eesti majanduse toimimise seisukohalt. Strateegia aga majandusvaldkonna mõjutamist otseselt ei adresseerinud ning otseselt majanduskeskkonda või ettevõtlust mõjutavaid eesmärke strateegias polnud.

Nagu ka eelpool öeldud, pole küberjulgeoleku otsest mõju majandusele eriti uuritud. Töö autor otsustas siiski küsida ekspertide subjektiivset hinnangut strateegia mõjust majandusele, jättes teadlikult täpsustamata, mida majanduse ja mõju all täpselt silmas peetakse. See võimaldas aru saada vastanud ekspertide arusaamisest küberjulgeoleku laiemast, julgeolekupoliitikat

ületavast mõjust. Asjakohane on siinkohal märkida, et KJS 2008 koostajad on Euroopa Liitu käsitlevas osas muuhulgas arvamusel, et: „poliitikas tuleb selgelt eristada riigi julgeolekumõõdet ja majanduskeskkonda puudutavat osa ning teisalt üksikisiku õigusi ja turvalisust puudutavat osa.“

Küberjulgeoleku strateegial nägi otsest mõju majandusele 6 intervjueeritavat, kes kõik hindasid strateegia mõju positiivseks. Positiivse mõjuna toodi välja nii erasektori kaasamist küberjulgeoleku valdkonna toodete ja teenuste väljatöötamisel ja selle kaudu ka ettevõtete ekspordivõimaluste avardamist kui ka üldise (küber-)turvalisuse tõusu ning Eesti kui küberjulgeoleku valdkonnas innovaatori positiivset kuvandi mõju välisinvestoritele ja ekspordile.

3.2.2 KJS 2008 mõju julgeoleku- ja riigikaitse valdkonnale

Julgeoleku- ja riigikaitse valdkonna, ehk traditsioonilise julgeolekuvaldkonna arengut mõjutas strateegia ekspertide arvates väga tugevalt- 15 intervjueeritavat leidis, et strateegia on avaldanud valdkonnale positiivset mõju. Enamik vastanutest leidis, et selle mõju sõjalise riigikaitse valdkonnale oli väga suur, kuna Eesti leidis sellega NATOs oma teema, mille rolli nö „uste avajana“ on raske üle hinnata.

Tol ajal Siseministeeriumis töötanud ja hiljem Riigi Infosüsteemi Ametis (RIA) küberkriisideks valmisoleku valdkonda juhtinud Lauri Luht tõdeb intervjuus: “Strateegia omas sellele valdkonnale tohutut mõju. Nii eelpool mainitud NATO keskuse (CCDCOE) toomises Eestisse, Riigi Infosüsteemi Ameti (RIA) kui küberturvalisusega tegeleva ameti määratlemine[3], Kaitseliidu Küberkaitseüksuse (KL KKÜ) loomine, Siseministeeriumi valitsemisalas küberkuritegevuse vastase võitluse ja vastuluure sisustamise alustamine jne. Tekkis tohutu võimalus küberi sidustamise ja sisustamise kaudu saada ressurssi, mida ka erinevad asutused ära kasutasid. Lisaks saadi ka aru, et küberturvalisusega tegemiseks riigi tasandil on tarvis RIA-sse veidi rohkem kui vaid senist CERT-i. Ega tõenäoliselt päris täpselt ei teatud, kuid ressurssi igatahes eri teemadega tegelemiseks ressurssi eraldati. Suuresti selle tõttu suutsid ka uued energilised inimesed kasutada ära HOS (Hädaolukorra seaduse) tegemist 2008 aastal ja suruda küberi jaoks olulised teemad HOS-i sisse.“ (Luht 2018)

Endine Kaitseministeeriumi kantsler Lauri Allman lisab: “Strateegia omas suurt mõju. Arvestades, et KJS 2008 koostamist vedas KM (Kaitseministeerium), siis selle koostamine käis

[3] Riigi Infosüsteemi Amet (RIA) loodi valitsusasutusena 2011 aasta juunis, MKMi hallatava asutuse, Riigi Infosüsteemide Arenduskeskuse baasil.

kaasas reaalse võimearendusega. See andis uut hingamist juba 2003/2004 alanud NATO transformatsioonikampaania käigus Eesti KM poolt esitatud ideedele küberjulgeleku võimearenduseks.“ (Allman 2018)

CCDCOE teadur Kadri Kaska leiab samuti, et strateegia omas valdkonnale suurt mõju ennekõike teadvustamise tähenduses nii siseriiklikult kui ka NATOs. Kaska: “Riigisiseses plaanis mõjutas strateegia koostamise protsess ja selle tugev eestkõneleja (Heli Tiirmaa-Klaar) arengut vahest enamgi kui lõppdokument. NATOs andis KJS 2008 olemasolu Eesti häälele kaalu ja usutavust, laiemas plaanis toetas NATO CCDCOE edenemist ja liitlaste personali siia paigutamist, mistõttu oli pärast 2014. barjääri lihtsam ületada. KJS 2008 mõju julgeolekule ei olnud lineaarne ja ühene, aga keskkonda mõjutas see vaieldamatult ja pikemaajaliselt.“ (Kaska 2018)

Endine RIA rahvusvaheliste suhete juht ja enne seda Kaitseministeeriumis töötanud Luukas Kristjan Ilves hindab aga strateegia mõju valdkonnale laiemalt: „Oluline ümberkorraldus, sh MKM-le oluliste riigikaitseliste ülesannete määramine ning uue struktuuri loomine. Raske hinnata, kas see on olnud positiivne. Ühelt poolt oli see oluline samm laiapindse(ma) riigikaitse tekitamisel. Küberjulgeoleku artikli lisamine hädaolukorra seadusesse ning selle järgnev rakendamine RIA poolt oli esimene struktuurne riigikaitseline eraettevõtete hõlmamine.“ (Ilves 2018) Samuti tõdeb üks ekspert :„Kuna tänaseks on loodud küberväejuhatus, siis arvan, et selle vundamenti laoti KJS 2008 koostamisega.”

Asjakohane on siinkohal aga märkida, et tegelikult ei käsitlenud KJS 2008 otseselt riigikaitse ja julgeoleku probleeme ning seal polnud kajastatud ka selle valdkonna eesmärke. CCDCOE loomist käsitleti peatüki all „Tegevus rahvusvahelistes organisatsioonides“ lakooniliselt: „kindlustada NATO Küberkaitse Kompetentsikeskuse (CCDCOE) loomine Eestis ning keskuse akrediteerimine NATO poolt”.

Intervjueeritud eksperdi hinnangul omas strateegia peamiselt sümboolset, retoorilist ja ka inspireerivat tähendust: „Mõju oli kindlasti olemas, kuna strateegia koostamist ja elluviimist juhtis Kaitseministeerium. Kuigi riigikaitse aspekte strateegia ei käsitlenud ning teemad, mida käsitleti (kriitilise informatsiooni infrastruktuuri kaitse, infoturve, valdkonna kompetentsi suurendamine), otseselt kaitsevaldkonda ei kuulunud oli strateegia kaitse- ja julgeolekupoliitika oluline sümboolne ja retooriline instrument.“ Teine ekspert tõi samuti välja strateegia kaudse mõju aspekti: „Kaitseministeeriumi haldusalas pöörati antud teemale palju tähelepanu ning antud perioodi mahub CCDCOE sisuline käivitumine, Kaitseliidu

Küberkaitseüksuse (KL KKÜ) moodustumine ja Kaitseväe võimekuse kasv. Ei saa öelda, et see on kõik KJS 2008 otsene tulem, kuid KJS 2008 moodustas valdkonna arengut soodustava taustsüsteemi ning eelarveaastast pikema visiooni.“

Pernik tõdeb oma analüüsis, et strateegia elluviimise kestuse ajal peab olema võimalus vajaduse korral eesmärkide ja tegevuste muutmiseks või prioritiseerimiseks. Sellise täiendamismehhanismi puudumine tõi tema hinnangul kaasa ka selle, et paljud mõjukad küberjulgeolekualased algatused on teostatud väljaspool strateegia protsessi, näiteks tuues just kõik riigikaitse valdkonnaga seotud tegevused. (Pernik 2013) On tõesti ebaselge, miks neid tegevusi strateegias ette ei nähtud, kuna nii Kaitseliidu küberkaitseüksuse kui ka teiste riigikaitse valdkonna algatuste sünniaeg jääb strateegia loomisega samasse perioodi.

3.2.3 KJS 2008 mõju hariduse ja teaduse arengule

Strateegia hariduse ja teaduse arengule hindas positiivseks 10 intervjueeritut. Kõik hinnangu andnud tõdesid, et strateegia mõjutas valdkonna arengut konkreetsete algatuste kaudu. Üks intervjueeritud ekspert toob välja: „ KJS 2008 sisaldas punkte teaduse ja hariduse kohta. Üks konkreetsemaid tulemeid, mis minu jaoks sellega seondub, on TTÜ-TÜ küberkaitse magistriprogrammi[4] käivitumine 2009 (prototüüpmooduli katsetamine 2008), mille on tänaseks lõpetanud 190 magistrit. Mitmed neist jätkavad oma õpinguid doktorantuuris (sh vähemalt üks edukalt doktoritöö kaitsnud teadlane, kes jätkab oma teaduskarjääri Eestis). NATO CCD COE käivitumine antud perioodil oli samuti KJS 2008 ära märgitud kui toetamist vääriv. Ehkki tegemist oli paralleelselt käiva iseseisva protsessiga, andis see uue väljundi Eestis küberjulgeoleku teemadele keskenduvatele teadlastele, mis toetas KJS 2008 eesmärke ja vastupidi.“ Hariduse, teadus ja arendustegevuse valdkonnas seatud eesmärke hinnatakse strateegia analüüsis aga tagasihoidlikumalt: „Kuigi hariduse ning teadus- ja arendustegevuse (T&A) valdkondades on saavutused märkimisväärsed, siis kogu ühiskonda hõlmavat väga suurt infoturbealast kompetentsust ja teadlikkust saavutatud ei ole.” (Pernik 2013)

3.2.4 KJS 2008 mõju Eesti rahvusvahelisele tuntusele ja rahvusvaheliste suhete arengule

Strateegia mõju selles valdkonnas hindasid eksperdid positiivseks pea üksmeelselt: 18 vastanut olid arvamusel, et strateegia avaldas selles vallas positiivset mõju. Intervjuudes toodi välja just strateegia koostamise enda vahetut mõju innovaatilise „küberriigi“ kuvandi kujunemisele. Üks

[4] Tallinna Tehnikaülikooli ja Tartu Ülikooli ühine õppekava

intervjueeritud ekspertidest tõdeb: „KJS 2008 oli üks esimesi sellealaseid strateegiaid. See, kuidas peale 2007.a rünnakuid suudeti suhteliselt lühikese aja jooksul koondada erinevate valdkondade eksperdid ning suhteliselt kiiresti strateegia koostada, oli paljude arvates muljetavaldav. Eesti tegevustele, sh strateegiale on hiljem paljude poolt viidatud ning seda eeskujuks võetud.“ Üks tunnustatumaid Eesti küberturvalisuse eksperte, hilisem RIA juht Jaan Priisalu leidis, et kui Eesti ei oleks jätkanud strateegiliselt suunatud tegevusega, siis 2007 oleks jäänud üksikuks kurioosseks episoodiks ja strateegia lõi aluse Eesti tuntuse jätkumiseks (Priisalu 2018). Ka autori enda hinnangul väljendus strateegia positiivne mõju peamiselt just selle kaudu, et Eesti suutis end näidata võimekana uute julgeolekuohtudega toimetulekuks strateegilise planeerimise kasutamisel ning vastava kogemuse jagamisel oma liitlaste ja rahvusvahelise üldsusega.

3.3 Küberjulgeoleku strateegia 2014-2017 (KJS 2014) koostamine

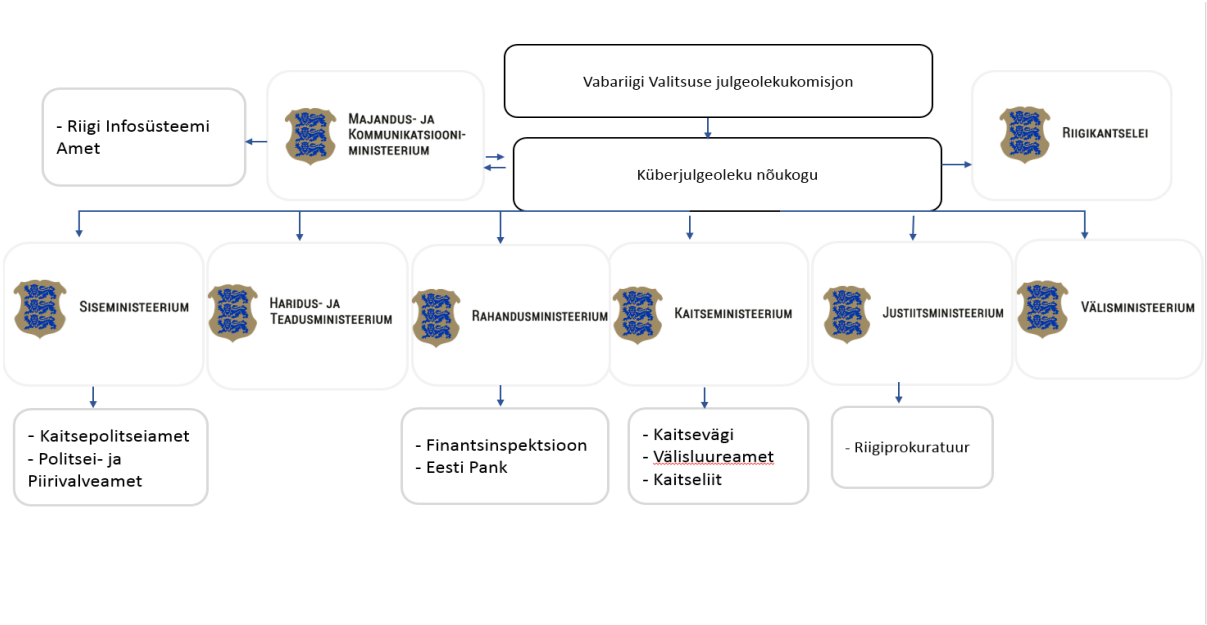
RKK poolt 2013. aasta kevadel koostatud analüüs (Pernik 2013) andis järgnevad poliitikasoovitused KJS 2008 koostamisel ja rakendamisel ilmnenud probleemide lahendamiseks, mis kattuvad pea täielikult avaliku halduse valdkonnas strateegiate koostamise sõlmküsimustega (Bryson 2011; Allison, Kaye 2005):

- Vajadus sidususe järgi teiste arengukavadega (nt. ühe ministeeriumi valitsemisala arengukavades peaksid sisalduma kõik selle ministeeriumi vastutusalasse kuuluvad KJSi eesmärgid.)
- Vajadus sidususe järgi eelarvevahendite planeerimisega (nt. kajastada rakendusplaanis iga tegevuse jaoks planeeritav summa /.../ja mille kohta antakse rakendusplaani täitmise aruandes aru.)
- Vajadus juhtkonna kaasamisele- suurendada poliitilise tasandi ja ametkondade kõrgeima otsustustasandi kaasatust /.../(tekitada „omanikutunne“ ministri, kantsleri ja asekantslerite seas) ning kasutada arengukava ministeeriumite töövahendina.
- Esitada jätkustrateegias või selle rakendusplaanis selge juhtimisstruktuuri kirjeldus.
- Lisaks rakendusplaani tegevuste teostajatele määrata kindlaks asutus, kellele kuulub peavastutus iga rakendusplaani tegevuse eest.
- Lähtuda jätkustrateegia eesmärkide ja tegevusvaldkondade kindlaksmääramisel hetkeolukorra analüüsist (sh küberjulgeoleku riskidest).
- Vältida jätkustrateegia rakendusplaanides kajastatud tegevuste ja projektide dubleerimist teistes strateegilistes dokumentides.

21. märtsil 2013 kiitis valitsus korraldusega nr 114 heaks „Küberjulgeoleku strateegia 2014–2017” koostamise ettepaneku (MKM 2012). Uues strateegias, mida nimetatakse ka jätkustrateegiaks (Pernik 2013), plaaniti kokku leppida info- ja kommunikatsioonitehnoloogiaga seotud riskide kindlakstegemise, haldamise ning maandamise üldised riiklikud eesmärgid ning viisid ja vahendid nende eesmärkide saavutamiseks. Strateegia koostamine ja järelevalve selle rakendamise üle oli täielikult üle viidud Kaitseministeeriumist Majandus- ja Kommunikatsiooniministeeriumi. Arengukava sihid ja tegevused puudutasid ettepaneku kohaselt viit valdkonda: kriitilise informatsiooni infrastruktuuri kaitset; infoturbealase kompetentsuse suurendamist; küberjulgeoleku tagamiseks vajaliku õigusruumi kujundamist; rahvusvahelist koostööd ning teavitustegevust.

Strateegia koostamise protsessi üldise koordineerijana nähti ette Küberjulgeoleku nõukogu, peamiselt ministeeriumide Vabariigi Valitsuse Julgeolekukomisjoni alakomisjoni, mis loodi KJS 2008 rakendamise raames. Küberjulgeoleku nõukogu (KJN) juhib Majandus- ja kommunikatsiooniministeeriumi kantsler ja selle koosseisu kuuluvad Kaitseministeeriumi, Siseministeeriumi, Välisministeeriumi, Justiitsministeeriumi, Rahandusministeeriumi, Haridus- ja teadusministeeriumi ja Majandus- ja kommunikatsiooniministeeriumi kantslerid, Riigikantselei, Kaitseväe, Riigi Infosüsteemide Ameti, Politsei- ja piirivalveameti, Kaitsepolitsei Ameti ning Teabeameti esindajad. (MKM 2012) . Antud juhtimisstruktuur on käibel ka praegu.

Joonis 2: Küberjulgeoleku nõukogu ja valdkonna juhtimisstruktuur (KJS 2018)



Strateegia koostamise ettepanekus (MKM 2012) pöörati suurt tähelepanu kaasamisele: koostamise protsessi plaaniti peamiste partneritena kaasata NATO CCDCOE, Rahvusvaheline Kaitseuuringute Keskus, erialaliidud ja teadusasutused. Strateegia koostamist nähti ette selle jaotamist mitmetesse töögruppidesse, mida juhiks KJNi poolt volitatud juhtgrupp. Sealhulgas oli plaanis luua riigikaitse töögrupp, mille ülesandeks oli tegeleda riigikaitseliste küberjulgeolekualaseid eesmärke määratlemisega. Siinkohal on asjakohane eraldi märkida, et ettepanekus märgitud strateegia eesmärkide seas polnud sarnaselt KJS 2008iga planeeritud riigikaitse aspekti eraldi käsitleda, kuigi vastav töögrupp oli planeeritud luua.

Strateegia koostamise lähtekohtadena tuuakse välja (*ibid*) vajadust leida tasakaal erinevate valdkondade vahel, mille all mõeldakse olukorra lahendamist, kus KJS 2008 eesmärke pole ministeeriumite arengukavades piisavalt kajastatud, ehk pole tagatud sidusust teiste arengukavadega (Pernik 2013). Koostajad viitavad ka vajadusele lähtuda eesmärkide seadmisel reaalsetest eelarve võimalustest. Kitsamate probleemidena nähakse vajadust kaasajastada kriitilise informatsiooni infrastruktuuri riskianalüüsid ning nähaklse lahendamist vajava probleemina ka Eesti tegelikku suutlikkust olla rahvusvaheliseslt küberjulgeoleku eestkõneleja.

17.09.2014, s.t rohkem kui aasta peale strateegia koostamise ettepaneku heakskiitmist ja peaaegu 2 aastat peale strateegia koostamise ettepaneku valitsusele esitamist (20.12.2012), võttis Vabariigi Valitsus vastu korralduse nr 390, millega kinnitati „Küberjulgeoleku strateegia 2014–2017" ja selle rakendusplaani aastateks 2014–2017 heakskiitmine. Koostamise ettepaneku kohaselt oli strateegia kooskõlastamiseks esitamise tähtajaks 1. oktoober 2013 (tegelik 10.03.2014) ja lõpptähtaeg Vabariigi Valitsusele esitamiseks on 1. detsember 2013 (tegelik 01.07.2014) (MKM 2012). Seega oli KJS 2014 koostamise ajaraam oluliselt pikem KJS 2008 omast, mis pidi plaani järgi mahtuma kõigest paari kuu sisse.

KJS 2014 üldeesmärgiks oli: „suurendada küberturvalisuse alast võimekust ja inimeste teadlikkust küberohtudest, tagamaks jätkuvat usaldust küberruumi vastu". KJS 2014 koostamise ettepanekus (MKM 2012) sõnastati ka järgmised alaeesmärgid:

1) Eesti kriitiliste teenuste infosüsteemid on küberohtude eest kaitstud;
2) Küberkuritegevusvastase võitluse tõhustamine;
3) Riigikaitselased võimed küberkaitse valdkonnas on välja arendatud;
4) Küberturbelahendusi loovatest ja pakkuvatest ettevõtetest on tekkinud tärkav majandusharu;
5) Toetustegevuste arendamine on tagatud;

Strateegia koostamise ettepanekus algselt toodud eesmärgid leidsid strateegia koostamise käigus olulist täiendamist ja muutmist. Lisandusid majanduse arengut mõjutavad eesmärgid, (sõjalise) riigikaitse küberkaitse arendamise mõõde ning küberkuritegevuse vastase võitluse tõhustamine.

Intervjueeritud eksperdid KJS 2014 loomise protsessi suhtes valdavalt kriitilised ning neist 8 osutasid tõsistele puudustele strateegia koostamise protsessi juhtimises. Eksperdid avaldasid arvamust, et: "peamiseks probleemiks oli vilets koordineeritus (sisuliselt koordineerimatus) MKMi poolt, sh vähene/olematu sisuline huvi asja vastu MKMis. See tingis omakorda selle, et koostööd/kaastööd oli vähe, arutelusid oli üksikuid ning nendest ei koorunud uut kvaliteeti (ega isegi kvantiteeti)". Teine intervjueeritud ekspert tõi samuti välja puudused MKMi poolses strateegia loomise juhtimises: "MKM poolne vedamine – mitu korda sai hobust vahetatud, veidi põlve otsas tegemine tuli lõpuks välja. Polnud ka sisulist fookust, et koostöö just paika saada + ressursside poolele tähelepanu ei jagunud", sama tõdes ka kolmas intervjueeritu: "Korralduslikult: kaootiline koordinatsioon (vahetuvad strateegia koordinaatorid)" . Kriitikat jätkus strateegia koostamise juhtimisele pea kõigi intervjueeritud ekspertide poolt: "Halb koordinatsioon, alates mingist hetkest teiste asjaosaliste eiramine koostajate poolt, samuti liigne kiirustamine. Sisuliselt eirati KJS 2008 rakendamise kohta tehtud kriitikat.", samuti toodi peamise probleemina välja: "Kiirustamine, vastuolud ametkondade ja isikute tasandil, huvipuudus, *leadershipi* ja *ownershipi* puudus" ja "Valdkonna ja strateegia koostamise protsessi halb juhtimine, kõik muu tulenes sellest" ning "Selge eestvedamise puudumine, koostajate erinev teadlikkus valdkonnas ning erinevad arusaamad probleemist ja sümptomist". Üks intervjueeritav seadis kahtluse alla ka kogu dokumendi kvaliteedi, seostades seda "Kiirustav, pinnapealne ja lõppastmes diletantlik eestvedamine. Ei otsitud visiooni ega kvaliteeti, otsiti tähtaegselt valminud paberit, öelgu see mida tahes."

Paraku jäi ka huvigruppide laiapõhjalise kaasamise plaan strateegia koostamisel osalenud autori hinnangul tegelikkuses napiks ning enamike töögruppide sisuline töö ei käivitunudki, mis avaldas ka otsest mõju dokumendi lõppkvaliteedile. Ekspertide hinnangul oli probleemiks: „Veniv protsess vähese omanduse ja kaasamisega. Osalemine liiga madalal tasemel riigi poolt. Vähene laiem konsulteerimine erasektori ning Eesti ühiskonna ning ka liitlastega. Üldiselt ebastruktuurne ning juhuslik." Samuti toob teine ekspert välja: „süstemaatilise situatsiooni ja haavatavuste teadusliku uurimise puudumine. Koostati peamiselt ametnike teadmistest lähtuvalt ametkondade vahelise kokkuleppena."

Nagu juba eespool öeldud, anti küberjulgeoleku koordineerimine valitsuse otsusega Kaitseministeeriumilt üle Majandus- ja Kommunikatsiooniministeeriumile. Valitsuse tegevusprogramm 2011–2015 teeb kaitseministeeriumi küll vastutavaks KJS 2008i elluviimise eest aastatel 2008–2013, kuid KJS 2008 juhtimisstruktuurina nähtud KJNi tegevust juhib MKM. Selline vastutuse hajumine ei aidanud kaasa KJS 2008 eesmärkide täitmisele (Pernik 2013). Uue strateegia, KJS 2014 koostamist ja rakendamist koordineeris täielikult MKM.

Kuigi osad intervjueeritavad pidasid MKMile küberjulgeoleku valdkonna koordinaatori ülesannete andmist positiivseks arenguks ning märgiks laiapindse riigikaitse kontseptsiooni rakendamise kohta, seati kahtluse alla nii MKMi pädevus kui ka huvi valdkonna sisulise koordineerimise vastu. MKM võttis küll riigi infosüsteemide osakonna juurde tööle valdkonnaga tegeleva töötaja, kuid nagu ka eelnenud intervjuudest selgus, seostati tekkinud raskusi ametikohal töötavate inimeste vahetumisega. Korduvalt viidati ka MKMi rolli ebaselgusele, sest kuigi KJS 2014ga on MKMile pandud vastutus küberjulgeoleku poliitika juhtimise ja strateegia elluviimise eest, polnud see ülesanne kajastatud ministeeriumi tegevust korraldavates õigusaktides. Ainuke säte MKM-i põhimääruses, mis võiks viidata sellisele ülesandele, on põhimääruse §20 p1, mis sätestab, et MKM-il on riigi infosüsteemide osakond, mille ülesandeks muuhulgas on riigi infopoliitika ja strateegia kujundamine informaatika valdkonnas ning vastavate õigusaktide eelnõude ettevalmistamine. Sellist regulatsiooni ei pea õiguseksperdid aga korrektseks, kuna MKM-i osakondade ülesanded peaksid jääma MKM-i valitsemisala ja põhiülesannete piiresse. Antud juhul on ühele MKM-i osakonnale antud ülesandeid, mille puhul on kaheldav, kas need on hõlmatud MKM-i valitsemisala ja põhiülesannetega. (Lextal... 2016, 43) Väärib märkimist, et hoolimata korduvatest ettepanekutest (Pernik 2013, Lextal...2016) pole küberjulgeolekupoliitika alased ülesanded siiani MKMi põhimääruses kajastatud (MKM põhimäärus 2017).

Strateegia rolli osas poliitika planeerimise instrumendina olid eksperdid erinevatel seisukohtadel, kuid valdavalt tõdeti, et KJS 2014 on selles rollis hädisem kui KJS 2008. Viis eksperti oli arvamusel, et strateegia siiski oli poliitika instrumendiks, seitse väljendasid aga arvamust, et strateegia kas polnudki plaanitud seda rolli täitma või ei sobinud selleks oma sisuliste vajakajäämiste tõttu. Negatiivse poole pealt tõid eksperdid välja: „Tervikliku poliitika planeerimist, pikemast visioonist rääkimata, KJS 2014 abil ei otsitud ega ole suudetud saavutada.“ ja „/.../strateegiline ambitsioon oli (võrreldes KJS 2008) märksa väiksem, strateegia sai üsna silmapaistmatu (paljude teiste riikide hulgas, kes olid oma strateegiad selleks ajaks koostanud), sihiks oli võetud praktiline, rakendatav ja mõõdetav tulemus, aga sellevõrra kannatas dokumendi ambitsioon ja loetavus.“ Üks ekspertidest võtab hinnangu kokku järgmiselt: „Poliitika planeerimise instrumendina oli ta kindlasti mõeldud. Eraldi küsimus on see, kui palju sellest reaalselt hiljem lähtuti tegevuste ja muude poliitikate planeerimisel. /.../Jätkuvalt ei jõudnud strateegia eesmärgid asutuste tööplaanidesse ega investeeringutesse. Õigusruumi analüüs ja korrastamine, mis oli ette nähtud juba KJS 2008 poolt, tehti sisuliselt osaliselt tingituna välise surve mõjul ära alles 2018.“

KJS 2014 seost teiste arengukavade hinnatakse ekspertide poolt positiivsemalt- kuue eksperdi arvamuse kohaselt oli olukord parem kui KJS 2008 puhul: „Kuna tegemist oli juba teise strateegiaga ning teadlikkus oli selleks ajaks tõusnud ka mujal, siis sellega arvestati rohkem ning vähemalt kohati üritati neid teiste dokumentidega nö linkida.“ Vaid kaks vastanut leidsid, et olukord oli hullem kui KJS 2008 puhul. KJS 2014 kohta koostatud analüüs (Rebane, Veiler 2018) polnud hinnangutes nii suuremeelne: „2014. aasta strateegia laiapindsus ja kõikide valdkondade katmine andis tervikpildist dokumendina hea ülevaate, kuid nõrkuseks oli sisemiselt ebapiisav sidusus: küberturvalisust käsitleti strateegias üksikute turvalisuste summana, kuid strateegilise planeerimise kui terviku tagamisega ei tulnud kehtiv strateegia piisavalt toime. Strateegia kehtivusperioodi jooksul sai ilmseks, et selline lähenemine ei suuda vältida oluliste funktsioonide dubleerimist ja väheste ressursside killustumist ning et olemasolev killustatus ei lahene iseenesest, eesmärkide ühte dokumenti koondamise teel.“

KJS 2014 põhieesmärkidena nimetasid intervjueeritavad peamiselt esimese strateegia eesmärkide elluviimise jätkamist ja valdkonna edasist arendamist. Mõne vastanu arvates püüti uue strateegiaga eesmärke täpsustada ning „rohkem detaili minna“, teised avaldasid aga arvamust, et pigem püüti esimese strateegiaga kaasnenud detailsusest lahti saada. Enamik strateegia põhieesmärgi kohta käivale küsimusele vastanutest rõhutab aga eesmärgi ebamäärasust ja sõnumite ebaselgust, näiteks toob üks ekspert: „Üldeesmärk/visioon on üsna laialivalguvalt sõnastatud ja sellele küsimusele on raske vastata. Strateegia põhifookus on selgelt kriitiliste teenuste infosüsteemide kaitsel ja võib öelda, et edasiminek strateegias sätestatud suunas oli märgatav koos KüTS (Küberturvalisuse seadus, jõustus mais 2018) regulatsiooni jõustamisega.“ Kuigi KüTSi väljatöötamisel lähtuti ennekõike vajadusest jõustada Eestis Euroopa Liidu Võrgu- ja Infoturbe Direktiiv (NIS), võeti seaduse väljatöötamisel paljus arvesse ka KJS 2008 ja KJS 2014 seatud eesmärke (KüTS 2018).

3.4 Kokkuvõte hinnangutest KJS 2014 koostamise ja rakendamise mõjudele

Käesolevas töö osas on uuritud ekspertide hinnanguid II küberjulgeoleku strateegia mõjude kohta majandusele, julgeoleku- ja riigikaitse valdkonnale, haridus- ja teadusvaldkonnale ning rahvusvahelisele suhtlusele. Kokkuvõttes olid eksperdid KJS 2014 mõjude suhtes palju skeptilisemad ja kriitilisemad kui KJS 2008i tulemusi hinnates, jäädes positiivsetes hinnangutes väga tagasihoidlikuks. Erinevalt eelmisest strateegiast oli KJS 2014 puhul aga tänu paremale indikaatorite süsteemile võimalik paremini hinnata strateegia eesmärkide täitmist üldiselt. Strateegia analüüsis tõdetakse, et eesmärkide saavutamise mõõdikute määratlemine oli õige ambitsioon ning kvantifitseeritavate sihtide seadmine leidis tähelepanu ja järgimist

vääriva praktikana äramärkimist ka rahvusvaheliselt, muuhulgas tugevdades Eesti positsiooni rahvusvahelistes küberturvalisuse indeksites. Strateegia elluviimisel selgus siiski, et paljud mõõdikud olid mittesisulised, nende formuleerimisele ei eelnenud piisavat analüüsi ning need ei suutnud seetõttu toetada pikaajalist strateegilist planeerimist. (Rebane, Veiler 2018)

3.4.1 KJS 2014 mõju majandusele

Erinevalt KJS 2008st oli KJS 2014 üheks eesmärgiks just majandusele positiivse mõju avaldamine, eesmärgiks oli soodustada küberturbelahendusi pakkuvate ettevõtete arengut. Eesmärgi täitmise edukuse mõõtmise indikaatoriks küberturbelahendusi loovate ning pakkuvate teadus- ja arendustegevuse asutuste ja ettevõtete osakaalu tõus majanduses (käibe alusel, suhtena SKPsse) vähemalt kahekordseks võrreldes 2013. aasta tasemega, mida polnud aga kindlaks määratud. Siiski hindas MKM Startup Estonia poolt koostatud mitteametliku ettevõtete kaardistuse põhjal, et kasvanud on nii ettevõtete arv kui ka käibe maht (Rebane, Veiler 2018).

Arvamust avaldanud seitsmest eksperdist nägid viis mõju pigem negatiivses värvingus, kuid üks ekspert tõdeb: „ KJS 2014-ga arenguhüpet ei tulnud, seega eristatav ühiskondliku mõõduga mõju on ilmselt väiksem kui KJS 2008 puhul. Päris tähelepanuta ei tasu jätta strateegia rakendamiseks kulutatud Euroopa Liidu struktuurifondide raha tähendust, aga ma ei tea, kuivõrd see on kulunud üritusturismi ja kommunikatsioonivaldkonda. Sektoraalne mõju seeläbi, et on kasvatatud nõudlust turbeteenuste, -testimise ja auditeerimise + kompetentsi järele, on kaalukam. Alahinnata ei tasu strateegia olemasolu fakti Eesti tajumisel turvalisusse investeeriva riigina. See töötab kokku Eesti digiriigi kuvandiga ja on mõjutatud ka üldisest majanduskeskkonnast ja turvalisusest, seega KJS 2014 puhast mõju on jällegi keeruline eristada.“

3.4.2 KJS 2014 mõju julgeoleku- ja riigikaitse valdkonnale

Riigikaitset käsitlev eesmärk strateegiasse selle koostamise käigus, algses strateegia koostamise ettepanekus seda polnud, mis annab autori arvates tunnistust strateegia koostamise protsessi paindlikkusest. Eesmärgiks oli tagada küberruumi kaitse aspekti kajastamine riigikaitse laias planeerimises, saavutades olukorra, kus küberkaitse on osa igapäevasest riigikaitsest. (KJS 2014)

Kasutatud termin küberkaitse pärineb esimesest strateegiast, kus see on avatud kui: „riigi kriitilise infrastruktuuri toimimist toetavate info- ja sidesüsteemide kaitse korraldamine, mis seisneb nii infotehnoloogiliste, organisatoorsete kui ka füüsiliste turvameetmete kasutuselevõtmises ja ajakohastamises“ (KJS 2008).

Viidete otsimisel, kuidas küberkaitse on laiapindses riigikaitses kajastatud, on avalikest allikatest leitav deklaratsioon, et Kaitseministeeriumi valitsemisala jätkab küberkaitse tähtsustamist nii rahvusvaheliselt kui riigisiseselt, kasutades selleks muulhulgas Kaitseliidu küberkaitseüksuse ning CCDCOE koostööst tekkivat sünergiat (Kaitseministeerium 2013). Kahjuks ei ole selle deklaratsiooni põhjal võimalik hinnata ja mõista, kuidas küberjulgeoleku aspekt riigikaitses tegelikult kajastatud on.

Strateegia kirjeldab riigikaitse valdkonna eesmärke aga üpris detailselt. Riigikaitseliste võimete arendamise all küberkaitse valdkonnas peetakse silmas olukorda, kus riigi käsutuses olevad tsiviil-, sõjalisel ja rahvusvahelisel koostööl põhinevad ressursid peavad suutma toimida adekvaatselt ka küberruumis ja riigikaitselised ressursid moodustama terviku riigi tsiviilstruktuuride juhtimisel toimiva küberruumi kaitsega, mis on väga ambitsioonikas eesmärk, kuna eeldab sisuliselt keskse juhtimisstruktuuri loomist. Nähakse ette ka sõjalise planeerimise ning tsiviilhädaolukordadeks valmistumise koordineerimist laiapindse riigikaitse põhimõtetest lähtuvalt ja rõhutatakse küberkollektiivkaitse ja rahvusvahelise koostöö arendamise vajadust. Küllalt täpselt kirjeldatakse ka sõjalise kaitse kübervõimeid: eesmärgiks on olukord, kus sõjalise kaitse kübervõimete arendamise tagajärjel on küberkaitse osaks laiapindsest kollektiivkaitsest. Rõhutatakse vajadust tagada riigikaitse valdkonna kõrge teadlikkus ja nähakse vajadust süsteemse koolitusprogrammi järele . (KJS 2014) Arusaadavatel põhjustel pole dokumendid, mis annaks võimalust strateegia täitmist hinnata, avalikkusele kättesaadavad ning piirduda tuleb analüüsis (Rebane, Veiler 2018) hinnanguga ja ekspertide poolt antud hinnangutega, mis annavad eesmärkide täitmisele positiivse hinnangu.

Intervjuudes asub aga osa eksperte täiesti vastupidisele seisukohale. Intervjueeritud ja riigikaitse valdkonnas tegevad olnud eksperdid avaldasid KJS 2014 mõju kohta riigikaitse valdkonnale arvamust, et: „Pigem mädalt, enamus asjad, mis ära tehti oleks tehtud ilmselt ka ilma strateegiata. Paljud asjad, mis tegemata on, omaks ilmselt täiendavat mõju.“, samuti „Vähemal määral kui KJS 2008, kuna KJS 2014 omanik ja eestkõneleja oli MKM, siis rakendati seda julgeolekupoliitiliselt vähem ja ma arvan, et ka riigikaitse valdkondade arengule ei olnud strateegial olulist mõju, kuigi KJS 2014 strateegia ja rakendusplaan käsitlesid seekord

ka küberkaitse aspekte.“ Kolmas ekspert asus seisukohale, et: “ Strateegias defineeritud julgeolekut ja riigikaitset puudutavad tegevused oleks tehtud ära strateegiaga või ilma; strateegiaprotsess üksnes motiveeris kavatsusi ära sõnastama, aga ei sidunud neid teiste vastutusaladega.“

Ekspertide enamuse arvamus pole üldiselt aga siiski nii kriitiline, küsitletutest seitse hindas KJS 2014 mõju valdkonnale positiivseks ja viis negatiivseks. Positiivsena tuuakse välja kaasatuse fakti ennast: „Sõjaline riigikaitse oli seekord hõlmatud ja aitas kindlasti kaasa küberi teadlikkuse tõstmisele sõjalises juhtimises.“ Samuti nähakse strateegia koostamisel mõju küberjulgeoleku aspekti teadvustamisel laiapindses riigikaitses: „Küber sai julgeoleku kavandamise ja laiapindse julgeoleku käsitluse osaks + tugevamalt riigikaitse alal suunana sisse.“

Püüdes KJS 2014 mõjule selles valdkonnas objektiivset hinnangut anda, ei saa siiski mööda vaadata asjaolust, et nii küberjulgeoleku kajastatus riigikaitse arengukavas ja eriti küberväejuhatuse loomine 2018 aasta suvel (ERR 2018) annavad tunnistust küberjulgeoleku käsitlemist riigikaitse osana ja nii KJS 2008 kui ka KJS 2014 koostamise protsessil oli sellele kindlasti tugev mõju.

4.4.3 KJS 2014 mõju hariduse ja teaduse arengule

KJS 2014 käsitleb haridus- ja teadusvaldkonda mitmes osas. Esmalt nähakse “Eesti maandab võimalikke küberjulgeolekuohte” nimelises alaeesmärgis ette, et:“küberjulgeoleku võime tagamiseks ja tõstmiseks võtab Eesti kasutusele sõltumatud küberturbelahendused, mida toetavad küberturbealane väljaõpe ja treeningvõimalused, teadus ja arendustegevus ning ettevõtlus.“ Tegevuste all täpsustatakse, et: “küberjulgeoleku spetsialistide järelkasvu tagamiseks luuakse täiendavaid rahvusvahelisel tasemel kõrgharidust ning täienduskoolitust pakkuvaid õppevorme (KJS 2014).“ Haridusteemat on käsitletud ka küberkuritegude vastast võitlust käsitlevas osas, kus tõdetakse, et üldsuse kõrgem teadlikkus küberjulgeolekuriskidest aitab ennetada küberkuritegevust ning nähakse lahendust küberteemade käsitlemisel kõikides haridustasemetel ning uuringutel ja analüüsidel põhineval teavitustegevuses. Tõdetakse ka, et küberjulgeoleku tagamist toetab intensiivne ja rahvusvaheliselt konkurentsivõimeline teadus- ja arendustegevus, mille all mõeldakse peamiselt tehniliste lahenduste loomist. Ühe huvitama eesmärgina nähakse ette ka küberjulgeoleku lahenduste targa tellimuse arendamist, kus turvaliste lahenduste loomiseks vajalikku teadus- ja arendustegevusse panustataks riigi toel.

Ette nähti ka vastavat tegevust koordineeriv ning riigikaitset, julgeolekut, majandusarengut ja akadeemilist ringkonda koondava nõukogu loomist (*ibid*), mille mitteteostumisest on autoril kõige enam kahju.

KJS 2014 seadis haridusvaldkonnas konkreetseks eesmärgiks Eestis tegutsevate kõrgharidusega küberturbespetsialistide arvu kahekordistumist 2017. aastal (võrreldes nende arvuga 2013. aastal). Kõrgharidusega küberturbespetsialistide all mõeldakse kas küberjulgeoleku erialadel akadeemilise kraadi omandanud ja/või küberjulgeolekuga seotud ülesannetega tegelevaid IKT kõrgharidusega spetsialiste. Strateegia analüüsis tõdetakse, et kuigi algastet ehk 2013. aastal valdkonnas tegutsenud spetsialistide täpset arvu teada pole ja eesmärgi täpne mõõtmine seega võimalik pole, on kvalitatiivse hinnangu kohaselt kõrgharidusega küberturbespetsialistide arv võrreldes 2013 aastaga vähemalt kahekordistunud. Täpset hinnangut oodatakse Praxise poolt läbiviidavast tööjõuvajaduse uuringust hiljemalt 2019. aasta alguseks.(Rebane, Veiler 2018)

Olgugi, et töö autor osales ise KJS 2014 väljatöötamisel ja rakendamisel, on raske ka tagantjärele hinnata, miks mõistlikud eesmärgid nagu nn tarka tellimust koordineeriva ekspertide nõukogu loomine, täiendavate õppevormide loomine jms lõppesid strateegia rakendamise edukuse hindamisel vaid kõrgharidusega küberturbespetsialistide arvu kasvu mõõtmisega. Arvestades kasvõi TTÜ poolt küberjulgeoleku eriala magistriprogammis 2013-2018 ettevalmistuse saanud tudengite arvu, on selge, et nende arvu kasv oli loomulik ning oleks pidurdunud vaid juhul, kui TTÜ oleks vastava õppekava sulgenud.

Strateegia mõju hinnangud ekspertide poolt olid küllalt erinevad- mõju hinnati negatiivses toonis viiel juhul, kuid neli eksperti leidis siiski, et mõju oli üldiselt positiivne. Näiteks toodi mõju hindamisel välja, et: " Pigem positiivset – sest mõtteharjutusena ja mõttesuundade ühtlustajana on mõlemad strateegiad oma eesmärki täitnud. Mõlemad KJS-id on siiski andnud valdkonna innovaatoritele võimaluse tuua mõni teema lauale." Samuti märkis üks ekspert: „Üldiseks eesmärgiks oli küberkaitse algteadmiste viimine iga põhikooli ja gümnaasiumi lõpetajani aineõpetajate kaudu ning liikuda süsteemsemate teadmiste andmiseni vastava ainekava kaudu. Rahvusvahelise küberkaitse suvekooli korraldamine doktorantidele ja noortele spetsialistidele, võistluste korraldamine õpilastele. Magistrikava edasine arendamine. Strateegia olemasolu aitas selleks kaudselt kaasa." Avaldati ka eelmisele täiesti vastupidist arvamust: „TTÜ/TU küber magistriprogramm on vast ainus asi mis tehtud on aga muus osas ja üldhariduskoolis antud teemaga tegelemine on nulli lähedane.", samuti: „Üksikud head

initsiatiivid – näiteid ju on, alates Põltsamaa ja Kehtna koolidest kuni krüpto magistrieriala käivitamiseni – ei pööra veel keskkonda. Süsteemseks lähenemiseks ei ole olnud poliitilist eestvedamist ja talendi juurdekasvatamine on lastud isevooluteed.“ Põltsamaa ja Kehtna koolide näide viitab neis koolides alguse saanud initsiatiivile pakkumaks õpilastele võimalust saada keskhariduse küberturvalisuse valdkonna süvendatud õpet, mis tõi näiteks Põltsamaa koolile 2017 aastal kaasa ka rahvusvahelise tunnustuse Euroopa kuriteoennetusauhinna näol (Maaleht 2017).

Autor asub intervjuude, analüüsi ja isikliku kogemuse põhjal seisukohale, et KJS 2014 rakendamine haridus- ja teadusvaldkonnale planeeritud mõju ei saavutanud. Samas aitas nii strateegia koostamise protsess ja selle hilisem rakendamine küberjulgeoleku aspektil tähelepanu hoida ja seda arvestada.

4.4.4 KJS 2014 mõju Eesti rahvusvahelisele tuntusele ja rahvusvaheliste suhete arengule.

KJS 2014 ambitsioonid ja eesmärgid on ka selles valdkonnas küllalt detailselt kirjeldatud ning seda on võimalik käsitleda konkreetse tegevusplaanina nö rahvusvahelise küberpoliitika vallas. Põhiliselt keskendutakse esindatusele ja nähtavusele rahvusvahelistes organisatsioonides Eesti seisukohtade levitamisel, inimõiguste ja põhivabaduste kaitsele küberruumis ja ka interneti haldamise temaatikale. Ühe eesmärgina nähakse EL tegutsemisvõime tugevdamist küberjulgeoleku vallas, tõstes liikmesriikide teadlikkust ja ühtse küberjulgeolekupoliitika arendamist. Loodetakse panustada ka küberjulgolekualase oskusteabe ja kogemuste jagamisele, strateegia näeb ette ka piiratud võimalustega vabakonnaga riikides abikäepoliitika ja turvaliste e-lahenduste propageerimise kaudu vaba ja turvalise küberruumi tekkele kaasaaitamist. Tõdetakse vajadust arendada ja tihendada koostööd liitlaste, partnerite ja lähinaabritega ning laiendada koostööformaati samameelsete riikidega.

Ekspertide arvamused jaotusid ka selle küsimuse hindamisel pea võrdselt. Seitse eksperti hindas mõju positiivses valguses ja kuus pigem negatiivselt. Positiivsetest hinnangutest võib iseloomustavana välja tuua: “Jällegi, siin on raske eristada KJSi Eesti muudest initsiatiividest, aga KJS 2014 olemasolu fakt on olnud toetav Eesti kaalukuse kinnistamisel. Mõni KJS 2014 valdkondlik probleemipüstitus on aidanud Eestil teatud teemasid rahvusvaheliselt vedada (nt piiriülesed ja ristsõltuvused; õppused riigikaitsevaldkonnas). Partneritel on olnud meie strateegiasse rohkem usku kui meil endil, olen korduvalt kogenud.“ Negatiivse hinnangu andjad rõhutasid peamiselt uudsete mõtete ja ambitsiooni puudumist: „Julgen öelda, et mitte

eriti. Virtuaalsaatkonnad ja digitaalne järjepidevus on pälvinud kindlasti tähelepanu, kuid väga paljud muud asjad on sarnased teiste riikidega. Lisaks ei avaldatud ju strateegiat kogu mahus ning üldisel tasemel ei tekitanud see minu hinnangul liiga palju lainetust väljaspool Eestit. Küll aga võis mõjuda nii mõnelegi riigile positiivsena sõnum, et Eesti keskendub asjade tõhusamaks muutmisele (...ju siis suuresti kõik juba olemas ja tehtud...)." Iseloomulik on ka arvamus : „KJS 2014 ajaks olid juba paljud maailma riigid koostanud ja vastu võtnud sarnased dokumendid. Seega tähelepanu sai Eesti kindlasti vähem. Kui 2007 sündmustest veel räägiti, siis strateegiatest enam niiväga mitte. KJS 2014 ei olnud ka nii ambitsioonikas, kui selles valdkonnas järjekorras teise instrumendina oleks võinud olla. Järjest rohkem hakkas tekkima olukord, kus maine ja *hype* olid suuremad kui reaalselt astutud sammud."

Strateegia analüüs on selle valdkonna hindamisel suhteliselt napisõnaline, tõdetakse, et Eestit loetakse endiselt rahvusvaheliselt küberjulgeolekupoliitika eestvedajaks ning Eesti suhted oluliste partnerriikidega on tugevad, toimivad NB8 ja B3 koostööformaadid[5], samuti nenditakse, et NATO ja EL koostööformaatides on küberjulgeoleku- ja turvalisuse teemade osatähtsus oluliselt suurenenud ning Eesti on mänginud olulist rolli ühtsete poliitikate suunamisel.(Rebane, Veiler 2018)

2014. aastaks kui KJS 2014 koostati, oli Eesti rahvusvaheline maine ja tuntus küberjulgeoleku valdkonnas väga kõrge. Ühe näitena võib tuua sama aasta sügisel allkirjastamiseni jõudnud lepingut Ameerika Riikide Organisatsiooniga (OAS), mille raames Eesti eksperdid nõustasid mitme aasta jooksul küberjulgeoleku strateegiate ja poliitikate väljatöötamist Ladina-Ameerika riikides (OAS...2014).

[5] Viidatud on Põhjala ja Baltimaade küberpoliitika koostööformaadile NB8 ja Balti riikide regulaarsele koostööle küberkaitse vallas B3

4. LÕPPJÄRELDUSED JA POLIITIKASOOVITUSED

Eesti asub täna rahvusvahelistes küberjulgeolekut käsitlevates edetabelite tipus (ITU 2017, EGA 2018). Eesti edusamme küberjulgeoleku tagamisel on maailmas korduvalt eeskujuks toodud ning vaieldamatult on tegemist Eesti kuvandi olulise osaga, mis eristab meid positiivselt teistest endistest Nõukogude Liidu poolt okupeeritud riikidest. Ka kõik intervjueeritud eksperdid tunnistavad küberjulgeoleku valdkonda Eesti teatud mõttes edulooks, tunnistades Eesti suurimaks saavutuseks peale rahvusvahelise maine just siseriikliku toimiva süsteemi loomist, mis on võimaldanud Eestil viimase 10 aasta jooksul ära hoida või lahendada kõik suuremad küberintsidendid. Eesti edu nn ID kaardi kriisi lahendamisel või sisuliselt puutumata jäämine maailmas 2017. aastal suurt kahju põhjustanud WannaCry ja NotPetya küberrünnetes (RIA...2018) pole seletatav juhusliku õnnega, vaid annab tunnistust valdkonna arendamisel tehtud õigetest otsustest, mis on aidanud kaasa valdkonna riskide laiema teadvustamisele ja valmisoleku tekkimisele ohtudega toimetulekuks. Raske on strateegiate rolli selles alahinnata.

Küberjulgeoleku strateegiatel on olnud oluline roll riiklike prioriteetide deklareerimisel, nende selgitamisel nii avalikkusele kui ka strateegia elluviijatele. Erinevalt erasektorist, kus strateegiad pole tavaliselt avalikuks kasutamiseks, „kannab“ avalik haldus oma strateegiaid „uhkelt ja avalikult“, kuna need teatud mõttes defineerivad ja legitimiseerivad avaliku halduse olemasolu ja tegevuse mõtte selles valdkonnas, andes nende elluviijatele strateegiaga seotud identiteedi ning aitavad selgitada juhtimisotsuseid huvigruppidele (Stewart 2004).

Eesti strateegiad küberjulgeoleku vallas on selgitanud meie seisukohti ja andnud tunnistust meie taseme kohta valdkonnas nii Eesti kodanikele endile, kui ka meie partneritele ja rahvusvahelisele avalikkusele. Strateegiate üldist rolli küberjulgeoleku tagamisel peeti oluliseks, eriti planeerimisdokumendina, mis mitte ainult ei võimalda luua struktuuri vaid ka aitab läbi arutada ning teadvustada valdkonna põhiprobleeme. Ekspertide hindasid strateegiate koostamise ja rakendamise protsessi mõju küberjulgeoleku kui probleemi teadvustamisele riigi julgeoleku probleemina hinnati nii KJS 2008 kui ka KJS 2014 puhul üldiselt positiivseks, kuna eksperdid olid suhteliselt üksmeelsel arvamusel, et ilma strateegiate koostamiseta poleks tekkinud süsteemset lähenemist sellele valdkonnale ning riigi juhtkonna ja laiema avalikkuse poolt poleks küberjulgeoleku vajalikkusest vajalikul määral aru saadud. 22st intervjueeritud eksperdist 20 avaldasid kindlast veendumust, et valdkonna strateegilist planeerimist strateegia koostamise kaudu tuleb jätkata, kaks vastanut olid arvamusel, et strateegiline planeerimine

võiks jätkuda läbi küberjulgeoleku valdkonna küsimuste integreerimise teistesse arengukavadesse.

2017 aastal hakkas Eesti koostama kolmandat küberjulgeoleku strateegiat, mis on Eesti jaoks juba kolmas riiklik küberjulgeoleku strateegia. Teise põlvkonna küberjulgeoleku strateegia on praeguseks mõneteistkümnel riigil ja Euroopa Liidul, kolmanda valdkondliku strateegiaga oleme maailmas esimeste riikide seas (KTS 2018) mis on tunnistus ka teatud küpsuse saavutamisest. Uus strateegia Küberturvalisuse strateegia 2019–2022 (KTS 2018) kiideti Vabariigi Valitsuse poolt 09.11.2018 heaks „Eesti infoühiskonna arengukava 2020“ lisana. Sellega liideti iseseisev küberjulgeoleku strateegia Infoühiskonna arengukavaga ning muudeti ka arengukava nime: küberjulgeolek asendati küberturvalisusega. Strateegias tõdetakse, et see on koostatud koos „Infoühiskonna arengukavaga 2020“ : „kuna seniste kogemuste põhjal peavad eduka digiriigi loomiseks ja arendamiseks infoühiskonna arendamine ja küberturvalisuse tagamine toimuma strateegiliselt ühtsena (*ibid*)“.

Tulevik näitab, millisel moel selline lähenemine mõjutab küberjulgeoleku valdkonna strateegilist juhtimist ja kas ning kuidas muutub valdkonna tajumine riigi julgeoleku ja riigikaitse komponendina. Intervjueeritud eksperdid pidasid küberjulgeolekustrateegiate koostamise ja rakendamise protsessi mõju oluliseks just küberjulgeoleku kui probleemi teadvustamisele riigi julgeoleku probleemina. Eksperdid olid suhteliselt üksmeelsel arvamusel, et ilma strateegiate koostamiseta poleks tekkinud süsteemset lähenemist sellele valdkonnale ning riigi juhtkonna ja laiema avalikkuse poolt poleks küberjulgeoleku vajalikkusest vajalikul määral aru saadud. **Poliitikasoovitusena (1)** näeb autor seega kindlasti vajadust jätkata küberjulgeolekustrateegiate koostamisega ning peab oluliseks küberjulgeoleku strateegia käsitlemist valdkondadeülese, kõrge prioriteediga ja kõrgetasemelise riikliku arengukavana. Soovitav oleks ka defineerida sisejulgeoleku valdkonna kui ka riigikaitse valdkonna poliitikakujundajate, Siseministeeriumi (SiM) ja Kaitseministeeriumi (KM), täpne roll strateegia koostamisel, elluviimisel ja selle järelevalvel ning piiritleda küberjulgeoleku strateegilise planeerimise osa nende valdkondade arengukavades. Üheks võimaluseks oleks ka SiM ja KM esindajatele eristaatuse andmine praegu MKMi poolt juhitavaks Küberjulgeoleku Nõukogus, tagamaks nende ministeeriumite suurem kaasatus ja „omanikutunne“ küberjulgeoleku valdkonna eest.

Hinnates küberjulgeoleku strateegiate koostamisega seotud probleeme avaliku halduse strateegiate üldiste probleemide taustal tuleb tõdeda, et nii strateegiate koostamisel esinesid tavapärased avaliku halduse strateegiate koostamisele omased sõlmprobleemid (Bryson 2011, Allison,Kaye 2005) ning mingeid olulisi, vaid küberjulgeoleku valdkonnale spetsiifilisi erisusi juhtumiuuringuga ei tuvastatud.

Suurimate probleemidena strateegiate koostamisel võib välja tuua probleeme kõrgema juhtkonna kaasamisega ja strateegiaprotsessi juhtimisega. Kui KJS 2008 puhul strateegia koostamise juhtimises ja eriti juhtkonna kaasamises erilisi probleeme ei nähtud, siis KJS 2014 koostamisel, kui teema uudsus ning ka päevakajalisus (võrreldes KJS 2008 koostamise ajaga, kus alles olid toimunud 2007 küberrünnakud) oli vaibunud, olid need probleemid juba väga aktuaalsed. KJS 2014 koostamist iseloomustatati tihti just juhtimisprobleemide kaudu, mida seostati nii vastutava ministeeriumi MKMi huvi- kui ka ressursipuudusega. Kuigi mõlema strateegia puhul tunnistati probleeme nii protsessi kui ka selle elluviimisega, tõdeti, et igal juhul oli tegemist poliitikate planeerimise ja rakendamise olulise instrumendiga.

Üldiselt saab rahul olla KJS sõnastuse selgusega. Strateegia põhieesmärkide seadmise ja sõnastamise edukus ning põhieesmärgi arusaadavus oli strateegiatel küll erinev, peegeldades otseselt strateegia koostamise aega ning olusid. Esimese strateegia koostamise ajal oli tegemist täiesti uue teemaga, kuid KJS 2014 toimusid juba ulatuslikud arutelud kasutatavate definitsioonide ja terminoloogia suhtes. Strateegiate sõnastus ja struktuur on aja jooksul muutunud konkreetsemaks ja täpsemaks, eesmärgid mõõdetavamaks (vt. lisa 2).

Kõige rohkem kriitkat pälvis seostatus teiste arengukavadega ja eriti eelarvete koostamisega ning tuleb asuda seisukohale, et see oli mõlema strateegia puhul suureks probleemiks, mis raskendas oluliselt strateegiate elluviimist. Strateegia kui valdkondlik arengukava peaks olema nii selle valdkonnaga seonduvate eelarveotsuste tegemisel kui ka mõjutama teiste arengukavade tegemist, vältides vastuolusid ja dubleerimist. Seda pole aga kahjuks tagada suudetud. **Poliitikasoovitusena (2)** näeb autor siin vajadust tugevdada Küberjulgeoleku Nõukogu (KJN) rolli järelevalvel strateegia elluviimise üle. Strateegias toodud eesmärkide saavutamiseks vajalike eelarvevahendite taotlemata jätmine, eesmärkide ignoreerimine või muutmine valdkondlikes arengukavades ja muudes planeerimisdokumentides peab olema põhjendatud ning vastavad otsused peavad olema teada teistele strateegia elluviimise eest vastutavatele asutustele. Vastasel juhul pole ka tulevikus välistatud, et strateegia elluviimine

takerdub ühe asutuse vastutusvaldkonnas tehtud otsuse tõttu, mis mõjutab oluliselt ka teisi valdkondi.

Kokkuvõtlikult võib tõdeda ka, et strateegiate koostamise käigus on küberjulgeoleku valdkonna strateegilise planeerimise põhiprobleemidele (Klimburg 2012;Bryson 2011; Hansen,Nissenbaum 2009) pööratud piisavalt tähelepanu. Küberjulgeoleku tagamist ja selle strateegilist planeerimist on käsitletud kui üleriigilist, mitmete osalistega protsessi ja juba KJS 2008 koostamisest alates on planeerimisse kaasatud ka erasektorit ja teisi huvigruppe.

Keerulisem on hinnata, kas vajadust tagada valitsusasutuste vaheline koostöö ja koordinatsioon ning koos sellega valitsusülese vaate olemasolu, arvestati piisavalt. Pigem tundub, et isegi siis, kui vastavat ambitsiooni planeerimisel oli, kujunes strateegiate rakendamine palju komplitseeritumaks ning mitmete ekspertide arvamust mööda olid erinevate ametkondade ja ministeeriumite lahknevad huvid (nn silotornid) ning keskse koordineerimise raskused peamisteks probleemideks strateegiate rakendamisel ning eesmärkide täitmisel. Oma osa on siin kindlasti ka Eesti küberjulgeoleku üldiselt detsentraliseeritud mudelil (Boeke 2017), mis nõuab strateegia koostamisel arvestamist ja tähelepanu, et asutuste funktsioonid, nende koordineerimine ja koostöö oleks selgelt defineeritud. **Poliitikasoovitusena (3)** tuleks lisaks eeltoodud poliitikasoovitustele 2 ja 3 selle probleemi lahendamiseks korrastada küberjulgeoleku valdkonna strateegilise juhtimise õiguslikud alused, seda eelkõige juhtivale ministeeriumile (MKM) vastavate volituste ja kohustuste määratlemise kaudu.

Töö teiseks eesmärgiks oli uurida hinnanguid strateegiate koostamise ja rakendamise mõju valdkondade arengule, mida peetakse küberjulgeoleku tagamise seisukohast olulisteks (Klimburg *et al* 2012, Hansen,Nissenbaum 2009, Brangetto, Kert-Saint Aubyn 2015 , ITU... 2018). Autori valitud valdkondadeks olid majandus, riigikaitse, haridus- ja teadusvaldkond ning rahvusvaheline suhtlus. Kõigis neis valdkondades hinnati küberjulgeoleku strateegiate koostamise ja rakendamise mõju positiivseks, seda isegi juhul, kui see mõju polnud strateegia eesmärkide seas koostamisel selgesõnaliselt määratletud. Osaliselt on see seletatav ka strateegiate kaudse mõjuga, mis aitas hoida valdkonda avalikkuse ja tippametnike huviorbiidis ja võimaldas saada toetust valdkonda arendavatele ideedele. Strateegiate mõju osas erinesid KJS 2008 ja KJS 2014 antud hinnangud küll märgatavalt, kuna enamikel juhtudel hinnati KJS 2014 mõju palju negatiivsemalt. Osaliselt on see kindlasti seletatav teema uudsusega KJS 2008 koostamise ajal, mis tagas ka suurema tähelepanu ning muutuste suurema märgatavuse.

Viimasena tuleb välja tuua, et Eesti strateegiatel on olnud ka oluline mõju küberjulgeoleku valdkonna võimearendusele: RIA muutmine valitsusasutuseks ja konkreetsete ülesannete ning õiguste määratlemine Küberturvalisuse seaduses, CCDCOE tegevuse toetamine, kaudne mõju küberväejuhatuse loomisele jne. Erinevate riikide küberjulgeoleku strateegiate analüüsimisel selgub, et hoolimata strateegiates võimeloomisele suure tähelepanu pööramisest on tegudeni jõudnud pigem vähesed riigid (Shafqat, Masood 2016).

Küberjulgeoleku strateegiad kui tervikprotsess on seega 2008-2018 avaldanud ekspertide hinnangul tajutavat positiivset mõju nii küberjulgeoleku tegelikule olukorrale kui ka Eesti rahvusvahelise maine ning konkurentsivõime kujunemisele. Eesti näite põhjal saab ka väita, et strateegiaprotsess aitab hoida üleval laiemat huvi valdkonna probleemide lahendamise vastu, mis avaldab otsest mõju ka valdkonna arendamisele väljaspool strateegias otseselt käsitletu. Hoolimata strateegiate koostamise ja rakendamise aja- ja ressursimahukusest võimaldab see valdkonna arengut süsteemselt juhtida ja on riigi seisukohalt otstarbekas ilmselt mitte ainult Eestis vaid ka teistes riikides.

Samuti ei leitud uurimuse käigus tõendeid, et küberjulgeoleku valdkonna strateegilise planeerimise probleemid erineksid oluliselt teistest avaliku halduse strateegiatele omastest probleemidest. Küberjulgeoleku valdkonna strateegilise juhtimise ees seisvate väljakutsetega toimetulekuks peavad osapooled seega otsima võimalusi riigiülese koordinatsiooni, arengukavade omavaheline seostatuse, eelarve planeerimise ja ressursside jaotusega seotud ning avalikus halduses tavapäraseks kujunenud probleemide lahendamiseks.

SUMMARY

THE IMPLICATIONS OF A CYBER SECURITY STRATEGY PROCESS TO A CYBER SECURITY IN ESTONIA 2008-2018

Toomas Vaks

This thesis studies the problems of public administrations' strategic planning in preparation and execution of cybersecurity strategies. It studies the case of Estonia where the third cybersecurity strategy was completed in 2018. In the years 2011-2017, in dealing with cybersecurity in the state's institutions, the author has continuously been exposed to statements that question the need for strategic planning in "the field of cyber" - primarily due to alleged uniqueness and planning problems in the field. The thesis examines the problems of strategic planning specific to cyber and evaluates its impact on the cybersecurity situation by monitoring Estonia's development in the field for the most recent 10-year period.

The main aim of this research is to study the problems of strategic planning of cyber security in the light of the theoretical framework of strategic planning of public administration, to understand the problems and possible peculiarities of its field. The second objective is to analyze and evaluate the perceived impact of the process of compiling and implementing cyber security strategies in Estonia for the general development of cyber security in Estonia as well as for the development of the selected supporting areas: economy, research and education, national defense and international relations.

Research was conducted as a case study. In addition to the analysis of policy papers and other relevant documents, main method used in the study was interviewing experts who were involved in the process of creating or implementation of cyber security strategies or were otherwise familiar with cyber security developments. All together 23 Estonian decisionmakers, top officials and top experts in the field of cyber security were interviewed for the survey.

Research draws the following conclusions:

- Strategy process has also indirect positive impact even to cyber security initiatives those are not part of the strategy;

- The process of drafting and implementing cybersecurity strategies sets high requirements for the involvement of senior management of stakeholder groups and organizations;
- The primary problem in the implementation of cybersecurity strategies in Estonia is the lack of connection with other national development plans and the budgeting process, i.e. resource management;
- The use of a decentralized model in establishing cybersecurity requires that particular attention be paid to ensuring the division of responsibilities, coordination and cooperation when drawing up the strategy;
- The primary problem in drawing up cybersecurity strategies has been management problems and decreasing political interest in the field after 2007;
- In the area of cybersecurity, it is necessary to continue with strategic planning as only this ensures a systemic approach to risk management at the national level;
- The influence of past strategies' preparations on the development of cybersecurity in Estonia has been predominant and is evident in the today's cybersecurity capabilities;
- The preparation, implementation, and impact of strategies have been systematically analysed and taken into account in subsequent Estonian cybersecurity strategies.

The thesis suggests that according to expert opinions the strategic planning of cybersecurity in 2008-2018 has had a significant positive impact on the Estonian cybersecurity situation as well as on the development of Estonia's international reputation and competitiveness. Based on Estonia's case study it can be concluded that strategy development and implementation process in the field of cyber security is beneficial also as a process as such.

The study also found no evidence that the problems of strategic planning in the field of cyber security differed significantly from other problems inherent in public administration strategies. Thus, in order to meet the challenges of strategic management in the field of cyber security, the parties need to look for ways to solve problems with state-wide coordination, the coherence of public sector strategies, budget planning and resource allocation, all those that have become common in public administration.

Keywords: cybersecurity, cyber security, IT security, cybersecurity strategy, strategy

KASUTATUD ALLIKATE LOETELU

Akadeemilised allikad

Allison, M., & Kaye, J. (2005). *Strategic planning for nonprofit organizations: A practical guide and workbook.* Hoboken, NJ: John Wiley & Sons, Inc

Areng L. (2015) *Liliputian States in Digital Affairs and Cyber Security.* The Tallinn Papers no. 4 NATO CCDCOE

Bailes A.J.K. (2009) *Does a Small State Need a Strategy?* Centre For Small State Studies Publication Series University of Iceland Occasional Paper 2-2009

Baxter, P., & Jack, S. (2008). *Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. The Qualitative Report,* 13(4), 544-559. Kättesaadav: https://nsuworks.nova.edu/tqr/vol13/iss4/2 (1.06.2018)

Béland D., Howlett M. (2016) *How Solutions Chase Problems: Instrument Constituencies in the Policy Process.* Governance: An International Journal of Policy, Administration, and Institutions, Vol.29, No.3, July 2016, 393-409.

Boeke S. (2017) *National cyber crisis management:Different European approaches.* Governance. 2018;31:449-464 Kättesaadav: https://doi.org/10.1111/gove.12309 (11.08.2018)

Brangetto P., Kert-Saint Aubyn (2015) *Economic aspects of national cyber security strategies. Project Report.* NATO CCDCOE 2015

Brudan, A. (2010). *Rediscovering performance management: systems, learning and integration.* Measuring Business Excellence, 14(1), 109-123.

Bryson J.M, Edwards, L.H., Van Slyke D.M. (2018) *Getting strategic about strategic planning research.* Public Management Review, 20:3, 317-339.

Bryson J.M. (2011) *Strategic Planning for Public and Nonprofit Organizations: A Guide to Strengthening and Sustaining Organizational Achievement*. Fourth Edition. Wiley and Sons

Burton J. (2013) *Small states and cyber security: The case of New Zealand.* Political Science 65 (2) 216-238.

Buzan, B., Hansen, L. (2010) *The Evolution of International Security Studies*. New York: Cambridge University Press, 2010

Buzan, B., Jaap, de W., Woever, O. (1998) *Security: a New Framework for Analysis.* Boulder, Colo: Lynne Rienner Publishers, 1998

Coker C. (2004) *The Future of War.* Oxford: Blackwell Publishing *via* Osinga F.P.B (2007) Teadus, strateegia ja sõda: John Boydi strateegiateooria *Riigikaitse raamatukogu* 2013

Creswell, J. W. (2003). Research design. Qualitative, Quantitative and Mixed Methods Approaches. (2nd edition). Kättesaadav: http://isites.harvard.edu/fs/docs/icb.topic1334586.files/2003_Creswell_A%20Framework%20for%20Design.pdf (01.07.2018)

Creswell J.W (2014) *Research design: Qualitative, Quantitative and Mixed Method Approaches.* 4th Edition. SAGE

de Kluyver C. A, Pearce II. J.A (2006) *Strategy: A view from the top* (second edition) Pearson Prentice Hall

Favoreu C., Carassus D., Maurel C. (2015) *Strategic management in the public sector: a rational, political or collaborative approach?* International Review of Administrative Sciences 2016, Vol. 82 (3) 435-453.

George B., Desmidt S.(2014) *A State of Research on Strategic Management in the Public Sector: An Analysis of the Empirical Evidence* . Strategic Management

in Public Organizations: European Practices and Perspectives. Routledge, 151 – 172.

Gillham, B. (2009). *Case Study Research Methods.* London: Continuum.

Hansen, L, Nissenbaum, H. (2009) *Digital Disaster, Cyber Security, and the Copenhagen School.* International Studies Quarterly International Studies Quarterly (2009) 53, 1155–1175 Kättesaadav: https://nissenbaum.tech.cornell.edu/papers/digital%20disaster.pdf (11.05.2018)

Hsieh, H. F., & Shannon, S. E. (2005). *Three approaches to qualitative content analysis.* Qualitative health research, 15(9), 1277 – 1288.

Kalu F., Bwalya J. (2017) *What Makes Qualitative Research Good Research? An Exploratory Analysis of Critical Elements* International Journal of Social Science Research vol 5 No. 2

Kaplan, R. S., Norton, D. P., & Sher, G. (2005). *The office of strategy management*. Harvard Business Review, 83(10), 72-80

Klimburg A.(2012) *National Cyber Security Framework Manual.* NATO CCDCOE

Kouremetis, M.(2015). *An analysis of Estonia's cyber security strategy, policy and capabilities.* In Proceedings of the 14th European Conference on Cyber Warfare and Security 2015, 404-412. Presented at the European Conference on Cyber Warfare and Security. Reading, UK: Academic Conferences and Publishing International.

Lujif E., Besseling K.,de Graaf P. (2013) *Nineteen National Cyber Security Strategies.* International Journal of Critical Infrastructure Protection, Vol. 9, Nos. 1/2, 2013

Laherand M.L. (2008). *Kvalitatiivne uurimisviis.* Tallinn, 2008

Lascoumes P., Le Gales P. (2007) *Introduction: Understanding Public Policy through Its Instruments- From the Nature of Instruments to the Sociology of Public Policy Instrumentation Governance:* An International Journal of Policy, Administration, and Institutions Vol. 20, No. 1, 1-21.

Lindström G.,Luiijf E.(2012) 2. *Political Aims and Policy Methods. National Cyber Security Framework Manual*. NATO CCDCOE, 44-65.

McSweeney B. (1996) *Review: Identity and Security: Buzan and the Copenhagen School* Review of International Studies Vol.22, No. 1 (Jan., 1996) 81-93

Meyer, C. B. (2001). *A Case in Case Study Methodology.* Field Methods, 13(4), 329-352.

Mintzberg, H. (1978) *Patterns in Strategy Formation* Management Science, Vol. 24, No. 9, 934-948

Mintzberg, H. (1993). *The pitfalls of strategic planning.* California Management Review, 36(1), 32-47.

Mintzberg, H (1994) *The fall and rise of strategic planning.* Harvard Business Review, January-February, 107-14

Mulgan, G (2009) *The Art of public strategy.* Oxford University Press , 2nd edition

Osinga F.P.B (2006) *Science, Strategy and War. The strategic theory of John Boyd. Routledge ,* 22-26.

Palys, T. (2008). *Purposive sampling.* via L. M. Given (Ed.) The Sage Encyclopedia of Qualitative Research Methods. (Vol.2). Sage: Los Angeles, 697-8.

Poister H. (2010) *The Future of Strategic Planning in the Public Sector: Linking Strategic Management and Performance.* Public Administration Review December 2010

Poister H., Streib (1999) *Strategic Management in the Public Sector.* Public productivity and Management review, vol.22 nr.3

Provan, K. G., & Kenis, P. N. (2008). *Modes of network governance: Structure, management, and effectiveness.* Journal of Public Administration Research and Theory, 18(2), 229-252.

Shafqat N., Masood A. *Comparative Analysis of Various National Cyber Security Strategies* (IJCSIS) International Journal of Computer Science and Information Security, Vol. 14, No. 1, January 2016 Kättesaadav: https://s3.amazonaws.com/academia.edu.documents/41883983/17_Paper_31121548_IJCSIS_Camera_Ready_pp._129-136.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1543781575&Signature=UKAXZzyY0GLaYuXOBd7H5OeB46k%3D&response-content-disposition=inline%3B%20filename%3DComparative_Analysis_of_Various_National.pdf (11.10.2018)

Simons, H. (2009). *Case Study Research in Practice.* Los Angeles: Sage Publications.

Stewart J.,(2004) *The meaning of strategy in the public sector* Australian Journal of Public Administration 63(4):16-21 December 2004

Wauters, B (2017) *Strategig management in the public sector: a tool for improving performance of ongoing operations or for redefining performance to meet new challenges?* Report to the European Comission's Public Administration and Governance Network

Õunapuu, L. (2014). *Kvalitatiivne ja kvantitatiivne uurimisviis sotsiaalteadustes.* Tartu: Tartu Ülikool.

Yin R.K (2011) *Qualitative Research from start to finish.* Guilford Press

Muud kasutatud allikad

Alas, R. (2005). *Strateegiline juhtimine.* Tallinn: Tallinna Raamatutrükikoda.

BNS (2007) *BNS uudis :14.11.2007 Eesti koostab küberjulgeoleku strateegia*. Kättesaadav: http://www.estemb.org/est/cat-445/aid-957 (22.11.2018)

Clausewitz, C.(2004) *Sõjast.* Eesti Keele Sihtasutus,195

EU Comission (2017) *Cyber Security Package* Kättesaadav: https://ec.europa.eu/digital-single-market/en/cyber-security (22.11.2018)

EGA (2018) *E- riigi Akadeemia: Rahvusvaheline Küberjulgeoleku indeks.* Kättesaadav: https://ncsi.ega.ee/ (25.11.2018)

ERR (2018) *Uudis: Kaitseväes alustab küberväejuhatus.* Kättesaadav: https://www.err.ee/847915/kaitsevaes-alustab-kubervaejuhatus (01.11.2018)

Internetstat (2018) *Interneti statistika.* Kättesaadav: https://www.internetworldstats.com/emarketing.htm (20.11.2018)

ITU (2018) *Guide to Developing a National Cybersecurity Strategy. Co-publication of 12 partner organisations, facilitated by ITU* .Kättesaadav: https://www.ccdcoe.org/sites/default/files/multimedia/pdf/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf (12.11.2018)

ITU (2018) *United Nations International Telecommunication Unions Global Cybersecurity Index Report 2017.* ITU Kättesaadav https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci.01-2017-pdf-e.pdf (05.08.2018)

Kaitseministeerium (2013) *Riigikaitse arengukava 2013-2022.* Kättesaadav: http://www.kaitseministeerium.ee/riigikaitse2022/riigikaitse-arengukava/index.html (12.10.2018)

Kivirähk J (2017) *Avalik arvamus ja riigikaitse.* Kaitseministeeriumi tellitud uuring. Kättesaadav: http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/avalik_arvamus_ja_riigikaitse_oktoober_2017.pdf (2.07.2018)

KJS (2008) *Küberjulgeoleku strateegia 2008-2013.* Kättesaadav: https://valitsus.ee/.../kuberjulgeoleku_strateegia_2008-2013.pdf (01.07.2018)

KJS (2014) *Küberjulgeoleku strateegia 2014-2017.* Kättesaadav: https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf (01.07.2018)

KJS (2018) *Eesti Infoühiskonna arengukava ja Küberturvalisuse strateegia* . Kättesaadav: http://eelnoud.valitsus.ee/main/mount/docList/a7b5d0eb-f973-40a8-84e6-7e755e52cffe?activity=2#3FqzuuOE (25.11.2018)

KüTS (2018) *Küberturvalisuse seaduse seletuskiri.* Kättesaadav: https://www.koda.ee/sites/default/files/content-type/content/2017-10/seletuskiri_k%C3%BCberturvalisuse%20seadus.pdf (21.10.2018)

Leimann, J., Skärvad, P-H. & Teder, J. (2003). *Strateegiline juhtimine.* Tallinn: Külim.

Lextal (2016) *Kübervaldkonna õigusanalüüs Riigi Infosüsteemi Ameti tellimusel*, kättesaadav: https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/kubervaldkonna-oigusanaluus-lextal-2016.pdf (11.08.2018)

Maaleht (2017) *Uudis: Põltsamaa ühisgümnaasiumi direktor: lihtne just pole, aga saame hakkama! Kooli küberkaitse õpe pälvis Euroopa kuriteoennetuse peaauhinna.* Kättesaadav: http://maaleht.delfi.ee/news/maaleht/uudised/poltsamaa-uhisgumnaasiumi-direktor-lihtne-just-pole-aga-saame-hakkama?id=80499520 (11.11.2018)

McNamara, C. (2007) *Field guide to nonprofit strategic planning and facilitation.* Minneapolis: Authenticity Consulting.

MKM (Majandus- ja Kommunikatsiooniministeerium) (2012) *„Küberjulgeoleku strateegia 2014-2017" koostamise ettepanek Vabariigi Valitsusele.* Kättesaadav http://eelnoud.valitsus.ee/main/mount/docList/2ca5a031-6b4d-45c3-8a14-43406bd8afcb?activity=1#f2U9TnzE (11.09.2018)

MKM(2014) *Eesti infoühiskonna arengukava.* Majandus- ja Kommunikatsiooniministeerium. Kättesaadav: https://www.mkm.ee/sites/default/files/elfinder/article_files/eesti_infouhiskonna_arengukava.pdf (09.10.2018)

MKM PM (2018) *Majandus- ja Kommunikatsiooniministeeriumi põhimäärus.* Kättesaadav: https://www.riigiteataja.ee/akt/12934222?leiaKehtiv (01.11.2018)

NAS (1990) *National Academy of Sciences, Computer Science and Telecommunications Board report. Computers at Risk:Safe Computing in the Information Age.* Kättesaadav: https://www.nap.edu/catalog/1581/computers-at-risk-safe-computing-in-the-information-age (01.10.2018)

OAS (2014) *Press release: Organisation of American States and Estonia Sign Cooperation Agreement on Cyber Security* Kättesaadav: *http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-445/14 (01.11.2018)*

O'Ņeill P.(2016) *The cyberattack that changed the world,* The Daily Dot, May 20, 2016. Kättesaadav: https://www.dailydot.com/layer8/web-war-cyberattack-russia-estonia/ (11.09.2018)

OSCE (2009) *The OSCE concept of Comprehensive and Co-operative Security.* An overview of Major Milestones (SEC/CPC/OS/167/09) Kättesaadav : https://www.osce.org/cpc/37592 (11.10.2018)

Pernik P. (2013) *Küberjulgeoleku strateegia 2008–2013 analüüs.* Rahvusvaheline Kaitseuuringute Keskus, Tallinn. Edastatud autorile juuni, 2018

Rahandusministeerium (2006) *Strateegilise planeerimise käsiraamat.* Rahandusministeerium Tallinn Veebruar 2006 . Kättesaadav : http://www.enl.ee/UserFiles/ENL%20Strateegiakool/rahandusminplaneerimine.pdf (26.05.2018)

Rebane L., Veiler K. (2018) *„Küberjulgeoleku strateegia 2014-2017" lõpparuanne.* Majandus- ja Kommunikatsiooniministeeriumi aruanne Vabariigi Valitsusele 20 aprillil 2018. Kärbitud avalik versioon asutusesiseseks kasutamiseks mõeldud dokumendist edastatud autorile 14.10.2018

RIA (2018) *Küberturvalisuse aastaraamat 2018.* Riigi Infosüsteemi Amet. Kättesaadav:https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria-kuberturvalisus-2018.pdf (13.08.2018)

TTÜ (2018) *ID kaardi kaasuse õppetunnid.* Tallinna Tehnikaülikool. Kättesaadav: https://www.ria.ee/sites/default/files/content-editors/EID/id-kaardi_oppetunnid.pdf

USA (2003) *National Strategy to Secure Cyberspace.* Kättesaadav: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

Intervjuud

Allman, L.(2018) *Intervjuu.* Autori kirjalik intervjuu 11.10.2018

Ekspert 1 (2018) *Intervjuu.* Autori kirjalik intervjuu 13.09.2018

Ekspert 2 (2018) *Intervjuu.* Autori kirjalik intervjuu 17.09.2018

Ekspert 3 (2018) *Intervjuu.* Autori kirjalik intervjuu 29.08.2018

Ekspert 4 (2018) *Intervjuu.* Autori kirjalik intervjuu 28.08.2018

Ekspert 5 (2018) *Intervjuu.* Autori kirjalik intervjuu 04.09.2018

Ekspert 6 (2018) *Intervjuu.* Autori kirjalik intervjuu 04.09.2018.

Ekspert 7 (2018) *Intervjuu.* Autori kirjalik intervjuu 05.09.2018

Ekspert 8 (2018) *Intervjuu.* Autori kirjalik intervjuu 25.08.2018

Ilves, L.K. (2018) *Intervjuu.* Autori kirjalik intervjuu 03.09.2018

Kaska K. (2018) *Intervjuu.* Autori kirjalik intervjuu 18.09.2018

Koort, E. (2018) *Intervjuu.* Autori kirjalik intervjuu 03.09.2018

Kotka, T. (2018) *Intervjuu.* Autori suulise (osalise) intervjuu märkmed 24.09.2018.

Luht, L. (2018) *Intervjuu.* Autori kirjalik intervjuu 02.09.2018

Maaten, E. (2018) *Intervjuu.* Autori kirjalik intervjuu 12.09.2018

Mägi, K. (2018) *Intervjuu.* Autori kirjalik intervjuu 13.09.2018

Peterkop T. (2018) *Intervjuu.* Autori kirjalik intervjuu 13.09.2018

Priisalu, J. (2018) *Intervjuu.* Autori kirjalik intervjuu 09.09.2018

Rebane, L. (2018) *Intervjuu.* Autori kirjalik intervjuu 09.09.2018

Saks, M. (2018) *Intervjuu.* Autori kirjalik intervjuu 27.08.2018.

Sikkut, S. (2018) *Intervjuu.* Autori kirjalik intervjuu 04.09.2018.

Tikk, M. (2018) *Intervjuu.* Autori kirjalik intervjuu 18.09.2018

LISAD

Lisa 1. Uurimisküsimuste struktuur

Strateegia ja/või strateegilise planeerimise komponent	**Küsimused intervjuudeks**	**Allikas**
Strateegia koostamise juhtimine ja probleemid (nt Organisatsioonide juhtide ja vajalike huvigruppide kaasatus; juhtgrupi tegevus)	*Mis olid peamised probleemid küberjulgeoleku strateegiate koostamisel ja kas need erinevad tavapäraselt avaliku halduse strateegiatele omastest probleemidest?*	Teoreetiline kirjandus. Intervjuud ekspertide ja protsessi osalistega. Strateegiate hindamise kokkuvõtted, eduraportid ja -hinnangud. Rahvusvaheliste organisatsioonide raportid.
Strateegia põhieesmärkide seadmise ja sõnastamise edukus (põhieesmärgi arusaadavus, sõnumite selgus, ühiste eesmärkide kokkuleppimine)	*Millised olid küberjulgeoleku strateegiate põhieesmärgid ja kas need tegelikult täideti?*	Intervjuud ekspertide ja protsessi osalistega. Strateegiate hindamise kokkuvõtted, eduraportid ja -hinnangud. Rahvusvaheliste organisatsioonide raportid.
Seostatus teiste strateegiatega (arengukavadega), eelarvete koostamisega; üleriigiline mõõde ja valitsusülene mõõde;	*Kas ja kui siis milline oli küberjulgeoleku strateegiate seos teiste arengukavadega?*	Intervjuud ekspertide ja protsessi osalistega. Strateegiate hindamise kokkuvõtted, eduraportid ja -hinnangud. Regulatsioonide analüüs

Strateegia ja/või strateegilise planeerimise komponent	**Küsimused intervjuudeks**	**Allikas**
Küberjulgeolekustrateegia koostamine poliitika planeerimise ja rakendamise osana, protsessile üldine elluviimine ja selle seire;	*Kas küberjulgeoleku strateegiaid tajuti laiemalt poliitika kujundamise tegelike instrumentidena? Kas protsessis osalenud ja huvigrupid hindavad küberjulgeoleku strateegiate loomist positiivselt?*	Intervjuud ekspertide ja protsessi osalistega. Strateegiate hindamise kokkuvõtted, eduraportid ja -hinnangud. Rahvusvaheliste organisatsioonide raportid. Regulatsioonide analüüs Teoreetiline kirjandus
Hinnang strateegia ja selle koostamise protsessi mõju küberjulgeoleku kui probleemi teadvustamisele riigi julgeoleku probleemina;	*Millised olid küberjulgeoleku strateegiate põhieesmärgid ja kas need tegelikult täideti?*	Intervjuud ekspertide ja protsessi osalistega. Strateegiate hindamise kokkuvõtted, eduraportid ja -hinnangud. Rahvusvaheliste organisatsioonide raportid. Regulatsioonide analüüs Teoreetiline kirjandus
Hinnang strateegia ja selle koostamise mõjule konkreetsete valdkondade arengule;	*Kas ja kui siis millist mõju omas strateegia ekspertide arvates majanduse, julgeoleku- ja riigikaitse valdkondade, hariduse ja teaduse ning Eesti rahvusvahelisele tuntusele ning rahvusvaheliste suhete arengule?*	Intervjuud ekspertide ja protsessi osalistega. Strateegiate hindamise kokkuvõtted, eduraportid ja -hinnangud. Rahvusvaheliste organisatsioonide raportid. Regulatsioonide analüüs Teoreetiline kirjandus
Hinnang strateegia põhieesmärkide elluviimisele ja Eesti üldisele olukorrale küberjulgeoleku tagamisel.	*Mida peetakse Eesti suurimaks õnnestumiseks küberjulgeoleku valdkonnas?*	Intervjuud ekspertide ja protsessi osalistega. Strateegiate hindamise kokkuvõtted, eduraportid ja -hinnangud. Rahvusvaheliste organisatsioonide raportid.

Lisa 2. Strateegiate sõnastuse võrdlus

	KJS 2008	KJS 2014	KTS 2018
Visioon	Küberjulgeolek Eestis tugineb eeskätt riigi kui terviku küberruumi haavatavuse vähendamisele.	Eesti suudab tagada riigi küberjulgeoleku ning toetada avatud, kaasava ja turvalise infoühiskonna toimimist.	Eesti on kõige küberturvalisem digitaalne riik
Põhieesmärgid	Eestis on laiaulatuslikult rakendatud astmeline turvameetmete süsteem, mis tagab Eesti riigi küberjulgeoleku; Eesti on väga suure infoturbealase kompetentsuse ja teadlikkusega riik; Infosüsteemide turvalist ja laialdast kasutamist toetab proportsionaalne õiguslik regulatsioon; Eesti on küberjulgeoleku tõhustamiseks tehtava rahvusvahelise koostöö üks juhtriike.	Küberjulgeoleku strateegia nelja aasta eesmärk on suurendada küberturvalisuse alast võimekust ja inimeste teadlikkust küberohtudest, tagamaks jätkuvat usaldust küberruumi vastu.	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.
Valdkondlikud eesmärgid	Turvameetmete süsteemi arendamine ja üleüldine rakendamine; Infoturbealase kompetentsuse suurendamine ; Küberjulgeolekuks vajaliku õigusruumi kujundamine; Rahvusvahelise koostöö arendamine; Küberjulgeoleku alane teavitustegevus.	Oluliste teenuste infosüsteemide kaitse tagamine ; Küberkuritegevus vastase võitluse tõhustamine ; Riigikaitseliste võimete arendamine küberkaitse valdkonnas; Eesti maandab võimalikke küberjulgeolekuohte; Eesti arendab valdkonnaüleseid tegevusi.	Eesti on jätkusuutlik digitaalne ühiskond, millel on tugev tehnoloogiline vastupanuvõime ja valmisolek kriisidega toimetulekuks ; Eestis on tugev, innovaatiline, teaduspõhine ja globaalselt konkurentsivõimeline küberturbe sektori ettevõtlus ning teadus- ja arendustegevus, mis katab riigi jaoks olulised võtmekompetentsid; Eesti on arvestatav ja tugev partner rahvusvahelisel areenil; Eesti on ühiskonnana küberteadlik ning tagatud on valdkonna spetsialistide järelkasv.

Lisa 3. Intervjuu küsimused

UURIMISTÖÖ KIRJALIKU INTERVJUU KÜSIMUSTIK

1. Kas olite ise (vahetult) seotud I või II küberjulgeolekustrateegia (I KJS – Küberjulgeoleku strateegia 2008-2013 ja II KJS- Küberjulgeoleku strateegia 2013-2017) koostamisega?
2. Kas olete Küberjulgeoleku nõukogu liige?
3. Kas osalete või olete osalenud küberjulgeoleku strateegiate mõjude või tulemuste hindamisel?
4. Mis oli Teie arvates I KJS peamine eesmärk ja kas see täideti?
5. Mis olid Teie arvates I KJS koostamise peamisteks probleemideks?
6. Kas Teie arvates oli I KJS poliitika planeerimise instrument?
7. Kas Teie arvates võeti I KJS eesmärke arvesse teiste riiklike strateegiate koostamisel ja poliitika planeerimisel?
8. Kas ja kui siis millist mõju omas I KJS Eesti majanduse arengule?
9. Kas ja kui siis millist mõju omas I KJS Eesti julgeoleku- ja riigikaitse valdkondade arengule?
10. Kas ja kui siis millist mõju omas I KJS Eesti hariduse ja teaduse arengule?
11. Kas ja kui siis millist mõju omas I KJS Eesti rahvusvahelisele tuntusele ning rahvusvaheliste suhete arengule?
12. Mis oli Teie arvates II KJS peamine eesmärk ja kas see täideti?
13. Mis olid Teie arvates II KJS koostamise peamisteks probleemideks?
14. Kas Teie arvates oli II KJS poliitika planeerimise instrument?
15. Kas Teie arvates võeti II KJS eesmärke arvesse teiste riiklike strateegiate koostamisel ja poliitika planeerimisel?
16. Kas ja kui siis millist mõju omas II KJS Eesti majanduse arengule?
17. Kas ja kui siis millist mõju omas II KJS Eesti julgeoleku- ja riigikaitse valdkondade arengule?
18. Kas ja kui siis millist mõju omas II KJS Eesti hariduse ja teaduse arengule?
19. Kas ja kui siis millist mõju omas II KJS Eesti rahvusvahelisele tuntusele ning rahvusvaheliste suhete arengule?
20. Mida peate Eesti suurimaks õnnestumiseks küberjulgeoleku valdkonnas?
21. Kas olete osalenud 2018 aasta Küberjulgeoleku strateegia väljatöötamisel?
22. Kas ja kui siis miks peate vajalikuks küberjulgeoleku strateegiate edasist koostamist, s.t ka peale 2018 aastal valmiva uue strateegia valmimist?

23. Teie nimi
24. Kas tohib viidata uurimistöös Teie intervjuule nimeliselt?