TALLINNA TEHNIKAÜLIKOOL
Majandusteaduskond
Ragnar Nurkse innovatsiooni ja valitsemise instituut

Merike Jõesaar

VÄIKERIIGI KÜBERJULGEOLEKU VÕIMEKUST MÕJUTAVAD TEGURID: EESTI ID-KAARDI 2017. A TURVANÕRKUSE JUHTUMI KOGEMUS

Magistritöö

Õppekava HAHM03/11, 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 13 204 sõna sissejuhatusest kuni kokkuvõtte lõpuni.

Merike Jõesaar ……
(allkiri, kuupäev)
Üliõpilase kood: 124769HAHM
Üliõpilase e-posti aadress: merike.maad@gmail.com

Juhendaja: Maarja Toots, MA
Töö vastab kehtivatele nõuetele

……
(allkiri, kuupäev)

Kaitsmiskomisjoni esimees: Dr. Erkki Karo
Lubatud kaitsmisele

……
(nimi, allkiri, kuupäev)

SISUKORD

LÜHIKOKKUVÕTE

Infotehnoloogia ja interneti laialdane kasutamine on muutunud oluliseks komponendiks ühiskonnas ning küberruumi tekkega seotud ühiskondlikest muudatustest ei ole puutumata jäänud ka senised arusaamad riikide võimekusest. Seega räägitakse üha enam väikeste riikide võimalustest saavutada traditsiooniliselt suurriigile omane võimekus erinevates valdkondades (Katzenstein 1984; Thorhallsson 2018; Nye 2010). Magistritöö uurimisprobleem on: kuidas väikeriik tagab oma küberjulgeoleku võimekuse? Uurimisprobleemi täpsustav teoreetiline uurimisküsimus on: kuidas mõjutab riigi väiksus tema küberjulgeoleku tagamise võimekust. Magistritöö eesmärk on selgitada välja siseriiklikud tegurid, mis mõjutavad väikeriigi küberjulgeoleku võimekust.

Töö on juhtumiuuring fookusega Eestis 2017. aastal aset leidnud ID-kaardi turvakiipide turvanõrkuse avastamisel, mis on Eesti jaoks olulise mõjuga sündmus riigi funktsioneerimise seiskohast. Küberjulgeoleku-temaatikale viitab antud juhtumis asjaolu, et mõjutatud olid nii riiklikult oluline elektrooniline teave ja teenused (mh elutähtsad teenused), olulisel kohal olid küberrünnakute ennetamine ning riigi sotsiaalsete ja majanduslike protsesside toimimise tagamine. Juhtumi lahendamiseks kasutas riik nii infotehnoloogilisi kui ka organisatoorseid vahendeid. Magistritöö annab ka võimaluse selgitada välja, kas teaduskirjanduses esitatud teoreetilised väited väikeriikide julgeoleku võimekuse kohta kehtivad ka küberruumi kontekstis või vajab teooria täiendust.

Uuringus selgus, et klassikaline väikeriikide teoreetiline käsitlus, kus väikeriik on vähe võimekas (mh julgeoleku tagamisel), ei pruugi olla piisav ning vajab täiendamist. Küberruumi ja võimu mõiste muutumisega saavad riikide füüsiliste ressursside kõrval oluliseks ka riikide tegevused (nt tehnoloogiline areng, teadlikkus küberruumist jms), oskused (infotehnoloogia nutikas kasutamine), väiksus (nt informaalsed suhted, väikesed süsteemid jms). Seega võivad väikesed riigid saavutada küberjulgeoleku võimekuse suurriikide kõrval ja ees.

Võtmesõnad: väikeriik, haavatavus, küberjulgeolek, võim, võimekus.

SISSEJUHATUS

Riigi suurus on läbi aegade mõjutanud võimekust tulla toime julgeoleku[1] tagamisega. Kuna klassikaliselt puuduvad väikesel riigil selleks piisavad ressursid, on nimetatud küsimus väikeriigi peamiseid murekohti (Hey 2003, 4; Wilberg 1996, 22).

Väikeriike kirjeldav teooria sai alguse pärast külma sõja lõppu ning selles rõhutatakse väikeriigi haavatavust ja vähest võimekust erinevates valdkondades toime tulla. Julgeoleku puhul keskendutakse enamasti julgeoleku faktoritele (kes ohustab ja milline on oht), julgeoleku tagamise võimalustele ning sellega seonduvatele väljakutsetele (nt ressursside nappus) (Wivel *et al* 2014, 4; Wilberg 1996, 21; Knudsen 1996, 5; Thorhallsson 2018, 17).

Alates 1980ndatest on teooria teinud läbi muudatuse – kui varem toodi valdavalt välja vaid väikeriigi puuduseid (nt ressursside nappus), siis enam ei keskenduta vaid sellele, mida riik omab, vaid ka sellele, mida riik teha suudab (ehk milline on riigi võimekus[2] ja milliseks võib selle tulemusena kujuneda riigi võim). Enam ei räägita sellest, et väikeriigil pole võimu, vaid vastupidi – riik on võimeline saavutama võimu vaatamata oma väiksusele. (Vital 2006, 77; Thorhallsson 2018, 19; Nye 2010, 1) Muutuse põhjus on uus maailmapilt – enam ei oma tähtsust vaid konventsionaalne sõjaline võimekus, vaid uued väljakutsed, nagu näiteks küberruumi teke traditsiooniliste (maa, õhk, vesi, kosmos) sfääride kõrvale (Bayuk *et al* 2012, 1; War in the ... 2010). Tehnoloogia areng ja kättesaadavus tingib selle, et riigi rikkus ja võimekus sõltuvad tema oskustest teha tarku valikuid ning kasutada ära tehnoloogiaid, mitte niivõrd füüsiliste ressursside olemasolust (Castells 2010, 372). See tähendab, et klassikaline väikeriigi teooria ei pruugi enam täielikult oma eesmärki täita (Mouritzen, Wivel 2005; Thorhallsson 2018).

Küberruumi tekkimine uue kontekstina on seotud tehnoloogia arengu ja kättesaadavusega ning see on saanud igapäevase elu lahutamatuks osaks. Näiteks oli 2017. aastal 53% maailma majapidamistest internetiühendus (ICT Facts and ... 2017, 2) ning igapäevaselt kasutab internetti

[1] Julgeolek on seisund, mille puhul määratud teave, varustus, isikud, tegevus ja rajatised on kaitstud spionaaži, sabotaaži, õõnestustegevuse, terrorismi ja kahjustamise, samuti kaotsimineku või loata avalikustamise eest (Militerm *sub* julgeolek).

[2] Töö tarbeks kasutatud ingliskeelses originaalkirjanduses kasutatakse riikide iseloomustamiseks enamasti sõnu '*power*' (eesti keeles võim, võimsus), '*capacity*', '*capability*' ja '*ability*' (eesti keeles võime, võimekus, suutlikkus). Sellest tulenevalt kasutatakse töös riikide iseloomustamiseks mõistet 'võimekus', mis tähendab, et võimet (ehk suudet või oskust midagi teha) on üle keskmise, et selle abil saavutada võim, mida antud töös mh väikeriikide puhul käsitletakse (AMSS *sub* võimekus). Kindlate terminite tõlkimisel kasutatakse kindlaid termineid ka eesti keeles (nt '*hard power*' – 'kõva jõud').

(nt kaupade ostmiseks ja müümiseks, teenuste kasutamiseks ja pakkumiseks ning omavaheliseks suhtlemiseks) umbes 3,58 miljardit inimest (Statistics).

Võttes arvesse küberruumile omistatavaid väga unikaalseid tunnuseid, nagu näiteks riigipiiride ülesus, kättesaadavus jms, ning ka seda, et põhimõtteliselt on kõik *online*, on tekkinud olukord, kus iga küberruumi osaleja võib mõjutada teise tegevust igal ajahetkel ja ükskõik millisest maailma nurgast. Seega on päevakorda kerkinud termin kübervõim (*cyber power*), mis sõltub ressurssidest, mis iseloomustavad küberruumi ning loovad, kontrollivad ja edastavad elektroonikal ning arvutitel põhinevat infot. Omades kübervõimu on nii üksikisikul kui ka riikidel võimalik saavutada meelepäraseid tulemusi ehk käsutada kedagi või otsustada millegi üle. Seoses küberruumi ja kübervõimu mõiste tekkimisega on muutunud ka võimu (*power*) ja võimekuse (*capacity; ability*) mõiste riikide iseloomustamisel. (Nye 2010, 1–3)

Väikeste suveräänsete riikide osakaal maailmas ei ole mitte kunagi olnud nii kõrge kui praegu (Thorhallsson 2018, 17). Ka ei ole mitte kunagi varem olnud nii suure tähelepanu all nende ellujäämine (mh julgeoleku-teemad) (Hey 2003, 3). Tehnoloogia areng ja küberruumi teke on väikeriigi uurimustest kerkinud küsimus, kas jätta kõrvale klassikalised lähenemised väiksusest tulenevatest puudustest ning keskenduda hoopiski eelistele ja võimalustele, mida väiksus võib pakkuda (nt Katzenstein 1984; Nye 2010).

2007. aasta oli maailma jaoks unikaalne ja murranguline. Esmakordselt toimus poliitiliselt motiveeritud küberrünnak, kus sihtmärgiks olid Eesti riigiasutused ja erafirmad ning rünnakuks kasutati tuhandeid võrku ühendatud eraisikute arvuteid üle maailma (Czosseck *et al* 2011, 24; Shackelford 2010, 22). Väga oluline kirjeldatud juhtumi osas on rünnaku objekt ehk Eesti, mis on tituleeritud tehnoloogiliste lahenduste mõttes võimekaks väikeriigiks, kus riiklike ja erasektori teenuste (mh elutähtsate teenuste) kättesaadavus sõltub suuresti info- ja kommunikatsioonitehnoloogiate ning interneti olemasolust, ja et Eesti suutis rünnakutele ka vastu seista.

Eelnevast tulenevalt on käesoleva magistritöö **uurimisprobleem:** kuidas tagab väikeriik oma küberjulgeoleku võimekuse? Uurimisprobleemi täpsustamiseks püstitab autor teoreetilise **uurimisküsimuse**: kuidas mõjutab riigi väiksus tema küberjulgeoleku tagamise võimekust?

Magistritöö **eesmärk** on selgitada välja siseriiklikud tegurid, mis mõjutavad väikeriigi küberjulgeoleku võimekust. Eesmärgi saavutamiseks püstitatakse järgmised uurimisülesanded:

1. Selgitada välja väikeriigi teooriast ja küberjulgeoleku käsitlustest tulenevad siseriiklikud tegurid, nendest tulenevad eelised ja võimalused, mis võivad mõjutada väikeriigi küberjulgeoleku võimekust.
2. Analüüsida Eesti julgeolekupoliitika kujundajate ja ekspertide seisukohti väikeriigi küberjulgeoleku tagamise võimalustest üldiselt ning siseriiklikest teguritest, mis mängisid rolli 2017. aasta ID-kaardi turvariski juhtumi lahendamisel.
3. Analüüsida teooria, dokumendianalüüsi ja ekspertarvamuste tulemusi, vastata töö uurimisküsimusele, teha töö teemaga seonduvad järeldused ning anda poliitikasoovitused.

Magistritöö empiirilise uurimuse läbiviimiseks kasutatakse näitena Eesti ID-kaardi 2017. aasta turvanõrkuse ilmnemise juhtumit, mis puudutas ligi 800 000 Eesti poolt välja antud dokumendi kiipi, mille abil saab inimene end elektrooniliselt identifitseerides kasutada ligi 5000 avaliku- ja erasektori e-teenust. (Buldas *et al* 2018, 5; ROCA Vulnerability ...) Antud juhtum on oluline seetõttu, et toob esile riigi sõltuvuse info- ja kommunikatsioonitehnoloogiast ning internetist, mis on vajalik inimeste harjumuspärase elu (e-teenuste kasutamise), turvatunde ning riigi toimimise seisukohast, sest „teoreetiliselt oleks olnud võimalik luua ohvri virtuaalne koopia ja kasutada seda isiku tuvastamiseks, tema eest allkirjade andmiseks ja talle mõeldud andmete dekrüpteerimiseks, seda ka kaarti füüsiliselt omamata“ (Küberturvalisus 2018, 5). Nimetatud juhtumi lahendas Eesti pigem edukalt. Eelnevat kokku võttes on põhjendatud käesoleva töö **aktuaalsus.**

Nii Eesti kui ka rahvusvahelises kirjanduses on pühendatud väga palju teadusartikleid väikeriigi temaatikale ning võimu saavutamisele rahvusvahelises kontekstis rahvusvahelistest suhetes. Enamasti on keskendutud näiteks väikeriikide administratiivsele võimekusele haldusjuhtimises (nt Sarapuu 2010; Randma-Liiv 2002; Lowenthal 1987; Randma-Liiv, Sarapuu 2019 jne), majanduslikule ja innovatsioonivõimekusele (Katzenstein 1984; Kattel *et al* 2010), tavapärasele julgeoleku võimekusele (Hey 2003; Thorhallsson 2018; Knudsen 1996). Siseriiklikest teguritest, mis väikeriigi küberjulgeoleku võimekust mõjutavad, on kirjutatud vähe (Burton 2013, 216), enamasti keskenduvad tööd riigi väiksusega seotud puudustele ning nendest üle saamisele rahvusvahelise koostöö abil. Seega võib käesolevat tööd pidada pigem **uudseks.**

Lähtudes töö iseloomust, kasutab autor uurimuse teostamiseks **kvalitatiivset uurimismeetodit,** sest see on sobilik protsesside ja nende tähenduste uurimiseks (Ghauri, Grønhaug 2004, 98) ning selle lähtekoht on tegeliku elu kirjeldamine (Hirsijärvi *et al* 2005, 152). Lisaks annab meetodi

kasutamine võimaluse teha uurimist, teooria testimist ning uue teadmise loomist paralleelselt töö käigus (Bouma, Atkinson 1995; Frankel, Devers 2000).

Uurimuse läbiviimiseks vajalikud andmed saadakse dokumendianalüüsi ja poolstruktureeritud intervjuude kaudu, mis viiakse läbi valdkonna poliitikakujundajate või ekspertidega Eestist, kes puutusid Eesti ID-kaardi turvariski ilmnemise ja lahendamise perioodil sellega otseselt või kaudselt kokku.

Magistritöö jaguneb kolmeks peatükiks. Esimeses osas antakse ülevaade uurimisprobleemi teoreetilistest alustest, teises kirjeldatakse ja põhjendatakse uurimuse meetodit ja valimit ning kolmandas selgitatakse Eesti ID-kaardi turvanõrkuse näitel välja siseriiklikud tegurid, mis mõjutavad väikeriigi küberjulgeoleku võimekust. Töö tulemusena tehakse järeldused ning antakse valdkondlikud poliitikasoovitused.

Uurimuse teostamise tegi keerukaks töö kirjutamise momendil käimasolev kohtuprotsess, milles Eesti Politsei- ja Piirivalveamet süüdistab Gemalto AG-d ID-kaardi turvariskist mitteteavitamises ning et ID-kaardi turvariski läbiviidud julgeolekuhinnangud on osaliselt salastatud.

1. UURIMISPROBLEEMI TEOREETILINE RAAMISTIK

1.1. Küberjulgeoleku terminoloogia

Eesliite „küber-“ kasutamine on väga laialdane nii professionaalsetes, akadeemilistes kui ka tavaringkondades ning sageli kasutatakse mõisteid valimatult ja eritähenduslikult (Cavelty Dunn 2008; Luiijf *et al* 2013). Ka teooria ei defineeri mõistet üheselt, sest see hõlmab endas erinevaid elemente (näiteks info-, tehno-, võrgu- jms). Eesti küberjulgeoleku strateegia 2014–2017 defineerib lisas 2 eesliidet „küber-“ terminina, mis on seotud omavahel suhtlevate infotöötlusvahenditega (Küberjulgeoleku strateegia 2014–2017).

Järgnevalt määratleb autor magistritöös kasutatavaid küber-termineid, et luua alus uurimisinstrumentide loomiseks ja uurimistulemuste analüüsiks. Kuna magistritöö puhul on tegemist Eesti kaasusega, kasutatakse mõistete defineerimisel esmalt Eesti kübervaldkonna strateegiadokumente ning kui see ei ole piisav, kasutatakse muid asjakohaseid allikaid.

Küberruum on arenenud eraldiseisvaks ja arvestatavaks sfääriks traditsiooniliste (maa, õhk, vesi, kosmos) kõrval (Bayuk *et al* 2012, 1; War in the ... 2010) ning selle unikaalsus sõltub asjaolust, et see on inimese loodud ning nimetatud sfääridest koos tehnoloogia arenguga kõige kiiremini muutuv (Nye 2010, 4). Küberruumi mõiste kasvas 1980ndatel välja ulmeromaanidest (Libicki 2007, 5), kuigi küberruumi kontseptsiooni aluseks olev idee, et inimesed suudavad masinatega suheldes luua alternatiive tavapärasele keskkonnale, tekkis juba 1950ndatel (Ottis, Lorents 2010). Sealt edasi on interneti ja arvutite kasutamine levinud plahvatuslikult ning tänapäeval ei seostata seda enam pelgalt internetti ühendatud arvutiga.

Küberruumi definitsiooni osas ei ole ühtset arusaama (Ottis, Lorents 2010). Eesti küberjulgeoleku strateegia aastateks 2008–2013[3] ütleb, et „küberruum on arvutitel ja arvutisüsteemidel põhinev digitaalne ruum, mis toetab tänapäevase infoühiskonna toimimist ja koosneb peamiselt interneti poolt võimaldatud tegevuskeskkondadest ja igapäevaste toimingute lihtsustamiseks loodud digitaalsetest andmekogudest“ (Küberjulgeoleku strateegia 2008–2013, 41). Rahvusvaheline Telekommunikatsiooni Liit lisab definitsioonile info ja telekommunikatsiooni vahendid ning

[3] Käesolevas magistritöös ei ole küberrruumi defineerimiseks kasutatud dokumenti „Küberjulgeoleku strateegia 2014–2017“, sest see on sama valdkonna strateegia varasema versiooni jätk, mis ei defineeri mõisteid uuesti ega teisiti.

inimfaktori (Recommendation ITU-T X.1205), kuid ei täpsusta, kuidas küberruumi elemendid omavahel suhtlevad. Ottis ja Lorents (2010) pakuvad välja, et küberruum on ajast sõltuv kogum omavahel seotud infosüsteemidest ja inimestest (kasutajad), mis nende süsteemidega suhtlevad.

Küberruumi osalejate variatiivsus ning nende erinev võime mõjutada riikide julgeolekut ja stabiilsust on väga lai, ulatudes valitsusvälistest üksustest (nt kriminaalsed ühendused[4], vilepuhujad julgeolekuorganisatsioonidest[5], muud isikud või ühendused[6], kes soovivad ellu viia oma poliitilisi või strateegilisi eesmärke) kuni valitsusteni (Burton 2018, 2; Wood 2015; Greenwald *et al* 2013; Leyden 2016). See tähendab, et küberjulgeoleku puhul tuleb vaadelda kõiki nimetatud osapooli ja ka nende liitlasi. Arvestada tuleb nende suurenevat mõju ühiskonnale, poliitikale ja majandusele ning ka seda, et nende vastu võitlemine ning nende tegude avastamine ja karistamine võib osutuda keeruliseks või isegi võimatuks (Lonsdale 2016).

Nagu eelnevast lugeda võib, on teoreetikud ja praktikud (nt riikide strateegiadokumentides) pakkunud küberruumi osade ja osaliste tarbeks välja väga erinevaid seletusi, kuid enamus neist nõustub, et küberruum koosneb globaalselt ühendatud riistvarast, tarkvarast ja andmetest ning inimfaktorist (Ottis, Lorents 2010). Küberruum hõlmab kõiki osalisi, kes või mis on selle keskkonnaga seotud (Fischer 2009, 11) ning üksteist selles keskkonnas mõjutavad. Et mõista küberruumi keerukat olemust, ei tohi kõrvale jätta aja faktorit. Aeg märgib küberruumis sündmuste kogumit, mis hõlmab kõigi küberruumi osaliste omavahelisi suhteid ja annab küberruumile mõõtme (Ottis, Loretns 2010).

Küberruumi osade omavaheline sõltuvus on tekitanud olukorra, kus ühe elemendi haavatavus võib ohtu seada kogu süsteemi – ühest ohtlikust personaalarvutist (loe: inimesest, kes seda kasutab) võib käivituda protsess, mis halvab terve riigi tegevuse ja käivitab relvastatud konflikti. Seetõttu on tehnoloogilise arengu eeliste kõrvale tekkinud ka mõisted „küberoht“, „küberkaitse“, „küberjulgeolek“ ja „kübervõim“, mis on n-ö „kuumad“ teemad riikide julgeoleku seisukohast ning rahvusvahelistes suhetes. (Eriksson, Giacomello 2006, 222). Seega võib väita, et iga kord,

[4] Nt Islamic State of Iraq and al-Sham (ISIS), kelle motiivid võivad olla nii poliitilised kui ka seotud finantsilise kasu saamisega.
[5] Nt Edward Snowden, kes on endine CIA analüütik ja Ameerika Ühendriikide riikliku julgeoleku agentuuri (*National Security* Agency) töötaja, kes on vastutav 2013. aasta mais aset leidnud Ameerika Ühendriikide ajaloo suurima andmelekke eest (lekkisid salastatud siseriiklikud julgeolekudokumendid). Tema motiiv oli teavitada maailma Ameerika Ühendriikide julgeolekuagentuuride järelevalvetegevustest.
[6] Nt isik, kelle motiiv oli loomade õiguste eest võitlemine.

kui tehnoloogia või võrgusüsteemide arengus toimub positiivne edasiminek, kasvab samaväärselt oht maailmakorrale.

Et antud töö keskendub Eesti kaasusele, siis tähendab küberjulgeolek „kõiki elektroonilise teabe, teabekandjate ning -teenustega seotud toiminguid, mis mõjutavad riigi julgeolekut", ning küberjulgeoleku tagamise eesmärk on läbi mitmesuguste tegevuste „vähendada küberruumi haavatavust, /.../ ennetada küberrünnakuid ning taastada rünnakute korral võimalikult kiiresti infosüsteemide toimimine" (Küberjulgeoleku strateegia 2008–2013, 40). Küberjulgeoleku üks osa on küberkaitse, mis on „riigi kriitilise infrastruktuuri toimimist toetavate info- ja sidesüsteemide kaitse korraldamine, mis seisneb nii infotehnoloogiliste, organisatoorsete kui ka füüsiliste turvameetmete kasutuselevõtmises ja ajakohastamises", mille tegevustest on antud töö kontekstis märkimist väärt infoturve (mis on küberjulgeoleku tagamise alus) ehk „riigi poliitiliste, sotsiaalsete ja majanduslike protsesside toimimiseks vajalike infosüsteemide talituspidevuse tagamine" (*ibid.*, 41). Küberohuks ja -riskiks võib eeltoodud definitsioonide põhjal nimetada olukorda (kahju) või selle tekkimise tõenäosust küberruumis, mis seab ohtu küberjulgeoleku. Küberohud ja -riskid realiseeruvad nii kübertegevuste (nt küberkuriteod või oskamatus tehnoloogiaga ümber käia) kui ka tegevusetuse (nt vananenud võrgutehnoloogia tähelepanuta jätmine) tulemusena, mis tähendab, et tegevus või tegevusetus on toime pandud võrgu- või infosüsteemide abil või need on sihtmärgiks (Goodman, Brenner 2002; Hansen, Nissenbaum 2009, 1155).

Oluline on ära märkida küberruumi erinevus füüsilisest keskkonnast, kuigi need mõlemad on oma olemuselt mitmetasandilised. Küberruumi väga suur mõjuala ei ole sageli hoomatav ja seetõttu kaitstav: haavatavus võib ilmneda igal ajahetkel, erinevates situatsioonides ja küberruumi osades ning rünnaku võib toime panna etteaimatamatu (kuritegelik või hoolimatu[7]) isik või isikugrupp, kelle motiivid võivad olla erinevad (Taipale 2009). Lisaks suurele ruumile on oluline võtta arvesse küberruumi kättesaadavust ja odavust, millele viitab asjaolu, et tavakodaniku arvuti ja oskused võivad seada ohtu riigi suveräänsuse või tekitada mõnele ettevõttele suurt moraalset või rahalist kahju.[8] Eelnevat arvestades on pea ilmvõimatu kaitsta kogu küberruumi. Näiteks toob Jamie Shea (2016) oma artiklis välja, et samal ajal kui riik või organisatsioon üritab iga olulist majandusliku või sõjalise infrastruktuuri osa iga ajahetkel turvata, võib ründaja valida vaid ühe objekti ning keskenduda 100%liselt vaid selle hävitamisele. Kui keegi arvab, et ta parasjagu mõnele

[7] Küberohu tekitab ka hoolimatu inimene, kes kasutab vananenud tarkvara ning mõtleb, et „see (kahju) temaga ei juhtu" (autor).
[8] Kui inimene ja tema tehnika on piisavalt võimsad või rünnatav objekt nõrgalt turvatud (autor).

haavatavusele ei keskendu (sest see pole hetkel oluline), siis õnnetus võib tabada ikkagi – küsimus ei ole selles, kas midagi juhtub, vaid millal see juhtub (*ibid.*).

Veel üks oluline küberruumiga seotud aspekt on, et selle infrastruktuur on suurelt osalt erasektori omanduses, mis tähendab, et valitsus ei saa seda kontrollida ega turvata, nagu on võimalik tema enda puhul (Gross 2016, 115), ning väga palju asju juhtub väljaspool riigi kontrolli isegi kõige võimsamate riikide puhul (Nye 2010, 1). Riigi huvi erasektori vastu seisneb selles, et muuhulgas haldab erasektor kriitilisi riigi toimimiseks olulisi infrastruktuuri osi ning erasektori intellektuaalsetel varadel põhineb riigi üldine majanduslik heaolu. Lisaks ei piirne küberruum riigipiiridega, vaid on riikideülene nähtus, mis hägustab veelgi omistamise, rollide või vastutuse piire, mis võivad olla nii riigisisesed kui ka rahvusvahelised.

Võrreldes püsivusega füüsilises ruumis on küberruum väga kergesti muutuv/muudetav ning suured muutused (näiteks riigi jaoks olulise info kustutamine) võivad toimuda minutite jooksul ning kahjud võivad olla kolossaalsed[9] (Nye 2010, 4).

Anonüümsus ja omistamise problemaatika on küberruumi nurgakivid, mis ühelt poolt tuleneb küberruumi avatusest ja võimalusest teha tegusid distantsilt ning peita oma jälgi küberruumis ja teiselt poolt defineerimise keerukusest. Seega pahategija identifitseerimine on väga raske, kui mitte öelda võimatu[10]. (Payne 2003, 412; Lupovici 2016, 338). Omistamise keerukus tekitab omakorda karistamise problemaatika – kui süüdlane pole selge ega tegu tõendatud, siis pole võimalik karistada (Kello 2013, 33).

Küberruumi asümmeetrilisust näitab asjaolu, et küberrünnakuid on võimalik teha ilma nähtavate tagajärgedeta füüsilises maailmas. Seetõttu on „tavainimesel üsna raske vahet teha, kas näiteks pangateenus on seiskunud küberrünnaku, tehnilise rikke või plaaniliste hooldustööde tõttu“ (Tiirmaa-Klaar 2009), või kas küberruumis edastatud info jõuab adressaadini muutmata või avamata kujul (adressaat ei pruugi teadagi, et kuritegu on sooritatud ja millal see juhtus).

Lähtuvalt töö teemast on oluline selgitada küberjulgeoleku võimekuse tähendus.

[9] Näiteks Eesti on andnud RIA peadirektorile õiguse ohtlik arvuti Eesti internetist välja lülitada, kui tegemist on olulise mõjuga küberintsidendiga või arvuti haldaja ei saa ise õigel ajal seda lahendada (Lõugas 2017).
[10] 2007. aasta Eesti riigi ja erasektori vastu suunatud küberrünnaku kohta arvatakse, et ründaja puhul oli tegemist Venemaaga, kuid tõestada seda ei ole olnud võimalik, mistõttu ei ole esitatud ka süüditust. (Vaidya 2015, 4).

Suveräänse riigi tugevuseks peetakse selle ühiskondlikku, majanduslikku ja poliitilist võimekust kombineerituna sõjalise võimekusega, mis omakorda näitab riigi võimekust kaitsta oma territooriumi ja inimesi nii, et need saaksid omalt poolt tugevdada riigi majandust. Sõltuvus internetist ja infosüsteemide haavatavusega kaasnevad küberohud on viinud julgeoleku võimekuse kontseptsiooni uuele tasemele. Riigi haavatavus küberruumis sõltub tema tehnoloogilisest arengust (millisel tasemel ja kui palju on riigis toimuv seotud infotehnoloogiliste lahendustega), aga ka võimekusest tulla ründamise asemel toime enda kaitsmisega potentsiaalsete või realiseerunud ohtude eest. See omakorda on arendanud välja kübervõimu (*cyber power*) mõiste, mis sõltub uuest kontekstist maailma poliitikas, küberruumist (Nye 2010, 1). Kübervõim põhineb erinevatel ressurssidel, mis loovad, kontrollivad ja edastavad elektroonikal ja arvutitel põhinevat infot: infrastruktuure, arvutivõrke, tarkvara ja inimeste kompetentsi. Omades kübervõimu, on võimalik saavutada meelepäraseid tulemusi, mõjutada sündmusi või luua eeliseid nii küberruumi sees kui ka väljas (*ibid*, 4, vt ka Weber 1947, 152). Küberjulgeoleku tagamise võimekus võiks eelnevalt toodud küberjulgeoleku ja kübervõimu definitsiooni järgi tähendada üle keskmise suutlikkust mitmesuguste tegevuste ja erinevate ressursside, mis loovad, kontrollivad ja edastavad elektroonikal ja arvutitel põhinevat infot (Nye 2010, 1), kaasabil „küberruumi haavatavuse vähendamist, küberrünnakute ennetamist ning rünnakute korral võimalikult kiiresti riigi poliitiliste, sotsiaalsete ja majanduslike protsesside tarbeks kasutatavate infosüsteemide toimimise taastamist, kasutades ja ajakohastades nii infotehnoloogilisi, organisatoorseid kui ka füüsilisi turvameetmeid“ (vt ka Küberjulgeoleku strateegia 2008–2013, 40). Nimetatud definitsioon on väga üldine ega täpsusta tegevusi, siseriiklikke tegureid ja nende mõju ega võrreldavaid küberjulgeoleku võimekust näitavad tulemusi. Ka ei ole autor leidnud ühtegi asjakohast teoreetilist käsitlust, pigem annavad vastuseid riikide küberjulgeoleku võimekuse saavutamise kohta erinevad riikidesisesed ja ka nende ülesed (nt Euroopa Liidu, ISO jms) standardid, juhised ja strateegiad.

Üks võimalus, kuidas riikide küberjulgeoleku võimekust mõõta, on rahvusvahelised küberjulgeoleku indeksid, milles võrreldakse riikide valdkonnaga seotud riiklike protseduuride, institutsioonide või tegevuste olemasolu. Kaks indeksit, milles muuhulgas käsitletakse ka Eestit ja milles uuritakse ka siseriiklikke tegureid, on *Global Cybersecurity Index* (edaspidi ITUI) ja *National Cyber Security Index* (edaspidi NCSI). Mõlemad põhinevad avalikult kättesaadaval infol, mille põhjal arvutatakse iga indeksis osaleva riigi skoor, mis määrab ära riigi võimekuse võrreldes teiste riikidega. ITUI mõõdab Rahvusvahelisse Telekommunikatsiooni Liitu (International Telecommunication Union, edaspidi ITU) kuuluvate liikmesriikide pühendumist küberjulgeolekule, et tõsta valdkondlikku teadlikkust globaalsel tasemel, ja keskendub viit tüüpi

mõõdikutele, milleks on õiguslikud, tehnilised, organisatsioonilised, võimekuse ja koostöö näitajad (Global Cybersecurity Index). NCSI mõõdab riikide valmisolekut ennetada küberohte ja tulla toime küberintsidentidega ning kirjeldab võrdluses olevate riikide parimaid praktikaid, andes teistel võimaluse oma võimekust toodud näidete varal parandada. NCSI jagab mõõdikud nelja gruppi, milleks on riigi seadusandlus, küberjulgeolekuga tegelevad organisatsioonid, koostöö ja tulemused (nt poliitikad, tehnoloogiad või programmid). (Rikk 2018)

Autor ei ole kohanud ühtegi küberjulgeoleku võimekuse mõõtmise vahendit, mis eristaks riike nende suuruse järgi, pigem hinnatakse, kas valdkonnaga seotud riiklikud protseduurid, institutsioonid või tegevused on loodud või mitte. Kuidas mõõdikute sisu, kvaliteet või mõju avalduvad riigi küberjulgeoleku võimekuses, ei analüüsita, seda peavad (kahjuks) näitama reaalsed juhtumid ja nende lahendamine.

1.2. Väikeriigi määratlus

Väikeriikide uurimisel on kõige problemaatilisemaks osutunud mõiste „väike" defineerimine ning konsensust selles, milliseid kvalitatiivseid või kvantitatiivseid kriteeriume ja näitajaid mõiste määratlemisel kasutada, ei ole saavutatud (Maass 2009, 65; Pace 2000, 107; Baehr 1975, 459; Kattel *et al* 2010, 65). Ka on erinevatel teoreetikutel tekkinud küsimus, kas väiksuse puhul ongi vaja ühese definitsioonini jõuda või annab laialivalguvus paindlikkuse ja rohkem vabadust või peaks määratlus olema hoopis range ehk põhinema kvantitatiivsetel näitajatel. (Baehr 1975, 459; Maass 2009, 66) Sellest tulenevalt võibki väikeriigi defineerimisel eristada suhtelist ja absoluutset kriteeriumit, millest esimene ütleb, et väiksus sõltub kontekstist ja võrdlusest teise poolega, ning teine vastab küsimusele, millal omab suurus tähtsust. Esimese puhul võib riigi väiksust defineerida pigem teiste riikidega võrreldes näiteks rahvusvaheliste suhete kontekstis, teist aga siseriiklike (või sotsioloogiliste) nähtuste selgitamiseks (Randma-Liiv, Sarapuu 2019; Maass 2009).

Ilmselt kõige laiem riigi väiksust määrav kriteerium on rahvastiku suurus, mis on ka näide riigi suuruse absoluutsest määratlusest. Thorhallsson (2018, 18) toob välja, et enamik sotsiaal- ja majandusteadlasi määratlevad riiki väikesena, kui selle alaline populatsioon jääb alla 10–15 miljoni inimese piiri, Maailmapanga definitsioon piirab riigi väiksuse koguni 1,5 miljoni elanikuga (The World Bank 2018) ning eri määratlusi on veelgi. Sarnaselt populatsiooni suurusega võivad väiksuse kriteeriumiteks olla ka muud füüsilised tunnused, nagu näiteks territooriumi, majanduse

või sõjaväe suurus, kuid need pole väikeriigi teoorias nii levinud, sest väiksuse muud aspektid määrabki ära eelkõige populatsiooni suurus (Maass 2009, 71–72).

Rahvusvahelistes suhetes kõrvutatakse riike nende võimu (*power*) järgi, mis traditsiooniliselt seostub otseselt eeltoodud ressursside kriteeriumitega – riik omab võimu, kui tal on teatav ressurss (inimkapital, maa jms) ja oskused seda millegi saavutamiseks kasutada. Kui riik on väike, siis on ta võimetu ja nõrgem pool asümmeetrilises suhtes (nt Vital 2006). „Võimekus" on väikeriigi teoorias riigi suuruse suhtelises määratluses n-ö uus lähenemine, sest võimu mõiste on külma sõja järgsest perioodist alates nihkunud võimult, mida riik omab, võimule, mida riik teostab (Thorhallsson 2018, 19). Olemasolev, absoluutsel suurusel põhinev teooria ei täida moodsas maailmas, kus domineerivad uued väljakutsed, nagu näiteks kliimamuutustega seonduvad looduskatastroofid, küberrünnakud, terrorismi kasv, põgenikekriisid, *online*-propaganda kampaaniad jms, enam riikide määratlemise puhul oma ülesannet (Mouritzen, Wivel 2005, 4; Thorhallsson 2018, 17).

Kui vaadelda väiksust julgeoleku kontekstis, tuleb arvesse võtta riikide väiksuse erinevust. Näiteks on Rothstein (1968, 14, 21) defineerinud väikeriiki järgnevalt: väike võim on riigil, mis tunnistab, et ta ei ole võimeline ise oma julgeolekut tagama, seega võib iga riik olla kas nõrgem või tugevam pool sõltuvalt sellest, millised on tema võimalused. Magistritöö autori arvates on antud määratlus oluline, kuid selgituseks võib lisada asjaolu, mis võimu mõistet täpsustab. Nimelt on 21. sajandil võimu kontseptsioon muutunud. Traditsiooniliselt tähendab võim nn kõva jõudu (*hard power*)[11], mis seostub eelkõige sellega, mida riik omab (nt territoorium, sõjaline võimekus, majanduslik suurus) ja mille tulemusena saab teda traditsioonilises mõttes pidada võimsamaks pooleks (sest ta võidab nt sõja). Tänu teaduse, tehnoloogia ja majanduse arengule ei ole füüsilistel varadel enam võimu määratluses nii suurt tähtsust ning võim ei tähenda enam füüsilisi ressursse, vaid võimekust muuta riikide käitumist, olles atraktiivne kultuuri, poliitiliste ideaalide ja poliitikatega, milles võim avaldub nimetatud näitajate toel poliitilise keskkonna muutmisena ehk pehme jõuna (*soft power*). (Nye 1990, 154, 166–167) Pehme jõu rakendamise etaloniks võib tuua küberruumi, mille iseloom ja kasutamine on tüüpilised näited võimust selle sajandi globaalses poliitikas. Võim sõltub kontekstist ning küberruum on maailma poliitikas väga oluline uus kontekst, mille abil näiteks poliitilist keskkonda muuta, sest tehnoloogia arenedes saavad võimule ligi ka muidu nõrgad või

[11] Traditsiooniliselt keskendub kõva jõud sõjalisele sekkumisele, sunniviisilisusele jms, selleks et saavutada mingeid riiklikke huve teise riigi suhtes.

vähem võimekad riigid (Nye 2010, 1). See muudab tavapäraseid ühiskondlikke suhteid, sh riikidevahelist suhtlust, ja muu hulgas ka võimekust tagada julgeolek. (Nye 1990; Nye 2010; Katzenstein 1984) Küberruum näitab hästi, et julgeolekuga ei pea seonduma vaid füüsiline oht (nagu näiteks kõva jõuga üldjuhul kaasneb), seega võib riik teoreetiliselt oma suveräänsusest ilma jääda ühegi piisa vereta ning põhimõtteliselt ükskõik kui traditsiooniliselt väikese ja nõrga riigi või valitsusvälise subjekti tegude tagajärjel (Knudsen 1996, 6; vt ka pt 1.3).

Thorhallsson (2006, 8) pakub riigi suuruse defineerimiseks välja multifunktsionaalse lahenduse, mis hõlmab kuut kategooriat absoluutseid ja suhtelisi näitajaid, mis iseloomustavad riigi siseriiklikku ja rahvusvahelist käitumist (nt otsuste tegemise protsessis) ning seda, kuidas teised riigid nendesse suhtuvad. Need kuus kategooriat (suurust) on: fikseeritud suurus (territoorium ja populatsioon), suveräänsus (võimekus hoida oma territooriumi suveräänsena ja valitseda seda kompetentselt), poliitiline suurus (militaarne ja administratiivne võimekus, võimekus välispoliitiliste konsensuste saavutamiseks, sisemine ühtekuuluvus), majandus (SKP suurus ja arenguvõimalused), tunnetuslikus (kuvand riigi sees ja riigist väljas riigi võimekusest), eelistused (riigijuhtide ambitsioonid, prioriteedid riigi mõjuulatusest rahvusvahelises mõttes; riigi võimekus neid täita). Raamistik võtab arvesse nii riigisiseseid kui ka -väliseid suuruse või väiksuse aspekte. Riigisisene võimekus määrab ära riigisisesed ressursid ja nende oskuspärase kasutamise, riigiväline võimekus viitab suurusele rahvusvahelises kontekstis ja võimekusele tegutseda rahvusvahelisel areenil, esindades oma parimaid külgi (Thorhallsson 2006, 14). Viimane annabki autori arvates aluse kasutada definitsiooni lisaks väikeriigi käitumise määramisele ka riigi suuruse hindamiseks, sest nagu eespool välja toodud, on võimu mõiste tänapäeval muutunud nii, et oluliseks saab selle suhtelisus ning see, millisena riik paistab.

Käesolevas magistritöös kasutab autor eeltoodud definitsiooni, sest see hõlmab endas nii väiksuse suhtelisust kui ka riigisiseseid tegureid. Kuigi esmapilgul võib tunduda, et definitsioon on laialivalguv, siis annab see autori arvates hoopis võimaluse väga erinevatel väikeriikidel sobituda antud konteksti ning seega erinevate lähenemistega uuringutesse ja situatsioonidesse. On väga oluline, et riigi „väiksus" ei läheks definitsioonide piirangute tõttu kaduma (Maass 2009, 80).

1.3. Väiksusest tulenevad eelised ja võimalused väikeriigi teoorias

1.3.1. (Küber)julgeoleku tegurid

Julgeoleku võimekuse uurimiseks tuleb riik asetada poliitilisse konteksti, sest julgeoleku perspektiivi on vaja võrrelda mingite väliste asjaoludega. Analüüsides riigi julgeoleku võimekust või selle suureks või väikeseks tituleerimise aluseid, tuleb aru saada riikide võimete erinevusest väikeriigi kui nõrgema poole vaatenurgast. Julgeoleku tagamisel mängivad rolli mitmed asjaolud, nagu näiteks riigi geograafiline asukoht (võimsa riigi läheduses), ohustaja ja oht (kes ohustab ja milline on oht ning selle realiseerumine), ajaloolised suhted ja poliitikad seoses võimsa riigiga ning koostöö, mis võimaldab võimete erinevust stabiliseerida (Knudsen 1996, 4–5, 9).

Riigi sõjaline võimekus sõltub väikeriigi teoorias lisaks eeltoodud asjaoludele ka ressursside piiratusest – esiteks ei võimalda vähene inimressurss luua suurt sõjaväge ning teiseks ei võimalda rahalised vahendid soetada kallist sõjatehnikat või ehitada -rajatisi. Järelikult on väikeriigid haavatavad – nad ei ole suutelised endast suuremaid riike ründama ega ka ise oma julgeolekut tagama (mis tähendab, et eelised või võimalused puuduvad) (Vaicekauskaité 2017, 7–8).

Väikeriigi julgeolekuga seotud eeliste või võimaluste osas on Knudseni (1996, 8) arvates väikeriigi teooriast kõrvale jäänud kaks väga olulist teemat. Esiteks see, mida väikeriik saab ise oma julgeoleku tagamiseks ära teha, nagu näiteks oskuslik diplomaatia (või muud siseriiklikud protsessid). Teiseks arvab ta aga, et väikeriigid ei saa tegelikkuses ise oma ellujäämist pikaajalises plaanis mõjutada, sest seda teevad välised faktorid (nagu nt suurriikide poliitikad, liidud, kuhu väikeriigid astuvad), ning niikaua, kuni väikeriigid nende faktoritega kaasa lähevad, on nende julgeolek kindlustatud.

Koostöö küsimust käsitleb rahvusvaheliste suhete teooria, milles on väga olulisel kohal väikeriigi-temaatika ja millest leiab suurema osa võimalusi, mille abil väikeriigid saaksid väiksusest tulenevaid piiranguid leevendada (mh ka julgeoleku tagamine). Nagu teiste teooriategi puhul on ka nimetatud teoorias väikeriik haavatav ja vähe võimekas ning püüab leida oma nišši. Kui see nišš on piisavalt oluline mõne tugeva partneri (nt NATO jms) jaoks, pakub tugev partner väikesele riigile võimalusi olla võimekam või oma käekäiku mõjutada (nt olla kaitstud ohustaja eest) (Vital 1967; Walt 1987; Mouritzen, Wivel 2005). Liitudesse astumisel on oluline roll siseriiklikul võimekusel – nt võib nišiks olla oskuslik riigivalitsemine, mis annab partnerile kindluse, et liidus

panustavad kõik, ja enne, kui liit peaks väikeriigi tegemistesse sekkuma, suudab ta ise hakkama saada (Jervis 1978, 172).

Seega on tähtis enne partnerite peale lootma jäädes mõelda, mida väike riik saab riigisiseselt oma julgeoleku tagamiseks ära teha. Näiteks võib väike riik leida eeliseid ja võimalusi oskuslikult kombineeritud institutsioonidest ja protsessidest (Rothstein 1968, 29; Thorhallsson 2018, 18; Kattel *et al* 2010, 72). Oluliseks on saanud teaduse ja tehnoloogia ärakasutamine ning n-ö digitaalne võimekus küberruumis. Muuhulgas põhineb tänapäeval moodne sõjaline võimekus ja digitaalselt arenenud riigi julgeolekuga seonduv infotehnoloogial, mis tõstab efektiivsust, kuid teeb samas sõltuvaks ja haavatavaks igasuguse suurusega riigi, sest oht võib ähvardada ükskõik millisest maailma paigast ja põhimõtteliselt ükskõik kelle käe läbi. Informatsiooni ja digilahenduste ärakasutamine (nt produktiivsuse suurendamine tegevuste automatiseerimisega) võib anda ka väikesele riigile võimaluse muutuda suurte riikide kõrval võimsaks (Goodman 2010, 11; Areng 2014, 2, 5; vt ka pt 1.1. ja 1.2.) ning muutunud maailmas on suured võimukad riigid kaotanud võimaluse organiseerida maailma nii, nagu nemad seda tahavad (Buzan, Segal, 1996, 7, 10).

Seoses eeltooduga on päevakorda kerkinud riikide kübervõim ja küberjulgeolek, mida väikeriigi teoorias ei ole eraldi käsitletud. Seda, kas ja kuidas väikeriik enda küberjulgeoleku tagab, tuleb kaudselt tuletada muudest lähenemistest (nagu nt väikese riigi haldusvõimekus, võimu mõiste muutumine, innovatsiooniteooria, rahvusvaheliste suhete teooria jms), mis ütlevad, et pigem on väike riik vähe võimekas ning see on seotud väheste ressurssidega, mida riik omab.

Ka töös vaadeldud küberjulgeoleku temaatika ei diferentseeri riike nende suuruse järgi ega anna otseselt aimu, kuidas mõjutab riigi väiksus küberjulgeoleku tagamise võimekust või kas väiksus annab mingeid eeliseid. Erisuse toob välja eelnevalt mainitud võimu mõiste muutumine, riigi digitaalne areng ja sõltuvus sellest ning riigi funktsionaalsus, sest enam ei pea riigi julgeoleku ohustamiseks ilmtingimata kuulutama välja sõda konventsionaalses mõttes, riikliku julgeolekukriisi tekitamiseks piisab infotehnoloogiast ja internetist sõltuva elutähtsa teenuse halvamisest küberruumis, mida saab selle omaduste tõttu teha iga küberruumis osaleja. Seega võib iga infotehnoloogiast sõltuv riik olla julgeoleku mõttes kas võimas või haavatav ning üks ega teine ei sõltu vaid tema suurusest klassikalises mõttes, vaid ka muudest teguritest.

Kokkuvõttes võib öelda, et julgeoleku mõttes on väikesed riigid suurte riikidega võrreldes pigem nõrgad ja haavatavad. Vaadeldes riike küberjulgeoleku kontekstis (vt ka pt 1.1), kerkivad julgeoleku tagamisel lisaks füüsilistele ressurssidele üles ka oskused, seega on küberjulgeoleku tagamise võimekuse juures oluline vaadelda nii majanduslikku võimekust ja üldist haldusvõimekust kui ka riigi tunnetusliku võimekust.

1.3.2. Administratiivsed tegurid

Rahvastiku suurus on üks määravamaid riigi suuruse näitajaid ning sellest sõltub, mil viisil riik toimib. Antud peatükk vaatleb, kas ja kuidas mõjutab väiksus riigi institutsionaalset struktuuri ja poliitilist ning administratiivset käitumist, mis on olulised mh ka küberjulgeoleku tagamisel.

Väikese populatsiooni all peetakse silmas eelkõige seda, et riigi inimressurss on piiratud. Farrugia (1993, 221) toob välja, et seetõttu põhinevadki sellised suhted kitsal kommuunil ja on kogukonna sees väga personaliseeritud, millele Benedict (1966, 26; 1967, 49) lisab, et nimetatud suhted baseeruvad rollidel[12], millega inimesed väikeses riigis igapäevaselt kokku puutuvad, ning see võib tähendada, et olulised pole mitte inimese oskused, vaid see, kes ta on ja keda ta tunneb. Situatsioonis, kus kõik tunnevad kõiki, muutub roll eriti oluliseks, ning mida väiksem on ühiskond, seda tavapärasemaks sellised suhted saavad ja seda rohkem võivad need mõjutada riigi valitsemist (Sutton 1987, 15).

Teine oluline väiksusest tulenevat ressursipuudust puudutav küsimus on riigi funktsioonide täitmine – et riik toimiks, peab ta täitma peamiselt elanike heaolu kindlustamisega seotud funktsioone. Kõige selle juures ei ole vahet, millise suurusega riik on. Kui inimressurss on väike, räägitakse sageli ka prioriseerimisest, kuluefektiivsusest ja multifunktsionaalsetest ametikohtadest (Randma-Liiv 2002, 377, 379), mis võib tekitada olukorra, kus mõned riigi funktsioonid jäävad täitmata või need toimivad ressursi puuduse (nt kompetentsete erialaspetsialistide defitsiidi) tulemusena ebaefektiivselt. Suurte valitsemiskulude tõttu võib valitsus kaaluda riigi funktsioonide delegeerimist erasektorisse või valitsusvälisesse organisatsiooni, kui vähese ressursi mõju sealseidki võimalusi ära ei nulli.

[12] Näiteks võib riigi president olla samal ajal naabrinaine, lapse lasteaiakaaslase ema, spordiklubi või korporatsiooni kaaslane, mistõttu võib väga palju inimesi väikese populatsiooniga riigis öelda, et nad tunnevad presidenti isiklikult ja vastupidi. (autori märkus).

Rahvastiku suurus mõjutab nii riigi ülesannete täitmist kui ka poliitilisi valikuid ning väikeriigi puhul on seda tõlgendatud nii negatiivses kui ka positiivses võtmes.

Negatiivses mõttes tähendab väike rahvastik puudust või piirangut saada hakkama riigi valitsemisega, sest see võib olla suuresti mõjutatud üksikisikute otsustest (nt ainus valdkonna ekspert, kes on kompetentsist olenemata valdkonna tippjuht), informaalsetel suhetel (tekitades mh korruptsiooni võimalikkuse ja demokraatia vähenemise), toimuda ebakompetentselt (ametis on kellegi tuttav, oskused ei ole määravad) või olla riigi kontrolli alt sootuks väljas (Lowenthal 1987, 37; Sarapuu 2010, 24; Randma-Liiv, Sarapuu 2019, 4; Randma-Liiv 2002, 381). Halb valitsemine võib aga omakorda pärssida riigi üldist arengut ja seega ka võimekust.

Positiivses mõttes annab riigi väiksus aga eeliseid[13]. Näiteks võimaldab väike kogukond suuremat riigisisest koostööd ühtse eesmärgi nimel, sest kõik tunnevad kõiki ning seega võib iga ametnik, ettevõtja või teadlane pöörduda lihtsa vaevaga ja kiiresti vajaliku instantsi poole, läbimata bürokraatlikke või institutsionaalseid piiranguid (Brock 1987, 15). Veelgi enam, personaalse tutvuse puhul võib usaldus tekkida kergemini kui täiesti võõra inimesega suheldes (Sarapuu 2010, 39). See puudutab ka suhteid riigist väljaspool elavate kodanikega, mis tähendab, et neid saab suunata tegutsema oma riigi arengu hüvanguks. Koostööle aitavad kaasa informaalsed suhted (nt usalduse teke), riigi lamedad juhtimisstruktuurid ja kuvand valitsusest, mis on inimesele väga lähedal (Sutton 1987, 15; Thorhallsson 2000, 85–86). On ka täheldatud, et personaalsed ja informaalsed suhted väikeriikides on mõjutanud oskust saavutada väga kergesti konsensus ja vältida erimeelsusi. See tuleneb populatsiooni väiksusest, sest väikeriigi inimene ei tea kunagi, millises rollis võib ta kellegagi tulevikus kohtuda. See tõenäosus väheneb populatsiooni kasvuga. (Lowenthal 1987, 39) Multifunktsionaalsuse puhul on positiivse joonena välja toodud suuremat ülevaadet asjadest, manööverdamisruumi ja kiirust asjaajamisel (nt üks minister mitme valdkonna peale) (Sarapuu 2010, 30, 38), mis võimaldab muutusi paindlikumalt koordineerida, edastada ning probleemidega kiiremini toime tulla (bürokraatia jääb vahele) (Hoscheit 1992, 274; Farrugia 1993, 223; Randma-Liiv 2002, 387).

Kokkuvõttes võib öelda, et väiksus mõjutab riigi haldusvõimekust nii positiivselt kui ka negatiivselt ning sõltub sellest, millised on riiki juhtivate inimeste administratiivsed või poliitilised valikud.

[13] Mida teinekord on nimetatud müütideks (vt Randma-Liiv, Sarapuu 2019, 4).

1.3.3. Majanduslikud tegurid

Majanduse suurus on teine oluline, kuigi vähem kasutust leidev näitaja väikeriigi teoorias. Joenniemi (1998, 62) toob välja, et riigi majanduslik võimekus võiks olla väiksuse definitsioonis olulisemal kohal, sest riigi efektiivsuse jaoks ei ole oluline mitte toores sõjaline võim, vaid pigem see, kuidas riik suudab teistega majanduslikult konkureerida (käituda targalt, ingl *smart*). Võiks tunduda loogiline, et kui riigi majanduslik võimekus on väike (madal SKT, vähesed loodusvarad, avatud majandus, sõltuvus väliskaubandusest jms), siis pole tal ressurssi põhimõtteliselt mitte millekski – riik peab tegema parimad võimalikud valikud ja oma tegevusi väga rangelt prioriseerima (nt e-teenused vs füüsiliselt kättesaadavad teenused riigi valitsemisel). Põhjus aga, miks majanduse suurust väga oluliseks riigi suuruse mõõdikuks ei peeta, on tõsiasi, et kuigi väike majandus seab riikidele mitmeid väljakutseid, ei tähenda see alati ületamatuid piiranguid, sest neid saab lahendada õigete poliitiliste valikutega ressursside paigutamisel ja alternatiivsete lahenduste leidmisega, nagu on tehtud näiteks Singapuris, Eestis jt riikides (The World Bank ...; Thorhallsson 2018, 18; Rothstein 1968, 29). Oluline on seega inimkapital, mis suudaks riigi majanduslikku ja administratiivset võimekust mõjutada (mh küberjulgeoleku tagamist).

Kui vaadelda innovatsiooniteooriat, siis selles on ühe väikeriigi tunnusena välja toodud, et väiksus on piirang majanduse arengule ja innovatsioonile, sest puudub finantsiline võimekus ja inimkapital, et panustada teadusesse, arengusse jms (nt Kattel *et al* 2010). Praktikas on aga tõendeid, et kui väheste võimalustega riik on mingis valdkonnas nõrgem pool, siis on tal võimalus parandada seda läbi uuenduste ja arengu, sest väiksus ning koostöö- ja suhtlusvõimalused võivad olla võtmetegurid innovatsiooni ja majanduse arengu saavutamisel. (*ibid* 66–67; Areng 2014) Näiteks võivad tõhusad institutsioonid ja infotehnoloogilised lahendused panustada majanduskasvu enam, kui riigi asukoht või tõhus väliskaubandus. Edu võib tuua ka riigi kujundamine mingil elualal rahvusvaheliselt juhtivaks (nt kübejulgeolek, e-teenused), sest seda nõuab vajadus jääda ellu kuluefektiivsuse ja uute turgude taustal (Kattel *et al* 2010, 72; Joenniemi 1998, 62).

1.3.4. Tunnetuslikud tegurid

Üks oluline ja huvitav muutuja väikeriigi teoorias on tunnetuslikkus või poliitiline kommunikatsioon, mis viitab mingitele ideedele või ambitsioonidele riigi enda mõjuulatusest (Thorhallsson 2006; Thorhallsson 2018). Nimetatud teguri puhul on tähtis asjaolu, et kasutades tunnetuslikkust, tekib ka väikesel riigil võimalus panna positiivse kuvandi (mingite eeskujulike

saavutuste) abil teisi riike ennast järgima või oma soove kuulda võtma (Nye 2010; Buzan, Segal 1996) või kasutada seda siseriikliku tegurina oma rahvas usalduse ja turvatunde tekitamiseks ning seeläbi võimu saavutamiseks. Julgeoleku tagamisel seostub tunnetuslik võimekus eelkõige nn pehme jõu kasutamisega, mille üks osa on kuvand riigi positiivsetest saavutustest ehk reputatsioon, mille oskuslik kasutamine võimaldab saada üle või juhtida kõrvale negatiivse varjundi nõrkusest, mis üldjuhul väiksusega seostub (Thorhallsson 2018). Kuvandi presenteerimisel on aga kindlasti oluline, et riik peab suutma lubatud ka tagada ehk see peab olema usutav ning nähtav riigi tegudes. (Goodman 2010, 106)

Kokkuvõtteks võib öelda, et julgeoleku tagamisel on väikesel riigil võimalus kasutada nn pehmet jõudu, kuid oluline on, et riik suudaks antud lubadust ka garanteerida.

2. METOODIKA JA VALIM

Magistritöö teoreetilises osas tuvastati, et siseriiklikke tegureid, mis mõjutavad väikeriigi küberjulgeoleku võimekust, on vähe uuritud. Mitmed autorid, kes on väikeriigi teemaga tegelenud (nt Sarapuu 2019; Thorhallsson 2018; Maass 2009; Burton 2013), on andnud edasisi soovitusi väikeriigi-temaatika võimalikult mitmekesiseks uurimiseks.

Lähtudes magistritöö eesmärgist, on uurimuse läbiv teema siseriiklikud tegurid, mis mõjutavad väikeriigi küberjulgeoleku võimekust. Töö spetsiifikast lähtudes kasutab autor uurimuse teostamiseks kvalitatiivset uurimismeetodit. Seda seetõttu, et siseriiklike tegurite mõju kohta väikeriigi küberjulgeoleku tagamisel on vähe andmeid, see sobib protsesside, strateegiate ja nende tähenduste uurimiseks (Ghauri, Grønhaug 2004, 98), selle lähtekoht on tegeliku elu kirjeldamine, kus objekti püütakse uurida tervikuna, ning vastatakse küsimusele „kuidas“ ja „miks“ mingid sündmused juhtuvad (Hirsijärvi *et al* 2005, 152; Yin 2018, 15; Yin 1994, 9). Ka annab kvalitatiivse meetodi kasutamine võimaluse juhtumi uurimiseks ja teooriate testimiseks ning koos andmete kogumisega on võimalik luua uusi teoreetilisi lähtekohti, milles andmete kogumine ja analüüs toimuvad samaaegselt (Frankel, Devers 2000; Bouma, Atkinson 1995). Alasuutari (1996, 34–38) on kvalitatiivset uurimust võrrelnud „mõistatuse lahendamisega, kus iga vihje peab sobima väljapakutud lahendusega“ ning kuna kvalitatiivse uurimuse tulemused ei ole käsitletavad kui faktid laiema kogumi kohta, vaid on pigem kirjeldused, mõisted ja teooriad konkreetsest nähtusest, siis üldistuste tegemine tähendab konkreetse nähtuse sobitamist mingisse konteksti ning selle kohta saadud teadmisest tähenduse andmist ühiskonna jaoks laiemalt. Sellest tulenevalt on kvalitatiivne uurimismeetod kasutatav väikeriigi uuringuteks ning sobilik antud töös püstitatud eesmärgi täitmiseks.

Magistritöö on üksikjuhtumi uuring, mille uurimisobjekt on Eesti, mida võib tituleerida väikeriigiks (vt ka pt 1.2.). Riigi julgeolekupoliitika alusdokument ütleb, et „digitaalsed teenused on riigi lahutamatu osa, milleta riik ei saa tänapäevasel viisil enam toimida, ja see suurendab võimalike rünnete mõju riigi julgeolekule“ (Eesti julgeolekupoliitika alused, 5). Töös näitena kasutatav üksikjuhtum on Eestis 2017. aastal aset leidnud Eesti poolt ID-1 formaadis välja antud kohustusliku dokumendi turvakiipe puudutava turvanõrkuse avastamine, mis oli Eesti jaoks oluline sündmus ja vajas seetõttu kiiret ja otsustavat reageerimist, et ohtu ei satuks Eesti riigi funktsioneerimine. 2018. aasta aprilli seisuga on kõik selle turvanõrkusega seotud kaartide

sertifikaadid uuendatud või tühistatud ning ei ole teada ühtegi juhtu, kus seda turvanõrkust oleks ära kasutatud (Buldas *et al* 2018, 5).

Antud üksikjuhtum võimaldab testida olemasolevat väikeriigi teooriat, esitada sellele väljakutseid, seda laiendada või pakkuda alternatiive (Yin 1994, 38–40). Kuigi üksikjuhtumi uurimuse kui meetodi puudusena on välja toodud teadusliku ranguse, usaldusväärsuse ja statistiliste üldistamisvõimaluse vähesust (Noor 2008, 1603), ühendab Eesti ID-kaardi turvanõrkuse kaasus endas väikeriigi, riigi sõltuvuse info- ja kommunikatsioonitehnoloogiast ning internetist, ohu riigi toimimisele, küberjulgeoleku tagamise võimekus ning siseriiklikud tegurid, mis seda mõjutavad. Seega on üksikjuhtumi analüüs asjakohane magistritöö uurimisprobleemi nähtuse mõistmiseks ja väikeriigi teooria testimiseks. Üldistuse tegemisel saab antud töö tulemusi kasutada tulevaste uuringute aluseks ja võrdlemiseks. (Yin 2018, 20; Yin 1994 30–32) Samuti võimaldab üksikjuhtumi uuring vältida oluliste asjaolude kaotsiminekut, mis suurema valimi korral juhtuda võib (Mahoney, Goertz 2006, 238).

Magistritöö empiirilise osa ülesanded on:

1. Analüüsida Eesti julgeolekupoliitika kujundajate ja ekspertide seisukohti siseriiklikest teguritest, mis mängisid rolli 2017. aasta ID-kaardi turvariski juhtumi lahendamisel.
2. Analüüsida teooria, dokumendianalüüsi ja ekspertarvamuste tulemusi, vastata töö uurimisküsimusele, teha töö teemaga seonduvad järeldused ning anda poliitikasoovitused.

Uurimistöö ainestiku moodustab teooria ja avalikult kättesaadavate dokumentide analüüs ning läbiviidud poolstruktureeritud ekspertintervjuud. Teooria eesmärk oli luua magistritöö teoreetiline raamistik uurimisvahendite loomiseks ja uurimistulemuste analüüsiks (Yin 2018, 106). Töös esitatud teoreetilisi seisukohti toetab dokumendianalüüs, kuna töös on kasutatud Eesti julgeolekupoliitika alusdokumente, mis annavad ülevaate Eestist ja selle riiklikest seisukohtadest antud teemal.

Intervjuu küsimustik on koostatud, lähtudes töö eesmärgist, ning autor ehitas selle üles kui vestluse teemal, kuidas väikeriik tagab oma küberjulgeoleku võimekuse Eesti 2017. aasta ID-kaardi turvariski juhtumi näitel. Intervjuude raamküsimused on esitatud magistritöö lisas 1. Intervjuud on lindistatud ja transkribeeritud. Pärast intervjuude transkribeerimist on kõrvutatud kõikide intervjueeritavate arvamust samade teemade ja korduvate märksõnade kohta, mis on seotud väikeriigi küberjulgeolekut mõjutavate siseriiklike teguritega. Nimetatud jaotus on alus

magistritöö analüüsiosale ning võimaldab teha järeldusi antud teema kohta. Samuti aitab see välja selgitada, kas küberruumi konteksti avaldumisega ning võimu definitsiooni muutumisega tekib väikeriigi teoorias seni käsitlemata, kuid katmist vajavaid väikeriigi küberjulgeoleku võimekust mõjutavate siseriiklike teguritega seonduvaid teemasid, mh riigi väiksusest tulenevaid eeliseid ja võimalusi antud valdkonnas.

Magistritöö intervjuud on viidud läbi Eesti küberjulgeoleku poliitika kujundajatega või ekspertidega (vt lisa 2), kes puutusid kokku 2017. aasta ID-kaardi turvariski avastamise ning lahendamisega või kes on Eesti (küber)julgeoleku valdkonna poliitika kujundajad. Intervjueeritavate hariduslik ja töökogemuslik taust on erinev, mis eelduse kohaselt annab võimaluse saada teema kohta erinevaid vaateid ja lahendusi ning muuta uurimistöö tulemus mitmekesisemaks ja huvitavamaks. Küberjulgeoleku poliitikakujundamise valdkonnas töötamine garanteerib uuritava teema tundmise ning kogemuse, mille kirjeldamine annab lahenduse töö uurimisprobleemile (Kvale 2006, 481). Turvakaalutlustel ja vastavalt intervjueeritavate soovidele on läbi viidud intervjuude tulemused anonüümsed ja teada vaid töö autorile. Et illustreerida analüüsi, on töös kasutatud intervjuude fragmente, mis on markeeritud, kuid pole seostatavad intervjueeritavatega. Intervjuudest enamus viidi läbi suuliselt (v.a üks, mis viidi läbi kirjalikult) ajavahemikul 23. november kuni 11. detsember 2018, nende pikkus oli 1,5–2 tundi. Intervjuu viidi läbi 8 isikuga soovitud 10st, kahjuks ei õnnestunud intervjueerida Politsei- ja Piirivalveameti (edaspidi PPA) esindajat, kes intervjuu palvele ei vastanud, kuid kes oli oluline osaline uuritavas juhtumis. PPA osa kompenseeris Riigi Infosüsteemide Ameti (edaspidi RIA) intervjueeritavad, kes töötasid antud juhtumis PPA-ga väga tihedas koostöös.

3. ANALÜÜS JA ARUTELU

3.1. Eesti ID-kaardi turvanõrkuse juhtum

Käesolevas töös on väikeriigi küberjulgeoleku võimekust mõjutavate siseriiklike tegurite seletamise näiteks valitud Eesti, mis on 2017. aasta andmete järgi väikese elanikkonnaga (umbes 1,3 miljonit), suhteliselt suure pindalaga (umbes 45 000 km^2), keskmise tulutaseme, majandusliku ning innovatsioonivõimekusega riik. Samas on Eesti tuntud kui suur panustaja globaalsesse küberjulgeolekusse, e-teenuste kasutamise, infotehnoloogiliste lahenduste propageerimise liider ning teenäitaja maailmas (e-Governance Academy ...; Üldandmed). Seega vastab Eesti töö kontekstis väikeriigi määratlusele. Eesti valitsuse strateegiadokumentides on infotehnoloogia jätkusuutlikus ja inimeste areng selles valdkonnas seatud väga kõrgele kohale riigi majandusarengu saavutamise ja julgeoleku tagamise seisukohast (Eesti infoühiskonna arengukava ... 2013; Eesti julgeolekupoliitika alused; Küberjulgeoleku strateegia 2008–2013; Küberjulgeoleku strateegia 2014–2017; Küberturvalisuse strateegia 2019–2022).

Eesti igapäevane elu on väga tihedasti läbi põimunud digitaalsetest lahendustest. Eestis on kõrge mobiilse lairiba (EstWin) kasutuse määr (koguni 91% majapidamistest kasutas seda ülikiire interneti tarbeks 2017. aastal) ja laialdaselt kättesaadavad 4G võrgud. 85% Eesti elanikkonnast kasutas 2017. aastal internetti, mis on rohkem kui Euroopa Liidus keskmiselt. Eesti on veebis pakutavate avalike teenuste ja nende kvaliteedi osas Euroopa Liidu liider ning ületab Euroopa Liidu keskmist digitaalsete oskuste ja kodanike internetikasutuse poolest, (Europe's Digital Progress ...). Eesti on ka riik, mis suudab pakkuda maailmas unikaalseid digilahendusi ja nende kasutamise sagedust riigi valitsemises, millest erilist esiletoomist vajab elektrooniline isikute identifitseerimise süsteem ja selle kasutamine.

Tänaseks on Eestis olnud elektrooniline isikute identifitseerimise süsteem, mis põhineb ID-kaardil, 16 aastat. Riigis on umbes 5000 avaliku ja erasektori e-teenust, mida saab kasutada elektroonilise ID-kaardi, vastava riist- ja tarkvara ning interneti abil oma isikut tõendades. (ROCA Vulnerability ...) See tähendab, et väga palju riigi- ja erasektori igapäevasest asjaajamisest toimub interneti ja e-teenuste vahendusel ning see eeldab elektroonilist isikutuvastamist. Näiteks kasutas 2017. aastal 90% Eesti inimestest e-panganduse teenuseid ja 78% e-valitsuse teenuseid (nt 95% üksikisiku tuludeklaratsioonidest täideti interneti vahendusel; 31% häältest anti 2017. aasta

valimistel elektrooniliselt), mis on Euroopa Liidu üks kõrgemaid. (Europe's Digital Progress ...) Oluline on märkida, et kõik Eesti elutähtsate teenuste pakkujad sõltuvad oma tegevuses infotehnoloogiast ning ligi pooltel ei ole sellele alternatiivseid lahendusi (Projekti „Elutähtsate teenuste ... 2016). Muuhulgas on elutähtis teenus ka elektrooniline isikutuvastamine ja digitaalne allkirjastamine ise (HOS § 36).

Elektrooniline identiteet on kogum andmeid, mis paneb isiku elektroonilises keskkonnas kokku tema füüsilise identiteediga, mida on Eestis igal inimesel mõlemas sfääris üks. Elektroonilise identiteedi toimimine põhineb avaliku võtme infrastruktuuril (*public key infrastructure*), mis tähendab, et identiteeti saab elektrooniliselt tuvastada kahe krüptograafilise võtme abil, millest üks on avalik ja teine salajane (privaatne). (Elektrooniline identiteet eID) Elektroonilist identiteeti kasutades saab Eestis teha kolme toimingut, milleks on autentimine, digiallkirjastamine ja (de)krüpteerimine. Autentimine tähendab kinnituse andmist oma identiteedi kohta ning kontrollimehhanismi selle identiteedi tõesuse tuvastamiseks (AKIT *sub* autentimine). Digiallkirjastamine annab võimaluse tõestada andmeallika autentsust, kontrollida andmete terviklikkust, tagada sõnumi saatmise salgamatust ehk kaitsta üksust võltsimise eest. Digiallkiri on Eesti juriidilises mõttes võrdne omakäelise allkirjaga (AKIT *sub* digitaalsignatuur). Krüpteerimine võimaldab andmeid matemaatiliste algoritmide abil salastada nii, et selle sisu ei ole ilma dekrüpteerimiseta kättesaadav (AKIT *sub* krüpteerimine). ID-kaardiga tehakse nimetatud kolme toimingut kahetasandiliselt ehk teadmiste- ja omandipõhiselt (ID-kaardi omanikul on sertifitseeritud kaart ning ta teab kaardi PIN-koode, allkiri arvutatakse matemaatiliselt ning see on ainulaadne iga allkirjastaja ja dokumendi puhul) (AKIT *sub* autentimine).

2017. aasta 30. augustil teavitasid Masaryki ülikooli[14] teadlased Eestit turvariskist, mis puudutas mh ka alates 2014. aasta oktoobrist väljastatud umbes 800 000 Eesti ID-, digi-ID, diplomaadi ID- ja e-residendi kaardil kasutatavat kiibi tarkvara ning mis tähendas, et kiibi avalikust võtmest oli piisava arvutusvõimsuse olemasolul võimalik faktoriseerida salajane võti. (Nemec *et al* 2017; Küberturvalisus 2018, 9). ID-kaardi juhtumi puhul oli seda oluline kaitsta küberrünnete eest ja säilitada selle turvaline toimimine, mis tähendab informatsiooni konfidentsiaalsuse, autentsuse, käideldavuse ja tõestatavuse tagamist. Turvanõrkuse ära kasutamine oleks kahtluse alla pannud kõik sama tüüpi kiipidega varustatud kaartidega tehtud autentimise ja allkirjastamise operatsioonid. ID-kaardi turvarikkumise ilmnemisel oli olemas võimalus, et teenusepakkuja peab

[14] Centre for Research on Cryptography and Security at Masaryk University.

ID-kaardi kasutatava tarkvara sertifikaadid tühistama ning Eesti riik ei saa sellele kuidagi vastu seista (Buldas *et al* 2018, 5–6).

Antud turvajuhtum omas rahvusvahelist mõõdet ega puudutanud vaid Eestit ja selle elektroonilist identifitseerimisvahendit. Haavatavad olid ka mitmed muud sarnased infotehnoloogilised vahendid isikute tuvastamiseks, erinevate tehnoloogiafirmade toodete turvamoodulid, kiibiga maksekaardid jms. Üle kogu maailma arvati kokku olevat mõjutatud kümneid miljoneid seadmeid, milles olevaid vigaseid võtmeid oleks olnud võimalik identifitseerida väga kiiresti ning täiesti tavalise sülearvuti abil ja ka suurte andmemahtude puhul. (Nemec *et al* 2017; ROCA Vulnerability ...). Eesti jaoks oli juhtum kriitilise tähtsusega eelkõige seetõttu, et elektroonilist isikutuvastamist kasutas igapäevaselt väga palju inimesi (nt 2017. aasta veebruaris anti 6 miljonit, 2018. aasta samal ajal aga juba 10 miljonit allkirja), lisaks oleks teenuse kasutuskõlbmatuks muutumine häirinud paljude riiklike ja erasektori teenuste kasutamist ning mõjutanud oluliselt riigi igapäevast toimimist (ROCA Vulnerability ...). Väga huvitavaks teeb juhtumi asjaolu, et Eesti suutis ainsa riigina ID-kaardi tarkvara kauguuendada ning sertifikaadid peatada, teiste riikide lahendus olukorrale päädis ID-kaartide füüsilise uuendamise ja sertifikaatide tühistamisega (Küberturvalisus 2018, 12).

Seega annab Eesti ID-kaardi turvanõrkuse juhtum võimaluse uurida, kuidas väikeriik tagab oma küberjulgeoleku võimekuse ning milline mõju on sellele riigi väiksusel. Kuigi antud juhtumit ei käsitletud kui hädaolukorra ohtu, mis oleks hädaolukorra seaduse järgi tähendanud hädaolukorra lahendamise plaani rakendamist, viitab küberjulgeoleku-temaatikale asjaolu, et käsitletava juhtumi puhul olid mõjutatud nii riiklikult oluline elektrooniline teave, elektroonilise teabe kandjad kui ka elektroonilised teenused (mh elutähtsad teenused), milles oli olulisel kohal küberrünnakute ennetamine ning riigi sotsiaalsete ja majanduslike protsesside toimimise tagamine. Juhtumi lahendamisel võttis riik kasutusele nii infotehnoloogilised kui ka organisatoorsed abinõud ning olukorra lahendamisel tuli taastada ID-kaardi turvalisus ning samal ajal tagada teenuse toimivus (vt ka Küberjulgeoleku strateegia 2008–2013, 40).

3.2. Ekspertintervjuude ja dokumendianalüüsi tulemused

3.2.1. Eesti toimetulek ID-kaardi turvariski juhtumi lahendamisel

Intervjueeritavate hinnang Eesti ID-kaardi turvariski juhtumi lahendamise toimetuleku kohta oli üldjoontes positiivne – kõik vastajad leidsid, et Eesti sai hästi hakkama (mh ka kriisi ajal tekkinud probleemidega), kuid kas tulemuseni jõuti kõige efektiivsemaid võtteid kasutades, oli vähemalt poolte vastajate arvates kaheldav.

Intervjueeritav A: *„Läks hästi ma ütleks ... poleks nagu midagi juhtunudki.“*

Peamiseks edu näitajaks peeti turvalisuse kindlustamist ning juhtumi lahendamise kiirust. Mitte ühegi inimese elu ei sattunud ohtu, elektroonilise identifitseerimise teenust ja sellest sõltuvaid teenuseid suudeti edasi pakkuda ning juhtumit ei kasutanud keegi omakasu eesmärgil ära.

Kõik intervjueeritavad mainisid, et juhtumi järgselt ei ole täheldatud inimeste usalduse vähenemist Eesti riigi digiteenustesse, mh elektroonilise identifitseerimise teenuse kasutamisel. Seda peeti üheks suurimaks võiduks, mis kindlustab, et inimesed kasutavad digiteenuseid ka edaspidi. Pooled vastajatest tõid usaldusega seonduvalt välja, et üldist paanikat ei tekkinud või et see ei eskaleerunud, kuigi tänapäeva tehnoloogiliste vahenditega (nt sotsiaalmeedia) oleks see võinud juhtuda väga kiiresti. Kõik intervjueeritavad tõid usalduse jätkuvuse näiteks 2017. aastal toimunud kohaliku omavalitsuse valimisi, kus elektrooniliselt hääletas rekordiliselt suur arv hääletusel osalenuid (Elektroonilise hääletamise ...).

Intervjueeritav D: *„ “Tavalisele lehelugejale“ käib see ID-kaardi tehniline asi üle pea, seega on see ainult ja ainult usalduse küsimus. Piisab sellest, kui see üks kord murtakse, ning siis on väga suur jama majas.“*

Ka ei ole intervjueeritavate arvates märgatud Eesti tugeva IT- või küberjulgeoleku kuvandi kadumist rahvusvahelisel tasemel, sest Eesti näitas, et suutis esmalt ise ennast kokku võtta ja hakkama saada, ega jäta seesuguseid juhtumeid kellegi teise lahendada.

Juhtumi edukale lahendamisele viitavad ka juhtumijärgselt Eestis koostatud analüüsid ja Eesti strateegiadokumendid, mis peavad samuti oluliseks, et Eesti „e-ajaloo üks kaalukamaid kriisijuhtimisoperatsioone“ lahendati kiiresti, turvaliselt, säilis Eesti inimeste usaldus e-riigi vastu

ning Eesti e-riigi kuvandi rahvusvahelises mõttes ei saanud kahjustada (Buldas *et al* 2018, 5, 26; Eesti riigi kriitiliste ..., 1; ROCA Vulnerability ...). Küll aga toovad nt näiteks Tallinna Tehnikaülikoolis (edaspidi TTÜ) läbi viidud ID-kaardi kaasuste õppetundide uuring (edaspidi TTÜ uuring) ja ka Riigikontrolli kriitiliste andmekogude turvalisuse ja säilitamise audit (edaspidi audit) välja asjaolusid, mis oleks võinud olla paremini lahendatud (Buldas *et al* 2018; Eesti riigi kriitiliste ...).

3.2.2. Siseriiklikud tegurid ID-kaardi turvariski juhtumis

Siseriiklikest teguritest, mis mängisid juhtumi lahendamisel rolli, mainiti intervjuudes kõige enam tehnilise kompetentsi olemasolu Eestis kohapeal (Eesti tarkvarainseneride kompetentsid on ära kaardistatud ja nende valmisolek ning vajadusel alternatiivid teada) ja ametkondadevahelist ning era- ja avaliku sektori koostööd (peeti väga heaks), protseduuride olemasolu ning kiirust asjaajamisel (tänu paindlikkusele), mille tingis vähene bürokraatia ja inimeste tundmine (mis võrdub usaldusega), ettevalmistust (nt ID-kaartide kauguuendamist oli varem kasutatud, õppuse käigus oli sarnast juhtumit harjutatud, 2007. aasta küberrünnakute kogemus, kriisijuhtimise süsteemi olemasolu). Eriliselt toodi välja riigijuhtide koostöötahet ja väga kiiret reageerimist.

Intervjueeritav A: *„Noh, me mõtlesime, et peaminister on noor oma ametis ... ja veel see erakondlik kuuluvus ja arvamus ID-kaardist ..., kuid õnneks saadi kohe aru, et me ei tee nalja ... ja öeldi, et piiranguid ei tehta, tehku me see asi korda. Väga positiivne näide, ma ütleks.“*

Intervjueeritav D: *„/.../ tal (peaministril) polnudki justkui muud võimalust, et usaldada ametkondi ja nõuandjaid ja see, et riigis kõik tunnevad kõiki, võiski olla tema ainsaks garantiiks ajakriitilises situatsioonis.“*

Intervjueeritav D: *„PPA ja RIA koostöö sujus hästi, keegi ei hakanud järgima nii väga oma jurisdiktsioone, kriisiolukorras sa pead seda teadvustama ja kiiresti tegutsema.“*

Intervjueeritav E: *„See on jah huvitav, et kuidas kriisis aduti kohe, et bürokraatiaks pole aega ... Öeldi, et võta telefon ja helista kohe X-ile ja uuri, ega ta parasjagu kuskil Aafrikas konverentsil ei ole.“*

Juhtumiga seotud dokumentides välja toodud siseriiklikud tegurid, mis antud juhtumit mõjutasid, kattusid suurelt osalt intervjuudes nimetatuga. Peamiselt toodi välja juhtimise, koostöö, kompetentsiga (mh infovaradega) seonduv (Buldas *et al* 2018; Eesti riigi kriitiliste ...).

Kõige kriitilisemateks teguriteks märgiti intervjuudes üldist siseriiklikku võimekust ja valmisolekut, sest nii nagu igas kriisis, oli ka antud juhtumi puhul oluline tegur (reageerimis)aeg. Üldise siseriikliku võimekuse all pidasid kõik vastajad silmas, et Eesti suutis kõiki oma võimalusi koondades kiiresti ise olukorraga hakkama saada.

Intervjueeritav D: *„Krüpto on hea ja seda peabki kasutama, kuid sinna peale peab ehitama organisatoorse turbe kihi. /.../ Kõigepealt tuleb oma kodu turvaliseks saada ja siis tuleb minna teisi õpetama.“*

Ka TTÜ uuring ja audit viitavad antud juhtumi puhul eeltoodud asjaoludele (Buldas *et al* 2018; Eesti riigi kriitiliste ...). Näiteks nimetatakse Eesti küberjulgeoleku ja küberturvalisuse strateegiates digitaalse ühiskonna turvalise ja tõrgeteta toimimise üheks komponendiks riigiasutuste võimekust ning tegevusi selle saavutamiseks (Küberturvalisuse strateegia 2019–2022; Küberjulgeoleku strateegia 2014–2017). Ka ITUI ja NCSI mõõdavad ja peavad oluliseks mh erinevatest komponentidest koosnevat siseriiklikku võimekust, et riik saaks oma küberjulgeoleku tagada (Global Cybersecurity Index; Rikk 2018).

Seega oli oluline tehnilise kompetentsi olemasolu Eestis kohapeal, oma IT-süsteemidest ja kompetentsidest ülevaate omamine (mh nende seisukorrast ja kriitilisusest), koostööd kõigi osapoolte vahel, üleüldist valmisolekut (ettevalmistust ja teadlikkust; läbiharjutatud stsenaariume õppustel), juhtumi kommunikatsiooni (sh ametkondade vahel ning elanikele). Nimetatud tegurid tagasid intervjueeritavate arvates situatsiooni kiire ja pigem tõrgeteta lahendamise.

Intervjueeritav C: *„Suvaline tarkvarainsener ei tee sul seda asja korda, on vaja insener-julgeolekuspetsialisti, kes teab, kuidas asjad Eesti puhul käivad ... teda on vaja kohe ja ta peab olema kohapeal olemas.“*

Intervjueeritav E: *„Kui võimekust oleks pidanud otsima väljast, siis oleks olnud väga tõsine probleem.“*

Kõige toetavamaks siseriiklikuks teguriks pidasid intervjueeritavad nii riigijuhtide kui ka rahva usaldust ja üleüldist asjaga kaasa tulekut, koostööd ja orienteeritust ühisele eesmärgile juhtum ära lahendada, teadlikkust (sh varasemad tehnilised lahendused), lühikesi kommunikatsioonilinke ja seda, et kõik tunnevad kõiki ning vajadusel saab väga kergesti tegutseda ka väljaspool formaalseid strateegiaid ja struktuuri, mida kriisiolukord teinekord kiireima lahenduseni jõudmiseks nõuab. Üle pooltel juhtudest nimetati toetava tegurina riigi väiksust – väikest inimeste hulka ning väikseid tehnilisi ja riiklikke süsteeme, mis protsesse antud juhtumi puhul lihtsustasid.

Intervjueeritav B: *„Tegelikkuses lahendus tuli sellest, et Eestis pannakse kriisi puhul seljad kokku.“*

Intervjueeritav A: *„Eestis kõik tunnevad kõiki, see valdkond on väga spetsiifiline ja inimesed, kes sellega on töötanud, on olnud aastaümneid samad. ... väike kogukond töötab ... kindel partnerite võrgustik töötas, aja jooksul leitud. Inimesed on kõige taga.“*

Intervjueeritav C: *„Riskijuhtimine nõuab struktuuri ja strateegiat, kuid sellesse ei tohi kinni jääda, see ei tööta paraku ja jama see ei lahenda, jama lahendavad inimesed.“*

Intervjueeritav G: *„Oli õnne, et saime varasemat tehnilist lahendust taaskasutada ja võtsime sellest võimalusest kinni.“*

Kõige suuremad väljakutsed ID-kaardi turvariski juhtumis olid intervjueeritavate sõnul seotud ressurssidega, nagu näiteks pädevate ja usaldusväärsete oskuste nappus ning riiklik sõltuvus suurettevõttest, kes ID-kaardi turvalahendust tarnis. Kui tehniliste ekspertide puuduse väljakutse suutis Eesti antud juhtumis lahendada erasektoris töötavate ekspertide kaasamisega, siis suhtlemisoskuses suurte korporatsioonidega (nt õiguslikus mõttes) peaks Eesti kompetentsi kasvatama.

Intervjueeritav D: *„Eesti on väike, meil on eksperte vähe.* Per capita *on meil hästi läinud.“*

Intervjueeritav B: *„Üldjuhul teadlased hoiavad infot kinni sarnaste*, 0-day *juhtumite*[15] *puhul, ja sa annad info sellele, kes on mõjutatud, ja annad talle aega. Kuid nad ei osanud arvestada sellega, et maailma suurim selle valdkonna ettevõte ei olnud sugugi aus oma klientide suhtes.“*

Ka audit ja TTÜ uuring toovad olulise väljakutsena välja ekspertide nappuse, teadmuse koondumise ühe inimese kätte ning järelkasvu problemaatilisuse. Näiteks toob TTÜ uuring välja, et tegelikkuses oli nii RIA-l, PPA-l kui ka SMIT-il[16] (ID-kaardi juhtumi osapooled) puudu tehnilisest võimekusest (teadmised, oskused ja inimressurss) ID-kaardi valdkonnas, seega otsiti abi asutustest väljastpoolt. (Buldas *et al* 2018; Eesti riigi kriitiliste ...) Kompetentside nappus antud juhtumis saatuslikuks ei saanud, kuid tulevikus ei pruugi see olla jätkusuutlik, sest nii infosüsteemid kui ka küberohud muutuvad keerulisemateks ja suuremateks (Küberturvalisuse strateegia 2019–2022).

Pooled intervjueeritavatest mainisid võimaliku väljakutsena juhtumi avalikustamist, eelkõige seetõttu, et sellele järgnev ühiskondlik reaktsioon võib olla ettearvamatu situatsioonis, kus riik tunnistab, et olukord on kriitiline ja lahendust pole.

Intervjueeritav C: *„Paljud riigid ei tule avalikult sellega välja, oodatakse ja vaikitakse asi maha ja kui midagi juhtub, siis seletatakse tagantjärele ja otsitakse vabandusi.“*

Intervjueeritav A: *„Oluline oli vältida paanikat. Et ei hakkaks keegi raha pangast välja võtma, et ravimite soovijad ei ummistaks EMO-sid.“*

Ressursi nappusega seotud väljakutsega toodi välja ka tehniliste lahenduste leidmise keerukus – kuidas ja kui kiiresti suudetakse turvarisk maandada, kuidas teha inimeste jaoks situatsioon võimalikult arusaadavaks ja lihtsaks ning kuidas inimesed sellega kaasa minema panna.

Kaks vastajat märkisid väljakutsena ära, et Eestis kasutatavad infotehnoloogilised süsteemid ei ole nende kogemusele toetudes väga hästi kaardistatud, seega on raske aru saada, millises seisus need tegelikkuses on. Näiteks toodi välja, et mitmed organisatsioonid pidid kiirkorras oma vananenud infotehnoloogilised lahendused välja vahetama ning ilmnes ka muid süsteemidega seonduvaid

[15] Tarkvara turvanõrkus, mida kasutaja ei tea.
[16] Siseministeeriumi infotehnoloogia- ja arenduskeskus.

asjaolusid, mis muidu oleks jäänud avastamata. Positiivse märgina toodi välja, et kuna süsteemid on pigem lihtsad ja väikesed, on neid lihtne hooldada, ümber korraldada.

Intervjueeritav G: *„Kes veel vanade süsteemide peal elasid, nendel ei jäänud muud teha, kui esmalt karjuda ja siis oma süsteemid kiiresti ära uuendada /.../ keegi ju niisama töötavat süsteemi välja ei vaheta, isegi kui see on moraalselt vananenud.“*

Sarnase probleemi toovad välja ka TTÜ uuring ja audit, mis viitasid asjaolule, et esines puudusi ID-kaardi ning kriitiliste andmekogude kohta käivast ajakohasest informatsioonist (nt sõltuvuste kaardistused, riskihinnangud jms), mille oleks pidanud ära tegema igapäevaste tegevuste käigus ja mis oleks hõlbustanud juhtumi lahendamist. (Buldas *et al* 2018; Eesti riigi kriitiliste ...)

Osalt väljakutse ja osalt takistusena toodi välja olemasolevate alternatiivide ebapiisavust. Esmalt tähendab see avalikus sektoris alternatiivi puudumist elektroonilisele isikutuvastamisele (mis ei oleks füüsiline isikutuvastamine, sest mõnel juhul ei ole see e-teenuse kasutamiseks võimalik). Teiseks toodi välja õppuste käigus harjutamist ning harjutuste mitmekesisust, mis aitaks erinevaid olukordi paremini ja kiiremini mõista ning lahendada. Kolm vastajat arvasid, et senisest rohkem peaks harjutama olukorda, kus kriisi ajal tuleb säilitada ka osapoolte tavapärane töö (teenuse toimivus), või et ollakse valmis järsuks töörežiimi muutuseks. Näiteks toodi ID-kaartide kauguuendamisel tekkinud süsteemide jõudlusprobleem, mida oleks ühe intervjueeritava arvates saanud vältida varasema koormustestimise kogemuse olemasoluga. Ka viidati juhtumi lahendamisega seotud inimeste väga suurele töökoormusele seoses kriisi haldamise ning tavapärase töö jätkumise kindlustamisele. Lisaks toodi välja võimalus, et ID-kaartide füüsilise vahetamise korral oleks võinud tekkida ruumi- ja tööjõudpuudus vastavates asutustes.

Intervjueeritav C: *„Alternatiivid võiks olla. Ja teadlikkus võiks olla parem. Me ei lähe ju tagasi paberi ja pastaka peale, kui digi ei toimi. See ei ole võimalik ega adekvaatne.“*

Osalt väljakutse ja osalt takistusena toodi välja juhtumi kommunikatsioon. Näiteks peeti küsitavaks juhtumist avalikkusele teatamist peaministri tasandil, juhtumi osapooltele info edastamist (kohati oli info edastamise ajaks juba vananenud) ning inimestele ID-kaartide kauguuendamiseks vajalike juhiste andmise vasturääkivust. Samas arvasid kõik, et oluline oli, et valitsus tunnistas probleemi – see aitas kinnistada usaldust (vältida paanikat), et kõik saab korda

ja juhtum lahendatakse. Ka TTÜ uuringus peeti problemaatiliseks ja osapoolte vahelist koostööd takistavaks asjaoluks õige ja õigeaegse info jõudmist asjaosalisteni (Buldas *et al* 2018, 31).

Nii väljakutse kui ka takistusena tõid kaks vastajat välja, et puudujääke oli kriisi juhtimises. Nimelt et kriisi osapoolte ülese juhtimisorgani lahendus oli konarlik, puudus nn üks „erivolitustega kriisihaldur", kelle ülesanne oleks olnud vaid kriisi hallata, mitte tegeleda ka mõne osapoole igapäevase toimimisega.

TTÜ uuring toob olulise väljakutsena välja, et ID-kaardi juhtum ei kätkenud endas hädaolukorra või intsidendi tunnuseid vaid tegemist oli turvariskiga (kriisilaadse juhtumiga), millel oli Eestile oluline mõju. Defineerimise küsimus tekitas teatavad probleeme juhtumi rollide ja vastava käitumise määramisel, mis küll antud juhtumi lahendamisel olulisteks takistusteks ei kujunenud. Juhtumi järgselt selgub TTÜ uuringust, et oli osalisi, kes soovisid selget kirjapandud juhist ning neid, kes piisavalt vabadust sarnaste olukordade lahendamiseks. (Buldas *et al* 2018, 26–27)

Väga olulisi takistusi antud juhtumis välja ei toodud, peeti tähtsaks, et juhtum lahendati ning et puudujääkidest õpitakse.

3.2.3. Täiendavad tegurid ID-kaardi turvariski juhtumis

Et mõista juhtumit mõjutanud konteksti, paluti intervjueeritavatel nimetada muud tegurid, mis võisid Eesti toimetulekut ID-kaardi juhtumis mõjutada. Täiendavate tegurite all peeti silmas faktoreid, mis ei ole seotud riigi haldusvõimekusega.

Esmalt toodi välja õnne ja juhuste kokkulangemist – Eestil oli varasem kogemus (st arusaam riskidest ja ohtudest oli olemas nagu ka mehhanismid olukorraga toime tulemiseks) ning hetkel teadaolevalt ei kasutanud keegi haavatavust ära.

Kõik intervjueeritavad tõid olulise täiendava tegurina antud juhtumi puhul välja ajakriitilisuse. Nimetatud olukord tekkis asjaolust, et ID-kaardi kiibi haavatavuse info saamise ja sellekohase teadusartikli avaldamise vahel oli sisuliselt kaks kuud ning artikli avaldamise tulemusena võis suureneda risk turvanõrkuse ärakasutamiseks (ROCA Vulnerability ...).

Intervjueeritav A: *„Meie president kommenteeris, et see oli nagu auto parandamine sõidu pealt. Me omavahel ütleme siiani, et see oli ikka nagu ralliauto parandamine sõidu pealt."*

Intervjueeritav H: *„Uudis tuli põhimõtteliselt eelmisel päeval, mis tähendas et me ei teadnud riski ulatust. /.../ näiteks kas või seda, kas eelmiste valimiste tulemused on kehtivad. Või kas üldse midagi enam kehtib.“*

Väga oluliseks täiendavaks teguriks peeti Eestit ja selle poliitilisi otsuseid minevikus. Näiteks toodi välja riigi igapäevaelu väga suurt sõltuvust infotehnoloogilistest lahendustest, mille puhul nimetati mõjuks küberruumi ning selles kaasnevate võimaluste, aga ka riskide ja ohtude teadvustamist ning püüdu viimaseid ennetada. Eesti olukorrateadlikkusele viitab ka asjaolu, et Eesti on viimastel aastatel saavutanud kõrged kohad erinevates küberjulgeoleku ja infotehnoloogia arengut mõõtvates indeksites (nt 3. koht NCSI, 5. koht ITUI, 17. koht Info- ja kommunikatsioonitehnoloogia arengu indeksis) (Estonia).

Intervjueeritav B: *„Asjad peavad olema kontrolli all, sa pead tundma oma süsteeme ja pead saama aru, mis on oht, mis mõju see tekitab ja sul peab olema arusaam sellest, mis saab, kui intsident juhtub. Intsident on vältimatu nagunii.“*

Intervjueeritav D: *„Mida rohkem sa infotehnoloogiat kasutad, seda rohkem muutub küberjulgeolek sulle tähtsaks. Eesti on siin päris pikka aega olnud. Seega ta tõstab julgeolekuvaldkonna prioriteediks.“*

Intervjueeritav C: *„Kui riigi tehnoloogiline sõltuvus puudub, siis küberjulgeolek on täielik, Eesti valik on olnud vastupidine.“*

Väga oluliseks peeti asjaolu, et kõrge tehnoloogilise arengu saavutamine tekitab teatavaid piiranguid, sest digitaalse infrastruktuuri arendamine ja kasutusele võtmine on olnud väga suur ja kulukas töö, ning kui juhtub, et see enam kasutust ei leia, siis tegelikkuses pole Eestil riiklikku võimet tagasi paberimajanduse juurde pöörduda. Inimressurssi ja rahalist võimekust võib jääda väheks. Lisaks tuleb arvestada, et infotehnoloogilised lahendused on loodud protsesside efektiivsemaks muutmiseks ja kuluefektiivsuse saavutamiseks ning tagasiminek ei ole seetõttu enam mõistlik ja võimalik. Eesti ressursid on piiratud ning see on intervjueeritavate arvates oluline tegur.

Intervjueeritav C: *„Noh, meil on tehnoloogilised süsteemid loodud, sest meil ei olnud raha, et asi füüsiliselt toimuks.“*

Intervjueeritav A: *„Eestis on seda tehtud väga väikeste ressurssidega ... selles situatsioonis peavad olema oskused väga head, pead tegema väga head valikud ja olema nutikas. Annaks jumal, et järgmine intsident oleks sama lihtsasti lahendatav.“*

Antud uuringus vaadeldud dokumentidest selgub, et digiteenuste kasutamine omab suurt majanduslikku mõju ja loob ühiskonnale märkimisväärset lisandväärtust ning et alternatiivi Eestis e-teenustele ei ole (Küberturvalisuse strateegia 2019–2022).

Teiseks spekuleeriti intervjuudes, et ehk ei olnud Eesti tol hetkel just kõige huvitavam juhtum maailmas (turvarisk hõlmas nimelt ligi kümmet riiki, lisaks eraettevõtteid, erinevat tarkvara jms) või tagas tugev IT-kuvand julgeoleku, sest tugevat riiki pole mõtet rünnata. Kahjuks ei ole kumbki väide kontrollitav, aga vastajate meelest oli tähtis teadvustada, et ohtu ei oleks kindlasti tohtinud alahinnata, sest nn ROCA haavatavuse ärakasutamiseks vajalik tehnika ja oskused ei oleks olnud kättesaadavad suvalisele inimesele, kuid nn irratsionaalne, piisavate ressurssidega ründaja, kelle motiivid võivad olla ajendatud mis tahes ideedest, oleks need suutnud endale hankida (vt ka ROCA Vulnerability ...; Nemec *et al* 2017).

Intervjueeritav E: *„Tegemist on elutähtsa teenusega, millest sisuliselt sõltub riigi funktsioneerimine, seda ei saa ega tohi alahinnata.“*

Kolm intervjueeritavat tõid välja tõsiasja, et Eesti sõltub väga palju tehnoloogiast, mis on kellegi teise toodetud. Seega ei saa riik seda ise kontrollida, kuid peab olema valvel võimaliku turvaprobleemi ilmnemisel.

Kõik vastajad tõid välja asjaolu, et Eestis on inimesed harjunud internetti ja e-teenuseid igapäevaselt kasutama, mis võis mõjuda nii negatiivselt kui ka positiivselt. Negatiivses mõttes tekitas see abitusetunnet ja paanikat. Positiivses mõttes inimesed mõistsid, miks on juhtumi lahendamiseks oluline koostööd teha. Nii uuendati sisuliselt viie kuuga 94% ID-kaartidest, mida kasutati igapäevaselt elektrooniliseks identifitseerimiseks (ROCA Vulnerability ...).

Intervjueeritav A: *„See on igapäevane toimimine ... inimesed on harjunud sellega, kui miski ei tööta, siis on natuke nagu abitu seis.“*

Ka toodi intervjuude käigus välja Eesti kultuurilist tausta ning ajaloolise mineviku mõju. Kriisi ajal annab riigijuhtide avatus ja olukorrast teavitamine võimekuse väga edukaks koostööks, sest mitte ükski eestlane ei taha, et kodumaal midagi juhtuks. Inimesed võtavad olulisi juhtumeid tõsiselt.

Muude teguritena nimetasid kõik intervjueeritavad ka sidemete loomist ja hoidmist väliskoostööpartneritega (nt NATO, Euroopa Liit, CERT-d[17] vms).

Intervjueeritav C: *„Paljudes riikides ja ettevõtetes oli jama, mitte vaid Eestis ... rahvusvaheline keskkond oli soosiv ja kõik said aru, et Eestit mõjutab see kõige rohkem. Eesti ei ole üksi sel hetkel, kõik elasid kaasa.“*

Intervjueeritav E: *„Eesistumise ajal olid just pahavara NotPetya ja Wannacry skandaalid raputanud maailma. Seega oli vaja kokku tuua eesistumise ajal CSIRT[18] Euroopa Liidus ... Eesti sai seda ära kasutada ka ID-kaardi juhtumi ilmnedes. Koostöö ja infovahetus ja kas või vajadusel paluda abi on väikeriigile väga oluline ... proportsionaalselt olulisem ehk kui suurriigile, kuid ka suurriigid peavad seda kasutama, sest küberruum on väga suur ja ettearvamatu ...“*

3.2.4. Tegurid, mis mõjutavad riigi küberjulgeoleku võimekust

Kõige olulisemate mõjuritena toodi välja küberruumi iseloomu, riigi tehnoloogilise arengu taset ning seda, kui palju riik ise tahab ja suudab seda kontrollida. Lisaks märgiti ära, et rünnak sõltub ründaja motiividest ja võimekusest (vt ka pt 1.1).

Intervjueeritav B: *„Tundub, et täna iga mees suudab varrukast tõmmata lause, et „Cyber is very important“, aga sellega riiki ei päästa ... pead aru saama, mida see tegelikkuses tähendab.“*

Kõiki eeltoodud mõjureid mainiti ka riigi väiksusega seonduvalt. Negatiivsena toodi välja ressursipuudust (mh raha, kompetentse, prioroteerimisvajadust seoses kulukate riigi funktsioonidega jms), mis teeb haavatavaks ning võib teha tugevatest partneritest sõltuvaks (kui ta neid suudab leida). Positiivsena mainiti, et vaest ja digitaalse arenguta riiki ei soovi ega saagi

[17] Computer Emergency Response Team (RIA küberintsidentide käsitlemise osakond), „tuvastab, jälgib ja lahendab Eesti arvutivõrkudes toimuvaid küberintsidente, teavitab ohtudest ning korraldab ennetustegevusi“ (Küberintsidentide käsitlemine ...)
[18] Computer Security Incident Response Team.

keegi rünnata. Samas tõdeti, et kõik nimetatud asjaolud ei pruugi kehtida vaid väikeste riikide puhul, sest kõik sõltub ikkagi konkreetsest riigist ja olukorrast.

Intervjueeritav C: *„Mõnel kliendil võib olla sama suur käive, kui Eestil on riigieelarve, Eesti pole mingi näitaja isegi siis, kui pool riigi elanikkonnast on mõjutatavad.“*

Intervjueeritav A: *„SK ID Solutions AS – nende äril pole vahet, kas Eesti 1,3 miljonit või Poola 40 miljonit nimest. Ettevõtte jaoks on tehnoloogiaga seotud kulud samad ja ta tahab seda raha tagasi saada iga suurusega riigilt. Luksus on olla väikeriik.“*

Intervjueeritav A: *„Pättide huvi on väikeste riikide vastu väike ... Meil oli siin vahel nali, et nad ei suuda Eestit kaardilt üles leida, see on nii väike ja ebahuvitav. Teisalt sõltub motivatsioonist ... et näitame Eesti e-upsakusele koha kätte.“*

Samadele asjaoludele viitavad ka ITUI ja NCSI, kus küberjulgeolekule pühendunud valdkonda panustajate, valdkonnateadlike, kõrgema küberohtude ennetusvalmiduse ja küberintsidentidega toimetuleku võimega riikide seas on absoluutses mõttes nii väga suuri (nt USA, Venemaa) kui ka väga väikeseid (nt Mauritius, Holland, Eesti) riike, kusjuures nii mõneski regioonis juhivad väikesed riigid oma tulemustega suurte ees (Rikk 2018; Global Cybersecurity Index).

Lisaküsimusena uuriti intervjueeritavatelt, kas riigi väiksus mõjutab tema küberjulgeoleku võimekust millegi poolest teistmoodi kui konventsionaalse julgeoleku võimekust. Kõik vastanud tõid välja, et esiteks sõltub julgeoleku võimekus sellest, mida selle all mõeldakse: kas tegemist on ründe- või kaitsevõimekusega. Võimekus füüsilises sfääris eeldab, et riigil on ressurssi osta sõjatehnikat ja seda mehitada. Küberruumis saavad aga määravaks ka teadmised ja oskused (rahaliste ressursside kõrval). Selle poolest on väikesel riigil võimalus olla võimekam, sest küberrelv kui ründe- või kaitsevõime võib olla väikeriigile kättesaadavam.

Intervjueeritav D: *„Kaitsespetsiifiline lähenemine. Eesti puhul ainuvõimalik lähenemine. Me ei saa rünnata ega ähvardada, see on suurte riikide pärusmaa, kel on ka konventsionaalsed võimed vajadusel vastu lüüa.“*

Intervjueeritav B: *„Kui sa arvad, et perfokaardid on OK, siis oled kaitstud, ja kui keegi tahab neid perfokaarte endale, siis pead ostma tanke, et neid kaitsta.“*

3.2.5. Väiksusest tulenevad eelised küberjulgeoleku kontekstis

Kõige enam tõid intervjueeritavad väiksuse eelistena välja füüsilist väiksust, mis tähendab vähe inimesi, väikeseid süsteeme, informaalseid suhteid, usaldust, kogukonnatunnetust, multifunktsionaalseid ametikohti, tahet ellu jääda ja midagi saavutada, kiirust otsuste vastuvõtmisel, jäiga bürokraatia vähesust ja ressursside puudumist, tõhusat era- ja avaliku sektori koostööd aga ka seda, et väike võib olla ründaja jaoks ebahuvitav. Mõnel juhul ei olnud vastajad kindlad, kas nimetatud eelised on vaid väikeriigile omased (nt tahe ellu jääda ja midagi saavutada, spetsialistide kogukonna olemasolu, ressursside puudumine (nt teadlikkus)), mitmel juhul toodi välja, et nimetatud eelis võib olla tegelikkuses hoopis puudus.

Intervjueeritav A: *„Nt Eestil on üks CERT, me pole nii rikkad, et hoida erinevaid era- ja avaliku sektori jaoks. See on andnud meile eelise, et üks suur pilt on ees ja omame ülevaadet.“*

Küsimustele, kas Eesti on nimetatud eeliseid oma küberjulgeoleku võimekuse loomisel ära kasutanud, oldi pigem neutraalsed.

Intervjueeritav C: *„Tahe on väga oluline, kui sul seda pole, siis sa ei tee mitte midagi. Kas tahad, et sul see võimekus on, või mitte. Eesti tahab, et tal see võimekus on, ja teeb kõik selleks, et küberjulgeoleku võimekust saavutada. Ilma selleta tänapäeval ei saa enam hakkama.“*

Avaliku ja erasektori koostöövõrgustiku näide on Eesti väiksuse eeliste ära kasutamise etalon, mida suured riigid on püüdnud mõista ning üle võtta. Eesti on küberjulgeolekuga seonduva inimressursiga hea näide – teatakse, mida on vaja teha ja kust vajalikud kompetentsid saadakse, ning väga oluline on, et kompetentsid on olemas Eestis kohapeal. Ka toodi välja informaalsed suhted ja võimalust neid kiiresti kasutada ning jäikadest bürokraatlikest struktuuridest (kui neid on) mööda minna. Ka toodi välja, et inimesed, kes hetkel küber-kogukonnas teadmuse ja kompetentsi moodustavad, on töötanud väga mitmetel erinevatel valdkonnaga seotud ametikohtadel nii era- kui ka avalikus sektoris, seega omavad riigi küberjulgeoleku olukorrast terviklikku ülevaadet ja oskavad tegutseda vastavalt vajadusele. Kiirust otsuste langetamisel ja elluviimisel on intervjueeritavate sõnutsi täheldatud nii 2007. aasta küberrünnakute, 2017. aasta ID-kaardi juhtumi aga ka muude (töös käsitlemata) juhtumite näitel. Pooled vastanutest tõid välja,

et Eesti on teadlikult vastu võtnud otsuse oluliste juhtumite puhul asi avalikustada ning eelis seisneb selle, et väike kogukond suudab kiiresti aru saada, mis ta peab tegema ning ka kiiresti vastavalt tegutseda.

Intervjueeritav B: *„Suurriigil on keeruline aru saada sellest koostööst, mis meil erasektoriga on küberjulgeoleku alal.“*

Intervjueeritav D: *„Usalduses pole väga küsimust, see on olemas, kui sa inimest tunned.“*

Probleemse kohana toodi välja kriisi juhtimise teatavat puudulikkust, mis oleks eespool nimetatud eeliste kontekstis võimaldanud paremat toimimist, kui isikud ja funktsioonid on paigas ning koostöös läbi harjutatud.

Pooltes intervjuudes toodi välja, et Eesti pole piisavalt ära kasutanud taakvara vähesust ja väikeste süsteemide eelist, sest nagu ID-kaardi juhtumi puhul välja tuli, ei mõista ka väga olulise tähtsusega riiklikud organisatsioonid, et taakvara tekkimist tuleks igal juhul vältida, ning Eestil, kes sõltub väga paljuski digiteenustest, peab olema kontroll oma infotehnoloogiliste lahenduste üle (seda enam, et süsteemid ei ole suured).

Intervjueeritav E*: „Küberjulgeolekus üldine julgeolek on, et asjad peavad olema uued ja tarkvara peab olema uus. See on ohutu, sest pahalased ei ole jõudnud kõiki nõrkusi välja selgitada. See on väga oluline.“*

IT-riigi ja küberjulgeoleku eestvedaja maine on tegur, mida Eesti rahvusvaheliselt jõudsalt ära kasutab, kuid võiks seda rohkem teha. See tegur pole küll otseselt seotud väiksusega, kuid võib anda hoopis uue eelise. Kaks intervjueeritavat tõid välja, et Eesti võiks ennast pakkuda välja kui testplatvormi e-teenuste ja toodete katsetamiseks terviklikus süsteemis (mh meie digitaalselt kogutud andmetega) – väiksus annab kompaktsuse ning olemasolevad toimivad tehnoloogiad kindluse. Eesti on ennast juba tõestanud kompetentse infotehnoloogilisi lahendusi kasutava ja edendava riigina, seega on vajalik seda ära kasutada, et ennast suurte tehnoloogiaettevõtete silmis atraktiivseks tegevuspaigaks muuta. Sest kui riik suudab pakkuda atraktiivseid ja kõrgetasemelisi võimalusi vastava valdkonna ettevõtetele ja spetsialistidele, siis võib siseriiklik kompetents digivaldkonnas veelgi paremaks muutuda. Olulise lisamõjuna pakkusid intervjueeritavad välja

tugevate partnerite leidmise võimalust, et kasvatada oma oskusi ja arvestatavust ka globaalsete suurettevõtetega suhtlemisel.

Intervjueeritav C: *„Suudame riigi kui terviku toimimist ette näidata, see on kõva argument ja võiks olla väikeriigi trump ... las testivad oma asju siin meie peal.“*

Intervjueeritav C: *„Meil käiakse õppimas meie kogemustest jms. Ütleks, et digi on olulisem ... siin ei käida puhtaid metsi imetlemas ...“*

3.3. Diskussioon, järeldused ja poliitikasoovitused

Käesoleva uurimuse objekt on Eesti 2017. aasta ID-kaardi turvariski juhtum, milles peeti nii ekspertintervjuudes kui ka dokumendianalüüsi tulemusena oluliseks siseriiklikku võimekust juhtumi lahendamisel. Esiteks oli tegemist väga ajakriitilise juhtumiga, mille lahendust väljastpoolt riiki ootama jäädes oleks turvarisk võinud samal ajal realiseeruda. Teiseks oli ohus Eesti kui küberjulgeoleku ja e-teenuste propageerija ja eestkõneleja rahvusvaheline kuvand, mille kadumine oleks seadnud kahtluse alla Eesti tegevused selles vallas (mh partnerlussuhted ja initsiatiivid ehk saavutatud nn pehme jõud rahvusvahelisel tasandil).

Töö empiirilises osas selgus, et nimetatud juhtumit **mõjutasid kõige enam** riiklike ressurssidega seonduvad tegurid, nagu näiteks **kohapealne tehniline kompetents** (mida nimetati ka kõige kriitilisemaks), milleta ei oleks suudetud lahenduseni jõuda. Teiseks oluliseks teguriks oli **teadlikkus riigi sõltuvusest infotehnoloogiast ja internetist ning sellega kaasnevatest võimalikest küberohtudest ja -riskidest.** See tähendas, et Eesti oli varasemalt mõelnud protseduuridele, mis andsid juhiseid käitumiseks sarnase juhtumi puhul, koordinatsiooniks, siseriiklike tehniliste kompetentside ja ametkondade ning erasektori koostöö võimalusteks, nutikuseks kasutada tehnoloogiat tegevuste efektiivsemaks muutmiseks. Väga toetasid ka varasemalt välja töötatud kriisijuhtimise mehhanismid, läbiviidud õppused ning katsetatud tehnilised lahendused.

ID-kaardi juhtum oli ajakriitiline ning selles mängisid oma osa ka sellised abstraktsed tegurid, nagu **tahe, õnn** ja **juhus.** Nimelt toodi intervjuudes ning ka juhtumijärgsetes analüüsides välja, et juhtumi lahendamisel esines puudusi (nt vananenud infotehnoloogiliste lahenduste kasutamine, puudujäägid kriisijuhtimise ülesannete selguses, kohati ebaselge kommunikatsioon jms), mis

oleksid olnud ennetavalt lahendatavad, ning et tehniline lahendus, mis kaasa aitas (kauguuendamine) oli üks vähestest alternatiividest, mis oli parasjagu olemas. Nimetatud asjaolusid toetab ka töö teoreetilises osas välja toodud küberjulgeolekuga ja riiklike valikutega seonduv, mis tähendab, et nimetatud tegurid mõjutavad riigi küberjulgeoleku võimekust ka väljaspool ID-kaardi juhtumit. Seega võib järeldada, et infotehnoloogiliselt arenenud riigi teadlikkus ning teadlik ja ennetav tegevus töötab nii küberruumis aset leidvate juhtumite kui ka kriisisituatsioonide puhul, kuid oluline on aru saada, et küberruum on hoomamatu ning seal varitsevad ohud võivad olla väga erinevad ning ründajad väga erinevate motiividega ning see **ei sõltu riigi suurusest**. Seega tuleb lisaks teadlikkusele rõhuda ka ennetustegevuste kvaliteedile, kontrollile ning mitmekesisusele. Lõpuks võib öelda, et küberjulgeoleku võimekus tagamises on mh olulisel kohal tahe ise selle jaoks midagi ära teha. **Eelnevast tulenevalt teeb magistritöö autor poliitikasoovituse (1): määrata kindlaks, millise aja tagant, kuidas ja mis ulatuses tuleb hinnata ja kontrollida riiklikult oluliste asutuste infotehnoloogiliste lahenduste ajakohastamist, vältida nn taakvara tekkimist ja kindlustada tehnoloogia vastupanuvõimet igapäevaselt ja kriisisituatsioonis.**

Nagu mainitud, oli ID-kaardi juhtum ajakriitiline, seega on oluline välja tuua ka **siseriiklikud tegurid**, mis olid sel puhul **eelistena** toetavad, kui mitte öelda määravad. Nimelt nimetati intervjuudes kiirust asjaajamisel, mille tingisid eelkõige **usaldus, mitteformaalsus (suhted, koostöö, tegevusvabadus, paindlikkus jms), multifunktsionaalsus, väikesed infotehnoloogiliste lahenduste süsteemid, koostöö, avatus**. Enamik nimetatud teguritest kattuvad dokumendianalüüsi leidudega, kuigi nt mitteformaalset asjaajamist otseselt ei mainita, multifunktsionaalsuses nähakse ka teatavaid puudusi (nt ülekoormus samaaegse kriisijuhtimise ja asutuse igapäevase toimimise tagamisel) ning mitteformaalseid suhteid kas ei mainita või ei peeta jätkusuutlikeks. Samuti tekitas intervjueeritavates kahtlusi, kas nt koostöö või mitteformaalsete suhete kasutamine on alati just riigi väiksusega seotud või toimib see ka nt suure riigi ühe valdkonna kogukonnas. Väikeriigi teooria kattub samuti nii intervjuude kui ka dokumendianalüüsi leidudega, nimetades välja toodud tegureid **riigi väiksuse ja väikese populatsiooni tulemuseks**, mis võib avalduda nii positiivses kui ka negatiivses võtmes (vt ka pt 1.3.2.). Põhjuste üle, miks dokumendianalüüs täielikult teooriat ja intervjuude tulemusi ei toeta, võib magistritöö autor vaid spekuleerida. Näiteks võib mitteformaalne suhtlus olla väikeses kogukonnas ja personaliseeritud suhete puhul nii igapäevane, et seda peetakse tavapärase asjaajamise ja bürokraatia osaks ega eristata rangetest käitumisjuhistest. Seega võib eeltoodust järeldada, et ID-kaardi juhtumis andis **riigi väiksus toetavaid asjaolusid** administratiivsete tegurite näol, mis väljendusid eelkõige

koostoimes (sest eraldiseisvalt võivad mõned nimetatud tegurid ilmneda ka suurte riikide puhul) ning **asjaajamise kiiruses** ja **paindlikkuses**, eeldusel, et eelmises lõigus välja toodud teadlikkus ja ennetustegevused oleks loodud.

Suurimad **väljakutsed on seotud oskuste ja pädevusega** avalikus sektoris ning võimalik, et ka väljaspool seda. Eelkõige napib usaldusväärseid tarkvarainsenere, teiseks puudub Eestil oskus suhelda suurte ettevõtetega, mille kaupadest/teenustest ollakse riiklikult sõltuvad. See tähendab, et teadmus praktiliselt puudub või ei pruugi olla asjakohane, sest selle järgi pole igapäevaselt vajadust ega ressursse tegevuseta hoidmiseks. Ka võib juhtuda, et teadmus koondub ühe isiku või väga kitsa ringi inimeste kätte, mida peeti nii töö teoreetilises kui ka empiirilise osa uurimuses nii negatiivseks kui ka positiivseks asjaoluks. Positiivsena võib välja tuua ülevaatlikkust asjadest, negatiivsena aga riski, et teadmus võib „minema jalutada“, ning kui alternatiiv või järelkasv puudub, siis on oluline osa riigi küberjulgeoleku võimekusest kadunud. Seega võib järeldada, et oskused on olulised ning see **ei sõltu riigi suurusest**, vaid küberruumi keerukusest, küll aga võib määravaks saada ressursside nappus, mis sõltub suuresti riigi suurusest, kuid on leevendatav oskuslike valikute tegemisega riigi valitsemises. **Eelnevast tulenevalt teeb magistritöö autor poliitikasoovituse (2): Tagada pikaajaline, pädev, usaldusväärne ja jätkusuutlik teadmus tarkvarainseneride näol, hoida nimetatud tuumkompetentsid Eestis ning säilitada riigi võimalus neid vajadusel kasutada; soodustada ja hoida valdkondlikku era- ja avaliku sektori koostööd, mis annab võimaluse kompetentside varieeruvuseks.**

Väga oluline osa Eesti küberjulgeoleku tagamise võimekusest on nn **tunnetuslikel teguritel, riigi ambitsioonidel ning poliitilistel valikutel** – riik on seadnud kõrged eesmärgid ning peab neid täitma, sest kohati ei ole enam võimalik ega mõistlik minna tagasi füüsilise asjaajamise juurde riigi pakutavates teenuste osutamisel. Nagu eelnevalt mainitud, mõjutab Eesti küberjulgeolekut väga suur tehnoloogiline sõltuvus igapäevases asjaajamises. Selle suurim tugi on kasutatavus, mis põhineb usaldusel oma riigi valitsuse vastu. Kui usaldus peaks kaduma, siis muutub pea 20 aasta tegevus infotehnoloogiliste lahenduse väljatöötamisel, juurutamisel ning kasutusele võtmisel mõttetuks. Väikeriigi teoorias on usalduse teke seotud riigi väiksuse ja kogukonnatundega (ning mh ka sooviga säilitada harjumuspärane elu ning hoida riiki), mida ilmestas ka ID-kaardi juhtumi intervjuudes välja toodu ning mida rõhutati dokumendianalüüsi tulemustes. Kui kaob Eesti küberjulgeoleku võimekuse kuvand, kaotab Eesti võimaluse kasutada nn pehmet jõudu enda maksma panemiseks globaalselt. Nagu mainitud, oli ka ID-kaardi juhtumis usaldusel kandvamaid rolle – selle olemasolu toetas juhtumi lahendamist ning selle säilimine tehnoloogiliste lahenduste

kasutamise jätkusuutlikkust. Seega võib järeldada, et küberjulgeolek, mis põhineb väga keerukatel infotehnoloogilistel lahendustel, mis on tavainimese jaoks sageli mõistetamatud, põhineb suuresti usaldusel **ega sõltu riigi suurusest**. **Väikese riigi eelis** võib olla usalduse kergem avaldumine võrreldes suurriigiga ning väikese riigi väike inimressurss ja kogukonnatunnetus on selle alus. Igal juhul peab riik oma tegevusega kindlustama usalduse jätkuvuse mh tehnoloogiliste lahenduste kasutamise osas.

Väikeriigi teooriast käis läbi ka riigi **väiksus ja majanduslikud** (mh innovatsiooniga seotud) **tegurid**, mis on klassikaliselt riigi väiksusest tulenevad puudused, kuid mida **saab oskuslikult kasutades muuta eelisteks**. Intervjuudes ja dokumendianalüüsis toetas seda Eesti kui väikeriigi ressursside piiratus – nimetati vajadust tegevusi prioriseerida, otsida kaalukaid koostööpartnereid, riigi funktsioonide kulukust ning kuluefektiivsemate ja nutikamate lahenduste otsimist riigi toimimiseks ning väiksuse ärakasutamist selleks. ID-kaardi juhtumis oli uuenduslikkuse kasutamise näiteks lisaks riigi tehnoloogilisele arengule (mis on küberjulgeoleku vajaduse eelduseks) ka ID-kaartide sertifikaatide kauguuendamine, mis osutus Eestis vajalikuks, sest mh puudusid ressursid kaarte füüsiliselt uuendada. Kauguuendamise tehnoloogia oli olemas ja kasutatav osalt tänu teadlikule ennetustööle, aga ka juhusele, sest küberruum on nii hoomamatu, et isegi suured riigid ei suudaks kõiki ohtude ja riskidega seotud asjaolusid ette näha. Kauguuendamist ei kasutanud mitte ükski teine turvanõrkuse juhtumis osalenud riik. Seega saab järeldada, et küberjulgeoleku tagamise võimaluse annab **piiratud ressursside puhul nutikate lahenduste kasutamine**, mis saab tänu tehnoloogia arengule ja kättesaavusele võimalikuks ka väikesele riigile, mitte ainult suurtele. Riigi roll on soodustada ja toetada ideede genereerimist ning nende elluviimist nt teaduse- ja arendustegevuse kaudu koostöös ülikoolide ja eraettevõtetega. **Eelnevast tulenevalt teeb magistritöö autor poliitikasoovituse (3): Defineerida küberjulgeolek Eesti majandusarengu konkurentsivõime elemendina, arendada küberturbega seonduva majandusharu loomist Eestisse, kasutades ära riigi väiksust ja atraktiivsust infotehnoloogia ja küberjulgeoleku propageerijana, mis toetaks ka eelnevat poliitikasoovitust ning oleks abistav tugevate partnerlussuhete loomisel küberjulgeoleku alal.**

Töö käigus uuriti ka **julgeoleku erinevusi küberruumis ja konventsionaalses mõttes**. Teooria tõi välja, et julgeoleku seisukohalt mängivad rolli mitmed asjaolud, nagu näiteks riigi geograafiline asukoht, ohustaja ja oht, riikidevahelised ajaloolised suhted ja poliitikaseosed, koostöö võimsa riigiga, füüsilised ressursid. (Knudsen 1996, 4–5, 9) Seoses küberruumi tekkega on olukord

muutunud ning nt geograafiline asukoht ja sõjaväelise rasketehnika suurus ei mängi julgeolekus enam nii olulist rolli. Nagu eelnevalt mainitud, saavad oluliseks riigi tehnoloogiline areng ning oskused (nt leida nutikaid lahendusi ning kasutada pehmet jõudu). Seda toetab ka ekspertide arvamus ning dokumendianalüüsi tulemused. Seega võib järeldada, et **tehnoloogia, teaduse arengu ja küberruumi tekkimisega ei sõltu võim riigi suurusest ning nii võim kui ka riigi suurus on suhtelised mõisted, sõltudes kontekstist**. Küberi kättesaadavus tähendab seda, et võimu mõiste on muutunud ning võimule pääsevad ligi ka väikesed ja klassikalises mõttes nõrgad riigid, ning haavatavad võivad olla ka suured ja võimsad riigid.

ID-kaardi juhtum tõestas, et Eesti sai nii tegelikkust kui ka ekspertide intervjuude ja dokumendianalüüsi tulemusi kõrvutades hästi hakkama. Kõige olulisemad edu näitajad olid, et suudeti iseseisvalt hakkama saada Eesti jaoks niivõrd olulise küberjulgeoleku riskiga, kindlustada turvalisus, pakkuda teenuseid kriisihetkel ning säilitada usaldus selle ajal ning järel, mis kindlustas Eesti digiteenuste jätkuva kasutamise ning tugeva küberjulgeoleku võimekusega riigi maine maailmas.

Seega võib kokkuvõtteks öelda, et küberjulgeoleku võimekuse võib saavutada ka klassikalises mõttes väike ja võimetu riik.

Väikeriikideteooriad näevad väikeriiki julgeoleku kontekstis enamasti vähe võimekana ega käsitle tehnoloogia kättesaadavusega esile kerkivaid võimalusi. Seega tuleks autori arvates küberruum kui uus kontekst asetada väikeriigi teooriasse. Kuna Eesti 2017. aasta ID-kaardi juhtum ja selle lahendamine ei ole täielikult ülekantav kõigile väikeriikidele, tuleks teemat rohkemat juhtumite põhjal sügavamalt uurida.

KOKKUVÕTE

Küberruum on uus normaalsus, mis kätkeb endas nii võimalusi kui ka ohtusid ning kus kohtuvad igasuguse suurusega osalejad, mh suured ja väikesed riigid. Seoses tehnoloogia arenguga mõjutavad küberohud ning nendega toimetulek tugevalt riikide igapäevast toimimist. Sellest tulenevalt on küberjulgeolek saanud riikide julgeolekukäsitluses keskse koha.

Klassikaline väikeriikide teoreetiline käsitlus, kus väikeriik on julgeoleku tagamises vähe võimekas (nt Hey 2003; Wilberg 1996;Wivel *et al* 2014; Knudsen 1996), ei pruugi oma eesmärki enam täita. Tänapäeval on situatsiooni muutunud ning küberruumi kontekstis, kus füüsiliste ressursside kõrval saavad oluliseks ka riikide tegevused (nt teadlikkus jms) ja oskused (infotehnoloogia ära kasutamine) ehk siseriiklikud tegurid, võivad väikesed riigid saavutada võimu ja võimekuse suurriikide kõrval ja ees (nt Nye 1990; Nye 2010).

Eelnevast tulenevalt oli magistritöö uurimisprobleem: kuidas tagab väikeriik oma küberjulgeoleku võimekuse? Uurimisprobleemi täpsustamiseks püstitab autor teoreetilise uurimisküsimuse: kuidas mõjutab riigi väiksus tema küberjulgeoleku tagamise võimekuse?

Magistritöö empiirilise uurimuse läbiviimiseks kasutati näitena Eesti ID-kaardi 2017. aasta turvanõrkuse juhtumit, mis puudutas ligi 800 000 Eesti poolt välja antud dokumendi kiipi, mille abil saab inimene end elektrooniliselt identifitseerides kasutada avaliku- ja erasektori e-teenuseid. (Buldas *et al* 2018, 5) Antud juhtum on oluline seetõttu, et see näitab, kui palju sõltub digitaalse infrastruktuuri toimimisest ühiskonna tavapärane toimimine tervikuna, milliseid ohte võib küberruum seoses sellega endast kujutada ning milliseid väljakutseid pakkuda. Samuti võimaldas nimetatud juhtum uurida, kuidas väikeriik olulise ja ajakriitilise sündmusega toime tuli ja millised siseriiklikud tegurid mõjutavad väikeriigi küberjulgeoleku võimekust, mis oli ka magistritöö eesmärgiks.

Lähtudes töö iseloomust, kasutati uurimuse teostamiseks kvalitatiivset uurimismeetodit, mis andist võimaluse teha uurimist, teooria testimist ning uue teadmise loomist paralleelselt töö käigus (Bouma, Atkinson 1995; Frankel, Devers 2000). Uurimuse läbiviimiseks vajalikud andmed saadi dokumendianalüüsi ja valdkonna poliitikakujundajate või ekspertidega läbi viidud poolstruktureeritud intervjuude kaudu.

Uurimuse tulemusena selgus, et küberjulgeoleku võimekust võib saavutada ka klassikalises mõttes väike ja võimetu riik ning siseriiklikel teguritel ja väiksusest tulenevates eelistel on selles oluline osa.

Töö peamised leiud on järgnevad:

- **Esmalt** võib öelda, et küberjulgeoleku tagamise võimekuse eelduseks on riigi tehnoloogiline areng ning riigi sõltuvus sellest.
- **Teiseks** toetab küberjulgeoleku võimekuse tagamist teadlikkus küberruumiga seonduvast ning riigi võimalustest ja oskustest (kompetents) sellega toime tulla eelkõige iseseisvalt või koostöös valdkondlike partneritega.
- **Kolmandaks** oluliseks teguriks on tunnetuslikkus, milles olulist rolli mängib usaldus tehnoloogia, selle kasutamise ja intsidentide lahendamise turvalisuse vastu.

Väikeriikide teooriad on julgeolekuvõimekust traditsiooniliselt vaadelnud eelkõige väiksusest tulenevate puuduste, väljakutsete ja haavatavuste kaudu ega hõlma küberjulgeoleku aspekti. Seoses küberruumi tekkega on aga olukord muutunud ning töö järeldused kinnitavad suuresti väikeriigide julgeoleku asjaolusid, mis seostuvad eelkõige ressursside oskusliku ära kasutamisega ega toeta seega enam täielikult traditsioonilist lähenemist. Seetõttu tuleks küberruum kui uus kontekst võtta arvesse väikeriigi teooriates ning teemat sügavamalt edasi uurida.

SUMMARY

NATIONAL FACTORS AFFECTING CYBER SECURITY CAPABILITIES OF SMALL STATES: ESTONIA`S EXPERIENCE WITH THE 2017 ESTONIAN ID CARD SECURITY VULNERABILITY CASE

Merike Jõesaar

The research topic of this master's thesis is: how does a small state ensure its cybersecurity capabilities? The specific research question addressed within this research topic is: how does a state's small size affect its capabilities in ensuring cybersecurity? The purpose of this master's thesis is to identify national factors that affect a small state's cybersecurity capabilities.

In the theoretical part of this thesis, it is determined that small states have been an interesting field of research within international relations, however, very little research has been done on national factors affecting a small state's cybersecurity capabilities. How a small state ensures its cybersecurity must be derived indirectly from other approaches, such as a small state's administrative capacity, changes to the concept of power, innovation theory, international relations theory, etc., which indicate that a small state is rather less powerful (in terms of security), which is tied to limited state resources (Hey 2003; Wilberg 1996; Wivel et al 2014; Knudsen 1996). The cybersecurity topic examined in this thesis likewise does not differentiate states according to their size, nor is does it directly indicate how a state's small size afffects its cybersecurity-ensuring capabilities, or whether its small size may offer any advantages. The distinction is apparent in changes to the concept of power, a state's digital development and its dependence thereon, as well as a state's functionality, as war in its conventional sense no longer necessarily has to be declared in order to threaten a state's security; in order to create a national security crisis, it suffices to paralyze and internet technology- and internet-dependent vital service in cyberspace, which, due to the latter's characteristics, can be done by any participant thereof (Nye 1990; Nye 2010, etc.). Thus, any information technology-dependent state can, in terms of cybersecurity, be either powerful or vulnerable, and neither one nor the other is dependent exclusively upon its size in the classical sense, but rather upon other factors as well. Therefore, in the context of the capability to ensure cybersecurity, it is essential to examine a state's economic capabilities, its general administrative capacity as well as its cognitive capacity (in the context of soft power), which, from the position of a small satte, provide both positive as well as negative aspects.

Regarding the specifics of the thesis, the author uses a qualitative research method to conduct their research. Limited data exists regarding the effects of national factors on ensuring cybersecurity in a small state, and thus the use of this method provides an opportunity to examine the case as well as test these theories simultaneously. The materials used in this thesis are comprised of theory and the analysis of publicly accessible documents as well as semi-structured expert interviews conducted with experts from the cybersecurity field or parties to the ID card case.

This thesis is a case study which, in its empirical part, focuses on the discovery in Estonia in 2017 of a security vulnerability affecting the security chips of ID cards, an event of significant impact for Estonia in terms of the functioning of the state. Although this incident was not treated as a risk of an emergency, which pursuant to the Emergency Act would have meant the implementation of an emergency response plan, the cybersecurity issue is apparent in the fact that in the case being examined, information of national importance, carriers of electronic information as well as electronic services (including vital services) were affected, and the prevention of cyberattacks and the ensuring of the social and economic functions of the state were also key. In resolving the case, the state utilized both information technology as well as organizational measures, and while resolving the situation, it was necessary to restore the security of ID cards while simultaneously ensuring the functioning of vital services (Cyber Security Strategy 2008-2013, 40).

The results of this thesis reveal that cybersecurity capabilities can also be achieved by a state that is small and powerless in the classical sense, and that national factors and the skillful utilization of advantages offered by small size play a significant role in this.

The primary findings of this thesis are as follow. **Firstly**, it can be said that a prerequisite for the capability to ensure cybersecurity is a state's technological development and the state's dependence thereon. This, however, is not tied to a state's size, but rather its choices, which may arise from a desire to be innovative, but also a need to survive. **Secondly**, a prerequisite for the capability to ensure cybersecurity is awareness of that which is related to cyberspace as well as the state's ability and skills (competence) to cope with it either independently or in cooperation. While awareness is not directly dependent on a state's size, small size, with its small systems, small population, etc., may provide advantantages, if one takes into account oversight of few things and systems and thus the opportunity to act very quickly in case a threat arises or materializes. A state's skills are and are not dependent upon the size thereof. What become decisive on one hand are

existing resources that can be utilized to generate and expand knowledge, and which a small state may be lacking. On the other hand, the ability to find alternatives and be clever are crucial, and this does not depend on a state's size, but rather, for example, its will, and it provides even a small state the opportunity to prove itself capable. It is essential that these skills are present on site in a state, as in the event of cyber risks, the prevention thereof as well as the materialization of threats, the time it takes to respond and resolve the situation becomes a decisive factor. **Thirdly**, a factor in cybersecurity capabilities is cognition, in which trust in technology, its use and the security of the resolution of incidents play a significant role. Trust is not dependent upon the size of a state, however, in the context of the small size of a state, achieving trust may be simpler than in larger states, which indicates an advantage for small size.

According to most definitions of small states, a state's small size is traditionally associated with vulnerability, shortcomings that are a result of its small size as well as challenges, and are not directly related to the matter of cybersecurity. Based on the results of this thesis, it can be said that the theoretical claims and empirical conclusions presented in this thesis largely overlap in terms of small states and their resources and the skillful utilization of resources. With the manifestation of a cyberspace context and changes in the definition of power, yet-unaddressed issues that require further study nonetheless emerge in small state theory involving national factors affecting small states' cybersecurity capabilities, such as advantages and opportunities arising from a state's small size in the security field, which otherwise generally focuses on shortcomings that are the result of one's small size. Thus, cyberspace as a new context needs to be taken into consideration in small state theory, and this topic should be researched further and in greater depth.

KASUTATUD ALLIKATE LOETELU

AKIT = Andmekaitse ja infoturbe leksikon. Cybernetica, https://akit.cyber.ee , 26. detsember 2018.

Alasuutari, P (1996). *Researching Culture: Qualitative Method and Cultural Studies*. London, Thousand Oaks; New Delhi: SAGE Publications.

AMSS = Ametniku soovitussõnastik. Eesti Keele Instituut, http://www.eki.ee/dict/ametnik/ , 26. detsember 2018.

Areng, L. (2014). Lilliputian States in Digital Affairs and Cyber Security. – *Tallinn Paper.* No. 4. Kättesaadav: https://ccdcoe.org/multimedia/lilliputian-states-digital-affairs-and-cyber-security.html , 17. november 2018.

Baehr, P. (1975). Small States: A Tool for Analysis. – *World Politics*, Vol. 27, No. 3, 456–466.

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., Wreiss, J. (2012). *Cyber Security Policy Guidebook*. New Jersey: John Wiley and Sons. Kättesaadav: https://the-eye.eu/public/Books/IT%20Various/cyber_security_policy_guidebook.pdf , 16. november 2018

Benedict, B. (1966). Problems of Smaller Territories. – *The Social Anthopology of Complex Societies*. (Ed.) M. Banton. London: Tavistock Publications, 23–36.

Benedict, B. (1967). Sociological Aspects of Smallness. – *Problems of Smaller Territories*. (Ed.) B. Benedict. London: Athlone Press, 45–55.

Bouma, G. D., Atkinson, G. B. J. (1995). *A Handbook of social science research*. Oxford: Oxford University Press.

Brock, C. (1987). The Educational Context. – *The challenge of scale: Educational development in the small states of the Commonwealth*. (Eds.) K. Bacchus, C. Brock. London: Commonwealth Secretariat, 11–25. Kättesaadav: https://books.google.ee/books?id=6B8-gZS0LE4C&pg=PP3&source=gbs_selected_pages&cad=2#v=onepage&q&f=false , 30. november 2018.

Buldas, A., Jung, M., Kuivjõgi, K., Tallinn, L., Osula, A-M., Ottis, R., Priisalu, J., Vaks, T. (2018). *ID-kaardi kaasuse õppetunnid*. Tallinn: Tallinna Tehnikaülikool. Kättesaadav: https://www.ria.ee/sites/default/files/content-editors/EID/id-kaardi_oppetunnid.pdf , 25. november 2018.

Burton, J. (2013). Small States and cyber security: The case of New Zealand. – *Political Science,* Vol. 65, No. 2, 216–238.

Burton, J. (2018). Cyber Deterrence: A Comprehensive Approach? – *CCDCOE*. Kättesaadav: https://ccdcoe.org/sites/default/files/multimedia/pdf/BURTON_Cyber_Deterrence_paper_April2018.pdf , 10. november 2018.

Buzan, B., Segal, G. (1996). The Rise of "Lite" Powers: A Strategy for the Postmodern State. – *World Policy Journal*, Vol. 13, No. 3, 1–10.

Castells, M. (2010). *End of Millenium. The Information Age: Economy, Society, and Culture.* Vol. III, 2nd ed. Malden; Oxford: Wiley-Blackwell. Kättesaadav: http://www.mediastudies.asia/wp-content/uploads/2016/09/Manuel_Castells_End_of_Millennium_The_Information_Age.pdf , 25. november 2018.

Cavelty Dunn, M. (2008). Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. – *Journal of Information Technology & Politics,* Vol. 4, No. 1, 19–36. Kättesaadav: https://www.researchgate.net/publication/233310365_Cyber-Terror-Looming_Threat_or_Phantom_Menace_The_Framing_of_the_US_Cyber-Threat_Debate , 6. november 2018.

Czosseck, C., Ottis, R., Talihärm, A-M. (2011). Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security. – *International Journal of Cyber Warfare and Terrorism*, Vol. 1, No. 1, 24–34. Kättesaadav: http://www.irma-international.org/viewtitle/61328/ , 25. november 2018.

e-Governance Academy Yearbook 2015. Year of Growth. (2016). /Koost: A. Vahtra-Hellat. Tallinn: e-Governance Academy. Kättesaadav: https://ega.ee/wp-content/uploads/2016/09/ega-aastaraamat-2015-ENG-final.pdf , 23. detsember 2018.

Eesti infoühiskonna arengukava 2020. (2013). Majandus- ja Kommunikatsiooniministeerium. Kättesaadav:https://www.mkm.ee/sites/default/files/elfinder/article_files/eesti_infouhiskonna_arengukava.pdf , 8. november 2018.

Eesti julgeolekupoliitika alused. Kaitseministeerium. Kättesaadav: http://www.kaitseministeerium.ee/sites/default/files/sisulehed/eesmargid_tegevused/395xiii_rk_o_lisa.pdf , 18. november 2018.

Eesti riigi kriitiliste andmekogude turvalisuse ja säilitamise tagamine. Riigikontrolli aruanne Riigikogule. Riigikontroll. Tallinn, 14. mai 2018. Kättesaadav: https://www.riigikontroll.ee/DesktopModules/DigiDetail/FileDownloader.aspx?AuditId=2462&FileId=14200 , 26. detsember 2018.

Elektrooniline identiteet eID. Riigi Infosüsteemi Amet. Kättesaadav: https://www.ria.ee/et/riigi-infosusteem/elektrooniline-identiteet-eid.html , 26. detsember 2018.

Elektroonilise hääletamise statistika. Valimised. Kättesaadav: https://www.valimised.ee/et/valimiste-arhiiv/elektroonilise-hääletamise-statistika , 22. detsember 2018.

Eriksson, J., Giacomello, G. (2006). The Information Revolution, Security, and International Relations: (IR) Relevant Theory? – *International Political Science Review / Revue internationale de science politique*, Vol. 27, No. 3, 221–244.

Estonia. National Cyber Security Index. Kättesaadav: https://ncsi.ega.ee/country/ee/ , 23. detsember 2018.

Europe's Digital Progress Report 2017. European Commission. Kättesaadav: https://ec.europa.eu/digital-single-market/en/scoreboard/estonia , 8. november 2018.

Farrugia, C. (1993). The Special Working Environment of Senior Administrators in Small States. – *World Development*, Vol. 21, No 2, 221–226.

Fischer, A. E. (2009). *Creating a National Framework for Cybersecurity: An analysis of issues and options.* New York: Nova Science Publishers.

Frankel, R. M., Devers, K. J. (2000). Study Design in Qualitative Research – 1: Developing Questions and Assessing Resource Needs. – *Education for Health*. Vol. 13, No. 2, 251–261.

Ghauri, P., Grønhaug, K. (2004). *Äriuuringute meetodid. Praktilisi näpunäiteid*. Tallinn: Külim.

Global Cybersecurity Index. International Telecommunications Union. Kättesaadav: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx , 16. detsember 2018.

Goodman, M. D., Brenner, S. W. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. – *International Journal of Law and Information Technology*. Vol. 10, No. 2,139–223.

Goodman, W. (2010). Cyber Deterrence. Tougher in Theory than Practice? – *Strategic Studies Quarterly*, Vol. 4, No. 3, 201–135. Kättesaadav: https://apps.dtic.mil/dtic/tr/fulltext/u2/a527974.pdf, 6. november 2018.

Greenwald, G., MacAskill, E., Poitras, L. (2013). Edward Snowden, the whistleblower behind the NSA surveillance revelations. – *The Guardian*, 9 June. Kättesaadav: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance , 10. november 2018.

Gross, J. R. (2016). Hack and be Hacked: A Framework for the United States to Respond to Non-state Actors in Cyberspace. – *California Western International Law Journal*, Vol. 46, No. 2, 109–145. Kättesaadav: https://scholarlycommons.law.cwsl.edu/cwilj/vol46/iss2/3 , 05. november 2018.

Hansen, L., Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. – *International Studies Quarterly*, Vol. 53, 1155–1175. Kättesaadav: https://nissenbaum.tech.cornell.edu/papers/digital%20disaster.pdf , 29. november 2018.

Hey, J. A. K. (2003). Introducing Small States Foreign Folicy. – *Small States in World Politics: Explaining Foreign Policy Behavior*. (Ed.) J. A. K. Hey. Boulder; London: Lynne Rienner Publishers, 1–12.

Hirsijärvi, S., Remes, P., Sajavaara, P. (2005). *Uuri ja kirjuta*. Tallinn: Medicina.

HOS = Hädaolukorra seadus. RT I, 03.03.2017, 1.

Hoscheit, J.-M. (1992). Administrative adaption in the context of regional integration: Luxemburg and the European Community. – *Public Administration in Small and Island States*. (Ed.) R. Baker. West Hartford, CT: Kumarian Press, 265–282.

Hughes, R. B. (2009). *NATO and Cyber Defence: Mission Accomplished?* Kättesaadav: https://www.atlcom.nl/ap_archive/pdf/AP%202009%20nr.%201/Hughes.pdf , 08. november 2018.

ICT Facts and Figures 2017. (2017). Geneva: International Telecommunications Union. Kättesaadav: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf , 25. november 2018.

Jervis, R. (1978). Cooperation under the security dilemmas. – *World Politics*, Vol. 30, No. 1, 167–214.

Joenniemi, P. (1998). From Small to Smart: Reflections on the Concept of Small States. – *Irish Studies in International Affairs*, Vol. 9, 61–62.

Katzenstein, P. J. (1984). *Small states in world markets: industrial policy in Europe*. Ithaca; London: Cornell University Press.

Kattel, R., Kalvet, T., Randma-Liiv, T. (2010). Small States and Innovation. – *Small States in Europe: Challenges and* Opportunities. (Ed.) R. Steinmetz, A. Wivel. Aldershot: Ashgate, 65–85.

Kello, L. (2013). The Meaning of the Cyber Revolution: Perlis to Theory and Statecraft. – *International Security*, Vol. 38, No. 2, 7–40.

Knudsen, O. F. (1996) Analysing Small-State Security: The Role of External Factors. – *Small states and the security challenge in the new Europe*. (Eds.) W. Bauwens, A. Clesse, O. F. Knudsen. London; Washington: Brassey's, 3–21.

Kvale, S. (2006). Dominance Through Interviews and Dialogues. – *Qualitative Inquiry.* Vol. 12, No. 3, 480–500.

Küberintsidentide käsitlemine CERT-EE. Riigi Infosüsteemi Amet. Kättesaadav: https://www.ria.ee/et/kuberturvalisus/cert-ee.html , 31. detsember 2018.

Küberjulgeoleku strateegia 2008–2013. Kaitseministeerium. Kättesaadav: https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf , 7. november 2018.

Küberjulgeoleku strateegia 2014–2017. Majandus- ja Kommunikatsiooniministeerium. Kättesaadav: https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf , 7. november 2018.

Küberturvalisus 2018. Tallinn: Riigi Infosüsteemi Amet. Kättesaadav: https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria-kuberturvalisus-2018.pdf , 25. november 2018.

Küberturvalisuse strateegia 2019–2022. Majandus- ja Kommunikatsiooniministeerium. Kättesaadav: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf , 23. detsember 2018.

Leyden, J. (2016). Plymouth `animal rights` teen admits Florida SeaWorld cyberattack. – *The Register*, 29 June. Kättesaadav: https://www.theregister.co.uk/2016/06/29/seaworld_plymouth_teen_hacker_pleads_guilty_denies_airline_bomb_hoax_tweets/ , 10. november 2018.

Libicki, C. M. (2007). *Conquest in Cyberspace: National Security and Information Warfare.* Cambridge: Cambridge University Press.

Lonsdale, D. J. (2016). Britain's Emerging Cyber-Strategy. – *RUSI Journal*, 29 September. Kättesaadav: https://rusi.org/publication/rusi-journal/britain%E2%80%99s-emerging-cyber-strategy , 05. november 2018.

Lowenthal, D. (1987). Social features. – *Politics, Security and Development in Small States*. (Eds.) C. G.Clarke, T. Payne. London: Allen & Unwin, 26–49.

Luiijf, E., Besseling, K., De Graaf, P. (2013). Nineteen National Cyber Security Strategies. – *International Journal of Critical Infrastructure Protection,* Vol. 9, No. 1, 3. Kättesaadav: https://www.researchgate.net/publication/261950643_Nineteen_National_Cyber_Security_Strategies , 4. november 2018.

Lupovici, A. (2016). The "Attribution Problem" and the Social Construction of "Violence": Taking Cyber Deterrence Literature a Step Forward. – *International Studies Perspectives*, Vol. 17, No. 3, 322–342.

Lõugas, H. (2017). *RIA peadirektor saab õiguse ohtlik arvuti Eesti internetist välja lülitada*. Kättesaadav: https://geenius.ee/uudis/ria-peadirektor-saab-oiguse-ohtlik-arvuti-eesti-internetist-valja-lulitada/ , 10. november 2018.

Maass, M. (2009). The Elusive Definition of the Small State. – *International Politics*, Vol. 46, No. 1, 65–83.

Mahoney, J., Goertz, G. (2006). A Tale of Two Cultures: Contrasting Quantitative and Qualitative Research. – *Political Analysis*, Vol.14, 227–249.

Militerm [Terminibaas] http://termin.eki.ee/militerm/ (26.12.2018).

Mouritzen, H., Wivel, A. (2005). Introduction. – *The geopolitics of Euro-Atlantic integration*. (Eds.) H. Mouritzen, A. Wivel. New York: Routlege, 1–10. Kättesaadav: https://www.taylorfrancis.com/books/9781134457632 , 28. november 2018.

Nemec, M., Sys, M., Svenda, P., Klinec, D., Matyas, V. (2017). The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. – *CCS '17 Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, 30 October – 3 November 2017, Dallas, Texas, USA. New York: ACM, 1631–1648. Kättesaadav: https://acmccs.github.io/papers/p1631-nemecA.pdf , 26. detsember 2018.

Noor, K. B. M. (2008). Case Study: A Strategic Research Methodology. – *American Journal of Applied Sciences*, Vol, 5, No. 11, 1602–1604.

Nye, J. S. Jr. (1990). Soft Power. – *Foreign Policy*, No. 80, Twentieth Anniversary, 153–171.

Nye, J. S. Jr. (2010). *Cyber Power*. Cambridge: Center for Science and International Affairs. Kättesaadav: https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf , 25. november 2018.

Ottis, R., Lorents, P. (2010). Cyberspace: Definition and Implictions. – *5th International Conference on Information Warfare and Security*, Dayton, OH, US, 8-9 April. (Ed.) L. Armistead. Reading, UK: Academic Conferences Limited, 267−270. Kättesaadav: https://drive.google.com/file/d/0B7yq33Gize8yOGY0MGYwODEtODViZi00YTliLTg5ZjYtNTc3NDZmOGFjNDVi/view?hl=en , 7. november 2018.

Pace, R. (2000). Small States and the Internal Balance of the European Union: the perspective of small states. – *Enlarging the European Union: The Way Forward*. (Eds.) J. Gower, J. Redmond. Aldershot: Ashgate, 107–122.

Payne, K. (2003). The Fallacies of Could War Deterrence and New Direction. – *Comparative Strategy*, Vol 22, No. 5, 411–428. Kättesaadav: https://www.tandfonline.com/doi/abs/10.1080/01495930390261431 , 10. november 2018.

Projekti „Elutähtsate teenuste osutamist mõjutavate tegurite kaardistamise uuring“ kokkuvõte. (2016). Riigi Infosüsteemi Amet. Kättesaadav: https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/elutahtsate-teenuste-osutamist-mojutavate-tegurite-uuringu-kokkuvote.pdf , 22. detsember 2018.

Randma-Liiv, T. (2002). Small States and Bureaucracy: Challenges for Public Administration. – *TRAMES*, Vol. 6, No. 4, 374–389. Kättesaadav: http://web.a.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=1&sid=6a9d05f6-c3da-4069-a45e-d59f2be692dc%40sdc-v-sessmgr06 , 5. november 2018.

Randma-Liiv, T., Sarapuu. K. (2019) (ilmumas). Public governance in small states: From paradoxes to research agenda. – *A Research Agenda for Public Administration*. (Ed.) A. Massey. Edward Elgar. Manuscript.

Recommendation ITU-T X.1205. International Telecommunications Union. Kättesaadav: https://ccdcoe.org/sites/default/files/documents/ITU-080418-RecomOverviewOfCS.pdf , 27. november 2018.

Rikk, R. (2018). *National cyber security index 2018*. Tallinn: e-Governancy Academy. Kättesaadav: https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf , 16. detsember 2018.

ROCA Vulnerability and eID: Lessons Learned. Riigi Infosüsteemi Amet. Kättesaadav: https://www.ria.ee/sites/default/files/content-editors/kuberturve/roca-vulnerability-and-eid-lessons-learned.pdf , 9. detsember 2018.

Rothstein, R. L. (1968). *Alliances and Small Powers*. New York: Columbia University Press.

Sarapuu, K. (2010). Comparative Analysis of State Administrations: The Size of State as an Independent Variable. – *Halduskultuur – Administrative Culture*, Vol. 11, No. 1, 30–43.

Shackelford, S. (2010). Estonia three years later: A progress report on combating cyber attacks. – *Journal of Internet Law*, Vol. 13, Iss. 8, 22–29. Kättesaadav: https://files.meetup.com/17802942/Schakelford_Cyber%20Attacks_Estonia.pdf , 25. november 2018.

Shea, J. (2016). Resilience: a core element of collective defence. – *NATO Review Magazine*. Kättesaadav: https://www.nato.int/docu/review/2016/also-in-2016/nato-defence-cyber-resilience/en/index.htm , 10. november 2018.

Statistics. International Telecommunications Union. Kättesaadav: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx , 13. detsember 2018.

Sutton, P. (1987). Political aspects. – *Politics, Security and Development in Small States*. (Eds.) C. G. Clarke, T. Payne. London: Allen & Unwin, 3–25.

Taipale, K. A. (2009). Cyber-Deterrence. – *Law, Policy and Technology: Cyberterrorism, Information, Warfare, Digital and Internet Immobilization, IGI Global, 2010*. Kättesaadav: https://ssrn.com/abstract=1336045 , 5. november 2018.

The World Bank in Small States: Overview. The World Bank. Kättesaadav: https://www.worldbank.org/en/country/smallstates/overview , 15. november 2018.

Thorhallsson, B. (2000). *The Role of Small States in the European Union.* Aldershot: Ashgate.

Thorhallsson, B. (2006). The Size of States in the European Union: Theoretical and Conceptual Perspectives. – *Journal of European Integration*, Vol. 28, No. 1, 7–31. Kättesaadav: https://www.researchgate.net/publication/238315184_The_Size_of_States_in_the_European_Union_Theoretical_and_Conceptual_Perspectives , 14. november 2018.

Thorhallsson, B. (2018). Studying small states: A review. – *Small States & Territories*, Vol. 1, No. 1, 17–34.

Tiirmaa-Klaar, H. (2009). Cyber security: a part of internal, External and economic security. – *Information technology in public administration of Estonia. Yearbook 2008*. (Eds.) I. Odrats. Tallinn: Ministry of Economic Affairs and Communication, 85-86. Kättesaadav: https://www.digar.ee/arhiiv/et/raamatud/51713 , 10. november 2018.

Vaicekauskaité, Ž. M. (2017). Security Strategies of Small States in a Changing World. *Journal on Baltic Security*, Vol. 3, No. 2, 7–15. Kättesaadav: https://www.degruyter.com/downloadpdf/j/jobs.2017.3.issue-2/jobs-2017-0006/jobs-2017-0006.pdf , 15. november 2018.

Vaidya, T. (2015). *2001-2013: Survey and Analysis of Major Cyber Attacks*. Kättesaadav: https://arxiv.org/pdf/1507.06673v1.pdf , 10. november 2018.

Vital, D. (1967). *The inequality of states: a study of small powerin international relations*. Oxford: Clarendon Press.

Vital, D. (2006). The Inequality of States: A Study of the Small Power in International Relations. – *Small States in International Relations*. (Eds.) C. Ingebritsen, L. Neumann, S. Gstohl, J. Beyer. Seattle: University of Washington Press, 77-88.

Walt, S. M. (1987). *The origins of alliances*. Ithaca: Cornell University Press.

War in the fift domain (2010). The Economist. Kättesaadav: https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain , 10. november 2018.

Weber, M. (1947). *The Theory of Social and Economic Organization*. New York: Oxford University Press.

Wilberg, H. (1996). Security Problems of Small States. – *Small states and the security challenge in the new Europe*. (Eds.) W. Bauwens, O. F. Knudsen, A. Clesse. London, Washington: Brassey's, 21–41.

Wivel, A., Bailes, A. J. K., Archer, C. (2014). Setting the scene. Small states and international security. – *Small states and international security: Europe and beyond*. (Eds.) C. Archer, A. Wivel, A. Bailes. London; New York: Routledge, 3–25.

Wood, G. (2015). What ISIS really wants. – The Atlantic Daily, March. Kättesaadav: https://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/ , 10. november 2018

Üldandmed. Eesti.ee. Kättesaadav: https://www.eesti.ee/et/eesti-vabariik/eesti-vabariik/ueldandmed/ , 23. detsember 2018.

Yin, R. K. (1994). *Case Study Research: design and methods*. 2nd ed. Thousand Oaks: Sage Publications.

Yin, R. K. (2018). *Case study research and applications: design and methods*. 6th ed. Los Angeles: Sage Publications.

LISAD

Lisa 1. Poolstruktureeritud ekspertintervjuu küsimused

Põhiküsimused

1. Palun meenutage 2017. aastal toimunud ID-kaardi turvariski juhtumit Eestis, kirjeldage, mis juhtus. Selgitage, kuidas on see juhtum Eesti riigi jaoks oluline?

2. Kus ja kellena töötasite nimetatud juhtumi avastamise ja lahendamise ajal?

3. Kuidas hindate Eesti tegutsemist ja toimetulekut juhtumi lahendamisel? Millised olid teie arvates edu/ebaedu peamised aspektid, mille põhjal hindate tulemusi?

4. Millised siseriiklikud tegurid mängisid rolli nimetatud juhtumi lahendamisel? Millised olid kriitilisema tähtsusega ja miks?

5. Millised siseriiklikud tegurid toetasid või mõjutasid juhtumi lahendamist, millised olid väljakutsed ja takistused?

6. Millised täiendavad tegurid peale siseriiklike võisid Eesti toimetulekut ID-kaardi juhtumiga mõjutada? Millised tegurid olid kõige kriitilisema tähtsusega selles osas?

Täiendavad küsimused

1. Millised tegurid teie arvates mõjutavad üldiselt riigi küberjulgeoleku võimekust?

2. Kuidas mõjutab riigi väiksus riigi küberjulgeoleku võimekust? Millised võiksid olla sarnasused või erinevused suurte riikidega?

3. Kas väiksus loob küberjulgeoleku kontekstis ka mingeid eeliseid (milliseid)? Kui hästi on Eesti teie hinnangul neid eeliseid oma küberjulgeoleku võimekuse loomisel ära kasutanud?

4. Kas teie hinnangul mõjutab riigi väiksus tema küberjulgeoleku võimekust millegi poolest teistmoodi kui konventsionaalse julgeoleku võimekust? Milles need erinevused seisnevad?

Lisa 2. Intervjueeritud küberjulgeoleku eksperdid

Magistritöö raames läbiviidud intervjuud olid järgnevad:

1. Intervjuu A. Riigi Infosüsteemide Ameti juhtiveksper, oluline roll 2017. aasta ID-kaardi turvariski juhtumi lahendamise eestvedamises ning ametkondadevahelises kommunikatsioonis. Intervjuu viidi läbi 23.11.2018.

2. Intervjuu B. Riigi Infosüsteemide Ameti juhtiveksper, oluline roll 2017. aasta ID-kaardi turvariski juhtumi lahendamisel. Intervjuu viidi läbi 26.11.2018.

3. Intervjuu C. NATO Küberkaitsekoostöö Keskuse juhtiveksper, roll 2017. aasta ID-kaardi turvariski juhtumis oli seotud strateegilise kommunikatsiooni valdkonnaga. Intervjuu viidi läbi 26.11.2018.

4. Intervjuu D. TTÜ uurimisgrupi ekspert, roll oli 2017. aastal ID-kaardi turvariski tulemuste ekspertanalüüsi teostamises. Intervjuu viidi läbi 26.11.2018.

5. Intervjuu E. NATO Küberkaitsekoostöö Keskuse ekspert, roll 2017. aasta ID-kaardi turvariski juhtumis oli suhtlus Eesti välispartneritega (seos ka Eesti eesistumisega Euroopa liidus). Intervjuu viidi läbi 27.11.2018.

6. Intervjuu F. Kaitseväe juhtivteenistuja, roll valdkonnast ülevaate andmine kaitsevaldkonnas ja rahvusvahelisel tasandil. Intervjuu viidi läbi 29.11.2018.

7. Intervjuu G. Teadlane-krüptograaf, roll 2017. aasta ID-kaardi turvariski juhtumi lahendamisel. Intervjuu viidi läbi 11.12.2018.

8. Intervjuu H. Vabariigi Valitsuse meediavaldkonna ekspert, roll 2017. aasta ID-kaardi turvariski juhtumis oli seotud strateegilise kommunikatsiooni valdkonnaga. Intervjuu viidi läbi 10.12.2018 (kirjalikult).