Sisekaitseakadeemia
Sisejulgeoleku instituut

Viktor Kaljukivi

EESTI KÜBERJULGEOLEKU TAGAMINE LÄBI AVALIKU SEKTORI INFO- JA KOMMUNIKATSIOONITEHNOLOOGIA TARNEAHELA KONTROLLI

Magistritöö

Juhendaja:
Jaanika Puusalu, PhD

Kaasjuhendaja:
Andri Rebane, MA

Tallinn 2023

SISEKAITSEAKADEEMIA MAGISTRITÖÖ ANNOTATSIOON

Kolledž/instituut: Sisejulgeoleku instituut	Kaitsmise kuu ja aasta Juuni 2023
Töö pealkiri eesti keeles: Eesti küberjulgeoleku tagamine läbi avaliku sektori info- ja kommunikatsioonitehnoloogia tarneahela kontrolli.	
Töö pealkiri võõrkeeles: Ensuring Estonia's cyber security through control of the public sector ICT supply chain.	
Lühikokkuvõte: Magistritöö on kirjutatud eesti keeles, võõrkeelne kokkuvõte on tõlgitud inglise keelde. Töö maht koos lisadega on 95 lehekülge. Magistritöö eesmärk on hinnata riigi IKT valdkonna tarneahela usaldusväärsuse kontrollimise protsessi tõhusust ning teha ettepanekud selle täiendamiseks. Töö eesmärgi saavutamiseks püstitati neli uurimisülesannet, mille raames selgitati välja IKT tarneahela olemus ja ohud, kaardistati tarneahela kontrolli praktikad ning ekspertide seisukohad ja ettepanekud, ning analüüsiti teoreetilisi lähtekohti ja empiirilise uuringu tulemusi. Töö eesmärgi saavutamiseks ja uurimisülesannete täitmiseks kasutati uurimisstrateegiana juhtumiuuringut. Andmekogumismeetodina kasutati dokumendianalüüsi ja poolstruktureeritud intervjuusid, mille puhu kasutati eesmärgistatud valimit. Andmeanalüüsi teostamiseks kasutati programmi NVivo. Magistritöö tulemusena esitas autor ettepanekud Eesti avaliku sektori info-ja kommunikatsioonitehnoloogia tarneahela usaldusväärsuse tagamise protsessi loomiseks.	
Lisad: puuduvad	
Võtmesõnad: info- ja kommunikatsioonitehnoloogia, tarneahela juhtimine, küberjulgeolek, küberrünnakud, tarneahelarünnak.	
Võõrkeelsed võtmesõnad: information and communication technologies, supply chain management, cyber security, cyber attacks, supply chain attack.	
Säilitamise koht: Sisekaitseakadeemia raamatukogu	
Töö autor: Viktor Kaljukivi	
Olen koostanud lõputöö iseseisvalt. Kõik lõputöö koostamisel kasutatud teiste autorite tööd, seisukohad, kirjalikest allikatest ja mujal allikates saadud info on nõuetekohaselt viidatud. Olen nõus oma lõputöö avaldamisega elektroonilises keskkonnas.	
Allkiri: /allkirjastatud digitaalselt/	Kommentaar (soovi korral)
Vastab lõputöö nõuetele	
Juhendaja: Jaanika Puusalu	Allkiri: /allkirjastatud digitaalselt/
Kaasjuhendaja: Andri Rebane	Allkiri: /allkirjastatud digitaalselt/
Kaitsmisele lubatud	
Kolledži direktor/instituudi juhataja: Erkki Koort	Allkiri: /allkirjastatud digitaalselt/

SISUKORD

SISSEJUHATUS

Tänapäevases maailmas seavad digitaalsed tehnoloogiad ehk info- ja kommunikatsioonitehnoloogia (edaspidi IKT) ja selle komponendid, mida kasutatakse teabe kogumiseks, salvestamiseks, analüüsimiseks ning jagamiseks, uusi ootusi, nõudmisi ning väljakutseid kõigile kasutajatele: inimesetele, erasektori ettevõtetele, kes on samaaegselt nii IKT komponentide tootja kui ka kasutaja, ja avaliku sektori asutustele, kes on samaaegselt nii IKT komponentide tellijad, ostjad kui ka kasutaja. Tehnoloogia areng on väga kiire ning pidevalt võetakse kasutusele uusi tehnoloogiaid, sh lahendusi ja rakendusi nagu 5G, 6G, asjade internet, tehisintellekt (ingl *artificial intelligence - AI*), kvanttehnoloogia, mehitamata sõidukid ja palju muud. Samal ajal kasvab ühiskonna sõltuvus infotehnoloogia lahendustest. Hetkel on juba võimatu leida eluvaldkonda sh riigi pakutavaid teenuseid, mis ei oleks otseses või kaudses sõltuvuses IKT-st. Digitaalne tehnoloogia ja rakendused moodustavad konkreetsete eluvaldkondade ning laiemalt ühiskonna toimimiseks vajaliku taristu. COVID-19 kiirendas ühiskonna digiüleminekut veelgi ning samal ajal tõi välja olulised probleemid ja kitsaskohad küberturvalisuse tagamisel nt populaarsete rakenduste ja ebakvaliteetsete toodete turvanõrkused, võimalikud sisseehitatud tagauksed (Alawida, *et al*., 2022, pp. 8191–8196).

Eesti Vabariik on tehnoloogiliste lahenduste kasutuselevõtu valguses kinnistanud oma rahvusvahelist tuntust digiriigina tänu laialdaselt levinud digitaalsetele teenustele nagu X-tee, e-valimised, e- tervis ning digitaalse identiteedi ja paljude teiste avaliku sektori teenuste kaudu. Eesti Digiühiskond 2035 arengukava defineerib digiriiki kui „avalikus sektoris digitaalse tehnoloogia kasutamist avalike teenuste osutamiseks, avaliku halduse ja riigivalitsemise korraldamiseks“ (Majandus ja Kommunikatsiooniministeerium, 2021, lk 61). Digiriigi areng on pidev: koostatud arengukava üldeesmärgiks on muuta kiire internet kõigile Eesti elanikele kättesaadavamaks ning tagada, et Eesti küberruum oleks turvaline ja usaldusväärne (Majandus ja Kommunikatsiooniministeerium, 2021, lk 12). Kasutajate arvu suurendamisega suureneb ühiskonna sõltuvus tehnoloogiast ja selle kaudu pakutavatest teenustest veelgi. Riigi digitaalse taristu st riist- ja tarkvara toimimise ja usaldusväärsuse võtmekomponendiks on selle turvalisuse tagamine tehnoloogiste ja organisatoorsete meetmetega.

Digitaalsetel tehnoloogiatel on nüüdseks Eestis sedavõrd läbipõimunud roll mis tahes valdkonnas, et kõigi riskidega toimetulekut ei ole võimalik korraldada ühe planeerimisdokumendi kaudu. Küberturvalisuse põhimõtted ning selle kaasnevad tegevused nagu infoturbestandardite rakendamine on juba täna osaliselt integreeritud erinevatesse valdkondlikesse planeerimisprotsessidesse, kuid jätkusuutliku digitaalse keskkonna hoidmine ja arendamine eeldab lisaks küberohtude käsitlemisele valdkonda integreeritud teemana ka valdkondade ülest fokusseeritud koostööd, mille elluviimisse on kaasatud kõik asjassepuutuvad osapooled era- ja avalikust sektorist. Riigi toimimise seisukohalt on oluline hinnata riigihangetega seotud riske eesmärgiga välistada pakkujaid, teenuseid ja tooteid, mis võivad ohustada olulisi teenuseid (Vabariigi Valitsus, 2023, lk 11).

Sellest tulenevalt tuleb lisaks digiriigi jätkuarendamisele pöörata erilist tähelepanu loodud taristu ning avaliku- ja erasektori IKT-lahenduste kaitsmisele. Küberintsidendid, nimelt, võivad teoks saada ükskõik missuguse taristu osise ehk hangitud toote või teenuse tarneahela lüli nõrkust ära kasutades. Küberintsidendi mõju on aga tänapäeval suurem kui kunagi varem ja võib hõlmata (isiku)andmete kadu, ohtu inimeludele, teenuse kättesaadavust ning märkimisväärset rahalist kahju. Küberkuritegevuse, ühe levinuma küberintsidendi liigi kulud hõlmavad andmete kahjustamist ja hävitamist, varastatud raha, tootlikkuse kaotust, intellektuaalomandi vargust, isiku- ja finantsandmete vargust, omastamist, pettust, rünnakujärgset tavapärase äritegevuse häirimist, kohtuekspertiisi, häkitud andmete taastamist ja kustutamist. Seega on oluline digiriigi kübertuvalisuse tagamisel täiendavat tähelepanu pöörata kogu tarneahela turvalisuse tagamisele.

IKT tarneahel käesoleva magistritöö tähenduses on organisatsioonide, inimeste, tehnoloogia, tegevuste, informatsiooni ja ressursside süsteem, mis on vajalik, et toode või teenus jõuaks tootjalt kliendini (Demidov & Paoli, 2020, p. 1). Magistritöö on **aktuaalne**, sest IKT tarneahela julgeolek on muutunud aasta aastalt järjest olulisemaks ning tuleb täpsemalt uurida kuidas avaliku sektori asutustel on võimalik kontrollida tarneahela komponentide turvalisust. Magistritöö on oluline avaliku sektori asutustele ja elutähtsate teenuste osutajatele, kes peavad olema veendunud, et tarneahela komponendid on turvalised. IKT tarneahela turvalisuse tagamise vajaduse olulisusele pööratakse järjest enam tähelepanu nii Eestis (Vabariigi Valitsus, 2023, lk 11), Euroopa Liidus (Euroopa Komisjon, 2020, p. 1) kui ka NATOs (Valk, 2022, p. 90). Alates 2016. aastast Eestis läbiviidud avaliku arvamuse uuringud on näidanud, et küberturvalisuse osa on muutunud eestlaste jaoks järjest olulisemaks (Kont, 2023, lk 21).

Kõikides infosüsteemides, organisatsioonides ja protsessides tuleb arvestada küber- ja infoturbega, sest sellest sõltub Eesti ühiskonna turvalisus ja majandusedu. Tehnoloogia valikul peavad avaliku- ja erasektori asutused võtma arvesse julgeolekukeskkonda ja viimaseid tehnoloogilisi suundumusi (Eesti julgeolekupoliitika alused, 2023, lk 12). Küberturvalisuse üldise taseme tõstmine suurendab üldist julgeolekut ning ühiskonna jaoks kriitilise tähtsusega elutähtsate teenuste sujuvat ja katkematut toimimist. Samuti võib küberturvalisuse üldise taseme tõstmine aidata ennetada keskkonnaohte/-kahjusid, mis võivad kaasneda elutähtsate teenuste vastu suunatud rünnetega. Sellest tulenevalt algatas Euroopa Komisjon (edaspidi EK) Euroopa Parlamendi ja Nõukogu direktiivi, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, muudatuse. Muudatuse eesmärgiks on tõhustada Euroopa Liidu (edaspidi EL) liikmesriikide küberturvalisuse taset ning laiendada sektoreid, mis omavad EL riikide majandusele ja ühiskonna toimimisele olulist tähtsust (edaspidi NIS 2 direktiiv). Direktiivis rõhutatakse vajadusele tegeleda „tarneahelast ja tarnijasuhetest tulenevate küberturvalisuse riskidega“, sest seni ei ole tarnahelale pööranud piisaval määral tähelepanu (Euroopa Parlament, 2022, p. 43). Tarneahel koosneb paljudest komponentidest ning sisaldab mitmeid ohuvektoreid, mis tulenevad riist-ja tarkvarast ning selle haldusest sh tarneahelasse kaasatud alltöövõtjatest ning kõikide osapoolte personalist. Tarneahelale tähelepanu juhtimine on oluline, sest aitab vaadata ohte komplekssemalt. Teema aktuaalsust digiriigi vaates kinnitavad viimase viie aasta jooksul IKT tarneahelat tabanud küberrünnakud nagu NotPetya ja SolarWinds, mille tulemusel halvati teenuse toimimine. Seni suurim tarneahela rünnak nimega SolarWinds puudutas lausa 33 000 klienti üle maailma ning rünnaku raames said ründajad juurdepääsu konfidentsiaalsetele andmetele. Kusjuures 30% ohvritest ei olnud otseselt seotud ettevõtte SolarWinds pakutud teenustega (Willett, 2021, p. 8). Seega võib ühe tarneahela (kaudse) osise rünnak saada saatuslikuks kogu teenusele. Sellise situatsiooni vältimiseks on oluline tarneahela kontrolli tõhustamise uurimine.

Magistritöö on **uudne**, sest IKT tarneahela kontrollimise protsessi tervikuna ei ole Eestis varem uuritud. Varem on tarneahelat uuritud mõne konkreetse tehnoloogia kontekstis nagu „asjade internet“ (Singh, 2020, p. 20) ja tarneahela turvalisust militaar 5G võrkudes (Pernik, *et al.*, 2021). Pernik, *et al.* (2021) uuringus toodi välja, et 5G tarneahela riskide maandamiseks tuleb avaliku- ja erasektori asutustel teha tihedat koostööd ning vahetada informatsiooni riist- ja tarkvara turvanõrkuste ja personali taustakontrolli kohta. Samuti tuleb 5G võrkudes kasutada ainult usaldusväärseid partnereid. (Pernik, *et al.*, 2021, p. 33) Samu põhimõtteid tuleb rakendada kõikides avaliku sektori ja elutähtsate teenuste osutajate IKT tarneahelates, sest see

võimaldab muuta Eesti küberruumi turvalisemaks. Oluline on tagada, et IKT tarneahelas kasutatav riist-ja tarkvara oleks turvaline, partnerid usaldusväärsed ning kaasatud inimesed läbinud taustakontrolli.

Võttes aluseks pakutud IKT tarneahela definitsiooni, lähtub magistritöö vaatest, et tarneahel on usaldusväärne juhul, kui kõik tarneahelas osalevad komponendid st riist- ja tarkvara tootja, teenuste pakkujad ja nende alltöövõtjad ning kõikide osapoolte personal on usaldusväärsed. Sellest tulenevalt tuleb IKT tarneahela turvalisuse tagamisel hinnata ja maandata just nendest komponentidest tulenevaid riske. Eesti avaliku sektori süsteemide arendamiseks ja teenindamiseks on spetsiaalselt loodud riiklikud IKT asutused nagu Siseministeeriumi infotehnoloogia- ja arenduskeskus, Riigi Info- ja Kommunikatsioonitehnoloogia Keskus, Riigi Infosüsteemi Amet jt. Nende IKT asutuste arendusvõimekus on piiratud ning seetõttu ostetakse IKT tarneahela komponente (nt riist- ja tarkvara, tarkvara arendus, hooldus, haldus) sisse. See tähendab, et hankemenetluse planeerimisel ja läbiviimisel on oluline pöörata tähelepanu hankeprotsessis osalejatele ning vajadusel neid välistada. Magistritöö autor mõistab, et avaliku sektori asutusel ei ole võimalik kõiki tarneahela komponente 100% kontrollida. Vaatamata sellele tuleb aga astuda samme, et minimeerida tarneahelast tulenevaid riske. Eriti neid riske, mis võivad realiseeruda küberintsidendina nt küberründena, küberlekkena jne. Kontrollmehhanismi kehtestamine on autori hinnangul üks viis, kuidas riigi teenuste jätkusuutlikkuse tagamiseks tarneahela osiste usaldusväärsust kontrollida ning kontrolli läbi tarneahela usaldusväärsus tagada. See tähendab, et avaliku sektori asutustel ja elutähtsate teenuste osutajatel tuleb kontrollida tarneahela elemente veendumaks, et nad ei ohusta asutuste infosüsteeme, võrke ja nendes sisaldavaid andmeid. Magistritöö **uurimisprobleem** on püstitatud küsimusena „Kuidas tõhustada IKT valdkonna tarneahela kontroll Eesti avalikus sektoris?“. Sellest tulenevalt on püstitatud järgmised **uurimisküsimused**:

1. Millised on võimalikud riist-ja tarkvarast ning selle haldamisest, alltöövõtjatest ning ettevõtte ja avaliku sektori asutuse personalist tulenevad ohud riigi IKT tarneahelale?
2. Kuidas ja milliste kriteeriumite alusel oleks riigi IKT asutustel võimalik hinnata ja kontrollida kasutatava riist- ja tarkvara, riiklike ja riigi seisukohast oluliste infosüsteemide arendus- ja hooldusfirmade usaldusväärsust?
3. Kuidas ja millistel alustel oleks riigi IKT asutustel võimalik teostada usaldusväärsuse kontrolli alltöövõtjate ja nende personali üle?

4. Kuidas ja milliste kriteeriumite alusel oleks riigiasutustel ja nende valitsemisalas olevatel juriidilistel isikutel võimalik välistada riigihangetest ebausaldusväärseid pakkujaid?

Magistritöö **eesmärk** on hinnata riigi IKT valdkonna tarneahela usaldusväärsuse kontrollimise protsessi tõhusust ning teha ettepanekud selle täiendamiseks. Eesmärgi saavutamiseks ja uurimisküsimustele vastamiseks on püstitatud järgmised **uurimisülesanded**:

1. Teoreetilise kirjanduse analüüsi abil välja selgitada IKT tarneahela olemuse ja neid ohustavad aspektid.
2. Dokumendianalüüsi käigus kaardistada teiste riikide IKT tarneahela kontrolli ja usaldusvääruse hindamise parimad praktikad ning Eesti hetkeolukord.
3. Empiirilise uuringu (intervjuu) abil kaardistada Eesti avaliku- ja erasektori küber/IKT valdkonna ekspertide seiskohad ja ettepanekud tarneahela usaldusväärsuse hindamiseks.
4. Sünteesida teoreetiliste lähtekohtade ja empiirilise uuringu tulemusi ning töötada välja ettepanekud tarneahela kontrollimise protsessi loomiseks Eesti avaliku sektori IKT tarbeks.

Lähtudes pakutud IKT tarneahela definitsioonist tuvastas magistritöö tarneaheala neli nõrkust ehk võimalikku ründevektorit. Uurimisküsimustele vastamiseks ning uurimisülesannete täitmiseks analüüsib magistritöö tarneahela turvalisuse teemat neljast võimallikest ründevektorist lähtuvalt:

- **Riist- ja tarkvara**. Kuna Eesti avaliku sektori IT-majad kasutavad valmistoodetud või kohalike ja välisriigi IT-firmade käest tellitud tarkvara, kes omakorda võivad tellida arendusi kolmandalt osapoolelt, ei ole tarneahel läbipaistev ning riigil kui tellijal puudub kindel veendumus, et riist- ja tarkvara arendamisel on järgitud kõiki vajalikke küberjulgeoleku standardeid. Valdav osa avalikus sektoris kasutatavast riist- ja tarkvarast on sisse ostetav ning riigil puudub ülevaade selle tarneahelast alates tootmisest või arendusprotsessist kuni lõpptarbijani jõudmisest. Täiendavaks riskifaktoriks on tark- ja riistvara hooldus, mille raames on võimalik lõpptarbijat rünnata.
- **Haldus**. Tark- ja riistvara haldamiseks sõlmitud teenuslepingute raames antakse partneritele vajalikud juurdepääsud riigi IKT süsteemide erinevatele komponentidele, mida ebausaldusväärne partner võib kuritarvitada. Samuti võib lepinguline partner

ebapiisavalt panustada küberkaitsesse ja ega paranda turvanõrkusi: sellist olukorda saab küberrünnaku tegija kasutada ründevektorina riigiasutuse vastu. Eestis, kusjuures, on küberturvalisuse vastutus detsentraliseeritud ning iga infosüsteemi omanik ja elektroonilise teenuse pakkuja peab tagama oma süsteemide turvalisuse ja vastutama intsidendihalduse eest ennekõike ise.

- **Alltöövõtjad**. Erasektori panus e-riigi arengusse on märkimisväärne, mis tähendab, et partnereid on väga palju. Sellest tulenevalt tuleb tarneahela turvalisuse tagamiseks tellijal olla veendunud protsessidesse kaastatud tarnijate ja nende alltöövõtjate usaldusväärsuses.
- **Inimfaktor**. Viimane ründevektor on inimene, kes nii tahtmatu kui ka tahtliku tegevusega teenuse turvalist toimimist ohustada võib. Magistritöö raames analüüsitakse nii avaliku sektori asutuse kui ka koostööpartneri töötajast tulenevat potentsiaalset riski. Iga asutus peab olema veendunud, et inimene, kelle kätte usaldatakse juurdepääs andmetele ning äriprotsessidele, on usaldusväärne.

Magistritöö uurimisstrateegiaks on juhtumiuuring (ingl *case study*), mis autori hinnangul võimaldab saavutada magistritöö eesmärgi. Uurimisstrateegia aluseks on võetud (Stake, 1995, pp. 3–4) käsitlus, mille kohaselt tegemist on seesmise (ingl *intrinsic case*) juhtumi uuringuga. Töö raames on uuritavaks juhtumiks IKT valdkonna tarneahela usaldusväärsuse kontrollimise protsess. Uuringu raames kasutatakse kvalitatiivseid andmete kogumise meetodeid: dokumendianalüüs ja poolstruktureeritud ekspertintervjuusid. Dokumendianalüüs põhineb Eesti ja rahvusvahelistel õigusaktidel ning muudel strateegilistel ja valdkonnaga seotud dokumentidel, mis on avalikkusele kättesaadavad.

Poolstruktureeritud ekspertintervjuudesse oli kaasatud valdkonnaga seotud eksperdid ministeeriumitest, riigi IT-majadest ning erasektori asutustest, kelle teenused on elutähtsad IKT teenused, kriitilise infrastruktuuri ettevõtted või sõltuvad sellistest teenustest. Kokku intervjueeriti 6 eksperti.

Magistritöö koosneb kahest peatükist. Esimene peatükk käsitleb teemat teoreetilistele lähtekohtadele tuginedes. Avatakse tarneahela olemust, kirjeldatakse küberrünnaku teostamise protsessi ning tutvustatakse toimunud tarneahela rünnakuid. Teine peatükk tutvustab empiirilisi uuringuid: dokumendianalüüsi ja ekspertintervjuude tulemusi. Peatükis on kirjeldatud teiste riikide, organisatsioonide või ettevõtete poolt kasutuselevõetud või tulevikus rakendatavad

tarneahelakontrolli meetmed. Samuti on kirjeldatud hetkeolukord Eestis ning analüüsitakse ekspertintervjuudest saadud informatsiooni. Peatüki lõpus teeb autor ettepanekud võimaliku tarneahela kontrolli protsessi korraldamiseks koos vastutuse ja rollide jaotusega.

1.TARNEAHELAGA SEOTUD RISKID RIIGI JULGEOLEKULE

Käesolev peatükk tutvustab tarneahela ohtude teoreetilist käsitlust ning defineerib „usaldusväärsuse kontrolli“ mõistet magistritöö kontekstis. Esimene alapeatükk tutvustab, kuidas IKT tarneahelat saab Kopenhaageni koolkonna julgeolekuteooriale tuginedes vaadata kui üht julgeolekusektorit. Teises alapeatükis avatakse geopoliitilisi ohte, mis avaldavad mõju küberruumile läbi tarneahela ning tuuakse näiteid edukatest tarneahela rünnakutest. Kolmandas alapeatükis keskendutakse tarneahela olemuse avamisele, tutvustatakse võimalikke ohuvektoreid (riist- ja tarkvara, haldus, alltöövõtjad, inimene), mille kaudu on võimalik rünnakut teostada ning kirjeldatakse tarneaheala rünnaku elukaart. Neljandas alapeatükkis keskendutakse tarneahela usaldusväärsuse mõiste määratlemisele käesoleva magistritöö kontekstis.

1.1 Küberjulgeoleku valdkonna julgeolekustamise protsess Kopenhaageni koolkonna julgeolekuteooria kontekstis

Peale külma sõja lõppu hakati uurima sõjalise aspektidega mitte seotud julgeoleku probleeme. Selle tulemusena avaldasid 1998. aastal Barry Buzan, Ole Wæver ja Jaap de Wilde raamatu „Security: A new Framework of Analysis“, millest sai alguse Kopenhaageni koolkonna julgeolekustamise teooria. Traditsiooniline lähenemine julgeolekule fokusseeris eelkõige militaar ja poliitilistele aspektidele. Kopenhaageni koolkond haarab rohkem riigi julgeoleku seiskohalt olulisi ja julgeolekut mõjutavaid aspekte. Kopenhaageni koolkond eristab viis julgeolekusektorit: sõjaline, poliitiline, majanduslik, sotsiaalne ja keskkonnasektor. (Buzan, *et al.*, 1998, pp. 22–23). Buzan, Wæver ja de Wilde hinnangul muutub eksistentsiaalne oht referentsobjektile julgeolekuprobleemiks siis, kui julgeolekustaja käsitleb teemat ohuna ning auditoorium sellega nõustub. Järelikult julgeoleku mõiste ei ole iseenesest mõistetav, vaid ajas vastavalt ohtudele muutuv (Stritzel, 2007, pp. 359–361). Tavaliselt nimetatakse referentobjektiks riiki, kelle jaoks ellujäämine tähendab suveräänsuse säilitamist, kuid selleks võib olla ka rahvus, kelle eksistents on seotud identiteediga (Buzan, *et al.*, 1998, p. 36). Julgeolekustamise teooria põhikomponentideks on julgeolekustaja, auditoorium ja kõneakt, millel on keskne roll ning mis on suhtlusvahendiks kahe osapoole vahel (Täri, 2017, lk 17). Julgeolekustamise protsessi võib defineerida, kui julgeolekustaja kõneaktide kogumit, mis on suunatud laiemale auditooriumile eesmärgiga tutvustada kaitsmist vajavat objekti või

valdkonda kui uue julgeolekuprobleemina (Balzacq, 2011, p. 3). Siinkohal on oluline juhtida tähelepanu, et kõneakt ei ole ainult julgeolekustaja suuline kõne, vaid erinevate suhtlusvahendite kogum, mis võimaldab vahendada ja edastada mõtteid ja ideid auditooriumile. See tähendab, et kõneaktiks võib lugeda publikatsioone, strateegilisi dokumente nagu arengukavad ja tegevuskavad, seadusi ja muid normatiivakte.

Arvuti või võrkude kaitse ei ole eraldi komponentidena Kopenhaageni koolkonna järgi julgeoleku sektor. Aga kui vaadata riigi infosüsteemide ja võrkude kaitsmise vajadus ühe riigi julgeoleku valdkonnanna, siis kvalifitseerub küberturvalisus Kopenhaageni koolkonna julgeoleku sektoriks (Hansen & Nissenbaum, 2009, p. 1160). Samale järeldusele jõudis Kersti Oksaar (2014, lk 93), kes toob välja, et sellisel juhul on kübervaldkonna julgeolekustajate rollis riik, rahvusvahelised organisatsioonid ja korporatsioonid. Referentobjektiks võivad olla riik, ettevõtted, finantsinstitutsioonid, võrgud jne, mille eksistentsiaalseks ohuks on küberründed (kübersõda, -terrorism, -vandalism, -kuritegevus ja -spionaaž). (Oksaar, 2014, lk 28–32) Kuna efektiivne julgeolekustamise protsess peab olema auditooriumi keskne (Balzacq, 2005, p. 179) kuid auditooriumi mõiste ei ole selgelt defineeritud, siis Oksaar leidis, et auditooriumi saab jagada kolmeks grupiks: institutsionaalsed organid, avalikkus (avalik arvamus) ning tehnokraadid ja spetsialistid. Iga grupi pädevuses on volitada julgeolekustajat võitlema küberrünnetega (Oksaar, 2014, lk 35).

Sellest tulenevalt võib küberjulgeoleku olulisust riigi julgeolekule põhjendada läbi Kopenhaageni koolkonna julgeolekustamise teooria käsitluse. Eesti Vabariigi Põhiseaduse paragrahvi 2 esimene lause sätestab, et „Eesti riigi maa-ala, territoriaalveed ja õhuruum on lahutamatu ja jagamatu tervik.“ (Eesti Vabariigi põhiseadus, 1992). Riigil on õigus kaitsta ennast territoriaalse terviklikkuse rikkumise eest maal, merel ja õhus. Lisaks neile kolmele kaitsmist vajavale domeenile on alates 2007. aastast lisandunud veel üks oluline valdkond, milleks on küberturvalisus. Sellest hetkest hakati käsitlema küberjulgeolekut riigi julgeoleku osana. Küberturvalisuse komponendid ja nende haldamine koosneb protsessidest, kasutatavatest tehnoloogiatest ning protsessi kaasatud inimestest. Kuigi tehnoloogia ja protsessid ei ole kunagi 100% turvalised, siis täiendavate turvameetme ja reeglitega on võimalik tõsta turvalisuse taset ning vähendada riskitaset. Samas on kõige olulisemaks aspektiks inimesed, kes peavad reegleid järgima, sest tegelik turvalisus sõltub just meetmete rakendajast ehk lõppkasutajast. Hinnanguliselt 83% küberjulgeoleku intsidentidest on põhjustatud inimeste poolt (Kont, 2023, lk 4), üljäänud 17% intsidentidest on seotud tehniliste komponentidega nagu

riist-ja tarkvara ning küberrünnakutega nende vastu. See omakorda tähendab, et pahatahtliku ründaja jaoks on inimene peamine sihtmärk volitamata juurdepääsu saamiseks infosüsteemidele ja andmetele (Yeng, *et al.,* 2021, p. 472). Rünnaku objektiks võib sattuda iga inimene, kes osaleb tarneahelas, olgu see siis tellija või tarnija töötaja. Organisatsiooni infoturbekorraldamise perspektiivist võib pidada inimest kõige nõrgemaks lüliks. Inimese hooletu käitumine ja kehtestatud reeglite rikkumine võib lihtsustada rünnaku läbiviimist ning tõsta rünnaku edukust, sõltumata rakendatud infotehnoloogilistest ja organisatoorsetest meetmetest. Võimaliku rünnaku ennetamiseks või selleks, et muuta selle läbiviimist keerulisemaks, on oluline, et tarneahelas osalevate osapoolte personal oleks koolitatud, teadlik rakendatavatest meetmetest ja protsessidest ning neid täidetaks iga päev.

Küberjulgeolek tähendab hoiakute, käitumise, teadmiste ja teadlikkuse kombinatsiooni, mida organisatsiooni personal jäädvustab ja rakendab küberriskide ja -ohtude maandamiseks ning organisatsiooni teabe kaitsmiseks (Gioulekas, *et al*., 2022, p. 3). Eestis hakati laiemalt küberjulgeolekust rääkima alates 2007. aasta aprillist, kui pronksiöö ajal toimusid ulatuslikud küberrünnakud Eesti riigiasutuste ja Eestis tegutsevate ettevõtete vastu. Rünnakud kestsid kolm nädalat ning sellest sai esimene ulatuslik küberrünnak Euroopa riigi vastu. 2007. aasta aprilli sündmused näitasid, et küberründed on tõsine oht riigi julgeolekule ning tuleb võtta kasutusele meetmed riigi küberjulgeoleku tagamiseks. Rünnakud toimusid mitmes faasis: 27. aprillist kuni 29. aprillini ning 30. aprillist kuni 18. maini. DDoS-rünnaku teostamiseks rakendatud botnetid hõlmasid üle miljoni arvuti üle maailma (Tikk, *et al.,* 2010, p. 18). Juba järgmisel, 2008. aastal kehtestati küberjulgeoleku strateegia aastateks 2008–2013, millega defineeriti muuhulgas küberruumi, küberjulgeoleku ning küberkaitse mõisteid. Strateegia peamiseks eesmärgiks oli suurendada Eesti kriitilise infrastruktuuri ja sellega seotud teenuste vastupanuvõimet küberruumis olevatele ohtudele. See tähendab, et küberjulgeoleku julgeolekustamise protsess Eestis algas juba 2007. aastast.

Küberjulgeoleku julgeolekustamine jätkus ka rahvusvahelisel tasandil tehtud kõneaktide kaudu. Septembris 2014. aastal Walesis toimunud Põhja-Atlandi Lepingu Organisatsiooni (NATO) tippkohtumisel tõdeti, et küberründed muutuvad aina keerulisemaks ja ohtlikumaks ning võivad ohustada alliansi heaolu, turvalisust ja stabiilsust. Sellest tulenevalt tuleb tõhustada NATO võrkude ja infosüsteemide kaitset nende vastu. Kohtumisel võeti vastu deklaratsioon, milles kinnitati, et rahvusvaheline sõjaõigus rakendub ka kübermaailmas (Walesi tippkohtumise

deklaratsioon 2014, punktid 72–73). See näitab, et teoorias väljatoodud julgeolekustamise protsess toimus ka praktikas.

Kuni 2016. aastani eksisteerisid NATO tasandil kolm sõjalist domeeni: maismaa, õhk ja meri. Varssavis toimunud NATO tippkohtumisel otsustati lisada küberdomeen seni eksisteerinud sõjaliste domeenide hulka. Tippkohtumisel vastu võetud küberkaitselubaduse üheks punktiks (NATO, 2016, p. 5) oli tugevdada ja tõhustada riiklike võrkude ja infrastruktuuride küberkaitset. See tähendas, et iga liikmesriik peab välja töötama küberkaitse meetmed hübriid- ja küberohtude vastu. Samas kinnitati, et NATO riikidel on õigus aidata liikmeriiki, kes on sattunud küberrünnakute alla olukorras, kus Washingtoni lepingu artikkel 5 ei ole aktiveeritud. (Weitz, 2016, p. 10)

Toodud näidete puhul on hästi näha, kuidas küberjulgeoleku julgeolekustamine toimus NATO tasandil. NATO kui julgeolekustaja otsustas, et küberjulgeolek on oluline osa sõjalisest kaitsest (kõneakt) ning tegi otsused teatavaks kogu maailmale (auditooriumile). Siinjuures auditooriumiks võiks pidada NATOsse kuuluvaid riike, rahvusvahelisi organisatsioone ning NATOsse mitte kuuluvaid riike.

Sarnaselt toimus julgeolekustamise protsess Euroopa Liidu tasandil (Urciuoli, *et al.,* 2013, p. 52), mille raames Euroopa Komisjon ja Euroopa Parlament täitsid julgeolekustaja rolli läbi normatiivaktide. Alates 2013. aastast kehtis Euroopa Komisjoni määrus nr 526/2013 (küberturvalisuse määrus), mis asendati 2019. aastal (2019/881): määruse uues versioonis kutsuti muuhulgas üles tugevdama tarneahelaid (preambula punkt 4). Järgmise sammuna avaldas Euroopa Komisjon 2020. aasta detsembris uue ELi küberturvalisuse strateegia, mille eesmärgiks on suurendada ELi riikide suutlikkust ennetada tõsiseid küberintsidente ning tõsta riikide võimekust intsidentidele reageerimisel ja lahendamisel (Bendiek & Kettemann, 2021, p. 2).

IKT tarneahela turvalisuse tagamise vajadusele tähelepanu juhtimine tähendab, et küberjulgeoleku julgeolekustamise protsessi raames toimus eraldi IKT tarneaheahela julgeolekustamine. Järgmise sammu selles suunas tehti 2022. aastal, millal avalikustati Euroopa Liidu Nõukogu järeldused IKT tarneahela turvalisuse kohta. Dokumendis rõhutati vajadust hinnata digitaalvaldkonna tarneahelatest tulenevaid riske EL riikide julgeolekule ning rakendada meetmeid ebausaldusväärsete pakkujate välistamiseks riigihankementlustest

(Euroopa Liidu Nõukogu, 2022, pp. 7-8). Lisaks sellele tuuakse välja (Bendiek & Kettemann, 2021, p. 5), et rünnakuid IKT tarneahelatele võib kasutada relvana riikide või kriitilise taristu vastu. Eraldi mainitakse, et olukorra teevad keerulisemaks geopoliitilised pinged, mis tekivad muuhulgas seoses tehnoloogia üle kontrolli saamisega IKT tarneahelas poliitilistel ja ideoloogilistel eesmärkidel (Euroopa Komisjon, 2020, pp. 1-2).

Käesolevas alampeatükis analüüsiti küberturvalisust ja küberjulgeoleku valdkonna julgeolekustamise protsessi Kopenhaageni koolkonna julgeolekuteooria kontekstis. Kokkuvõttes võib tõdeda, et Kopenhaageni koolkond toob välja, et julgeoleku sektorid ei ole absoluutsed, vaid sõltuvad julgeolekustajast ehk otsustajate diskursuses/narratiivist. Teisisõnu midagi muutub julgeolekuprobleemiks diskursiivse poliitika kaudu. Küberjulgeolek on väga märkimisväärne näide, kuidas 2010-ndatel sai julgeolekustajate abil küberjulgeolekust oluline julgeoleku osa Eesti, NATO ja Euroopa Liidu liikmesriikidele ning seetõttu integreeriti küberjulgeoleku aspekte strateegiliste dokumentidesse. Küberjulgeoleku julgeolekustamise osaks sai IKT tarneaheala julgeolekustamine.

1.2 Geopoliitilised ohud tarneahela elementide usaldusväärsusele

Kübermaailma riskid tulenevad erinevatest ohuallikatest, mida klassifitseeritakse kas küberrünnaku teostaja (de Bruijne, *et al.*, 2017, p. 11) või motiivi alusel (Sailio, *et al*., 2020, pp. 7–22). Kusjuures mõlemas klassifikatsioonis on ohuallikana välja toodud riiklikud või riigi poolt rahastatud küberüksused, mis on hästi finantseeritud ja varustatud. Nende peamisteks eesmärkideks on digitaalne spionaaž ja teiste riikide avaliku sektori asutuste ning kriitilise infrastruktuuri vastu suunatud küberrünnakute läbiviimine.

Võib julgelt väita, et kõik riigid arendavad meetmeid ja üksusi enda riikliku IKT infrastruktuuri kaitsmiseks (Eestis täidavad sellist rolli Riigi Infosüsteemi Amet, Kaitseliidu Küberkaitse Üksus ja Kaitseväe Küberväejuhatus, kes tegelevad sõjalisteks eesmärkideks vajalike võrkude kaitsega), kuid vähestel riikidel on olemas võimekus küberrünnakute teostamiseks. NATO-sse mitte kuuluvatest riikidest on ekspertide hinnangul küberrünnakute läbiviimise võimekus olemas Venemaa Föderatsioonil (edaspidi *Venemaa*), Hiina Rahvavabariigil (edaspidi *Hiina*) ning Iraanil. (Klimburg, 2011, pp. 47–52)

Kaitsepolitsei hinnangul tulenevad Eestile suurimad küberjulgeolekuga seotud ohud Venemaast ja Hiinast (Kaitsepolitseamet, 2022, lk 26). Samal seisukohal on ka Välisluureamet (Välisluureamet, 2022, lk 19), kelle hinnangul on Venemaal suur kogemus küberoperatsioonide läbiviimisel (perioodil 2017–2021 on Venemaale omistatud 6 küberrünnakut) ning nad suunavad pidevalt ressursse küberrünnete võimekuse suurendamiseks. Venemaa kasutab küberdomeeni peamiselt kahe eesmärgi saavutamiseks. Esimene eesmärk on küberrünnakud kriitiliste infosüsteemide, teenuste ning taristu vastu, mille raames soovitakse varastada tundlikku informatsiooni või teha katkestusi kriitilise infrastruktuuri töös. Teine eesmärk on ühiskonna arvamusega manipuleerimine valeuudiste või informatsiooni moonutamisega, ehk informatsioonisõda, milles "/…/massimeedia, eriti televisioon ja ajakirjandus, mängivad palju olulisemat rolli kui kunagi varem" (Thomas, 2000, p. 338). Viimases aastaraamatus toob Kaitsepolitsei välja, et oht tuleneb ka Venemaa kodanikest, kes on tulnud Eestisse või muu Euroopa Liidu riiki elama ja töötama. Eelkõige puudutab see IT-sektorit, kuhu on tulnud palju Venemaa IT-spetsialiste. „On igati tõenäoline, et välismaal asuvaid Venemaa kodanikke püütakse kaasata Venemaa eriteenistuste luurelistesse tegevustesse" (Kaitsepolitseiamet, 2023, p. 23). Sellest tulevalt tuleb Eesti riigiasutustel ja elutähtsate teenuste osutajatel olla tähelepanelik ning veenduda, et asutuste arendusprotsessidesse Vene IT-spetsialistid ei ole kaasatud.

Venemaa käitumine kübermaailmas on selge ründava kallakuga (Shuya, 2018, pp. 4–6). Antud järeldust kinnitavad Venemaa poolt läbi viidud küberründed Eesti (2007), Gruusia (2008) ja Ukraina (2014 ja 2022) vastu. Gruusia vastu suunatud rünnakute sihtmärkideks valiti veebileheküljed, mille kaudu toimus infovahetus Gruusia valitsuse ja elanikkonna ning välispartnerite vahel nagu USA ja Suurbritannia saatkonnad Tbilisis. Lisaks sai rünnaku tõttu võimatuks elektrigeneraatorite rent, mis mõjutas elektrivarunduse tagamist riigis. Rünnakute raskendavaks ajaoluks oli see, et neid kasutati konventsionaalsete vägede toetuseks ehk sõjapidamiseks (Shakarian, 2011, p. 66).

Küberrünnakud Ukraina vastu algasid 2012. aastal ning kestsid kuni 2015. aasta detsembrini. Kui perioodi alguses rünnati enamasti veebilehti, siis märtsis 2015 tungisid Venemaa häkkerid Ukraina elektrivõrgu operaatori Kievoblenergo võrku. E-kirjas sisalduva pahavara abil õnnestus esmalt saada kontroll ühe töötaja arvuti üle. Rünnaku järgmises faasis saavutati kontroll elektrijaama juhtimissüsteemi üle, jäädes ise avastamata, mis võimaldas oodata sobivat aega rünnaku lõpule viimiseks. Detsembris algas rünnaku viimane faas, mille raames lülitati

välja elektrivarustuse tagamine ning vooluta jäi 225 000 klienti. Samuti oli elektriga varustamise taastamine raskendatud, sest süsteemi pääsuparoolid olid muudetud. (Shehod, 2016, pp. 3–7)

Lisaks sõjaliste operatsioonide toetamisele teostab Venemaa või Venemaa valitsuse poolt toetatavad häkkerite üksused küberrünnakuid, sealhulgas tarneahelaründed mittesõjaliste eesmärkide saavutamiseks nagu andmete vargus, spionaaž või teenuste toimimise katkestamine. Viimane suurim avastatud ja Venemaale omistatud tarneahela rünnak oli nn „SolarWinds“, mis mõjutas hinnanguliselt 33 000 sihtmärki. Nende sihtmärkide hulka kuulusid ka Ameerika Ühendriigi valitsusasutused ja suurettevõtted nagu Microsoft ja Cisco. Rünnak avastati 2020. aasta detsembris küberturvalisusega tegeleva Ameerika ettevõtte FireEye (alates 2022. aastast nimega Trellix) poolt, kes edastas informatsiooni võimaliku rünnaku kohta Ameerika Ühendriikide julgeolekuasutustele. Enda teenuste osutamisel kasutas FireEye firma SolarWind platvormi Orion, mis sattus küberrünnaku alla. Rünnaku uurimine veel käib, kuid tänaseks on teada, et rünnak algas aprillis 2019. aastal, millal pahalasel õnnestus pääseda ligi SolarWind infosüsteemile. Rünnaku esimene faas toimus platvormi testkeskkonnas, kus arendaja testis uusi tarkvaraversioone enne nende avalikustamist. Sama aasta novembriks oli pahavara sisaldav kood sisestatud Orioni tarkvara uude versiooni. Küberrünnaku tulemusena muudeti ja täiendati Orioni platvormi koodi selliselt, et tekkis tagauks, mille kaudu sai võimalikuks pääseda ligi platvormi kasutaja võrgule, tutvuda dokumentidega ja andmetega ning suurendada pääsuõigusi. 2020. aasta märtsis avaldas SolarWinds Orioni versiooniuuenduse ning võimaldas pahavara installida. Koos uuenduse paigaldamisega klientidele levis pahavara 33 000 SolarWinds kliendi vahel. (Raponi, *et al.*, pp. 8–10; Martinez & Duran, 2021, p. 542). Kuigi uurimine ei ole veel lõpuni jõudnud, on kogutud tõendusbaasi nagu logid, serverite ja koodi andmete alusel alust arvata, et rünnaku taga oli Venemaa sponsoreeritud häkkerrühmitus (Tran, 2021).

Kolm aastat enne SolarWinds rünnakust toimus ulatuslik tarneahelarünnak nimega NotPetya, mille viis läbi Kremli sponsoreeritud ühendus Energetic Bear (Eggrers, 2021, p. 883). NotPetya on pahavara, mis võimaldas rünnaku teostajale ligipääsu Microsoft Windows platvormi kasutatavatele arvutitele ning arvutite sisule. Seejärel krüpteeriti kogu arvuti sisu ja nõuti arvuti omanikult lunaraha failide dekrüpteerimiseks. Rünnak sai alguse Ukraina tarkvaraettevõtte Intellect Service loodud raamatupidamisetarkavara M.E.Doc kaudu. Ründaja sai M.E.Doc administraatori õigused ning lisas pahavara tarkvara sisse. Järgmise tarkvara uuendusega levis

pahavara M.E.Doc klientide seas, mille tulemusena nakatas arvuteid üle maailma finants, tervishoiu ning muudes sektorites (America's Cyber Defense Agency, 2018). Rünnaku ohvrite täpne arv ja rünnakuga seotud kahju on väga rakse välja tuua, kuid OECD (2020, p. 11) andmetel oli kahjumi suurus kondiitri-, toidu-, hoidmis- ning jookidega tegeleva ettevõtte Mondelez International 100 miljonit USA dollarit. Ravimifirma Merc&Co kahjumi suurus oli 1,3 miljardit USA dollarit. Logistikasektoris tegutsev A.P. Møller-Mærsk, kelle töö oli NotPetya tõttu halvatud, kaotas 300 miljonit USA dollarit, FedEx-i kahjum 400 miljonit USA dollarit, Prantsusmaa ettevõtte Saint-Gobain – 384 miljonit USA dollarit (Greenberg, 2018). Seega võib Greenbergi hinnangul NotPetya põhjustatud kogukahjum ulatuda 10 miljardini dollarini.

Lisaks neile kindlaks tehtud rünnakutele avaldas 2018. aasta märtsis Ameerika Ühendriikide Küberturvalisuse ja Infrastruktuuri kaitse agentuur teate (America's Cyber Defense Agency, 2018), milles hoiatas võimalikest Venemaa korraldatud tarneaheala rünnakutest USA valitsusasutuste, energeetika-, veervarustuse, tuuma-, lennunduse, - ja finantssektori ettevõtete vastu. Rünnakute sihtmärgiks olid väikesed ettevõtted, kes osutasid teenuseid ülalmainitud sektorites. Hoiatava teatega pakuti välja mitmeid tehnilisi soovitusi ja meetmeid, millega õnnesuts rünnakut takistada.

Venemaa valitsus saab väga hästi aru kübervaldkonnast tulenevatest võimalustest ja ohtudest. President Putin on kutsunud koostama plaani, et teha Venemaast IT-valdkonna ülemaailmseks liidriks, kuid samal ajal hoiatas, et Venemaa peab end küberterrorismiohu eest kaitsma. Plaani kohaselt tuleb Venemaal arendada uuenduslikke ettevõtteid ja asendada välismaised komponendid kodumaiste toodetega. (Blank, 2008, p. 503) Võttes arvesse, et Eesti on Venemaa naaberriik, on ta ohustatud Venemaa hübriidsõja poolt ning seega peab koos teiste Põhja-Euroopa riikidega rohkem panustama oma küberturvalisusesse (Gredzens, 2017, lk 21). Moskvas on hakatud rohkem tähelepanu pöörama Balti riikide mõjutamisele ja siseriiklikule lõhestamisele. Kasutades sisemisi ressursse, arendab Venemaa info- ja kübervõimekust, et destabiliseerida Eesti sisejulgeolekut ja olulisi riiklikke funktsioone. Et tõhusalt reageerida erinevatele küberrünnakutele, tuleb Eestil arendada kriisivõimekust. (Sazonov, *et al.,* 2020, lk 36)

Esitatud näidete põhjal võib kindlalt väita, et Venemaa kasutab tarneahela rünnakuid nii hübriidsõja vahendina, st konventsionaalse sõjapidamise toetamiseks, kui ka riikide

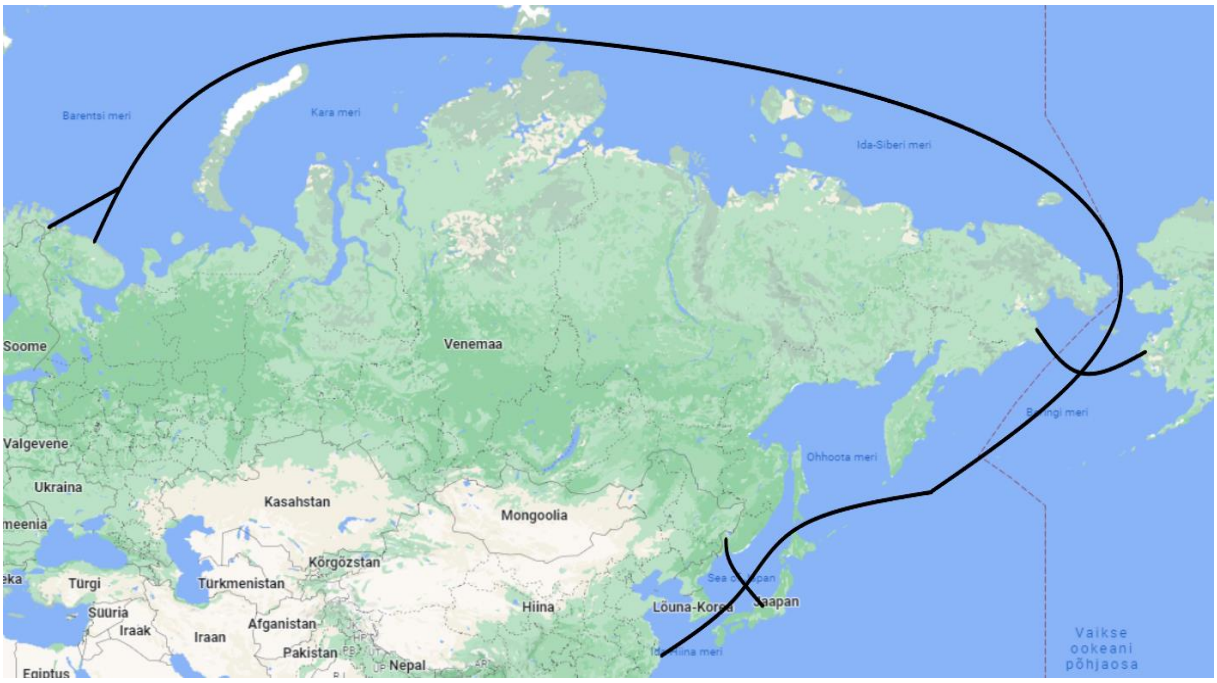
toimepidevuse ja elutähtsatse teenuste ründamiseks rahuajal. Lisaks sellele on kinnitatud, et Venemaa investeerib erasektori ettevõttetesse eesmärgiga võimaldada ettevõttetel laieneda välisturgudele ning pakutavate toodete või teenuste kaudu korjata luureandmeid. Juba 2017. aastal soovitasid nii Eesti Riigi Infosüsteemi Amet kui ka Leedu valitus mitte kasutada Venemaa tarkvarafirma Kaspersky tooteid nendes sisalduvate turvanõrkuste ja võimaliku seose tõttu Vene eriteenistustega. Järgmisel aastal avastas Leedu Küberkaitse Keskus Vene päritoluga taksofirma Yandex Taxi tarkvaras kriitilise nõrkuse, mis võimaldas koguda tundliku informatsiooni Leedu kodanike kohta ning edastada Venemaale (Zdanavičius, 2021, p. 257). Eesti toimepidevuse tagamiseks on oluline, et avaliku sektori asutuste ja elutähtsate teenuste osutajate IKT tarneahelad oleks usaldusväärsed kogu ahela vaates. Samuti võib väita, et lisaks rahuajale tõstab usaldusväärne IKT tarneahel küberturvalisust hübriid- ja konventsionaalse konflikti puhul.

Hiina tunneb samuti huvi Euroopa Liidu poliitika vastu ja Hiina tehnoloogia kasutamine mõjutab Euroopa Liidu sisejulgeoleku- ja justiitsvaldkondi (Wu, 2007, p. 169). Hiina mõjutustegevuse tagajärjed ei pruugi olla otsesed, vaid võvad mõjutada Eestit julgeolekut Euroopa Liidu tasandil tehtud otsuste kaudu. Et paremini kaitsta Hiina mõjutustegevuse eest, tuleb kohalikul tasandil teadvustada Hiinast tulenevaid riske. Näiteks majandusriskid, välisinvesteeringute ja ettevõtluse usaldusväärsus, hübriidkonfliktid ja küberohud, tehnoloogiaga seonduvad nüansid (sh Huawei seadmete kasutamine luure-eesmärkidel) ning Hiina otsuste mõju Eesti poliitilistele ringkondadele. (Koort ja Piip, 2021, pp. 4–8)

Hiina rakendab IKT võimekusi mitte ainult küberrünnakute teostamiseks teiste riikide vastu, vaid ka oma elanikkonna totaalseks jälgimiseks ning kontrolli all hoidmiseks. 5G ja 6G tehnoloogia levik koos riikliku näotuvastuse süsteemi rakendamisega võimaldab Hiina ametiasutustel tuvastada oma kodanikke tänavatel ning koguda informatsiooni iga isiku kohta. Totaalset jälgimist lihtsustab asjaolu, et kohalikud tehnoloogiatootjad koos teenindusettevõtetega on seotud riigi struktuuridega või kuuluvad kaudselt riigiaparaadile. (Läänemets, 2021) Siinkohal on oluline märkida, et Hiina on üks suurimaid tehnoloogia eksportijaid maailmas, pakkudes tehnilisi lahendusi teistele ettevõtetele ja riigiasutustele. Hiina riiklik teadus- ja infotehnoloogia programm näeb ette vajaduse suurendada investeeringuid tehnoloogiaga seotud teadus- ja arendustegevusse. Goldman (2020, pp. 269–273) leiab, et Hiinal on plaan ühendada suur osa elanikkonnast virtuaalseks impeeriumiks, kus domineerivad telekommunikatsioon, tootmine ja logistika. Hiina videovalve seadmed on kvaliteetsed, odavad

ning seetõttu laialdaselt kasutatavad, mis on tekitanud tõsiseid küsimusi seoses riikliku julgeolekuga. Selle valdkonna liidrid on Hickvision ja Dahua Technology, kes on vastavalt esimesel ja teisel kohal maailmas (Kaska, *et al*., 2019, p. 9). Kuna seadmete tootja on kohustatud tegema julgeolekuasutustega koostööd koduriigis, siis on põhjendatud kahtlus, et välismaal kogutud andmed võivad samuti olla edastatud Hiinale. Leedu Riikliku Küberkaitse Keskuse 2020. aastal avaldatud raportis tõdeti, et Leedu valitsusasutustes kasutatud Hiina ettevõte Hikvision ja Dahua Technology kaamerate tarkvaras on avastatud turvanõrkused, mida võib kasutada pahavara installeerimiseks ning küberrünnakute läbiviimiseks. (Zdanavičius, 2021 p. 269–270) Norras soovitati mitte investeerida Hikvisioni aktsiatesse, kuid põhjenduseks oli eetilised probleemid, sest firma tehnikat kasutatakse uiguuride koonduslaagrites. Mõlema firma tooteid on Ameerika Ühendriikide valitsus keelanud kasutada avaliku sektori objektidel alates 2018. aastast, kuid Eestis ei ole nende firmade tooted keelatud, ning mõlemad firmad osalesid 2021. aastal Politsei-ja Piirivalveameti väljakuulutatud hankes. (Salu, 2023)

Juba 2015. aastal nägi Hiina strateegia ette „informatsiooni Siiditee“ loomist ning Hiina tegi ettepaneku rajada piiriülese ja mandrite vahelise optiliste kaablite ühenduse. Soome oli projektist huvitatud ning samal aastal tellis uuringu, mis pidi hindama veealuse kaabli rajamisele esitatavaid nõudeid ja selle ehitamisega kaasnevaid mõjud, nn Artcic Connect projekt. Arctic Connect näeb ette Euroopa ja Aasia ühendamise Kirdeväila veealuste sidekaablite kaudu (Joonis 1.), mille rajab Hiina IKT ettevõtte Huawei Marine. Sellisel juhul avaneks Hiinal võimalus suurendada oma luureinfo kogumise võimekust ilma eriotstarbeliste veealuste luureoperatsioonide vajaduseta, kuna veealuste kaablite tehnoloogia pärineb Hiina ettevõttelt. (Jüris, 2020, pp. 146–150)



Joonis 1. Artic Connect ühenduse geograafiline paigutus (autori koostatud. Allikaks Jüris, 2020, lk 149).

Täiendavad Arctic Connect projektiga seotud riskid toodi välja 2019. aastal avaldatud Jyväskylä ülikooli raportis. Raporti kohaselt võib veealusest kaablist, kaabliga seotud rajatistest ja süsteemidest koguda luureandmeid näiteks pealtkuulamise, süsteemide häkkimise teel või pahavara süsteemi sisse imbudes. (Lehto, *et al*, 2019, pp. 13–22) Arctic Connect on hea näide, kuidas uue ühenduse loomisega kaasnevad suurendatud turvariskid. Hiina tehnoloogial põhinev merealuse ühenduse abil paraneb Hiina luureandmete kogumise ning küberkaitse võimekus. Lisaks võimaldaks Arctic Connecti ehitamine rakendada Hiinal veealust seirevõimet Põhja-Jäämerel vastase allveelaevade akustiliseks tuvastamiseks. (Jüris, 2021, p. 131)

Kui Lääs käsitleb Internetti ja sellega seotud tehnoloogiaid eelkõige tehnoloogilise keskkonnana, siis Hiina jaoks on Internet ennekõike kui inforuum, mida tuleb kaitsta riigi nõrgestamise ning riigi huvide kahjustamise eest. Sellest tulenevalt tuleb antud valdkond hoida riigi range kontrolli all. (Kaska ja Tolppa, 2020, lk 1) Hiina valitsus lähtub seisukohast, et strateegia ning tehnoloogia arenguga seotud eesmärgid peavad tulema riigi poolt ning ettevõttetel, kes viivad strateegiaid ellu, tuleb käituda vastavalt valitsuselt saabunud juhistele (Raud, 2016, p. 12). USA majandusajakirja Fortune andmetel kuuluvad 124-st suuremast Hiina ettevõttest 58 riigile, mille hulgas on ka infotehnoloogia sektori firmad. Kusjuures Fortune hindas ainult suurimaid ettevõtteid. Seega on Hiinas riigi omandis, riigi otsese- või kaudse

kontrolli all olevate ettevõttete arv suurem. Hiina näib aga keskenduvat rohkem küberspionaažile kui küberrünnakute läbiviimisele ning eelistab panustada pigem kommertsvõrkudele kui sõjatehnoloogiale. Hiina strateegia fookuseks on küberruumi asümmeetrilise eelise saavutamine tehnoloogilise innovatsiooni kaudu. Hiina tehnoloogiaettevõtted nagu ZTE ja Huawei, kasutavad oma seadmetes pahatahtlikku koodi, mille abil kogutakse teiste riikide ja inimeste andmeid, kuigi mõlemad ettevõtted eitavad süüdistusi. Hiina IKT suurfirmad Huawei ja ZTE pakkuvad oma riist-ja tarkvara ning ka muidu teenused (koolitused, platvormid) Hiina kaitseväele ja muudele valitsusasutele. Mõlemad firmad saavad otsefinantseerimist riigi poolt nende teadus- ja arendusprojektidele (Krekel, 2009, p. 49). Täna on Huawei ainus ettevõtte, kes suudab toota kõiki 5G võrgu komponente ning pakkuda neid konkurentidest madalama hinnaga. ZTE on üks maailma juhtivaid võrguseadmete pakkujaid. Selle peamised tooted on tuumik- ja transpordivõrgu komponendid, traadita ja püsijuurdepääsu võrgud, pilvandmetöötlus ja IKT lahendused energeetika sektorile. Sarnaselt Huaweiga on ZTE osaliselt Hiina riigi omanduses ja kontrolli all. (Kaska, *et al*, 2019, pp. 7–9). Mõlemat ettevõtet süüdistati küberspionaažis, nii 2018. aastal sai teatavaks (Reichert, 2018), et Huawei töötajad aitasid Hiina luureasutusel saada juurdepääsu teise asutuse võrgule. Järgmisel, 2019. aastal, esitas Poola spionaaži süüdistused kahele Huawei töötajale. Süüdistuste tõttu on mitmed riigid (nt Tšehhi) soovitanud vältida nende toodete kasutamist riiklikes ja julgeoleku seisukohast olulistes võrkudes (Pomfret ja Koper, 2019).

Hiinal on pikaajaline kogemus küberspionaaži operatsioonide teostamises. USA Justiitsministeeriumi andmetel on perioodil 2011–2018 90% majandusspionaaži juhtumitest teostatud Hiina poolt rahastatud küberrühmituste poolt (Kaska, *et al.*, 2019, p. 11). Täna on teada vähemalt 29 Hiina ametiasutustega seotud küberrühmitust, kelle ründeesmärkideks on teiste riikide valitsussektori asutused, finantssektor, teadusasutused, (sõja)tööstusettevõtted, lennundus, intellektuaalomand jne ([*Anon.*], 2023). Hiina küberspionaaž on muutunud probleemiks, mida sageli tõstatavad Euroopa riiklikud luure- ja küberjulgeolekuagentuurid oma avalikes hinnangutes (Kaska, *et al.*, 2019, p. 11). Küberspionaaži eesmärk on koguda teavet, püüdes samal ajal teisi riike mitte provotseerida. Hiina kasutab teabe kogumiseks kõiki olemasolevaod ressursse, olgu see Hiina päritolu teadlaste või välismaal elavate spetsialistide ja tudengite värbamine. (Pilichos, 2017, pp. 48–56) Nii sai 2021. aastal avalikuks, et Eesti ülikooli teadlane töötas Hiina sõjaväeluure heaks. (Koort ja Piip, 2021, lk 6)

Hiina sõjaline doktriin sätestab, et kübersõda on revolutsiooniline areng sõjapidamises ning peab olema odav, kaugeleulatuv ning efektiivne viis vaenlase ründamiseks (Lindsay, 2015, pp. 22–23) Vaatamata asjaolule, et Hiinal on olemas küberründe võimekus, kasutab Hiina küberdomeeni valdavalt küberspionaaži teostamiseks. See on IKT tarneahela turvalisusele sama ohtlik, sest Hiina seadmete ja tarkvara paigaldamine avaliku sektori ja elutähtsate teenuste osutajate võrkudesse võimaldab Hiina eriteenistustel pääseda võrkudele ja andmetele ligi. Lisaks eespool mainitule kohustab Hiina õigusraamistik (ingl *National Intelligence Law of the PRC 2017*) kodanikke ja ettevõtteid tegema koostööd luure- ja julgeolekuasutustega (Hoffman, 2018). Kusjuures termin „koostöö“ ei ole selgelt defineeritud ning võib tähendada klientide kohta informatsiooni edastamisest kuni koodi „tagaukse“ lisamiseni. Selle tagajärjeks on Hiina ametiasutustel juurdepääs miljonite inimeste andmetele üle maailma ja teiste riikide asutuste andmetele või ärisaladusele.

1.3 Tarneahela turvalisus

Magistritöö autor on otsustanud võtta fookusesse IKT tarneahela ründeid, kuna viimase viie aasta lõikes on toimunud mitmed suured tarneahela ründed, mis on avaldanud suurt mõju riikide majandusele ja julgeolekule. Lisaks sellele on 2019. aastal tarneahela kontrolli olulisus tõusetunud seoses uute tehnoloogiate kasutuselevõtuga. Näiteks 5G tehnoloogia turule toomisel tõdeti, et kuna 5G on oluline riigi julgeoleku tagamiseks, siis kasutatavad tooted peavad olema usaldusväärsed. Võrgu turvalisus peab olema tagatud selle loomisel, haldamisel ning tark- ja riistvara komponentide uuendamisel (Shafique, *et al.*, 2020, p. 4). Selle olulisust kinnitab Ameerika Ühendriikide ja Eesti vahel 2019. aasta novembris sõlmitud vastastikuse mõistmise memorandum 5G turvalisuse teemal. Memorandumi kohaselt on võrgu turvalisuse kindla ja tervikliku lähenemisviisi oluliseks osaks komponentide ja tarkvara pakkujate hoolikas ja täielik hindamine. Tarnijate ja nende pakutavate teenuste hindamine on oluline osa tarneahela julgeoleku tagamisel. Enne tarnijaga lepingu sõlmimist tuleb eelnevalt paika pandud kriteeriumite alusel hinnata võimalikke kaasneda võivaid riske (Matney & Fannin, 2014).

Küberdomeeni riske saab jagada neljaks kategooriaks: inimeste käitumisest tulenevad riskid, süsteemide ja tehnoloogiaga seotud riskid, puudulikest sisemistest protsessidest tulenevad riskid ning välistest mõjuritest tingitud riskid (detailne kirjeldus toodud tabelis 1). Esimeses kategoorias on kõik riskid, mis on otseselt seotud indiviidi käitumisega nagu tahtmatu eksimus reeglite vastu, puudulik koolitus ning ettekavatsetud pahatahtlik tegu (infosüsteemi pahavaraga

nakatamine, süsteemi nõrkuste ärakasutamine, andmete vargus või võltsimine). Tehnoloogia riskid tulenevad süsteemide valekonfiguratsioonist, turvameetmete mitte rakendamisest, puudulikust testimisest ning mitte sobiva või ebaturvalise riist- ja tarkvaravara kasutamisest. Sisemiste protsesside puudumine, puudulik monitooring ning kontroll personali ja hangete üle viib sisemiste riskide realiseerumiseni. Väliste riskide seas on näiteks puudulik õigusraamistik, tarnijaga seotud probleemid ning sõltuvus kolmandatest osapooltest, sh tarnijatest. (Biener, *et al.*, 2015, pp. 4–5).

Tabel 1. Küberdomeeni riskide jaotus (Biener, *et al.*, 2015, pp. 4–5)

Kategooria	**Kirjeldus**	**Elemendid**
1. Inimese käitumine 1.1 Tahtmatu 1.2 Tahtlik 1.3 Tegevusetus	1.1 Tahtmatud toimingud ilma pahatahtliku või kahjuliku kavatsuseta. 1.2 Tahtlikud ja ette kavatsetud toimingud eesmärgiga tekitada kahju. 1.3 Tegevusetus või suutmatus tegutseda konkreetses olukorras.	1.1 Vead, tegematajätmised. 1.2 Pettus, sabotaaž, vargus, vandalism. 1.3 Personali puudulikud oskused ja teadmised ning juhendmaterjalide puudumine.
2 Infosüsteemide ja tehnoloogia rikked 2.1 Riistvara 2.2 Tarkvara 2.3 Infosüsteemid	2.1 Füüsiliste komponentide riknemisega seotud riskid. 2.2 Riskid, mis tulenevad tarkvaravarast, programmidest, rakendustest. 2.3 Tõrked infosüsteemide töös.	2.1 Võimsuse ja jõudluse kadu, puudulik hooldus, riistvara on vananenud. 2.2 Ühilduvus, konfiguratsioonihaldus, muudatuste juhtimine, valed/puudulikud turvaseaded, koodivead, puudulik testimine. 2.3 Disain, spetsifikatsioonid, integratsioon ja keeruline arhitektuur.
3 Ebaõnnestunud sisemised protsessid 3.1 Puudulik kavandamine ja/või teostamine 3.2 Kontroll protsesside üle 3.3 Toetavad protsessid	3.1 Halb protsesside kavandamine või teostamine. 3.2 Puudulik kontroll protsesside üle. 3.3 Puudulikud toetavad protsessid. Vajalikud ressursid puuduvad.	3.1 Protsessi voog, dokumentatsioon, rollid, kohustused, hoiatused, informatsioonivahetus. 3.2 Staatuse jälgimine, mõõdikud, perioodiline ülevaatus, omaniku roll. 3.3 Vajalik personal, taustakontroll, raamatupidamine, koolitus ja arendus ning hanked.
4 Välised mõjurid 4.1 Katastroofid 4.2 Õigusraamistik 4.3 Äriprobleemid	4.1 Looduslikud ja inimlikud sündmused, mille üle organisatsioonil puudub kontroll ja mis võivad juhtuda ette teatamata.	4.1 Uputus, tulekahju, maavärin jne. 4.2 Eeskirjade järgimine, õigusaktid ja kohtuvaidlused.

4.4 Teenuste sõltuvused	4.2 Õigusraamistikust tulenevad riskid. 4.3 Ärimaastiku muutusega seotud riskid; 4.4 Riskid, mis tulenevad organisatsiooni sõltuvusest välistest osapooltest.	4.3 Probleemid tarnijaga, muutunud turutingimused ja majandustingimused. 4.4 Kommunaalteenused, hädaabiteenused, kütus ja transport.

Tabelis 1 nimetatud kategooriad katavad kõik küberturvalisusega seotud riskid, kuid selles toodud elemendid ei ole ammendavad, vaid annavad ainult indikatsiooni. Sellest tulenevalt võib elementide 4.2 „eeskirjade järgimine, õigusaktid ja kohtuvaidlused“ ja 4.3 „probleemid tarnijaga, muutunud turutingimused ja majandustingimused“ koosmõju tõlgendada nii, et risk tuleneb sellest, et välisriigist pärit tarnija allub eelkõige koduriigi õigusele, mis võib olla vastuolus tellija õigusega. Näiteks Hiina ja Venemaa, kus seadused kohustavad teha koostööd eriteenistustega. Magistritöö autori IKT tarneahela usaldusväärsuse hindamiseks valitud ründevektorid „inimfaktor“, „riist- ja tarkvara“, „haldus“ ja „alltöövõtja“, mis on tutvustatud sissejuhatuses (käesolev töö lk 8-9) kattuvad peaaegu täielikult Bieneri toodud küberdomeeni riskide jaotusega (tabel 2. lk 25).

Tabel 2. Riskide jaotuse kattuvus magistritöö fookuses olevate ründevektoritega (autori koostatud)

Riskikategooria	**Ründevektor**
1. Inimese käitumine	Inimfaktor
2. Infosüsteemide ja tehnoloogia rikked	Riist- ja tarkvara
3. Ebaõnnestunud sisemised protsessid	Haldus/Alltöövõtja/Inimfaktor
4. Välised mõjurid	Haldus/Alltöövõtja/Riist-ja tarkvara (tabel 1, elemendid 4.2 ja 4.3)

Selguse mõttes tuleb mainida, et antud töös on mõned Bieneri tabelis olevad elemendid nagu uputus ja tulekahju jäänud katmata, aga kuna nad ei soodusta IKT tarneahela (küber)rünnaku läbiviimist, siis autor otsustas neid skoopi mitte lisada.

Tarneahela riskide hindamisel peab pöörama erilist tähelepanu sellele, kas tarnija on oma tegudes iseseisev või on sõltuv teise riigi valitsusasutustest. Sõltuvus võib olla otsene ehk

valitsusasutus on ettevõtte omanik või osanik. Kaudse sõltuvuse puhul on valitsusasutusel olemas regulatiivsed meetmed ettevõtte otsuste ja toimingute mõjutamiseks. Sõltuvuse riski realiseerumisel võib teise riigi valitsus anda ettevõttele korralduse küberrünnaku korraldamiseks või rünnaku korraldamise abistamiseks pahavara installimise teel (Pilichos, 2017, p. 64).

Tarneahela juhtimine on strateegiline viis tarneahela vahendajate ühendamiseks, organiseerides nad teabe, materjalide ja ressursside vahetamise kaudu operatsiooni teostamiseks. (Singh, 2020, p. 6) Traditsioonilises tähenduses on tarneahel organisatsioonide, inimeste, tehnoloogia, tegevuste, informatsiooni ja ressursside süsteem, mis on vajalik, et toode või teenus jõuaks tootjalt kliendini (Demidov & Persi Paoli, 2020, p. 1). IKT valdkonnas on oluline, et tarnitav lahendus ja selle komponendid oleksid turvalised. Küberturvalisuse puhul hõlmab tarneahel suurt hulka ressursse (riist- ja tarkvara), salvestusruumi (avalik pilv või kohalik salvestuspind), jaotusmehhanisme (veebirakendused, veebipoed) ja haldustarkvara (European Union Agency for Cybersecurity, 2021, p. 7). IKT tarneahela rünnakul puhul on tegemist tahtliku pahatahtliku toiminguga (nt andmete sisestamine, asendamine või muutmine), mis tehakse IKT (riistvara, tarkvara, püsivara) haavatavuse loomiseks ja lõpuks ärakasutamiseks tarneahela mis tahes punktis, mille peamine eesmärk on teenuste toimimise häirimine või andmete vargus (Heinbockel, *et al.,* 2017, pp. 9–10) .

Tarneahelatest tulenevate küberjulgeolekuriskide juhtimiseks peavad organisatsioonid mõistma oma tarneahelaid, sealhulgas mitut alltarnijate kihti (Urciuoli, 2015, pp. 13-15). Tänapäeva tarneahelad on väga laiad ning nendesse on kaasatud palju ettevõtteid ja organisatsioone üle maailma. Näiteks 2019. aastal esitatud aruannetest on näha, et Apple tarneahel koosneb vähemalt 200 koostööpartneritest, Samsungi üle 2000, Google teeb koostööd rohkem kui 500 ettevõttetega 60-st riigist, Huawei tarneahelasse on kaasatud ca 1200 tarnijat ning IMB tegi koostööd 13 000 partneritega 100-st riigist. Siia lisanduvad edasimüüjad, haldus- ja hooldus ettevõtted, mis tähendab, et tarneahealaga seotud riskide maandamine on keeruline protsess. Selline olukord toob kaasa hulgalisi riske, mis võivad tuleneda riist- ja tarkvara hankijatest ja nende allhankijatest, riist- ja tarkvara komponentide tootjatest, tarneahela protsessidest ja nendesse kaasatud inimestest (McDaniel, 2013, pp. 315–316).

Küberjulgeolekuriskid on seotud kogu tarneahelaga ning võivad tuleneda kõikidest tarneahelasse kaasatud tarnijatest, nende tarneahelatest, nende toodetest või teenustest. Ohud

võivad olla seotud ahelas kasutatud toodetega ja teenustega või tarneahela enda nõrkuste ärakasutamisega. Näiteks pahavaraga nakatunud toodete kasutamine allhankija poolt või tarnija andmebaasi kompromiteerimine, mille tulemusena tagatakse ligipääs selleks volitamata isikutele või organisatsioonidele. (Boyens, *et al.*, 2022, pp. 20–22) Kusjuures riskid säilivad alates riist- ja tarkvara paigaldamisest kuni selle elukaare lõpuni. Rahvusvahelise tarneahela suureks plussiks on toote või teenuse lühendanud turule jõudmise aeg, tarnekiirus, komponentide mitmekesisus ning nende kättesaadavus. Miinuseks on teiste riikide tarneahelasse sekkumise ja tarneahela komponentide spionaažiks kasutamise oht. Selline oht tuleneb eelkõige Hiinast, Venemaalt, Iraanist ja Põhja-Koreast (Eggers, 2021, p. 881).

Tarneahela rünnakud ei ole uus nähtus, kuid erilist tähelepanu nendele pöörati peale 27.06.2017 toimunud laiaulatusliku tarneahela rünnaku nimega „NotPetya“, mille kahju ulatus 10 miljardini dollarini. Pärast rünnet juhtis Microsoft tähelepanu tarneahela rünnete probleemile ning prognoosis tarneahela rünnete kasvu. Isegi kui organisatsioon rakendab piisavalt meetmeid küberrünnete vastu, on tarneahela rünnakuid raske avastada, sest neid võib rünnata äripartneri kaudu. Rünnates tarneahela ühte ohvrit või tema pakutavat teenust, on ründajal võimalik minna mööda tarneahelast ning kompromiteerida mitu ahela osapoolt. (Arnek, 2021, p. 27).

Edukas küberrünnak koosneb seitsmest etapist (Villalón-Huerta, *et al.*, 2022, pp. 4–5):

1. Ettevalmistus/luure – selle raames kogutakse võimalikult palju informatsiooni ohvri kohta ning otsitakse nõrkusi, mida on potentsiaalselt võimalik ära kasutada. Näiteks uuritakse, millist riist- ja tarkvara ohver kasutab, mis on nende versioonid, kas ja milline viirusetõrje programm on kasutusele võetud.
2. Sobiva ründevektori/lahenduse ehk n-ö „küberrelva“ valimine – tavaliselt on tegemist pahavaraga, koodiga või muu riist- või tarkvarakomponentiga, mis võimaldab ettevalmistuse etapis avastatud nõrkuse ärakasutamist.
3. Tarne/paigaldus – pahavara sisaldava faili paigaldamine ohvri arvutisse või infosüsteemi.
4. Ärakasutamine – luuakse kanal pahavara installeerimiseks.
5. Pahavara installeerimine – paigaldatud pahavara kaudu tagatakse juurdepääs ohvri arvutile või infosüsteemile.
6. Kontrolli saavutamine – selle etapi raames installeeritud pahavara abil saavutatakse kontroll ohvri arvuti või infosüsteemi üle (nt ründajal on administraatori õigused) ning loodud eeldused rünnaku edasilevimiseks/eskaleerimiseks.

7. Eesmärgi saavutamine – saavutatav efekt sõltub rünnaku eesmärgist ning võib olla andmete vargus, andmebaasi krüpteerimine, töö- või teenuseprotsessi seiskamine, selle üle võtmine jne. Samuti on võimalik planeerida ja teostada edasirünnakuid ründaja samas võrgus kõikide seadmete vastu (korporatiivvõrk, koduseadmed jne).

Tarneahela rünnaku puhul võib protsess olla järgmine. Ettevõtte kasutab legaalset tarkvara, mis on tarnitud usaldusväärse tarnija poolt. Luurefaasis saab ründaja informatsiooni kastutatavatest tarkvaradest ning nende versioonidest. Seejärel analüüsib tarkvarade versioone ja nende nõrkusi ning valib sobiva ründevektori ehk kõige vähem kaitstud komponendi. Selleks võib olla ebaturvaline ühendus, puudulik küberturbe seadistus (nt avatud port või uuendamata viirusetõrje), küberhügieeni reeglite eiramine kasutaja poolt (nt õngitsuskirjas sisaldava veebilingile klikkimine või tundmatu välise andmekandja arvutisse ühendamine), ebausaldusväärne teenusepakkuja või tema töötaja, kes tahtlikult (altkäemaksu eest) võimaldab rünnaku toimimist. Seejärel valmistab pahavara nõrkuse ärakasutamiseks (2 etapp). Näiteks luuakse legaalse tarkvarapakkuja serveri kloon eesmärgiga, et järgmise tarkvara uuenduse ajal kliendi server pöörduks kloonserveri poole või pahavara lisatakse vabavaralise koodi sisse (Ladisa, *et al*., 2022, pp. 3–5). Peale tarkvara uuendamist laetakse kliendi serverisse pahavara käivitamist sisaldav fail, mis on peidetud legaalse tarkvara sisse. Järgmise sammuna jõuab pahavara kliendi seadme(te)sesse (etapid 3–6), kus toimub legaalse tarkvara installeerimine, mille taustal installeeritakse ka pahavara. Sellega lõpeb rünnaku kuues etapp, mille tulemusel on kliendiarvuti nakatatud ja ründajal täielik kontroll ohvri arvuti üle ning ligipääs andmetele.

Tarneahela rünnakute eeliseks on asjaolu, et selle kaudu on korraga võimalik rünnata suurt hulka ohvreid erinevatest sektoritest ning potentsiaalselt toob ründajale kaasa suure tulu. Tulu saajaks võib olla nii rünnaku läbiviija kui ka rünnaku tellija või sponsor. Tulu on kas otsene ehk rahaline väärtus (nt valuraha, varastatud informatsiooni edasimüük) või kaudne. Kaudse tulu alla võib liigitada varastatud informatsiooni kasutamine majandus- või sõjalise eelisseisundi saavutamiseks (Hiina ja Venemaa näide) ning vastaspoole toodete ja teenuste halvamine. Seda tüüpi rünnaku vastu kaitsmine nõuab tähelepanu mitmelt sidusrühmalt – tarkvaraarendajatelt ja -müüjatelt, kes kirjutavad koodi, süsteemiadministraatoritelt, kes haldavad tarkvara installimist, ja infoturbe kogukonnalt, kes avastavad rünnakuid ja töötavad välja turbelahendusi.

1.4 Tarneahela usaldusväärsus ja kontroll

„Eesti julgeolekupoliitika alused“ kohaselt on julgeolekupoliitika eesmärk kindlustada Eesti Vabariigi iseseisvus ja sõltumatus, eesti rahvuse, keele ja kultuuri kestmine, territoriaalne terviklikkus, põhiseaduslik kord, elanikkonna turvalisus ja ühiskonna toimimine (Vabariigi Valitsus, 2023, lk 4). Eesti julgeolekupoliitika võtab arvesse kõiki riigi julgeolekut mõjutavaid suundumusi ja tegureid. Üheks oluliseks teguriks on küberruum, mille protsesside, tarneaheahelate ja taristu arendamisel tuleb arvestada julgeolekuküsimustega. Era- ja avaliku sektori asutused peavad planeerima küberturvet kõikides infosüsteemides, organisatsioonides ja protsessides. Oluline on ennetada ja välistada sõltuvust autoritaarsetest riikidest ning tõhustada järelevalvet nende kontrolli all olevatest ebausaldusväärsetest ettevõtetest (Vabariigi Valitsus, 2023, lk 11). Tuleb tagada, et olukord küberruumis vastaks ohupildile, riiklike ja elutähtsate teenuste toimepidevus oleks tagatud ning teenused oleksid usaldusväärsed. Kuna IKT tarneahel on üks komponent teenuste tagamiseks, siis sellest võib järeldada, et riigi teenuste tagamiseseks vajalik IKT tarneahel peab samuti olema usaldusväärne ja ohutu. Käesoleva magistritöö fookuses on IKT tarneahela usaldusväärsuse tagamine läbi kontrolli.

Usaldusväärsus on tarneahela toimimise üks olulisemaid komponente, kuna sellel on oluline mõju tarnitavate toodete ja teenuste terviklikkusele ja kvaliteedile. Usaldusväärsust võib defineerida kui süsteemi või selle komponendi võime täita oma nõutud funktsioone kindlaksmääratud tingimustel kindlaksmääratud aja jooksul (Lukinskiy, *et al*., 2014, p. 120). Usaldusväärsuse kontroll käesoleva magistritöö tähenduses on protsess, mille raames hinnatakse neljast IKT tarneahela ohustavate ründevektoritest tulenevaid ohte, eesmärgiga veenduda IKT tarneahela ohutuses ning sellega ära hoida negatiivset mõju Eesti julgeolekule. Autori hinnangul on tarneahel usaldusväärne siis, kui kõik neli komponenti on läbinud kontrolli.

Pakutud definitsioon ei ole uus. Sarnast lähenemist kasutati Eestis ka varem. Jaanuaris 2023. aastal võeti vastu välisinvesteeringu usaldusvääruse hindamise seadus, mille eesmärk on reguleerida kindlaksmääratud majandusvaldvaldkondades tegutsevatesse ettevõtjatesse tehtavate välisinvesteeringute kontrolli. Investeeringu usaldusväärsuse hindamisega on võimalik ennetada ja tõkestada erineva väärtusruumiga kolmandatest riikidest lähtuvat ohtu julgeolekule ja avalikule korrale. (Majandus-ja Kommunikatsiooniministeerium, 2022, lk 18)

Välisinvesteeringu usaldusvääruse hindamise seaduse § 5 kohaselt toimub investeeringu usaldusväärsuse hindamine läbi loamenetluse, mille raames hinnatakse välisinvesteeringu mõju Eesti või muu Euroopa Liidu liikmesriigi julgeolekule ja avalikule korrale. Esitatud loa hindamisel osalevad Tarbijakaitse ja Tehnilise Järelevalve Amet (edaspidi TTJA) ning selle juurde loodud välisinvesteeringu komisjon, mis koosneb Kaitseministeeriumi, Majandus- ja Kommunikatsiooniministeeriumi, Rahandusministeeriumi, Siseministeeriumi, Välisministeeriumi, Kaitsepolitseiameti, Politsei- ja Piirivalveameti, Rahapesu Andmebüroo, TTJA, Välisluureameti ning Riigikantselei esindajatest. Välisinvesteeringu usaldusväärsuse hindamisel võetakse arvesse muuhulgas välisinvestori päritolu. Teisisõnu võetakse arvesse geopoliitilisi ohte.

Teine näide Eesti tarneahela usaldusväärsuse hindamisest on 2021. aasta detsembris muudetud elektroonilise side seadus. Muudatusega loodi sidevõrgus kasutatava riist- või tarkvara kontrollimise protseduuri. See tähendab, et sideettevõtjal tuleb teavitada TTJA-d võrgus kasutatavast riist- või tarkvarast ning taotleda kasutusluba. Meetme eesmärgiks on tagada sideteenuse osutamisel sidevõrgus kasutatava riist- või tarkvara ohutust riigi julgeolekule. Tulenevalt nimetatud seaduse §-st 87^3, saab riist- või tarkvara ohustada riigi julgeolekut selle tootjast või hooldus- või tugiteenuste pakkujast tuleneva kõrge riski tõttu või tehnilistest omadustest ja seadistustest. Riist-ja tarkvara ohutust hindavad julgeolekuasutused ja Riigi Infosüsteemi Amet. Hindamisel võetakse arvesse tootja, hooldus- või tugiteenuse pakkuja päritolu (geopoliitiline oht), riist-ja tarkvaras sisalduvaid turvanõrkusi ning toodete ja teenuste tarnevõimekust. Kui üks hindajast leiab, et kasutusloa taotluses nimetatud riist- või tarkvara võib ohustada riigi julgeolekut, siis taotluse kooskõlastamist otsustab Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu. Loamenetluse raames tehakse kindlaks, et sidevõrgus kasutusele võetav riist-ja tarkvara on ohutu, mis tähendab, et tegemist on usaldusväärsuse kontrolliga.

Mõlemal juhul on tegemist riigipoolse kontrolliga, mis nõuab märkimisväärset panustamist erinevate avaliku sektori asutuste poolt. IKT tarneahela usaldusväärsuse hindamisel on võimalik osaliselt vähendada hindaja koormust ning delegeerida hindamisprotsessi osasid kolmandatele osapooltele. Selleks on võimalik paluda, et tarneahelas osalevad osapooled sertifitseeriksid oma tooteid ja teenuseid rahvusvaheliselt tunnustatud standardi vastu (nt NIST, ISO standardid) või nõuda, et läbi oleks viidud audit sõltumatu audiitori poolt (Wills, 2021, p.

1178). Tarneahela komponentide usaldusväärsuse kontrolli delegeerimise praktikat käsitletakse pikemalt magistritöö teises peatükis.

Autor peab vajalikuks märkida, et sõltumata tarneahela usaldusväärsuse kontrollimiseks valitud meetodist, ei muutu protsessi lõppeesmärk ehk Eesti julgeoleku tagamine tarneahelas kasutatud komponentide ohutuse kaudu. Eesmärgi saavutamiseks ei ole määrav, kas kogu kontrollimise protsessi viib läbi riik, delegeerib kolmandatele osapooltele (sõltumatu audit või vastavus spetsiifilisele standardile (Masip-Bruin, *et al*., 2021, p. 6) või kasutatakse kombineeritud meetod. IKT tarneahela kontrollimise protsessi võimalikke meetmeid analüüsib autor magistritöö teises peatükkis. Töö teoreetilises osas fokuseeritakse IKT tarneahela kontrollile kui nähtusele, selle vajadusele ja tarneahelaga seotud ohtudele Eesti küberjulgeolekule.

Käeolevas peatükis läbi viidud teoreetiliste allikate analüüs toob välja, et IKT tarneaheala turvalisusel on oluline roll Eesti küberturvalisuse tagamisel. Eesti küberruumi kaitsmise vajadus kerkis esile 2007. aastal pronksiöö ajal, millal Venemaa tegi ulatuslikke küberrünnakuid Eesti avaliku-ja erasektori asutuste vastu. Seejärel tekkis Eestis diskussioon küberkaitsevõimekuse arendamise vajalikkusest (Oksaar, 2014, lk 62) ning astuti esimesi samme küberjulgeoleku tugevdamiseks, milleks oli 2018. aastal esimese küberjulgeoleku strateegia kehtestamine. Sellest sai alguse küberjulgeoleku julgeolekustamise protsess Kopenhaageni koolkonna julgeolekustamise teooria tähenduses. Selle kohaselt muutub oht julgeolekuprobleemiks siis, kui julgeolekustaja (antud kontekstis riik) hinnangul eksisteerib oht ning tema auditoorium sellega nõustub. Kuigi Kopenhaageni koolkond ei nimetanud alguses küberjulgeolekut viie julgeoleku sektori hulka, ei ole algsed määratud sektorid absoluutsed. See tähendab, et sektorite arv võib muutuda otsustajate narratiivist. Kersti Oksaare (2014, lk 93) analüüs näitas, et küberjulgeolekut on võimalik tõlgendada kui Kopenhaageni koolkonna teooria julgeolekusektorit. Alates 2010. aastast sai kübertuvalisus oluliseks julgeolekuosaks Eesti, NATO (Weitz, 2016, p. 11 ja Euroopa Liidu liikmesriikidele (Urciuoli, *et al.*, 2013, p. 52).

Erinevat liiki küberrünnakud toimuvad iga päeva nii era kui avaliku sektori asutuste vastu üle maailma. Erilist ohtu kujutavad aga riigi korraldatud või riigi poolt rahastatud rühmituste ründed. Selliste rünnakute toimumiseks on vajalik rahaliste ja inimressursside olemasolu ja juurdepääs vajalikele tehnoloogiatele. Eesti jaoks kujutavad ohtu eelkõige Venemaa, kellele on omistatud SolarWinds (Eggrers, 2021, p. 883) ja NotPetya tarneahela rünnakud, ja Hiina, kelle

tehnoloogia kasutamine IKT tarneahealas võimaldab nende riikide valitsusasutustele ja eriteenistustele saada juurdepääs võrkudele. IKT tarneahela rünnakutel on ulatuslik mõju (SolarWinds puudutas 33 000 klienti) ning kahjum (nt NotPetya kahjum ca 10 miljardit USA dollarit). Mõlemal riigil on olemas kindlad eesmärgid tarneahelarünnakute läbiviimiseks. Hiina fookuses on andmete vargus ja spionaaž. Venemaa kasutab rünnakuid lisaks spionaažile konventsionaalsete rünnakute toetamiseks.

See tähendab, et IKT tarneahelaga seotud riskide maandamine avaliku sektori ja elutähtsate teenuste osutamisel aitab tõsta Eesti küberjulgeoleku taset. Sellest tulenevalt tuleb teenuse või toote lõppkasutajal veenduda IKT tarneaheala komponentide ohutuses kogu nende elukaare jooksul. Võttes arvesse alapeatükkides 1.1 kuni 1.4 toodut, toob magistritöö autor välja, et üks viis komponentide ohutuse tagamiseks on IKT tarneahela usaldusväärsuse kontrolli teostamine. Käesoleva magistritöö käigus läbi viidud empiiriline uuring keskendub usaldusväärsuse kontrolli teostamise meetmete täiendamise võimaluste uurimisele.

2. IKT TARNEAHELA TURVALISUST TOETAVATE JA REGULEERIVATE TEGURITE ANALÜÜS

2.1 Metoodika

Magistritöö uurimisstrateegiaks valis autor juhtumiuuringu (ingl *case study*). Juhtumiuuring on toimunud tavatu või igapäevaste sündmuste empiiriline uuring, mille raames uuritakse põhjalikult ühte või mitu analoogset juhtumit (Kidron, 2007, lk 39). Selle abil on võimalik jälgida organisatsiooni, selle allüksust, isikute gruppi või ühtainsat isikut (Kidron, 2007, lk 94–96). Magistritöö autor valis juhtumiuuringu, sest see võimaldab keskenduda IKT valdkonna tarneahela usaldusväärsuse kontrollimise protsessi uurimisele. Magistritöös uuritavamaks juhtumiks on IKT valdkonna tarneahela usaldusväärsuse kontrollimise protsess.

Juhtumit võib määratleda erinevalt, selleks võib olla toimunud intsident, nähtus, sündmus, otsus, tegevus jne. Juhtumi definitsioon võib sõltuda uuritavast valdkonnast (Schwandt, & Gates, 2018, pp. 600-602). Samas leitakse, et „juhtumiuurimuse puhul on uurimuse keskmes juhtum oma terviklikkuses ja loomulikus kontekstis, mitte kategooriad ja muutujad“. (Strömpl, 2014)

Stake (1995, p. 237) tõlgendab juhtumiuuringu kui kombinatsiooni juhtumi uurimise protsessist ja uurimistulemustest. Juhtumiuuringu peamiseks eesmärgiks on konkreetse juhtumi mõistmine, mitte teiste samalaadsete juhtumite või üldise probleemi uurimine. Ta toob välja kolm peamist juhtumiuuringu tüüpi: seesmine (ingl *intrinsic case*), instrumentaalne (ingl *instrumental case*) ja kollektiivne (ingl *collective*) (Stake, 1995, p. 4). Seesmise juhtumi näol on tegemist ainulaadse juhtumi uuringuga, mille tundmaõppimine on uurimuse eesmärk iseeneses, mitte üldise nähtuse tundmaõppimine (Strömpl, 2014). Instrumentaalses juhtumiuuringus vaadeldakse samuti konkreetset juhtumit, kuid eesmärgiks on saada laiemat ülevaadet suurest probleemist või nähtusest. Kollektiivse juhtumiuuringu puhul on fookuses korraga mitu juhtumit ning püütakse saada laiemat ülevaadet mingist teemast (Crowe, *et al*. 2011, pp. 1-2) .

Lähtuvalt Stake´i pakutud juhtumiuuringute tüpoloogiast magistritöös on tegemist seesmise juhtumiuuringuga, sest töös ei uurita mõnd laiemat probleemi (nt kõikide võimalike küberrünnakute uuring või küberturvalisuse tagamisega seotud protsesside analüüs), vaid

uuritakse ainult ühte juhtumit, milleks on IKT valdkonna tarneahela usaldusväärsuse kontrollimise protsess.

Magistritöös püstitatud uurimisprobleemi lahendamiseks ning uurimisküsimustele vastamiseks on valitud kvalitatiivne lähenemine. Kvalitatiivse uurimistöö eesmärgiks on „kirjeldada ja seletada sotsiaalset tegelikkust inimeste individuaalsete tõlgenduste kaudu, teisiti öeldes tähenduste kaudu, mida inimesed omistavad tegelikkuse aspektidele.“ (Õunapuu, 2014, lk 56) Kvalitatiivse uuringu andmekogumis meetodiks võib olla avatud vaatlused, intervjuud ning dokumendi-, helisalvestite- ja ajaleheväljalõigete analüüs (Laherand, 2008, lk 18). Stake (1995, p. 64) hinnangul on juhtumiuuringu puhul väga oluline saada teiste inimeste hinnangud ja tõlgendused uuritava juhtumi kohta ning just intervjuu võimaldab uurijal saada hinnangute mitmekesisuse. Käesolevas magistritöös koguti andmeid dokumendianalüüsi ning poolstruktureeritud ekspertintervjuude kaudu.

Dokumendianalüüsiks kasutas autor ainult avalikkusele kättesaadavaid dokumente. Kuna magistritöö esimeses peatükis sai tõestatud, et küberjulgeolek on oluline aspekt nii Eesti kui ka Euroopa Liidu ja NATO julgeoleku tagamiseks, siis dokumendianalüüsi käigus on kasutatud Eesti, Euroopa Komisjoni, Euroopa Liidu Küberturvalisuse Ameti (ENISA), CERT-EU ning NATO kooperatiivse küberkaitse kompetentsikeskuse (NATO *Cooperative Cyber Defence Centre of Excellence*, edaspidi *CCDCOE*) poolt avaldatud magistri töö teemat puudutavad dokumendid. Samuti analüüsis autor küberkaitsega tegelevate erasektori ettevõtete avaldatud raporteid ja standardeid.

Selleks, et leida vastused magistritöö uurimisprobleemile ja uurimisküsimustele, otsustas autor viia läbi ekspertintervjuud. Poolstruktureeritud intervjuu sobib andmekogumismeetodina juhul, kui intervjueeritavale võimaldatakse rääkida uuritavast teemast võimalikult vabalt ning lisada rohkem informatsiooni kui uurija suutnuks ette näha. Lisaks on intervjueerijal võimalik vastuseid täpsustada (Laherand, 2008, lk 219).

Intervjueeritavate valimisel kasutati eesmärgistatud valimit. Eesmärgistatud valimi puhul lähtuv uurija oma teadmistest, kogemustest ja eriteadmistest mõne grupi kohta ning püütakse leida kõige tüüpilisemaid esindajaid (Teddlie, & Yu, 2007, pp. 79-81). Eesmärgistatud valimit kasutati seetõttu, et Eestis on piiratud arv eksperte, kellel on praktiline kogemus nii IKT tarneahelate kontrolli tagamisel kui ka seos Eesti julgeoleku tagamisega. Ekspertintervjuud viis

magistritöö autor läbi 6 eksperdiga, kelle puhul on täidetud mõlemad nõutud aspektid. Nendest 4 eksperti on avaliku sektori asutustest, kelle vastutusalas on küberkaitse korraldamisega, sh tarneahela kontrolliga seotud tööülesanded. Intervjueeritavad oli Majandus- ja Kommunikatsiooniministeeriumist, Riigi Info- ja Kommunikatsioonitehnoloogia Keskusest, Tervise ja Heaolu Infosüsteemide Keskusest ning Riigi Infosüsteemi Ametist. Lisaks avaliku sektori asutustele olid valimis 2 eksperti asutustest, mis on elutähtsate teenuste osutajateks hädaolukorra seaduse § 36 tähenduses, kuid ei ole avaliku sektori asutused. Viimase kahe aasta jooksul on toimud mitmed küberrünnakud tervishoiu sektori vastu nii Eesti kui ka välismaal. Novembris 2020. aastal rünnati Eesti Terviseametit ning varastati 9100 inimese isikuandmeid. Oktoobris 2022. aastal toimus rünnak suuruselt neljanda USA tervishoiu asutuste võrgustiku CommonSpirit Health´i vastu, mille tagajärjeks jäid ära planeeritud operatsioonid, tekkisid viivitused ravimite väljastamisel ning arstiaja broneerimisel. Teine ekspert esindab Eestis tegutsevat telekommunikatsiooni ettevõtet, kes osutab mobiiltelefoni- ja andmesideteenuseid era- ja avaliku sektori asutustele. Sellest tulenevalt otsustas autor lisaks avaliku sektori ekspertidele lisada valimisse just nende kahe sektori eksperte.

Intervjuu läbiviimisel eelistati vahetut suhtlust, kuid kahe eksperdi hõivatuse tõttu intervjuu läbiviimiseks kasutati MS Teams suhtlusplatvormi. Intervjuude transkribeerimiseks kasutati Tallinna Tehnikaülikooli kõnetehnoloogia labori avaliku kõnetuvastuse teenust Tekstiks. Transkribeeritud tekstid kodeeriti ja analüüsiti NVIVO rakenduse abil. Intervjuu küsimused on koostatud lähtuvalt uurimisküsimustest (vt Lisa 1, lk 92). Intervjuude eesmärgiks oli ekspertide arvamuste ja hinnangute kogumine, et võrrelda neid töö teoreetilise osaga. Saadud andmete põhjal teeb autor ettepanekud, kuidas on võimalik korraldada IKT valdkonna tarneahela kontrolli, et tõsta Eesti avaliku sektori küberjulgeoleku jätkusuutlikkust.

2.2 Dokumentide analüüs

Dokumendianalüüsiks kasutati sihistatud valimit, mis lähtub magistritöö spetsiifikast. Dokumendianalüüsiga töötati läbi Eesti Vabariigi ning rahvusvahelised strateegia-, õigusaktid ning muud dokumendid, mis on seotud küberturvalisuse valdkonnaga. Analüüsitud dokumendid aitasid luua parema pildi olemasolevatest IKT tarneahela kaitsmist puutuvatest regulatsioonidest, normidest ja soovitustest ning valmistuda ette ekspertintervjuudeks. Dokumendianalüüsi ja intervjuude raames otsiti vastuseid neljale uurimisküsimusele:

1. Millised on võimalikud riist-ja tarkvarast ning selle haldamisest, alltöövõtjatest ning ettevõtte ja avaliku sektori asutuse personalist tulenevad ohud riigi IKT tarneahelale?
2. Kuidas ja milliste kriteeriumite alusel oleks riigi IKT asutustel võimalik hinnata ja kontrollida kasutatava riist- ja tarkvara, riiklike ja riigi seisukohast oluliste infosüsteemide arendus- ja hooldusfirmade usaldusväärsust?
3. Kuidas ja millistel alustel oleks riigi IKT asutustel võimalik teostada usaldusväärsuse kontrolli alltöövõtjate ja nende personali üle?
4. Kuidas ja milliste kriteeriumite alusel oleks riigiasutustel ja nende valitsemisalas olevatel juriidilistel isikutel võimalik välistada riigihangetest ebausaldusväärseid pakkujaid?

Kõik valimisse valitud dokumendid on avalikult kättesaadavad ning loetletud allpool olevas tabelis 3.

Tabel 3. Dokumendianalüüsis kasutatud materjalid (autori koostatud)

Kood	Organisatsioon	Dokumendi pealkiri
EU või NATO poolt välja antud aktid		
RV 1	Euroopa Parlament	Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555, 14. detsember 2022 (küberturvalisuse 2. direktiiv).
RV 2	Euroopa Komisjon	ELi küberturvalisuse strateegia digikümnendi jaoks
RV 3	Euroopa Parlament	Euroopa Parlamendi ja nõukogu määrus (EL) 2019/881, 17. aprill 2019 (küberturvalisuse määrus).
RV 4	Euroopa Parlament	Euroopa Parlamendi ja nõukogu määrus (EL) 2021/241, 12. veebruar 2021.
RV 5	Euroopa Parlament	Ettepanek: Euroopa Parlamendi ja nõukogu määrus, mis käsitleb digielemente sisaldavate toodete küberturvalisuse horisontaalseid nõudeid ja millega muudetakse määrust (EL) 2019/1020
RV 6	Euroopa Parlament	Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2557, 14. detsember 2022, mis käsitleb elutähtsa teenuse osutajate toimepidevust ja millega tunnistatakse kehtetuks nõukogu direktiiv 2008/114/EÜ
RV 7	Euroopa Komisjon	Euroopa komisjoni soovitus (EL) 2019/534, 26. märts 2019, „5G-võrkude küberturvalisus“.
RV 8	Euroopa Liidu Küberturvalisuse Amet	ENISA Threat landscape for supply chain attacks
RV 9	Euroopa Liidu Nõukogu	Nõukogu otsus, 23. september 2013, ELi salastatud teabe kaitseks vajalike julgeolekueeskirjade kohta (2013/488/EL)
RV 10	Euroopa Komisjon	Ühisteatis Euroopa Parlamendile ja nõukogule, ELi küberkaitsepoliitika
RV 11	NATO	Primary Directive on CIS Security
RV 12	NATO	Security Within The North Atlantic Treaty Organization (NATO)
RV 13	US	Assessment of the critical supply chains supporting the U.S. information and communications technology industry

Rahvusvaheliste organisatsioonide standardid või juhised		
ST 1	ENISA	5G cybersecurity standards
ST 2	ENISA	ENISA Cybersecurity Threat Landscape Methodology
ST 3	NIST	Key Practices in Cyber Supply Chain Risk Management:
ST 4	ENISA	Risk Management Standards
ST 5	ENISA	ENISA Cybersecurity Market Analysis Framework
ST 6.	International Telecommunication Union (ITU)	Guide to Developing a National Cybersecurity Strategy 2nd Edition
ST 7	NIST	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations
ST8	MITRE	Supply Chain Attacks and Resiliency Mitigations. Guidance for System Security Engineers
Eesti sisesed küberturvalisust puudutavad õigusaktid ja standardid		
EE 1	MKM	Digiühiskonnna arengukava
EE2	MKM	Küberturvalisuse strateegia
EE 3	Riigikogu	Eesti julgeolekupoliitika alused
EE 4	Siseministeerium	Siseturvalisuse arengukava
EE 5	Ettevõtlus- ja infotehnoloogiaminister	Eesti infoturbestandard

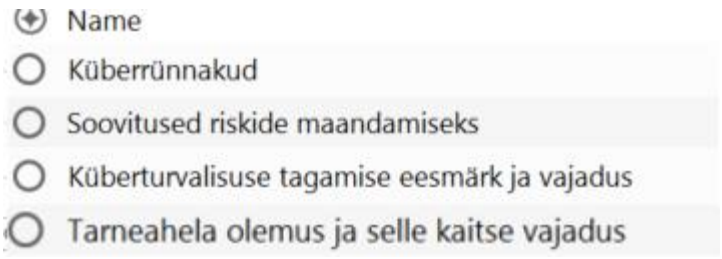
Dokumendialalüüsiks kasutas autor kvalitatiivset sisuanalüüsi. Kvalitatiivne sisuanalüüs võimaldab uurida huvipakkuvat nähtust ning saab algab sõnade või muude sisuüksuste leidmisega tekstist, eesmärgiga mõista sõnade vm sisu kontekstilist kasutamist. Kvalitatiivse sisuanalüüsi puhul võivad andmed pärineda artiklitest, raamatutest ja juhenditest ning võimaldavad autoril keskenduda teksti sisule ja konteksti tähendusele (Laherand, 2008. lk 290–298).

Dokumendianalüüsiks kasutati kolme tüüpi dokumente. Esimeses kategoorias on Euroopa Liidu institutsioonide, NATO ja USA asutuste poolt avaldatud õigusaktid, strateegiad ja raportid (dokumendi kood RV). Järgmisena leiavad käsitlemist rahvusvaheliste organisatsioonide standardid või juhised (dokumendi kood ST) ning kolmandana on Eesti-sisesed küberturvalisust puudutavad õigusaktid ja standardid (dokumendi kood EE). Kõik analüüsis kasutatud dokumendid on avalikult kättesaadavad.

Dokumendianalüüsi läbiviimiseks kasutati NVIVO 14 rakendust. Lähtuvalt uurimisküsimustest kasutati suunatud kodeerimist ning muud teemad jäeti analüüsi skoobist välja (Kalmus, *et al.*, 2015). Kodeerimisel loodi neli kategooriat, milleks on küberturvalisuse tagamise eesmärk ja vajadus, küberrünnakud, tarneahela olemus ja selle kaitsmise vajadus ning soovitused riskide

maandamiseks (tabel 4). Kategooriate loomisel lähtuti uurimisküsimustest ning nende omavaheline seos on toodud tabelis 5. Põhjalik ülevaade kasutatud koodipuust koos koodide esinemise sagedusega ning viidete arvuga on leitav Lisas 2 (käesolev töö lk 93). Iga kategooria on jagatud koodideks.

Tabel 4. Dokumendianalüüsi kategooriad (NVivo faili põhjal autori koostatud)



Tabel 5. Kategooriate seos uurimisküsimustega (autori koostatud)

Uurimisküsimus	**Kategooria**
1.Millised on võimalikud riist-ja tarkvarast ning selle haldamisest, alltöövõtjatest ning ettevõtte ja avaliku sektori asutuse personalist tulenevad ohud riigi IKT tarneahelale?	• Küberturvalisuse tagamise eesmärk ja vajadus. • Küberrünnakud
2. Kuidas ja milliste kriteeriumite alusel oleks riigi IKT asutustel võimalik hinnata ja kontrollida kasutatava riist- ja tarkvara, riiklike ja riigi seisukohast oluliste infosüsteemide arendus- ja hooldusfirmade usaldusväärsust?	• Tarneahela olemus ja selle kaitse vajadus
3. Kuidas ja millistel alustel oleks riigi IKT asutustel võimalik teostada usaldusväärsuse kontrolli alltöövõtjate ja nende personali üle?	• Soovitused riskide maandamiseks
4. Kuidas ja milliste kriteeriumite alusel oleks riigiasutustel ja nende valitsemisalas olevatel juriidilistel isikutel võimalik välistada riigihangetest ebausaldusväärseid pakkujaid?	

Esimene kategooria: Küberturvalisuse tagamise eesmärk ja vajadus

Esimeses kategoorias on viis koodi (tabel 6), mille fookuses on küberturvalisuse mõiste, küberturvalisuse tagamise eesmärgid ja küberturvalisuse olulises. Eraldi koodideks on ka küberohud ja küberriskid.

Tabel 6. Kategooria „Küberturvalisuse tagamise eesmärk ja vajadus“ koodid (NVivo faili põhjal autori koostatud)

Kood: küberturvalisuse mõiste

Esmalt otsiti **koodi „küberturvalisuse mõiste**“ järgi. Viidet küberturvalisuse mõiste definitsioonile leiti kolmes dokumendis RV 3, ST 6 ja EE 2 (siin ja edaspidi kasutatakse Tabelis nr 3 toodud koode). See tähendab, et küberturvalisust püütakse defineerida nii rahvusvahelistes õigusaktides ja standartides kui ka Eesti strateegiadokumentides. Samas on kõik kolm definitsiooni erinevad ning tõlgendavad küberturvalisust veidi erinevate nurkade alt. Dokumendi RV 3 kohaselt „küberturvalisus – tegevused, mis on vajalikud, et kaitsta võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid küberohtude eest“. ST 6 näeb küberturvalisust kui meetmete kogumit, mis sisaldab erinevaid juhtimis-, poliitika-, tegevus-, tehnilisi ja juriidilisi aspekte. EE 2 ütleb, et küberturvalisus on seisund, kus võrgu- ja infosüsteemid on kaitstud ohtude realiseerumise eest. Kuigi küberturvalisus on eri dokumentides defineeritud erinevalt, võib siiski järeldada, et põhimõte on sama, ehk küberturvalisus on võrgu- ja infosüsteemide kaitse küberohtudest erinevate meetmete kaudu. Selline definitsioon sarnaneb teooria osas (käesolev töö lk 13) toodud küberjulgeoleku tähendusega.

Kood: küberturvalisuse eesmärk

Teiseks otsiti dokumentidest koodu „ küberturvalisuse eesmärk“. Küberturvalisuse eesmärgile viidati samuti kolmel korral. RV 1-st selgub, et igal EU liikmesriigil tuleb koostada küberturvalisust puudutava strateegiadokument, milles määratakse strateegilised eesmärgid küberturvalisuse tagamiseks. Sellisteks dokumentideks osutusid EE 1 ja EE 2. EE 1 seab eesmärgiks „tagada digiriigi, -majanduse ja laiemalt digitaalse eluviisi kaitse“. EE 2 läheneb küberturvalisuse eesmärgile läbi küberturvalisuse rolli ehk „küberturvalisuse roll infoühiskonnas on tagada tingimused selleks, et IKT võimalusi saaks tõhusalt ja turvaliselt kasutada“.

Kood: küberturvalisuse olulisus

Kolmanda koodi „küberturvalisuse olulisus“ päringu tulemusel leiti, et küberturvalisuse olulisust rõhutavad kümme dokumenti (EE 1, EE 2, RV 1- RV5, RV 7, RV 10 ning ST 2). Euroopa Liidu tasandil on küberturvalisus „hädavajalik võrguühenduse ning ülemaailmse ja avatud interneti jaoks, mis peab toetama majanduse ja ühiskonna arengut“ ning iga digikomponenti sisaldava valdkonna investeeringute planeerimisel tuleb võtta arvesse küberturvalisuse aspekte (RV 2). Küberturvalisuse kõrge tase on vajalik edukaks digipöördeks (RV 4) ja Euroopa andmestrateegia rakendamiseks (RV 5). Võttes arvesse, et küberrünnakute arv kasvab ning nad muutuvad üha keerulisemaks, siis küberturvalisuse tagamine on strateegilise tähendusega (RV 7) ning katab erinevaid Euroopa Liidu poliitikavaldkondi, nagu justiits- ja siseküsimused, digitaalne ühtne turg ja teaduspoliitika (ST 2). Lisaks sellele on „küberturvalisus paljude kriitilise tähtsusega sektorite jaoks peamine tegur, mis võimaldab digiüleminekuga edukalt toime tulla ning digitaliseerimise majanduslikke, sotsiaalseid ja kestlikkuse eeliseid täielikult ära kasutada“ (RV 1). Sellest tulenevalt on oluline arendada liikmesriikide suutlikkust reageerida küberohtudele (RV 3) ning tugevdada koostööd EL ja NATO vahel (RV 10), sest küberturvalisus on tihedalt seotud ELi julgeolekupoliitikaga (RV 2). Eesti jaoks on küberturvalisus oluline osa riigi julgeolekust (EE 1) ning sellega arvestatakse kaitsevõime planeerimisel selliselt, et tõsta riigi suutlikkust ohtude ennetamisel ja tõrjumisel. Samuti on oluline integreerida küberturvalisuse komponente riigiasutuste ja oluliste teenuste pakkujate valmisolekut tagavatesse plaanidesse ning riskihinnangutesse (EE 2). Kokkuvõtlikult võib öelda, et küberturvalisus on oluline teema EL, NATO ja Eesti jaoks, kusjuures küberturvalisust on oluline tagada kõikides valdkondades, kus on võetud kasutusele digitaalsed komponendid. See annab kinnituse, et toimus teooria osas (käesolev töö lk 13-14) kirjeldatud kübervaldkonna julgeolekustamine.

Koodid: küberriskid ja küberohud

Järgmiseks päringuks kasutati koode „küberriskid“ ja „küberohud“. Tehnoloogia arenguga kaasnevad uued võimalused, kuid ka ohud ja riskid (EE 1), mis tähendab väljakutseid nende hindamisel (EE2, RV 1, RV 3). Sellest tulenevalt otsiti esmalt valimisse valitud dokumentidest, kuidas terminid „oht“ ja „risk“ on defineeritud. RV3 kohaselt on **küberoht** „võimalik asjaolu, sündmus või tegevus, mis võib kahjustada või häirida võrgu- ja infosüsteeme, nende kasutajaid ja teisi isikuid või neile muul viisil halba mõju avaldada“. Samale definitsioonile viidatakse ka dokumendis RV 1, milles on täiendus, et kui küberohul võib olla tõsine mõju võrgu- ja infosüsteemidele või selle kasutajatele ning sellega kaasneb märkimisväärne kahju, siis

tegemist on olulise küberohuga. Peamisteks küberohtudeks on küberrünnakud riigi- ja elutähtsate teenuste vastu (EE 2) ja ebaturvalised tooted (RV 5). RV 5 toob olulise aspektina välja, et „küberturvalisuse ohud võivad enne teatava sihtmärgini jõudmist levida mitmesuguste digielemente sisaldavate toodete kaudu, näiteks mitmest nõrkuse ärakasutamisest tekitatud ahelas“. Isegi kui algselt toode, olgu see riist- või tarkvara, oli turvaline, siis ohud võivad muutuda iga järgmise uuendusega. See tähendab, et ohuseiret tuleb teha toodete kogu elukaare jooksul. EE 2 juhib tähelepanu sellele, et Eesti sõltuvus digitaalsetest tehnoloogiatest on suur, mistõttu on küberohtude võimalikud mõjud meie jaoks võrreldes paljude teiste riikidega oluliselt kaalukamad. EE 5 toob välja, et ohud on erinevate organisatsioonide puhul tüüpilised ning nimetab üle saja ohu, millega tuleb Eesti avaliku sektori asutustel ja elutähtsate teenuste osutajatel arvestada (RV 6). Nende seas on erinevat tüüpi küberrünnakud, turvanõrkused, ebausaldusväärsed riist-ja tarkvara ning partnerid.

Kui küberoht oli defineeritud dokumentides erinevalt, siis **küberriski** definitsioon on neljas dokumendis (RV 1, RV 5, RV 12, EE 5) väga sarnane, kusjuures RV 1 ja RV 5 on identsed, ehk „intsidendist tingitud kahju või häire võimalus, mida tuleb väljendada sellise kahju või häire ulatust ja kõnealuse intsidendi esinemise tõenäosust arvesse võtva kombineeritud näitajana“. RV 12 ja ST 4 täiendavad, et riski realiseerumine ohustab teenuse konfidentsiaalsust, terviklikkust ja/või kättesaadavust. Teisisõnu teenus, infosüsteem või selles olevad andmed ei ole kättesaadavad, terviklikud või on sattud kolmanda osapoole kätte. Küberriskid ohustavad turgude toimimist, avaliku ja erasektori asutusi, elutähtsate teenuste osutajaid ning EL ja riikide julgeolekut (EE 2, RV 1). Riskid võivad tuleneda:

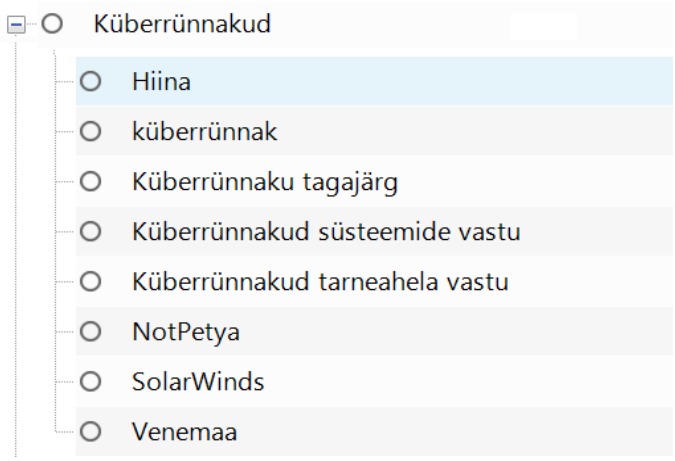
- inimesest (ST 7, RV 12);
- uue põlvkonna tehnoloogiast, nt 5G , plokiahel, tehisintellekt (RV 2, RV 7, EE 2);
- toodetest terve nende elukaare jooksul (RV 3, RV 5);
- riist-ja tarkvarast ning tootjast ja tarnijast (RV 2, RV 5, RV 10, RV 13);
- teenustest ja teenuste pakkujatest (RV 3, EE 1);
- tarneahelast (RV 1, RV 13);
- riikidest. RV 13 toob välja Hiina ja Venemaa, sest nendel (või nende polt rahastatud grupeeringutel) on olemas küberrünnakute võimekus;
- tööstusspionaažist (RV 1);
- välismaisest investoritest (RV 10).

Kuigi see loetelu ei ole ammendav ja olenevalt organisatsioonist võib esineda täiendavaid riske, võib siiski järeldada, et toodud riskid kattuvad magistritöö fookuses olevate riskivektoritega millele lisandus ka geopoliitilised, ehk riikidest tulenevad riskid, mida tutvustati töö teoreetilises osas (käesolev töö lk 15). Oluline on mõista, et riski realiseerimisel võib olukord eskaleeruda ning muutuda asutuse, sektori või riigiüleseks kriisiks. Riskide leevendamise vastutus on igal infosüsteemi omanikul ning riskide maandamiseks tuleb läbi viia riskianalüüse ja võtta kasutusele riskide maandamismeetmeid.

Teine kategooria: küberrünnakud

Teises kategoorias on kaheksa koodi (tabel 7), mille abil otsiti küberrünnaku definitsiooni ning viiteid küberrünnakutele ja nende tagajärgedele.

Tabel 7. Kategooria „küberrünnakud“ koodid (NVivo faili põhjal autori koostatud)



Koodid: küberrünnak ja küberrünnakud süsteemide vastu

Teiseks kategooriaks sai valitud „küberrünnakud“ ning dokumendianalüüsi jätkati koodidega „küberrünnak“ ja „küberrünnakud süsteemide vastu“. Küberrünnaku definitsioon oli toodud ainult dokumendis EE 2, mille kohaselt **küberrünnak** on „tahtlik tegevus võrgu- ja infosüsteemide kaudu kahju tekitamise eesmärgil“ (lk 41). Dokument EE 5 toob välja, et küberrünnakud on üldine mõiste ning rünnakute tüüpe on palju. Näitena tuuakse välja lunavara-, teenusetõkestus-, tarneahela ja suhtlusründeid, kuid loetelu ei ole ammendav. ST 8, RV 2 ja RV 10 viitavad, et küberrünnakute ohvriks võivad langeda avaliku sektori asutused, rahvusvahelised institutsioonid ja organisatsioonid, tsiviiltaristu, elutähtsate teenuste osutajad (nagu energeetika, tervishoid, logistika, finantssektor) ning IKT teenuste osutajad (tark- ja

riistvaratootjad). Näitena või tuua SolarWinds ja NotPetya rünnakuid, mis mõjutasid palju asutusi erinevatest valdkondades (käesolev töö lk 17-18). RV 2 märgib, et ca 13% ettevõttetest on sattunud küberrünnakute ohvriks ning kui arvuti on ühe korra pahavaraga nakatunud, siis ühe aasta jooksul nakatakse uuesti. Rünnakute ennetamist, avastamist ja tõkestamist peetakse oluliseks Euroopa Liidu, NATO ja Eesti tasandil (EE 2, RV 10).

Kood: küberünnaku tagajärg

Koodi „küberünnaku tagajärg" otsingu tulemuste kohaselt võib küberrünnaku tagajärjeks olla konfidentsiaalsuse (andmed satuvad kolmandate osapoolte kätte), terviklikkuse (andmed muudetud, teenused ei ole usaldusväärsed) või käideldavuse (teenus ei ole kättesaadav) kadu (EE 5, ST 8). EE 5 ja RV 13 kohaselt võib edukas rünnak olla alguseks uue ja veelgi suurema küberrünnaku läbiviimiseks, ehk tegemist on tarneahelarünnakuga. RV 8 lisab, et kuna riigiasutused ja suured firmad tõstavad pidevalt oma küberturvalisuse taset, sihivad ründajad aina rohkem asutustele teenuste pakkujaid. Kõige raskemateks tagajärgedeks on riigi sõjalise võimekuse kahanemine, ühiskonna ja majanduse destabiliseerimine ning demokraatia kahjustamine (RV 2, RV 7, RV 10, EE 2, ST 4). Nii juhtus 2008-ndal aastal Gruusias, kus küberrünnaku tõttu katkes sidevahetus Gruusia valitsuse ja koostööpartnerite vahel (käesolev töö lk 16).

Koodid: Hiina, Venemaa, NotPetya, SolarWinds

Käesoleva magistritöö alapeatükist 1.2 Geopoliitilised ohud tarneahela elementide usaldusväärsusele nähtub, et küberrünnakuid võivad teostada riiklikud (Venemaa, Hiina Rahvavabariik) või riikide poolt rahastatud küberrühmitused. Sellest tulenevalt otsiti dokumendianalüüsis seoseid kolmandatest riikidest tulenevate ohtudega ning läbiviidud rünnakutega. Selleks kasutati koode „Hiina", „Venemaa", „NotPetya", „SolarWinds". Hiinat mainiti neljas dokumendis: EE 2, RV 7, RV 8 ja RV 13. Dokumentidest selgub, et Hiinast tulenevat küberriski jäädvustatakse Euroopa Liidu (RV 7), USA (RV 13) ja Eesti (EE 2) tasandil. Eelkõige on riskid seotud Hiina tehnoloogia (riist- ja tarkvara) laialdase kasutuselevõtuga era- ja avalikus sektoris, mille kaudu tekkib Hiina ametiasutustel võimalus pääseda ligi tundlikele andmetele. Venemaast tulenevaid küberohte avastati viies dokumendis: EE2, EE 4, RV 8, RV 10 ja RV 13. Nii dokumendid EE 2, EE 4, RV 8 kui ka RV 10 näitavad, et Venemaa kasutab küberdomeeni konventsionaalses sõjapidamises. Näitena tuuakse välja küberrünnakuid Ukraina satelliitside ja energiataristu vastu. Lisaks seostatakse Venemaad

avalikuks saanud laiaulatuslike tarneahelarünnakutega nagu SolarWinds ja NotPetya (RV 8, ST 8).

Kood: **küberrünnakud tarneahela vastu**

Kategooria viimaseks koodiks sai „küberrünnakud tarneahela vastu“. Koodile andis vasteid kolm dokumenti. RV 2 nimetab tarneaheahela rünnakut üheks kõige suurema mõjuga küberrünnaku tüübiks ning kutsub Euroopa Liidu riike selle vastu võitlema (lk 17). Sellist tüüpi rünnakud on muutunud intensiivsemaks alates 2020. aastast, kui jaanuarist 2020 kuni juulini 2021 raporteeriti 24 tarneahelarünnakust (RV 8). Sama dokument tõdeb, et edukal tarneahelrünnakul on kaskaadi efekt, mis annab ründajale võimaluse korraga mõjutada suurt arvu organisatsioone, ettevõtteid ja kasutajaid. ST 8 lisab, et tarneahealarünnakuid on raske avastada sest:

- ahelasse on kaasatud palju osapooli (inimesed, teenuse osutajad, allhankijad, riist-ja tarkvaratootjad);
- neid on võimalik planeerida infosüsteemide ja teenuste ülesehitamise algstaadiumis (nt tagaukse tekitamine koodis, pahavarakoodiga elemendi tarnimine jne);
- ei pea ründama hästi küberkaitstud asutust, vaid sihitakse kõige nõrgemini kaitstud tarneaheala osapoolt.

Käesoleva kategooria „küberrünnakud“ dokumendianalüüs tõestas, et küberrünnakute potentsiaalsete ohvrite ring on väga lai ning hõlmab rahvusvahelisi organisatsioone, era- ja avaliku sektori asutusi erinevatest sektoritest ning üksikisikud. Eduka rünnaku tagajärjed võivad olla väga destruktiivsed ning mõjutada kõiki eluvaldkondi. Tarneahelarünnak on küberrünnaku tüüp, mis mõjutab korraga paljusid osapooli, kuid mida on raske avastada. Rahvusvahelisel tasandil on kinnitatud, et Venemaal ja Hiinal on olemas võimekus tarneahelarünnakute läbiviimiseks ning juhitakse tähelepanu IKT tarneahela kaitsmise vajadusele.

Kolmas kategooria: IKT tarneahela olemus ja selle kaitse vajadus

Kolmanda kategooria (tabel 8) fookuses on tarneahel ning seetõttu valiti koodideks tarneahela mõiste, tarneahelast tulenevaid riske ning magistritöö fookuses olevad tarneahela ründevektoreid.

Tabel 8. Kategooria „tarneahela olemus ja selle kaitse vajadus“ koodid (NVivo faili põhjal autori koostatud)

Kood: tarneahela mõiste

Tarneahela olemuse parimaks mõistmiseks on vaja tarneaheahelat defineerida. Selleks kasutati alamkategooria koodi „tarneahela mõiste“. Dokumentide ST 7, ST 8 ja RV 8 tähenduses on **tarneahel** protsesside, organisatsioonide ja ressursside kogum, mis on seotud lõpptoodete tarnimisest tootjast kasutajani. **Tarneahel** koosneb paljudest elementidest, millega tuleb arvestada ahela turvalisuse tagamisel. Nendeks võivad olla näiteks organisatsioonid, tööriistad, mida kasutatakse süsteemide ja süsteemikomponentide projekteerimiseks, tootmiseks, hankimiseks, tarnimiseks, integreerimiseks ja hooldamiseks (ST 7).

RV 8 täpsustab (p. 6), et tarneahelas on neli peamist komponenti:

- tarnija – üksus (võivad olla üksikisikud, isikute grupid ja organisatsioonid), mis pakub toodet või teenust;
- tarnija varad – elemendid, mida tarnija kasutab toodete või teenuste pakkumiseks;
- klient - üksus, mis tarbib tarnija tooteid või teenuseid;
- kliendi varad – rünnaku eesmärgiks olevad inimesed, riist-ja tarkvara, dokumendid, raha jne.

Selline jaotus võimaldab selgelt näidata, kuidas toimub tarneahelarünnak, mis on oma olemuselt kombinatsioon vähemalt kahest rünnakust. Esimene rünnak toimub tarnija vastu eesmärgiga pääseda ligi tema varadele. Teine rünnak on kliendi vastu (RV 8). Kusjuures rünnatav klient võib olla lõppeesmärk või vaheetapp lõppeesmärgini jõudmiseks. On oluline

aru saada, et üksik küberrünnak ei ole tarneahelarünnak, kuid sellest võib tulevikus saada tarneahealarünnak. See tähendab, et edukas üksik küberrünnak võimaldab jätkurünnakute läbiviimise mööda tarneahelat, mis toob kaasa ohvrite arvu ja nende kahju suurenemise.

Mida rohkem osapooli on tarneahelasse kaasatud, seda rohkem on komponente, mida võib rünnata. Siinjuures on oluline märkida, et tarneahelarünnaku oht algab toodete tootmisest ja või teenuste ostmisest ning säilib kogu nende elukaare jooksul (ST 7, ST 8, RV 13). Sellest tulenevalt peavad organisatsioonid selgelt mõistma oma tarneahelaid. Ilma tõhusa tarneahela juhtimise ja kontrollita on raske hallata riske, mis tulenevad tarneahelasse kaasatud elementidest ja komponentidest (RV 1, ST 3, ST 6).

Kood: **tarneahela mõju**

Järgmisena kasutati kood „tarneahela mõju“. Tarneahelarünnaku eesmärgid on samad, mis teiste küberrünnakute puhul. Konfidentsiaalsuse, terviklikkuse või käideldavuse kao tekitamine eesmärgiga avaldada negatiivset mõju ettevõtte missioonidele (ST 7, ST 8). Selle mõju ulatub teenuse taseme langusest, mis põhjustab klientide rahulolematust, kuni intellektuaalomandi varguseni või kriitilise missiooni ja äriprotsesside halvenemiseni (ST 7). Tarneahelarünnakud võivad mõjutada korraga paljusid kliente erinevatest riikidest (RV 1, RV 2) ja sektoritest (RV 1, RV 2) ning nendel võib olla pikk avastamise periood. ST 8 Tarneahelarünnaku eriliseks mõjufaktoriks on asjaolu, et ohver (RV 8 terminoloogias „klient“) isegi ei saa aru, et teda rünnatakse või avastab rünnaku alles aastate pärast. Näitena või tuua olukorra, kus kliendi süsteemid suhtlevad varem kontrollitud ning seetõttu usaldusväärsete süsteemidega, kuid uue tarkvarauuendusega toimub pahavara installeerimine. RV 10 toob välja, et eduka tarneahelarünnaku teostamiseks võib kasutada riist- ja tarkvarakomponente, mida ei peeta kõrge riskiastmega komponentideks. NotPetya küberrünnak on hea näide, kuidas raamatupidamise tarkvarast sai suuremahuline rahvusvahelise mõjuga tarneahelarünnak (käesolev töö lk 17).

Kood: tarneahela riskid

Tarneahelast tulenevaid riske on mainitud neljateistkümnes dokumendis (EE 1, EE 5, RV 1, RV 5, RV 8, RV 10 -RV 13 ning ST 3 – ST 8). Vastavalt esinenud vastetele võib riske kategoriseerida nelja näitaja alusel:

Ohustatud valdkonnad

EE 1 toob esile, et Eesti on kõrgelt arenenud digiühiskond, mis erinevalt paljudest teistest riikidest sõltub juba igapäevaselt eluliselt digiteenustest (lk 7). See tähendab, et rünnaku sihtmärgiks võib sattuda ükskõik milline era- ja/või avaliku sektori asutus, organisatsioon või üksikisik. Samas ei ole tegemist Eesti-sisese probleemiga. Tarneahela komponentide usaldusväärsuse tagamist peetakse oluliseks ka NATO-s (RV 11), kusjuures enne usaldusväärsuse kontrolli teostamist käsitab NATO igat tema süsteemiga ühendatud süsteemi esialgu ebausaldusväärsena (RV 9). Dokumendist RV 1 nähtub, et tarneaheturvalisuse tagamine ja tarneahelate riskide hindamine on oluline ülesanne kogu Euroopa Liidus. Dokumendis (RV 1) on nimetatud 11 kriitilise tähtsusega valdkonda (tabel 9).

Tabel 9. Kriitilise tähtsusega valdkonnad (autori koostatud)

Valdkond	Alamvaldkond
Energeetika	• Elekter; • Kaugküte- ja jahutus; • Nafta; • Gaas; • Vesinik.
Transport	• Lennutransport; • Raudteetransport; • Veetransport; • Maanteetransport.
Pangandus	
Finantsturutaristud	
Tervishoid	
Joogivesi	
Reovesi	
Digitaristu	
IKT-teenuste haldamine (ettevõtete vaheline)	
Avaliku halduse üksused	
Kosmos	

Rünnaku eesmärk

Dokumendianalüüsiks valitud dokumentide järgi on kõige populaarsemateks tarneahelarünnaku eesmärkideks andmete vargus (mainitud dokumentides RV 3, RV 13, ST 7, RV 10) ning ligipääs ja kontrolli omamine ohvri süsteemide ja võrkude üle (RV 13, ST 7,

ST 8). Kontroll süsteemide üle on vajalik teenuste tagamise tõkestamiseks või täielikuks katkestamiseks (nt rünnak Ukraina energiasektori vastu). Lisaks sellele võib eesmärgiks olla andmevahetuse katkestamine (EE 5), andmete muutmine ja kustutamine või nende krüpteerimine lunaraha välja pressimiseks (RV 10). Eraldi eesmärgina tuuakse välja saadud andmete edastamine luureasutustele ja spionaaž (RV 10, ST 7).

Rünnaku teostaja

Võrreldes muude tüüpide küberrünnakutega on tarneahelarünnakud keerulisemad ja nõuavad rohkem ressursse. Sellest tulenevalt seostatakse tarneahelarünnakuid eelkõige riiklike või riikide poolt rahastatud küberrühmitustega (RV 1, RV 8, RV 13). Seda kinnitab ka RV 13-s toodud (p. 70) 2020. aasta statistika, mille kohaselt omistati 25% tarneahelarünnakutest tarkvara vastu otse riiklikele või nendega seotud küberrühmitustele. RV 8 analüüsis perioodil jaanuar 2020 – juuli 2021 toimunud tarneahelarünnakuid, mille tulemusena selgus, et 66% rünnakute taga oli riiklikud või riigi poolt rahastatud küberrühmitused. Detailsed tulemused on toodud tabelis 10.

Tabel 10 Kokkuvõtte perioodil 01.2020-07.2021 toimunud tarneahelarünnakutest (allikas RV 8, p. 21)

Ettevõtte	**Kategooria**	**Aasta**	**Mõju**	**Seotud rühmitus**
Mimecast	Tarkvara	2021	Globaalne	APT29
SITA	Lennundus	2021	Globaalne	APT41
Ledger	Plokahela tehnoloogia	2021	Globaalne	-
Verkada	Füüsiline turvalisus	2021	Globaalne	Hacktivist Group
BigNox NoxPlayer	Tarkvara	2021	Regionaalne/riigi sisene	-
Stock Investment Messenger	Tarkvara	2021	Regionaalne/riigi sisene	Thallium APT
ClickStudios	Tarkvara	2021	Regionaalne/riigi sisene	-
Apple Xcode	Tarkvara	2021	Globaalne	-
Myanmar Presidential Website	Avalik sektor	2021	Regionaalne/riigi sisene	Mustang Panda APT
Ukraine SEI EB	Avalik sektor	2021	Regionaalne/riigi sisene	-
Codecov	Tarkvara	2021	Globaalne	-
Fujitsu ProjectWEB	Pilvetehnoloogia	2021	Regionaalne/riigi sisene	-
Kaseya	Tarkvara	2021	Globaalne	REvil Group
MonPass	Usaldusteenus	2021	Regionaalne/riigi sisene	Winnti APT Group
SYNNEX	Tehnoloogia edasimüüja	2021	Regionaalne/riigi sisene	APT 29

Microsoft Windows HCP	Tarkvara	2021	Globaalne	-
SolarWinds	Pilvetehnoloogia	2020	Globaalne	APT29
Accellion	Tarkvara	2020	Globaalne	UNC2546
Wizvera VeraPort	Identiteedihaldus	2020	Regionaalne/riigi sisene	Lazarus APT
Able Desktop	Tarkvara	2020	Regionaalne/riigi sisene	TA428
Aisino	Tarkvara	2020	Regionaalne/riigi sisene	-
Vietnam VGCA	Usaldusteenus	2020	Regionaalne/riigi sisene	TA413, TA428
NetBeans	Tarkvara	2020	Globaalne	-
Unimax	Telekom	2020	Regionaalne/riigi sisene	-

Riikide mõju võib olla kaudne, sest riigiasutused, eriti eriteenistused, võivad osutada „lubamatut mõju tarnijatele ja teenuseosutajatele“ (RV 1, p. 97.), mis asuvad või tegutsevad nende territooriumil. Selle tulemusel võivad ettevõtted tekitada nende toodetes ja teenustes varjatud nõrkusi või tagauksi. Erilist tähelepanu tuleb pöörata Hiina tootjatele, sest kohalik õigusraamistik kohustab ettevõtteid ja eraisikuid teha koostööd luure ja julgeolekuasutustega (käesolev töö lk 23)

Rünnaku vektor

Kuna magistritöös püstitatud uurimisküsimustele vastamiseks ning ülesannete täitmiseks on autor otsustanud analüüsida teemat lähtuvalt neljast ründevektorist, siis dokumendianalüüsi raames otsiti tugevaid seoseid autori fookusesse valitud vektoritega, milleks on riist-ja tarkvara, haldus, alltöövõtjad ja inimfaktor. Samal ajal otsiti ka teisi potentsiaalseid vektoreid, mille kaudu võib tarneahelarünnakuid läbi viia. Selleks kasutati alamkoode „rünnaku vektorid“, „tarkvara“, „riistvara“, „haldus“, ja „alltöövõtja“. Juba dokumentide eelanalüüsimisel avastas autor, et paljudes dokumentides (nt EE 5, RV 10, RV 13 jne) on ettevõtteid ja asutusi, kes teevad koostööd või pakuvad tooteid ja teenuseid, nimetatud üldistatud terminiga partnerid. Seetõttu lisati uus alamkood „partnerid“.

Rünnaku vektori definitsiooni on toodud dokumendis ST 8 (dokumendi lisa B-1), mille kohaselt on vektor teekond, mida kasutatakse rünnaku läbiviimiseks. Sobiva vektori leidmiseks teostab ründaja luuret (käesolev töö lk 27) ning valib ründeks kõige nõrgema koha tarneahelas. Selleks hangitakse teavet erinevatest valdkondadest ning rünnakuks valitakse kõige sobivam, lihtsam või odavam võimalus. Ülevaade valdkondadest ja seosed potentsiaalsete rünnaku vektoritega

on toodud autori poolt koostatud tabelis 11. Tabeli koostamiseks kasutati dokumendis RV 8 (pp. 8–9) toodud andmeid.

Tabel 11. Rünnaku luurefaasis otsitava informatsiooni seos rünnaku vektoriga (autori koostatud)

Rünnaku ettevalmistusel/luurefaasis otsitav teave		**Seos magistritöö fookuses rünnaku vektoriga**
Turul olemasolev tarkvara	Nt rakendused, andmebaasid, püsivara, monitooringu süsteemid, viirusetõrjed jne.	Tarkvara/Alltöövõtja/Haldus
Tarkvara kataloogid	Nt kolmanda osapoole kataloogid, vabavara jne.	
Tarkvarakood	Nt juurkood või teenuse osutaja või tootja enda poolt arendatud tarkvara.	
Süsteemide seadistused	Nt paroolid, võrgureeglid, tulemüüri seadistused jne.	
Andmed	Nt informatsioon asutusest, rakendatud turvameetmetest, omandatud sertifikaatidest, koostööpartneritest, personalist jne.	Alltöövõtja/Haldus/Inimene
Protsessid	Nt infoturbepoliitika, uuenduste poliitika, käitumisreeglid, töökorralduse reeglid, testimise ja paigalduste protsessid jne	
Riistvara	Nt kasutusel olev riistvara ja selle tootjad, kiibid, välised andmekandjad jne.	Riistvara
Inimesed	Nt, inimesed ja nende rollid organisatsioonis (turvainsener, süsteemiadministraator), inimeste pääsuõigused jne.	Inimene

Toimunud tarneahelarünnakute analüüsimisel on sageli väga raske avastada rünnakuks kasutatud vektorit, sest tänapäevased ahelad on pikad ja osapoolte arv on suur. Dokumendis RV 8 toodud statistika (p. 23) kohaselt jääb teenuseosutajate vastu tehtud tarneahelarünnakute puhul rünnaku vektor avastamata 66% juhtudel ning 16% juhtudel on rünnaku vektoriks tarkvarakomponendid.

Kood: partnerid

Kategooria järgmiseks koodiks valiti „partnerid“, et uurida partneritega seotud riske. Avaliku sektori digiareng, riigiteenuste kvaliteedi tõus ning innovatsioon saab toimuda ainult koostöös erasektoriga (EE 1, EE 2). Teisest küljest suureneb väliste osapoolte kaasamisega tarneahelarünnakute maastik (ST 8). Eesti avaliku sektori asutused ja elutähtsate teenuste osutajad täiendavad pidevalt oma süsteemide ja teenuste infoturbmeetmeid ning rakendavad rahvusvahelisi ja riigisisesed infoturbestandardid (EE 1, EE 2, EE 3, RV 10, RV 11). Koostööpartnerite turbemeetmed võivad olla nõrgemad (nt turbeeskirjade puudumine või nende eiramine, standartidele mitte vastamine, ebapädev või ebausaldusväärne personal) ning seetõttu

ründaja saab keskenduda tarneahelarünnakute planeerimisel just partneritele (ST 8, RV 13). Sellest johtuvalt tuleb partneri valikul olla ettevaatlik ning mõelda põhjalikult läbi teenuste ja toodete turvalisusega seotud aspektid. Kui välise teenuseandjaga sõlmitud lepingus on osapoolte tegevused kirjeldatud puudulikult või ebaselgelt, võivad turvameetmed kas isikute teadmatuse, puuduva kvalifikatsiooni või puuduvate ressursside tõttu jääda rakendamata (EE 5, lk 609). Samuti tuleb võtta arvesse, et Eesti turul tegutsevate ettevõtete tarneahelatesse on kaasatud rahvusvahelised ettevõtted, mis võivad olla mõjutatavad vaenulike riikide poolt ning seetõttu ohustada Eesti julgeolekut (ST 7, RV 10). Sarnase tulemuseni on jõudnud ka teoorias, kus toodi välja, et Hiina tehnoloogia kasutamisega kaasnevad täiendavad riskid (käesolev töö lk 20).

Kood: tarkvara

Kolmanda kategooria järgmise koodi „tarkvara“ abil otsiti tarkvara definitsiooni ning tarkvaraga seotud riske. Dokumendianalüüsiks kasutatud dokumentide seast defineerib ainult üks dokument (RV 5) tarkvara mõistet. Selle kohaselt on tarkvara elektroonilise infosüsteemi osa, mis koosneb arvutikoodist. Tarkvara usaldusväärsuse tagamine on Eesti kontekstis väga relevantne, sest EE 1 kohaselt on üheks planeeritavaks tegevuseks digiriigi turuplatsi käivitamine ning erasektorist standardteenuste sisse ostmine. Selle tulemusel muutub riigiteenuste osutamine säästlikumaks ja kiireneb nüüdisaegsete tehnoloogiate kasutuselevõtt. See tähendab, et ostetakse valmis tarkvarakomponente, mis omakorda võivad sisaldada kolmanda(te) osapool(t)e valmistarkvara komponente või baseeruda avatud lähtekoodil. Kuna kliendil puudub ülevaade tarkvara loomise protsessi kaasatud osapooltest ning nende loodud komponentidest, siis ei saa ta olla täielikult veendunud tarkvara ohutuses. Tarkvarauuenduste paketid pannakse kokku teenuse osutaja poolt ning lõppkliendil puudub võimalus veenduda, et uuenduspaketis olevad komponendid ei sisalda turvanõrkusi. (ST 7, EE 5) Antud nõrkust võib ära kasutada ka olukorras, kus uuenduse tööriistu haldab väline partner (EE 5). RV 8 toob välja, et ca 60% rünnakutest sihistavad just tarkvarakomponente.

Tarkvara loomine on dünaamiline protsess, mis on omaette tarneahel, mille raames kasutatakse ettevõtte enda või teise ettevõtte loodud komponente ning avalikest allikatest saadud avatud lähtekoode. Siinjuures on oluline võtta arvesse avatud lähtekoodiga tarkvara laialdast kasutamist. Sellega kaasneb suur arv riske nagu pahaloomulise koodi ja tagaukse sisestamine või nullpäeva nõrkused (RV 13). Kui tarkvara enne käidukeskkonnas kasutuselevõttu piisavalt ei testita või kui puuduvad korrektsed tarkvara vastuvõtmise ja kinnitamise protseduurid, võib

vastu võetud tarkvara sisaldada turvanõrkusi ja vigu tarkvara funktsionaalsuses (EE 5, p. 2;7.). Ebaturvaline ja juurdepääsupiiranguteta arenduskeskkond võimaldab selle arendajal ja selleks volitamata isikutel tarkvara manipuleerida või vead võivad tulla inimlike eksimuste tõttu (EE 5, ST 8, ST 13). RV 13 toob välja, et ründajad ei oota enam turvanõrkuste avalikustamist, vaid haaravad initsiatiivi, et lisada uusi turvaauke avatud lähtekoodiga projektidesse, mis toetavad ülemaailmset tarkvara tarneahelat ja seejärel kasutavad neid turvaauke ära (RV 13, p. 38).

Seega, tarkvara kasutamise suuremaks probleemiks on selle arendamisprotsessi läbipaistmatus ja kontrollimatus. Selle tagajärjel võib tarkvara sisaldada mitteteadaolevaid ning dokumenteerimata funktsioone, mida ründaja võib ära kasutada (EE 5).

Kood: riistvara

Riistvarast tulenevate riskide määratlemiseks kasutati koodi „riistvara“. Riistvara on füüsiline elektrooniline infosüsteem või selle osad, mis suudavad digitaalseid andmeid töödelda, talletada või edastada (RV 5). Riistvarast tulenevad riskid tulenevad eelkõige selles sisalduvatest tagaustest või dokumenteerimata funktsionaalsusest (RV 8). Sellised nõrkused ei ole kasutajatele nähtavad ja seetõttu on raskesti avastatavad testimis- ja sertifitseerimisprotsessi raames (RV 13, EE 5). Sarnaselt tarkvaraarendamisega, on riistvara tootmisesse kaasatud palju osapooli (RV 8), mis muudab riistvara tootmise ja haldamise elukaare jooksul (RV 11) läbipaistmatuks ja raskesti kontrollitavaks. Äripartneri kontrollimise protsessi raames märkamata jäänud nõrkused võimaldavad teostada rünnakuid kliendi vastu isegi olukorras, kus kliendil on rakendatud vajalikud turvameetmed (käesolev töö lk 27).

Kood: haldus

Kolmanda kategooria eelviimaseks koodiks on „haldus“. Avalikus sektori pakutavate teenuste riist- ja tarkvara haldab üldjuhul väline partner. Halduriks võib olla teenuse arendaja ise või tema poolt volitatud füüsiline- või juriidiline isik. Käesoleva töö kontekstis tähendab haldus teenuseks vajaliku infosüsteemi ning riist- ja tarkvara komponentide hooldamist, uuenduste installimist, komponentide välja vahetamist, seadistamist, administreerimist, komponentide utiliseerimist ning protsessidega seotud infovoogude juhtimist. Halduse teema muutub aina aktuaalsemaks, sest sisse ostetavate teenuste arv Eesti avalikus sektoris kasvab (EE 1, EE 2). Samal ajal on oluline tagada, et erasektori poolt pakutavad teenused oleksid turvalised ning ei seaks ohtu riigi julgeolekut ja elutähtsaid teenuseid (EE 3).

Dokumendid EE 5, ST 7 ja ST 8 kohaselt peetakse halduse nõrkusteks:

- Haldusprotsessi raames ebaturvaliste komponentide lisamise võimalust. Kliendil puudub võimalus detailselt kontrollida uuenduse sisu või uuendus toimub klienti teavitamata.
- Haldustööriistade ebaturvalisust või nende kaaperdamist ründaja poolt. Kui ründaja suudab tsentraalsed paiga- ja muudatusehalduse tööriistad üle võtta, saab ta levitada manipuleeritud tarkvara ühekorraga paljudesse IT-süsteemidesse (EE 5., lk 180). On oluline pidada silmas, et haldustööriist ise võib olla turvaline, kuid selle kasutamise viis viib riskide realiseerumiseni. Nt ebaturvalise autentimismehhanismi kasutamine, võrguliikluse mitte krüpteerime, avalike võrkude kasutamine, haldustööriista valeseadustus jpt võivad kaasa tuua volitamata juurdepääsu käidutehnoloogia komponentidele või taristule (EE 5).
- Haldusõiguste kuritarvitamist. Kui haldusõigused on dokumenteerimata (puuduvad reeglid kellele, millal, millise infole või funktsioonidele juurde pääseb) või lubatakse liiga laiad õigused, siis esineb õiguste kuritarvitamise risk. Näiteks uue konto loomine ning edastamine kolmandatele osapooltele, süsteemi volitamata turvaseadistuste muutmine, andmete kopeerimine/kustutamine või ligipääs tundlikule informatsioonile, mis põhjustab konfidentsiaalse teabe lekke.

Kood: personal

Kolmanda kategooria „tarneahela olemus ja selle kaitse vajadus“ viimase koodi „personal“ fookuses on potentsiaalsed riskid, mis tulenevad tarneahelasse kaasatud osapoolte personalist. Inimfaktorit kui potentsiaalset ründevektorit on mainitud kokku 7 dokumendis: EE 5, RV 11, RV 12, RV 13, RV 9, ST 3, ST 1, ST 7. Kuna inimfaktorit on osaliselt käsitletud eelmiste ründevektorite juures (personal, tarkvara ja haldus), siis käesolevas lõigus tuuakse välja seni kajastamata aspekte. Lisaks eelpoolmainitud protsessidesse kaasatud inimestele (tarkvaraarendus, haldus), võivad riskid tulla kliendi enda personali või tema organisatsiooni tööprotsessidesse kaasatud inimeste poolt. Kliendi töötaja võib tahtlikult või tahtmatult avaldada informatsiooni organisatsioonis või teenuses rakendatud turvameetmest, avalikustada tundlikku informatsiooni ning võimaldada ligipääsu ründajale (EE 5, ST 7, RV 12). EE 5 toob välja lisaks riski, mis tuleneb organisatsiooni külastajatest, koristajatest ja muudest kaasatud välistest töötajatest. Näitena tuuakse dokumentide ja IT-seadmete vargus, töötaja seadmetesse sisse logimist, nendesse pahavara installimist või asutuse infosüsteemide töö häirimist (arvuti, serveri või muu seadme välja lülitamine).

Võttes arvesse, et inimene on peamine sihtmärk rünnaku planeerimisel (käesolev töö lk 12) ning inimfaktorit on mainitud korraga mitme ründevektori juures, järeldab magistritöö autor, et tegemist on ühe olulisema ründevektoriga, millega tuleb arvestada IKT tarneahela usaldusväärsuse tagamisel.

Neljas kategooria: soovitused riskide maandamiseks

Viimases kategoorias (tabel 12) on seitse koodi, mis keskendusid soovitustele riist- ja tarkvarast, haldusest, alltöövõtjast ja inimfaktorist tulenevate riskide maandamiseks.

Tabel 12. Kategooria „soovitused riskide maandamiseks“ koodid (NVivo faili põhjal autori koostatud)

Dokumendianalüüsi viimases osas, kategooriaga „soovitused riskide maandamiseks“; uurib magistritöö autor dokumentides esinevaid soovitusi IKT tarneahela riskide maandamiseks ning selle komponentide usaldusväärsuse tagamiseks. Analüüsi teostamisel kasutati koode „alltöövõtja“, „haldus“, „partner“, „personal“, „riistvara“, „tarkvara“ ja „riskianalüüs“. Selguse huvides täpsustab autor, et dokumendianalüüsi eesmärgiks oli magistritöö eesmärgist ja uurimisküsimustest lähtuvalt otsida praktilisi soovitusi tarneahela usaldusväärsuse (nt usaldusväärsuse tõhustamiseks mõeldud protsessid jne) tagamiseks, mitte kaardistada spetsiifilisi tehnilisi meetmeid (nt süsteemide konkreetsed seadistused, turvaprotokollid jne).

Kood: riskianalüüs

Koodi „riskianalüüs“ päringu tulemused on kajastatud dokumentides RV 1, RV 2, RV 6, RV 8, RV 13 ja ST 3 - ST 8. IKT tarneahealast tulenevate riskide hindamiseks ning nende maandamiseks soovitavad kõik dokumendid kehtestada tarneahela riskijuhtimise protsessi. Riskijuhtimise protsess koosneb riskide kaardistamisest (riskianalüüs), maandamismeetmete

väljatöötamisest ja nende rakendamisest ning tõhususe hindamisest. Selle raames töötatakse välja sobivad reageerimisstrateegiad, poliitikad, protsessid ja protseduurid tarneahela riskide haldamiseks (ST 7). RV 1 ja RV 6 soovitavad samuti Euroopa Liidu riikidel rakendada riskijuhtimise protsessi, koostada riskianalüüse ning teha selles valdkonnas koostööd nii riikide tasandil kui ka küberturvalisuse eest vastutavate asutuste vahel. RV 6 pakub välja riskianalüüsi definitsiooni, Mille kohaselt on riskianalüüs üldine protsess, mille eesmärk on määrata kindlaks riski olemus ja ulatus, tehes kindlaks intsidendini viia võivad võimalikud asjakohased ohud ja nõrgad kohad, analüüsides neid ohte ja nõrku kohti ning hinnates sellest intsidendist tingitud potentsiaalset elutähtsa teenuse osutamise katkemist või häiret (RV 6., lk 176).

Soovituste kohaselt (RV 1, RV 2, RV 8, RV 13) tuleb IKT tarneahela riskide maandamiseks igal liikmesriigil kirjeldada IKT tarneahelad (protsessid, tarnijad, partnerid), jäädvustada riske, mis tulenevad kasutatavast tehnoloogiast, partnerist tulenev geopoliitiline oht, puudulikud protsessid ja normid ning rakendada vastumeetmeid. Selle raames on oluline proaktiivne komponent, ehk riskihindamine algab enne partneri valimist ning temaga lepingu sõlmimist (ST 3). Riskijuhtimise protsessi peab toetama vastav õigusraamistik ja toodete ja teenuste hindamismehhanismid (ST 6). Lisaks sellele tuleb kaasata ka partnerasutusi (RV 1, RV 2, RV 8). Selleks võivad olla julgeolekuasutused, kes aitavad teostada taustakontrolli ja hinnata geopoliitilisi ohte, teised riigiasutused, kelle ülesanneteks on riigiülese küberjulgeoleku tagamine (Eesti kontekstis on selleks asutuseks Riigi Infosüsteemi Amet) või EL ja NATO partnerid.

Organisatsiooni sees ei ole tarneahela riskijuhtimine ühe osakonna või üksikisiku ülesanne. Igas organisatsioonis peab olema rakendatud struktuur, mis koosneb tarneahelaga seotud ekspertidest. Nii soovitab ST 3 luua tarneahela nõukogu, mille töösse kaasatakse vajalike eksperte. ST 7 pakub kolmetasandilist vertikaalset struktuuri:

1. Tasand (tippjuhtkond). Määrab strateegilisi eesmärke, strateegiat, poliitikaid ja rakendusplaani.
2. Tasand (eesmärgid ja äriprotsessid). Keskastme tarneaheala riskijuhtimise strateegiad, poliitikad ja rakendusplaanid, mida kohandatakse konkreetse eesmärgiga ja äriprotsessiga.
3. Tasand (operatiivne). Äri- ja tehniliste nõuete koostamine ja hindamismehhanismide välja töötamine ning nende rakendamine.

Kokkuvõtvalt võib öelda, et tarneahela riskide juhtimiseks tuleb organisatsioonil luua toimiv mehhanism, mis kaardistab organisatsioonis kasutatavad tarneahelad ja nende komponenndid, koostab strateegilisi dokumente, monitoorib ja hindab seotud riske, töötab välja riskide maandamise meetmeid ning viib neid ellu. Oluliseks aspektiks on pidev riskiteemaline infovahetus teiste partnerasutustega nii riigi siseselt kui ka väliselt.

Koodid: partner, haldus, alltöövõtja

Dokumendianalüüsi raames ilmnes, et soovitused koodide „alltöövõtja“, „haldus“ ja „partner“ kohta on suures mahus sarnased. Sellest tulenevalt otsustas magistritöö autor kirjeldada neid ühes alampeatükis.

Tarneahelas osalevast partnerist tulenevate riskide maandamisel on kaks olulist aspekti, millega iga organisatsioon peab arvestama (EE 5, ST 6, RV 8). Esiteks, kliendi nõuded teenuste ja toodete küberturvalisuse tagamiseks. Teiseks on partneri enda ja tema alltöövõtjate küberturvalise meetmed, mille abil ta suudab tagada pakutava teenuse usaldusväärsust (ST 6, RV 11).

Kliendi üldised nõuded tarnijale ja ostetavale teenusele tuleb määratleda juba hankedokumentatsiooni koostamisel. Selle raames tuleb võtta arvesse (EE 5, ST 3, ST 6, RV 8, RV 11, RV 13):

- kuidas tarnija arendab, uuendab ning haldab toodet või teenust kogu elutsükli jooksul, sealhulgas milline on toote ja teenuse või nende komponentide käitlusest maha võtmise protsess;
- klassifitseerida varad ja teave, mida jagatakse partneriga või millele antakse juurdepääsu ning leppida kokku vastavad protseduurid ja reeglid;
- määratleda partneri kohustused organisatsiooni varade kaitsmisel, teabe jagamisel, talitluspidevusel, personali läbivaatamisel ja intsidentide käsitlemisel (vajadusel sõlmida konfidentsiaalsuse leping);
- sätestada toodete ja teenuste turvanõuded sh määrata standardid, millele teenus või toode peab vastama (vajadusel võib usaldusväärsuse tõendamiseks paluda toodete või teenuste sertifitseerimist sõltumata sertifitseerimisasutuse poolt);
- lisada kõik need kohustused ja nõuded lepingutesse;
- leppida kokku alltöövõtu lubatavus ning kokku lepitud reeglite rakendatavus alltöövõtjale;

- leppida kokku reeglites, mille alusel kliendil võimaldatakse jälgida toodete ja teenuste loomise protsessi, nende toimivust, teostada turvaauditeid, et kontrollida lepingutes sätestatud küberturvalisuse nõuetest kinnipidamist (partnerite regulaarne kontroll aitab hallata kübertarneahela riske, st teha kindlaks, kas kokkulepitud nõuded on täidetud, tuvastada võimalikud lüngad ja nõuda nende parendamist);
- nõuda tarnijatelt ja teenusepakkujatelt kinnitust, et teadlikult ei sisalda nende toode/teenus varjatud funktsioone ega tagauksi;

Lisaks sellele tuleb kliendil teostada valitud partneri ja tema poolt määratud võtmeisikute (nt administraatorid, haldurid jne) taustakontroll. Partneri usaldusväärsuse hindamisel võetakse arvesse muuhulgas tema päritolu ning tema potentsiaalne mõjutatavatus kolmandate riikide valitsusasutuste poolt (RV 1).

Omalt poolt peab tarnija informeerima klienti järgmistest aspektidest:

- kuidas toimub tema organisatsioonis ja tema partneritel toodete ja teenuste kavandamine ja arendamine (tootearendusprotsess), hooldamine, uuendamine ja kasutusest maha võtmine;
- milline on riskijuhtimise- ja infoturbepoliitika, millised infoturbereeglid ja kuidas on rakendatud;
- vajadusel esitama omandatud turvasertifikaate;
- mis regulaarsusega ja milliseid auditeid tehakse ning esitama eelmiste auditite raporteid;
- kuidas toimub personali taustakontroll.

Kood: personal

Kategooria „soovitused riskide maandamiseks“ koodi „personal“ alla on koondatud kõikide tarneaheales osalevate osapoolte heaks töötavad inimesed, sh ka need, kes otseselt ei osale toote või teenuse osutamise protsessis, nagu koristajad, audiitorid, külalised, hoone hoolduspersonal jne. Personali usaldusväärsuse hindamise vajadust on kirjeldatud dokumentides EE 5, RV 8, RV 11, RV 12 ja ST 8, mis tähendab, et seda peetakse oluliseks nii Eesti, Euroopa Liidu kui ka NATO tasandil.

Personali taustakontrolli protsess peab olema kavandatud nii, et oleks võimalik teha kindlaks, kas isik on lojaalne ning piisavalt usaldusväärne, et lubada temale juurdepääs organisatsiooni protsessidele ja informatsioonile ilma, et see kujutaks endast lubamatut julgeolekuriski (RV

12). See tähendab, et igas organisatsioonis peab olema kirjeldatud taustakontrolli protsess ning määratud vastutajad (RV 8, RV 11). Üldjuhul viiakse inimese taustakontroll läbi enne tema tööle võtmist (EE 5), vajadusel saab määrata täiendavat taustakontrolli olukorras, kus inimene vahetab rolli (nt liigub IT-abist IT-administraatori positsioonile) või talle antakse täiendavad õigused (ST 8). Kuid sellega taustakontrolli protsess ei lõpe, sest tööandja peab tagama isiku jätkuva sobivuse tema ametikohale, mida on võimalik tagada regulaarsete hindamistega. Nende raames hinnatakse inimese käitumise muutust, toimunud intsidente ning kas varem antud õigused on endiselt vajalikud (RV 12).

Üldjuhul viib partneri töötajate taustakontrolli läbi partner ise, kuid oluliste teenuste puhul peab klient enne partneri töötajale õiguste andmist läbi viima taustakontrolli vastavalt enda organisatsioonis kehtestatud reeglitele (EE 5).

Kood: riistvara

Kood „riistvara“ aitas leida meetmeid riistvarast tulenevate riskide maandamiseks. Tarneahelas kasutatava riistvara usaldusväärsuse tagamiseks tuleb jälgida, et riistvara komponendid (nt kiibid koos püsivaraga) oleksid toodetud usaldusväärse tootja poolt (EE 1, RV 11, RV 13, ST 1, ST 5), sh arvestades geopoliitilise olukorraga (RV 1). Eriti oluline on jälgida seda oluliste teenuste puhul (RV 11). Klient, teenuse osutaja ja riistvara tootja peavad pidevalt jälgima riistvara teadaolevaid nõrkusi ja vajalikke uuendusi. Turvanõrkused parandatakse esimesel võimalusel. Kui turvanõrkust ei ole võimalik parandada (nt uuendused ei ole kättesaadavad), siis tuleb rakendada täiendavaid turvameetmeid (EE 5).

Dokumendid EE 5, RV 11 ja ST 8 annab soovitusi, kuidas peab toimuma ohutu uue riistvara kasutuselevõtt. Enne riistvara kasutuselevõttu tuleb seda testida spetsiaalselt selleks otstarbeks loodud ja käidukeskkonnast eraldatud testkeskkonnas. Selle raames kontrollitakse toote funktsionaalsust, ühilduvust ja soovimatute kõrvaltoimete puudumist. Kõik testimise tulemused dokumenteeritakse. Täiendava meetmena pakutakse välja nõue riistvara sertifitseerimist sõltumatu ja rahvusvaheliselt tunnustatud sertifitseerimisasutuse poolt (RV 5, RV 11). Riistvara hoitakse ajakohasena konfiguratsioonihalduse ja muudatuste juhtimise kaudu kogu elutsükli jooksul (RV 11, p 16).

Kood: tarkvara

Järgmiseks koodiks valiti „tarkvara“, et leida lahendus tarkvaraga seotud riskide minimeerimiseks. Dokumendianalüüs näitas, et tarkvara puhul kehtivad ka riistvara peatükis toodud soovitused (usaldusväärne tootja, nõrkuste monitooring, testimine, sertifitseerimine). Võrreldes riistavara testimisega, toimub tarkvara testimine mitte üksnes enne selle paigaldamist, vaid perioodiliselt kogu arendusprotsessi jooksul. Lisaks tuleb koostöös partneriga hinnata, millist tarkvaraarendusmetoodikat kasutatakse, milline on süsteemi arhitektuur ja kavandatava süsteemi funktsionaalsed nõuded. Sellest tulenevalt tuleb valida sobivad turvameetmed ja arenduskeskkond. Tarkvara arendamisel, paigaldamisel, uuendamisel ja turvameetmete rakendamisel tuleb lähtuda rahvusvahelistest standartidest ning parimatest praktikates (EE 5, RV 11, RV 13, RV 8, ST 3, ST 8). Ideaalolukorras suudab klient luua reaalajas nähtavuse partneri arendusprotsessi üle, mis võimaldab tuvastada defekte ning ennetada vigu ja rikkeid (ST 3).

Kuna tarkvara arendamisel kasutatakse kolmandate osapoolte loodud või avatud lähtekoodi, siis protsessi läbipaistvuse tagamiseks soovitatakse (RV 13, ST 3, ST 7) kasutada tarkvara materjalide loendit, ehk TML-i (ingl *Software Bill of Materials*). TML annab ülevaate tarkvara arendusprotsessis kasutatud komponentide päritolu kohta ja võimaldab näha koodi ning hinnata selle kvaliteeti ja turvalisust (RV 13, p 68).

Kokkuvõttes võib öelda, et tark- ja riistvara usaldusväärsuse tagamiseks tuleb organisatsioonil koostada ning rakendada vastavad protsessid, mis lähtuvad standarditest ja parimatest praktikatest.

2.3 Ekspertintervjuude kokkuvõte ja analüüs

Käesolevas alapeatükis käsitletakse läbi viidud intervjuusid ning antakse ülevaade intervjuude tulemustest. Intervjuudes osales kuus eksperti. Detailne ülevaade kaasatud ekspertidest, nende tegevusvaldkondadest ning intervjuudega seotud tehnilistest detailidest on toodud tabelis 13. Intervjuud viidi läbi kas füüsiliselt eksperdi töökohas või digitaalselt MS Teams keskkonnas.

Tabel 13. Intervjuus osalenud eksperdid (autori koostatud)

Eksperdi kood	**Valdkond**	**Intervjuu aeg ja kestus**	**Intervjuu keskkond**
Ekspert 1	Riigi Info- ja Kommunikatsioonitehnoloogia Keskus	27.01.2023, 29 minutit	MS Teams
Ekspert 2	Tervishoiuasutus	10.02.2023, 53 minutit	Füüsiline kohtumine
Ekspert 3	Majandus-ja Kommunikatsiooniministeerium	09.02.2023, 35 minutit	MS Teams
Ekspert 4	Telekommunikatsiooni ettevõte	06.03.2023, 49 minutit	Füüsiline kohtumine
Ekspert 5	Tervise ja Heaolu Infosüsteemide Keskus	03.03.2023, 26 minutit	Füüsiline kohtumine
Ekspert 6	Riigi Infosüsteemi Amet	10.04.2023, 43 minutit	Füüsiline kohtumine

Intervjuude raames saadud andmete analüüsimiseks kasutati suunatud kodeerimist, mille raames loodi kaks kategooriat: **tarneahela ohud** ja **soovitused ohtude maandamiseks.** Kategooriate seosed uurimisküsimustega on toodud tabelis 14. Iga kategooriat jagati koodideks. Esimeses kategoorias on viis koodi. Koodide „alltöövõtjad“, „haldus“, „riist-ja tarkavara“ ja „inimene“ abil uuriti ekspertide hinnanguid konkreetsete ohtude kohta. Koodiga „tarneahela oht“ uuriti kui suureks ohuks peetakse tarneahelat tervikuna. Teises kategoorias on neli koodi: „alltöövõtjad“, „haldus“, „riist-ja tarkavara“, „inimene“. Võrreldes esimese kategooriaga, teises kategoorias ei ole kood „tarneahela riskid“ kasutusel. Selle põhjenduseks on asjaolu, et nelja ohu maandamisel on võimalik minimeerida tarneahela riske tervikuna. Detailne ülevaade koodipuust ja vastete esinemise sagedusest on esitatud tabelis 15.

Tabel 14. Intervjuu kategooriate seos uurimisküsimustega (autori koostatud)

Uurimisküsimus	**Kategooria**
Millised on võimalikud riist-ja tarkvarast ning selle haldamisest, alltöövõtjatest ning ettevõtte ja avaliku sektori asutuse personalist tulenevad ohud riigi IKT tarneahelale?	Tarneahela ohud
Kuidas ja milliste kriteeriumite alusel oleks riigi IKT asutustel võimalik hinnata ja kontrollida kasutatava riist- ja tarkvara, riiklike ja riigi seisukohast oluliste infosüsteemide arendus- ja hooldusfirmade usaldusväärsust?	Soovitused ohtude maandamiseks
Kuidas ja millistel alustel oleks riigi IKT asutustel võimalik teostada usaldusväärsuse kontrolli alltöövõtjate ja nende personali üle?	Soovitused ohtude maandamiseks
Kuidas ja milliste kriteeriumite alusel oleks riigiasutustel ja nende valitsemisalas olevatel juriidilistel isikutel võimalik välistada riigihangetest ebausaldusväärseid pakkujaid?	Soovitused ohtude maandamiseks

Tabel 15. Intervjuude koodipuu (NVivo faili põhjal autori koostatud)

Name	Files	References
Tarneahela oht		
Tarneahela oht	6	13
Riist-ja tarkvara	6	13
Inimene	6	22
Haldus	6	13
Alltöövõtjad	6	29
Soovitused ohtude maandamiseks		
Riist-ja tarkvara	6	19
Inimene	6	12
Haldus	6	9
Alltövõtjad	6	24

Kuigi mõlemat kategooriat analüüsiti eraldi, siis analüüsi tulemuste esitamisel toodi iga esimese kategooria ohu kohta soovitused ohu maandamiseks. Selline lähenemine võimaldab lihtsamini tutvustada nii esimeses kategoorias analüüsitud ohte, kui ka teises kategoorias toodud meetmeid ohtude maandamiseks.

Intervjuude raames küsiti ekspertide hinnanguid selle kohta, kui tõenäoliseks peavad nad rünnakut tarneahela vastu nelja vektori kaupa ning kui suur on rünnakuga seotud risk. Hinnangu andmiseks paluti kasutada 5-palli skaalat, kus 1 tähendab väga madalat riski ja 5 tähendab, et risk on väga suur. Vahepealsesse skaalasse jäävad 2- madal, 3 – keskmine, 4 – suur. Detailne ülevaade saadud vastustest on toodud tabelis 16. Autor juhib tähelepanu, et ekspert 3 ei ole igat vektorit eraldi hinnanud. Selle põhjuseks oli asjaolu, et kõik sõltub asutuses rakendatud maandamismeetmetest.

Tabel 16. Ekspertide hinnang rünnaku tõenäosuse vektorite kaupa (autori koostatud)

		Tarneahela rünnaku risk	**Vektor**			
			Riist-ja tarkvara	Haldus	Alltöövõtjad	Inimfaktor
Ekspert 1	Riski tase	3-4 vahel	2	1	4	4
Ekspert 2		3	2	3	2	5
Ekspert 3		4/5 vahel	-	-	-	-
Ekspert 4		3	2	2	2	5
Ekspert 5		2	2	2/3	3	5
Ekspert 6		3	4	3	2/3	3/4

Kategooria: Tarneahela oht, kood: tarneahela risk

Intervjuudes toodud tarneahela riskide kaardistamiseks valiti kood „tarneahela risk“. Enamus eksperte hindavad tarneahelast tulenevaid riske pigem keskmiseks või suureks. Sama ekspert 5 hinnangul on tarneahela risk keskmisest madalam, kuid ta märgib, et „*Kui ta sisse satub, siis mõju on kõrge*“. Ekspert 3 toob välja, et „*Tarneahel on kõige rohkem olulisust kavatanud ründevektor, ründeviis viimase paari aasta jooksul, kuid head lahendust ei ole mitte ühelgi riigil*“. Ekspert 4 leiab, et juhul kui tema organisatsioonis ei oleks rakendatud vastavad riskimaandamise mehhanismid, siis oleks tarneahela risk suurem. Kõik eksperdid tõid välja, et tarneahela riskid kogumina on piisavalt kõrged ning nendega tuleb tegeleda. Ekspertide hinnang ühtib käesoleva magistritöö teooria osaga, mille kohaselt kõik organisatsioonid peavad mõistma oma tarneahelaid ning juhtima tarneahelatest tulenevaid riske (käesolev töö lk 26).

Kategooria: Tarneahela oht, kood: riigi tähelepanu

Esimese kategooria järgmiseks koodiks valiti „riigi tähelepanu“, et uurida kuidas ja mis määral riik pöörab tähelepanu tarneahela ohtudele. Ekspertide hinnangul pööratakse riigi tasandil piisavalt palju tähelepanu tarneahela riskidele. Ekspert 6 lisas, et „… *see* (tarneaheala teema, autor) *tuleb ka väga palju konsultatsioonidel meie partnerriikidega meie liitlastega nii Euroopa liidus kui NATO-s*“. Ekspertide hinnang ühtib käesoleva magistritöö teooria ja dokumendianalüüsi osaga, kus tuuakse välja EL ja NATO tasandil toimuvat küberjulgeoleku sh tarneahela julgeolekustamise protsessi (käesolev töö lk 14) ning rõhutatakse koostöö vajadusele erinevate organisatsioonide vahel (käesolev töö lk 40).

Näitena tuuakse riigipoolsed **soovitused** riskide maandamiseks riigihangete korraldamisel, kuid ekspertide (eksperdid 1, 2 ja 5) hinnangul on tegemist pigem üldise soovitustega või riskidele tähelepanu juhtimisega (nt geopoliitilised ohud ning sellega seotud ebausaldusväärsele tehnoloogiale) ning asutused peavad ise otsustama, mida teha. Samas tunnistatakse (eksperdid 1, 2, 3, 4 ja 6), et head tööriista tarneahelariskide maandamiseks ei ole ning asutused peavad ise rakendama vastavaid meetmeid.

Kategooria: Tarneahela oht, kood: inimene

Inimfaktorist tulenevaid riske analüüsiti koodi „inimene“ abil. On oluline juhtida tähelepanu, et magistritöö teoreetilises käsitluses on inimest samuti nimetatud suurimaks riskifaktoriks (käesolev töö lk 12), mis oli kinnitatud ka statistikaga, mis näitas, et üle 80% küberintsidentide põhjustajaks on inimene. Dokumendianalüüs näitas (käesolev töö lk 53), et inimfaktori risk

võib tulla kliendi ja koostööpartneri personalist ning esineda kas eraldi, või koos teise riskiga (nt arendaja tahtlikult sisestab pahavarakoodi). Ekspertide vastustest samuti selgub, et kõige riskantsemaks tarneahelarünnaku vektoriks peetakse inimfaktorit (tabel 16) ning kaasnevaid riske on väga keeruline maandada. Seega, kinnitab nende hinnang teoreetilises käsitluses ja dokumendianalüüsis toodut. Eksperdid tõid välja, et:

„*Üks selline raskesti maandatav ja kõrge riskiga vektor.“* (ekspert 1)

„*Tegelikult vot see on, ma arvan, on kõige-kõige suurem risk. See on meie asutuses riskidest kõrgeks hinnatud. Ja, …paratamatu on see, et sa ei saa nagu midagi muud teha, kui seda mõju vähendada*“ (ekspert 2)

„*Ta* (inimene, autor) *on kõige olulisem lüli, mis tuleb tugevaks teha. Et sa võid rakendada mis iganes tehnoloogilisi meetmeid ja muid asju siin ja seal, sa ei saa kõike piirata. Et sul piisab ühest sellest väiksest vahelülist.* (ekspert 4)

„*Suurimad intsidendid hakkavadki inimestest see, kes istub arvuti ja klaviatuuri vahel. …aga kui ta veel pahatahtlik on, nagu süsteemiadministraator on pahatahtlik mõjutatud väliste agentide poole pealt, siis on ikka jama majas*“ (ekspert 5)

„See on endiselt üks suuremaid riske.“ (ekspert 6)

Kategooria: Soovitused ohtude maandamiseks, kood: inimene

Ekspertide intervjuude analüüs näitas, et on olemas ainult kaks meedet inimfaktorist tulenevate riskide maandamiseks (analüüsi **kood soovitused**). Esimene meede on taustakontrolli protsessi loomine ning teostamine enda ja partneri personali kohta. Eksperdid on üksmeelel, et enda töötaja taustakontrolli läbiviimine on oluliselt lihtsam kui partneri oma, eriti kui tegemist on rahvusvahelise ettevõttega. Inimese taustakontrolli tegemise vajadus ja selle põhjalikkus sõltub tema rollist. Mida kõrgemad on isiku pääsuõigused, seda suurem nende kuritarvitamise risk ning raskemad tagajärjed (käesolev töö lk 17). Täiendavaks ohuallikaks võib olla Eestis elav või töötav Vene IT-spetsialist, kellele antakse juurdepääs avaliku sektori või elutähtsate teenuse osutaja infosüsteemidele (käesolev töö lk 16). Võtmeisikuid (nt süsteemi- või turbeadministraator) tuleb kontrollida põhjalikumalt (eksperdid 3, 4, 5, 6). Partnerite personali kontrolli vajadus peab olema kirjeldatud nii hanke- kui ka teenuselepingutes (eksperdid 2, 4, 5,

6). Kolmes intervjuus (eksperdid 3, 4 ja 6) mainiti, et asutustel ei pruugi olla õiguslikku alust ning vajalikke tööriistu isiku põhjaliku taustakontrolli tegemiseks.

Teiseks meetmeks on personali õiguste haldamine, mis tähendab, et tuleb alati analüüsida, millised õigused on teenuse osutamiseks vajalikud ning millistel tingimustel õiguste kasutamine toimub (kõik eksperdid). Selleks tuleb igal organisatsioonil kehtestada vastavad protseduurid.

Eksperdid 2 ja 6 tõid eraldi välja, et taustakontrolli protsessis tuleb võtta arvesse geopoliitilisi riske. See tähendab, et arendusprotsessis tuleb välistada Venemaa ja Valgevene päritoluga tööjõu kasutamise. Kõikide ekspertide hinnangul avaldab inifaktor mõju kõikidele muudele vektoritele, ehk ka ülejäänute vektoritest tulenevate riskide maandamisel tuleb arvestada inimfaktoriga.

Kategooria: Tarneahela oht, kood: alltöövõtjad

Järgnevalt otsiti koodi „alltöövõtjad“ järgi. Alltöövõtjast tulenevat riski paigutasid eksperdid teisele kohale. Selle põhjuseks on alltöövõtja usaldusväärsuse hindamise keerukus. Ekspert 1 hinnangul on *„muutujate hulk on kõige suurem, mis seda riski tõstavad*“. Klient ei saa olla lõpuni veendunud, et alltöövõtja pakutav teenus täielikult vastab tellitule ning kõik lepingutingimused on korrektselt täidetud (kõik eksperdid). Isegi vastavussertifikaadi olemasolu ei garanteeri, et kõik vajalikud turbekomponendid on reaalelus rakendatud.

„Üks asi on see, et võidakse küsida serti, aga ma arvan, et see teadmine sellest, mis seal skoobis kirjas on, on asi, millest võiks rohkem rääkida. Mis seal kirjas on, ja kas see katab sinu teenuse ära“. (ekspert 4)

Kuna täna head tööriista ebausaldusväärse pakkuja välistamise ei ole, siis pakkusid eksperdid 1 ja 2, et partneri usaldusvääruse hindamist võiks aidata nö „usaldusväärsete partnerite loetelu“ olemasolu.

„*Tehakse see usalduspartnerite nimekiri ette. Ja kõik teised asutused saavad refereerida sedasama, nii-öelda ette teatud analüüsi ja selle all siis oma hankeid teha*“. (ekspert 1)

„Võiks olla mingi usalduse indeks. Suure kõrge mainega ettevõtted saaksid endale Euroopa

Liidu turul müüa usalduse indeksi, mingisuguses skooringu, mille alusel siis ma saaks nagu vaadata. Ja oleks mingi üldregister, kus kõik hindavad, kui usaldusväärne see ettevõte on olnud“. (ekspert 2)

Eksperdi 6 jaoks on alltöövõtja puhul oluline, et tellitud töö oleks teostatud kompetentsete personali poolt, kes on lepingus fikseeritud.

„… tarneahela kontekstis see probleem on ka suur, et sa lähed ja hangid väga tunnustatud ettevõttelt, kellel on väga tunnustatud tooted, mingisuguse toote ja teenuse. Kogu see usalduskrediit, millele sa nagu panustab, on need inimesed, kes on seal tipud... Aga need inimesed ei hakanudki sinuga tegelema… See on kõige suurem tarneahel rist meie vaatest, et seda ei teegi see proff, teatud standardile vastav inimene. Vaid seal tarneahela sees on keegi sootuks muu.“

Kategooria: Soovitused ohtude maandamiseks, kood: alltöövõtjad

Soovitused alltöövõtjast tulenevate ohtude maandamiseks analüüsitud koodi „alltöövõtja“ abil. Maandamismeetmeks on põhjalik kontroll enne hankemenetluse alustamist, läbimõeldud ja detailsete hanketingimuste seadmine ja vastavuskriteeriumite sätestamine (nt rahvusvaheliselt tunnustatud sertifikaadi olemasolu või auditeerimine). Ekspert 4 juhib tähelepanu, et üksnes sertifikaadi küsimist ei piisa. Vastavuskriteeriumid ei tulene ainult standartidest, vaid iga asutus saab kehtestada neid ise. Eelkõige see puudutab partneri riskijuhtumise süsteemi rakendamist või turvanõuete kehtestamist (eksperdid 3, 4, 5). Näidisloetelu sellistest nõuetest on lisatud magistritöö juurde (Lisa 3, käesolev töö lk 94) näidisloetelu on koostatud Telia Eesti AS turvadirektiivide alusel (Telia Eesti AS, 2022).

Ekspert 5 tõi välja, et praegu hindab iga asutus partnerite usaldusväärsust ja riske ise, mis tähendab, et sama teenuse hankimisel tehakse topelt tööd. Selle asemele võiks olla riigis üks kompetentsikeskus, kes vastutaks teistele avaliku sektori asutustele kesksete teenuste osutamise eest. Keskuse ülesandeks oleks muuhulgas teenusega seotud riskide juhtimine kogu tarneahela ulatuses. Sellisel juhul teised avaliku sektori asutused saaksid turvalist baasteenust ning saaksid suunata vabanenud ressurssi sisuteenuste arendamisele. Näitena tõi ekspert 2021. aastal loodud Riigi IT Keskuse, kes pakub IKT-alusteenuseid osadele riigiasutustele.

Alltöövõtjast tulenevate probleemide lahendamiseks tuleb koostada võimalikult detailne leping,

milles fikseerida kõik vajalikud komponendid, osapoolte õigused ja kohustused ning kontrollida selle täitmist (sh auditeerimine).

Kategooria: Tarneahela oht, kood: riist-ja tarkvara

Riist ja tarkvara ohud analüüsiti koodi „riist- ja tarkvara“ abil. Riist-ja tarkvarast seotud riske hinnatakse keskmisest madalamaks. Eksperdid tõid välja, et riist-ja tarkvara puhul sõltuvad riskid riist- ja tarkvara elementide rakendamisest infosüsteemide või teenuste arhitektuuris. Mida olulisem või kriitilisem element, seda suuremana tuleb riski käsitleda. Kuid üldiselt riist- ja tarkvara riski hinnatakse madalaks eelkõige selle tõttu, et kõikide intervjuudes osalenud ekspertide organisatsioonides on juba rakendatud vastavad maandamismeetmed. Kõik eksperdid tõid välja, et tarkvarakoodi kirjutamise protsessi ei ole võimalik lõppuni kontrollida, kuid seevastu panustatakse testimisele. Ekspert 2 tõi välja, et tema organisatsioonis on kasutusel palju spetsiifilist riistvara, mille tootja taustakontrolli läbiviimiseks ja testimiseks puudub vastav kompetents või sobivad tööriistad.

„*Olukord aga riistvaraga kindlasti on kõige hullemas olukorras. Et riistvara tõesti on see, mida me peame nagu usaldama. Google on üks tööriist. Üks variant on ka see, et sa teed ise taustauuringud nii öelda OSINTi* (peetakse silmas andmete kogumist avalikest allikatest, autor), *et otsid, kas sellega tarkvaratootjaga on või selle tootega on mingisuguseid probleeme ei olnud maailmas. Harva juhtub, et sa oled tõesti maailmas esimene, kes sellise toote ostab“.* (ekspert 2)

Kategooria: Soovitused ohtude maandamiseks, kood: riist-ja tarkvara

Intervjuudest tulnud soovituste analüüs koodi „riist-ja tarkvara“ järgi tuvastas, et enne tarkvara kasutuselevõttu või tarkvara uuenduse paigaldamist teostatakse põhjalikud testid test- ja *pre-live* keskkondades. Tarkvara paigaldus *live*-keskkondadesse on organisatsioonisiseselt reglementeeritud ning partneritel puudub võimalus tarkvara paigaldada kliendi keskkondadesse. Eksperdi 3 hinnangul on oluline võtta kasutusele tarkvara materjalide loendit (SBOM), et oleks täielik ülevaade arenduses kasutatavtest tarkvarakomponentidest. Riistvara hankimisel nõutakse standartidele vastavust kinnitavaid sertifikaate ning samuti läbitakse enne paigaldust testimistsükli. Ekspert 6 tõi välja, et testimiseks võib kaasata sõltumata partnerit kes „ *proovivad toodet tükkideks murda, või sisse murda ja annavad selle kohta raporti. See pikendab küll ajaraami.., aga annab meile kindluse.“*

Magistritöö autor juhib tähelepanu, et vaatamata ekspertide organisatsioonides rakendatud

maandamismeetmetele, eksisteerivad riist-ja tarkvaraga seotud riskid endiselt. See tähendab, et nendes organisatsioonides, kus riskijuhtimist ei ole või puudub võimekus iseseivaks riskimaandamis mehhanismi rakendamiseks, on riskid oluliselt kõrgemad.

Kategooria: Tarneahela oht, kood: haldus

Kategooria „Tarneahela oht" viimaseks koodiks oli „haldus, mille abil korjati ning analüüsiti ekspertide pakutud haldusega seotud ohte. Halduse risk on intervjueeritavate poolt samuti hinnatud piisavalt madalaks, sest nende organisatsioonides on haldusprotsess majasisene ning haldusega seotud tööliinid on detailselt reguleeritud. Dokumentides kirjeldatakse, kas, kellel, millistel juhtudel ja mis kanalite kaudu lubatakse halduse tööriistu kasutada. Näiteks, kas lubatakse kaughaldust või haldust teostatakse ainult kliendi ruumides (eksperdid 1, 2, 4, 5, 6). Ekspert 3 tõi välja, et nendes asutustes, kus halduseprotsess on delegeeritud välispartneritele, on riskid olulised suuremad.

„Me ei ole oma haldust välja andnud" (ekspert 1)

„*Kaughaldus reguleeritakse reeglina ära alati lepingus, siis hooldus või halduslepingus, seal on nimeliselt välja toodud, kellel need ligipääsud on."* (ekspert 2)

„... et tarnija teab, et tal on turvanõrkus ja tal on teavitusmehhanism paigas." (ekspert 3)

Kategooria: Soovitused ohtude maandamiseks, kood: haldus

Intervjuude analüüsist (kategooria „soovitused ohtude maandamiseks", kood „haldus") selgub, et riist-ja tarkvara ning halduse vektoritest tulenevate riskide leevendamisele aitab kaasa tõhus organisatsioonisisene riskijuhtimise protsessi rakendamine. Selle raames määratakse muuhulgas täpsed reeglid tark- ja riistvara kasutusele võtmiseks ning uuendamiseks, pääsuõigused, halduse reeglid. Oluline on kehtestada reegleid turvanõrkustest ja turvaintsidentidest teavitamiseks ning leppida kokku taastemeetmetes (eksperdid 3, 4).

„Turvanõrkustest teatamise kohustus lepingus. See eeldab, et tarnija teab, et tal on turvanõrkus ja tal on teavitusmehhanism paigas." (ekspert 3)

Ekspertide täiendavad tähelepanekud

Iga intervjuu lõpus küsis intervjueerija hinnangu, kas lisaks pakutud neljale ründevektorile on olemas veel potentsiaalsed vektorid, mida magistritöö autor ei ole maininud.

Neli intervjueeritavat (eksperdid 2,4, 5 ja 6) tõid välja kriitilist sõltuvust ühest tarnijast, mille puhul on kaks peamist riski:

- puudub alternatiiv pakutavale tehnoloogiale, mis toob kaasa ebaturvaliste toodete kasutamise;
- ettevõtte likvideerimise tagajärjel võib teenus võib.

Magistritöö autori hinnangul on esimene risk juba kaetud pakutud vektoritega (alltöövõtja, haldus, riist- ja tarkvara) ning teine risk ei kvalifitseeru IKT tarneaheale potentsiaalseks ründevektoriks, sest tegemist ei ole küberrünnakuga IKT tarneahela vastu (magistritöö lk 42–43).

2.4 Järeldused ja ettepanekud

Teooria osas kirjeldatud küberjulgeoleku julgeolekustamise protsess kinnitab, et küberjulgeolek sh IKT tarneahel on oluline komponent Eesti Vabariigi, Euroopa Liidu ning NATO julgeoleku tagamiseks (käesolev töö lk 13–14). Sellest tulenevalt parendavad ja täiendavad Euroopa Liidu ja NATO liikmesriigid pidevalt võimekusi kaitsta oma IKT infrastruktuuri küberrünnakute vastu. Küberrünnakute läbiviijaks on riiklikud või nende poolt sponseeritud rühmitused, kriminaalsed küberrühmitused ning üksikhäkkerid. Teooriast ja dokumendianalüüsist selgus, et kõige suuremaks ohuks on Hiina ja Venemaa või nende poolt rahastatud küberrühmitused, sest nendel on olemas võimekus tarneahelarünnakute läbiviimiseks (käesolev töö lk 43).

IKT tarneahela turvalisuse tagamise vajaduse olulisus leidis kinnituse kõikides magistritöö osades (teooria, dokumendianalüüs, intervjuud). Tarneahela rünnakute eripäraks on asjaolu, et tarneahela rünnakud mõjutavad korraga suurt hulka asutusi erinevatest sektoritest (käesolev töö lk 28). IKT tarneahelaga seotud riskide maandamine avaliku sektori ja elutähtsate teenuste osutamisel aitab tõsta Eesti küberjulgeoleku taset. Teenuse või toote lõppkasutaja peab olema veendunud, et IKT tarneaheala komponendid on usaldusväärsed kogu nende elukaare jooksul.

Tarneahela usaldusväärus tähendab, et kõik selle komponendid täidavad oma funktsioone kindlaksmääratud tingimusel (käesolev töö lk 29).

Uurimisküsimustele vastamiseks pakuti analüüsida teemat neljast ründevektorist (riist- ja tarkvara, haldus, alltöövõtjad, inimfaktor), lähtuvalt. Sellest tulenevalt oli oluline leida kinnituse, et pakutud jaotus aitab vastata uurimisküsimustele ja täita uurimisülesandeid. Teooriast selgus, et küberdomeeni riskid tulenevad inimesest, tehnoloogiast, protsessidest ning välistest mõjuritest (käesolev töö lk 25), mis kattus magistritöö fookuses olevate ründevektoritega. Lisaks selgus, et IKT tarneahelat võivad ohustada geopoliitilised mõjurid milleks on Hiina ja Venemaa (käesolev töö lk 15). Samade tulemusteni jõuti ka dokumendianalüüsi raames (käesolev töö lk 42), millest selgus, et analüüsi fookuses olevad dokumendid nimetavad samu vektoreid. Nimetatud ründevektoreid valideeriti ka intervjuude raames ning ekspertidel paluti lisaks neljale ründevektoritele nimetada täiendavaid vektoreid. Vastuseks toodi välja ühte täiendavat vektorit milleks on kriitiline sõltuvus ühest tarnijast (käesolev töö lk 68), kuid see on kaetud fookuses olevate vektoritega nagu alltöövõtja, haldus, riist- ja tarkvara. Sellest tulenevalt jõuti järeldusele, et magistritöös pakutud vektorite ning hiljem lisandunud vektori „geopoliitilise mõjurid“ analüüs aitab vastata püstitatud uurimisküsimustele ja täita magistritöö eesmärk.

Järgnevalt esitatakse uurimistulemused ja järeldused vastavalt magistritöös püstitatud uurimisküsimustele. Saadud vastustest selgub, kas püstitatud magistritöö eesmärk on täidetud. Samuti tehakse ettepanekud riigi IKT valdkonna tarneahela usaldusväärsuse kontrollimise protsessi tõhustamiseks.

Uurimisküsimustele saadi järgmised vastused:

1. **Millised on võimalikud riist-ja tarkvarast ning selle haldamisest, alltöövõtjatest ning ettevõtte ja avaliku sektori asutuse personalist tulenevad ohud riigi IKT tarneahelale?**

   Teoreetilistest allikatest ja empiirilisest uuringust selgus, et kõik neli küsimuse fookuses olevad ründevektorit (riist-ja tarkvara, inimesed, partnerid) ohustavad IKT tarneahelat. Lisaks sellele avastati, et IKT tarneahela turvalisust võivad mõjutada geopoliitilised ohud.

Personali ohud

Dokumentide (käesolev töö lk 53) ja ekspertide intervjuude analüüs näitas (käesolev töö lk 62), et IKT tarneahela suurimaks ohuks peetakse just inimest, mis ühtib teoorias toodud statistikaga, mille kohaselt on 83% küberintsidentidest toimub inimfaktori tõttu (käesolev töö lk 12). Seda kinnitab asjaolu, et inimfaktorit on mainitud ka teiste ohtude juures. See tähendab, et inimfaktor on korraga oht omaette, kui ka oluline riskivektor teiste ohtude juures. Personali ohud tulenevad koostööparterite töötajatest, asutuse enda personalist ning organisatsiooni tööprotsessidesse kaasatud inimeste nagu külalised, koristajad poolt. Inimene võib tahtlikult või tahtmatult avaldada informatsiooni organisatsioonis või teenuses rakendatud turvameetmest, avalikustada tundlikku informatsiooni, manipuleerida riis- ja tarkvara, sisestada pahavarakoodi, installida pahavara või jätta tagauksi süsteemile pääsemiseks. Lisaks sellele, on inimest võimalik mõjutada, et ta annaks ründajale ligipääsu tööarvutile, süsteemile ja võrgule või häiriks nende tööd (nt serveri või muu olulise komponendi välja lülitamine).

Riist-ja tarkvara ohud

Riist-ja tarkvarast tulenevad ohud on kirjeldatud nii teoreetilises käsitluses, kui empiirilises analüüsis. Teooria kohaselt võivad riist- ja tarkvara ohustada selle tootjast, hooldusteenuse pakkujast või tehnilistest omadustest ja seadustest (käesolev töö lk 30). Dokumendianalüüs tõi välja, et kuna riist-ja tarkvara arendamise protsessi on kaasatud palju osapooli, siis selle läbipaistvuse ja kontrollitavuse tagamine on väga raske (käesolev töö lk 44). Tihtipeale ostetakse valmis riist – ja tarkvarakomponente, mis võivad sisaldada kolmanda osapoole valmis komponente või baseeruda avatud lähtekoodil ning seetõttu sisaldada tagauksi või dokumenteerimata funktsionaalsusi. Tagajärjeks on andmete võimalik sattumine selleks volitamata isikute kätte, andmete muutmine või vargus. Riist-ja tarkvara nõrkused võivad ilmneda pärast uuendust, sest kasutajal on raske veenduda uuenduspaketti ohutuses (käesolev töö lk 52). Selle tulemusena esineb riist-ja tarkvara manipuleerimise või nõrkuste ärakasutamise risk. Ekspertintervjuust selgus, et riist-ja tarkvara riskid sõltuvad riist- ja tarkvara komponentide rakendamisest infosüsteemide või teenuste arhitektuuris. Mida olulisem või kriitilisem element, seda suurem on risk (käesolev töö lk 66).

Partneri ohud

Empiirilise analüüsi raames leiti, et halduse ja alltöövõtja ohud on väga sarnased ja omavahel läbi põimunud. Seetõttu jõuti järeldusele, et neid saab kokku liita ning

moodustada nimetada koondnimega „**partner(id)**“, mis tähendab ettevõtet või organisatsiooni, kes lepingu alusel pakub tooteid või teenuseid (käesolev töö lk 49). Teoorias mainiti, et igat organisatsiooni on võimalik rünnata tema partneri kaudu ning sellega kompromiteerida korraga mitu ahela osapoolt (käesolev töö lk 27). Dokumendianalüüsi tulemused kinnitavad teooria väidet ning täiendavad, et partneri riskid tulenevad kõikidest tarneahelasse kaasatud tarnijatest ning nende tarneahelatest ning suureneb osapoolte arvu suurendamisel (käesolev töö lk 50). Riskitase suureneb kui osa arendus või haldusprotsessis on delegeeritud partnerile, sest partneri usaldusväärsuse hindamine raske ning avaliku sektori asutustel ei ole häid mehhanisme partneri usaldusväärsuse hindamiseks (käesolev töö lk 64). Ebausaldusväärne partner võib tahtlikult lisada ebaturvalisi komponente, kuritarvitada talle usaldatud õigusi (nt luua uusi kasutajakontosid või anda pääsuõigused kolmandatele osapooltele). Täiendavaks riskiks on vajalike **turvameetmete mitte** rakendamine partneri pool, mis kergendab ründajal rünnaku teostamise (käesolev töö lk 53). Eesti turul tegutsevate ettevõtete tarneahelatesse on kaasatud rahvusvahelised ettevõtted, mis võivad olla mõjutatavad vaenulike riikide poolt (käesolev töö lk 51), ehk esineb ka teoorias välja toodud geopoliitiline oht (käesolev töö lk 22-23). Eksperdid paigutasid partnerist tulenevat riski teisele kohale (käesolev töö lk 64), sest partneri usaldusväärsuse hindamise on keeruline protsess ning kunagi ei saa olla täiesti veendunud, et partneri poolt pakutav tehnoloogia või teenus on ohutu.

Geopoliitilised ohud

Tuginedes teoreetiliste lähtekohtade analüüsi (käesolev töö lk 15) ja empiirilise analüüsi tulemustele (käesolev töö lk 41; lk 63) jõuti järeldusele, et lisaks uurimisküsimuses nimetatud ohtudele esinevad **geopoliitilised ohud**, mis tulenevad eelkõige Venemaast ja Hiinast ning nende poolt rahastatud küberrühmitustele. Hiina peamisteks eesmärkideks on andmete vargus ja spionaaž. Hiina tehnoloogia tootjad teevad koostööd valitsusasutustega ja eriteenistustega, mis võimaldab nende eriteenistustel pääseda ligi kliendi andmetele. Venemaa kasutab küberdomeeni andmete varguseks, spionaažiks, teenuste toimepidevuse katkestamiseks ning konventsionaalsete rünnakute toetamiseks.

2. **Kuidas ja milliste kriteeriumite alusel oleks riigi IKT asutustel võimalik hinnata ja kontrollida kasutatava riist- ja tarkvara, riiklike ja riigi seisukohast oluliste infosüsteemide arendus- ja hooldusfirmade usaldusväärsust?**

Riist-ja tarkvara kontroll

Dokumendianalüüs tõestas, et tarneahela turvalisuse tagamise üheks komponendiks on usaldusväärse ja kontrollitud riist-ja tarkvara kasutamine (käesolev töö lk 51-52). Selleks tuleb riigi IKT asutustel jäädvustada riske, mis tulenevad kasutatavast tehnoloogiast ning rakendada vastumeetmeid. Teooriast selgus, et lisaks turvalise tehnoloogia kasutamisele, on oluline jälgida, et tarneahelas kasutatava riist-ja tarkvara oleks toodud usaldusväärse tootja poolt (käesolev töö lk 21). Dokumendianalüüsist tuleb soovitus luua **riskijuhtimise protsess**, mille raames koostada riist-ja tarkvara riskianalüüs, töötada välja ja dokumenteerida protseduurid, maandamismeetmeid, monitoorida nende rakendamist ning hinnata nende tõhususe (käesolev töö lk 54). Tarkvara arendamisel tuleb nõuda jälgida parimad **tarkvara arendamise praktikaid ja standardeid** ning nõuda vastavussertifikaatide esitamist. Üheks selliseks praktikaks on tarkvara materjalide loendi koostamine (käesolev töö lk 59), mis aitab kliendil kontrollida arendusprotsessi ning kasutatud komponentide päritolu (käesolev töö lk 66). Veendumaks, et riist-ja tarkvara ei sisalda dokumenteerimata funktsionaalsusi, vigu ja turvanõrkusi, tuleb enne selle kasutuselevõttu põhjalikult testida. Ekspertide hinnangul ei pea iga asutus kontrollima ise. Olukorras, kus kliendil puudub testimise läbiviimiseks vajalik kompetents, siis komponentide hindamist või delegeerida sõltumatu partnerile (käesolev töö lk 66).

Arendus – ja hooldusfirmade kontroll

Teooriast on välja tulnud, et partnerite kontroll on oluline osa tarneahela julgeoleku tagamisel, eriti võttes arvesse geopoliitilistest mõjuritest tulenevaid ohte. Samale seisukohale jõuti dokumendianalüüsi raames (käesolev töö lk 43). Partneritest riskide maandamiseks, peab partnerite valik algama põhjaliku kontrolliga juba enne tarnijaga lepingu sõlmist. Avaliku sektori asutus või õigusaktiga määratud üksus (käesolev töö lk 30) hindab eelnevalt paika pandud kriteeriumite alusel hinnata võimalikke kaasneda võivaid riske. Ekspertintervjuudest selgus, et täna ei ole riigiüleselt koostatud partnerite hindamise metodoloogiat (käesolev töö lk 64) ning asutus paneb kriteeriumid ise. Kriteeriumid võivad puudutada partneri riskijuhtumise süsteemi rakendamist, turvanõuete kehtestamist (Lisa 3, käesolev töö lk 94), rahvusvaheliselt tunnustatud sertifikaadi olemasolu või auditeerimisnõuete täitmist (käesolev töö lk 65). Selliseid nõudeid määratletakse juba hankedokumentide koostamisel (käesolev töö lk 56). Riskide hindamisel tuleb muuhulgas võtta arvesse partneri päritolu, tema omandistruktuuri (käesolev töö lk 21) ning tema potentsiaalne mõjutatavatus kolmandate riikide

valitsusasutuste poolt (käesolev töö lk 57). Dokumendianalüüs rõhutas (käesolev töö lk 57), et oluliseks aspektiks on hinnata millised õigused (informatsiooni ja infosüsteemidele ligi pääsemiseks) ja mis tingimustel (teatud ruumides ja kellaaegadel) partneritele antakse. Samale seisukohale asusid ka eksperdid (käesolev töö lk 65-66).

3. **Kuidas ja millistel alustel oleks riigi IKT asutustel võimalik teostada usaldusväärsuse kontrolli alltöövõtjate ja nende personali üle?**

   Personali tasutakontrolli tegemise vajadus on kajastatud nii teoreetilises käsitluses (käesolev töö lk 24), kui ka empiirilises uuringus (käesolev töö lk 57). Puudulik kontroll asutuse enda ja partneri personali üle viib inimfaktorist tulenevate riskide realiseerimiseni (käesolev töö lk 24). Taustakontrolli eesmärk on veenduda, et inimene on usaldusväärne, et anda talle ligipääs vajalikule informatsioonile või protsessile. Kui taustakontrolli kohustus ei tulene õigusaktist, siis asutus peab ise korraldama taustakontrolli protsessi, määrama selle eest vastutavaid ning sätestama nõue parteri töötaja taustakontrolli läbiviimiseks lepingutes (käesolev töö lk 62). Esmane taustakontroll tuleb läbi viia enne inimese tööle võtmist, lepingu sõlmimist või tema rolli muutmist. Lisaks sellele on oluline teostada regulaarseid järel hindamisi, et veenduda inimese usaldusväärsuses (käesolev töö lk 57–58). Kontrolli raames tuleb hinnata vähemalt inimese käitumist, toimunud intsidente ning arvestada geopoliitiliste ohtudega (käesolev töö lk 64).

   Teisele ja kolmandale uurimisküsimustele sai autor vastused dokumendianalüüsist ja ekspertintervjuudest, kust selgus, et IKT tarneahela usaldusväärsust on võimalik tagada läbi tarneahela juhtimise, mille oluliseks osaks on tarneahela neljast komponentidest (riist- ja tarkvara, inimene, partnerid) tulenevate riskide maandamiseprotsess. Lisaks sellele tõi ekspertintervjuu tulemuste analüüs välja ühe **probleemkoha**. Selgus, et võrreldes julgeolekuasutustega, puuduvad muudel avaliku sektori asutustel ja elutähtsate teenuste osutajatel vajalikud tööriistad (eelkõige puudub õiguslik alus) personali põhjaliku taustakontrolli tegemiseks (käesolev töö lk 64). See tähendab, et kolmanda küsimuse vastuses kirjeldatule taustakontrolli protsessile, ei **pruugi rakendatud meetmed olla piisavalt tõhusad ning vajavad täiendamist eelkõige õigusraamistiku osas**.

4. **Kuidas ja milliste kriteeriumite alusel oleks riigiasutustel ja nende valitsemisalas olevatel juriidilistel isikutel võimalik välistada riigihangetest ebausaldusväärseid pakkujaid?**

Teooriast on selgunud, et infosüsteemide ja võrkude turvalisuse tagamise oluliseks osaks on nende komponentide ja tarkvara pakkujate hoolikas ja täielik hindamine (käesolev töö lk 24). Mida rohkem osapooli osaleb IKT tarneahela, seda suuremad riskid, et üks osapooltest võib olla ebausaldusväärne (käesolev töö lk 26). Sellest tulenevalt ebausaldusväärsete pakkujate riigihangetest välistamine on oluline osa IKT tarneahela usaldusväärsuse kontrollimise protsessist. Samadele aspektidele on viidatud ka dokumendianalüüsis ning on tehtud üldised soovitused hankemenetluseks ettevalmistamiseks (käesolev töö lk 55-56). Magistritöö teoreetilisest osast ega dokumendianalüüsist **ei selgunud** millistel kriteeriumitel oleks võimalik välistada ebausaldusväärsete pakkujate riigihangetest juhul, kui ettevõtte vastab kõikidele hanke kriteeriumitele. Ekspertintervjuude analüüsi tulemustest tuli küll välja, et riigi tasandil on juhitud tähelepanu Hiina ettevõtetest tulenevale riskile, kuid nende tehnoloogia kasutamine ei ole otseselt keelatud (käesolev töö lk 62). Seda kinnitab fakt, et Hiina tootjad endiselt osalevad riigihangetes (käesolev töö lk 20). Eksperdid tõid välja, et täna **puudub tõhus töörist** ebausaldusväärsete pakkujate välistamiseks (käesolev töö lk 64). Sellest tulenevalt uurimisküsimusele võib vastata, et **täna puuduvad selged kriteeriumid**, mille alusel on riigiasutustel ja nende valitsemisalas olevatel juriidilistel isikutel võimalik välistada riigihangetest ebausaldusväärseid pakkujaid.

Võttes arvesse teoreetiliste lähtekohtade ja empiirilise uuringu tulemusi ning järeldusi, teeb magistritöö autor **ettepanekud**, mis võimaldavad tõhustada Eesti avaliku sektori info- ja kommunikatsioonitehnoloogia tarneahela usaldusväärsuse.

1. Empiirilisest analüüsist selgus, et tarneahela juhtimine ning tarneahela komponentide turvalisuse tagamine peab olema süsteemne protsess. Sellest tulenevalt tuleb tunnistada IKT tarneahelat riigi julgeoleku komponendina, koostada metoodika IKT tarneahela juhtimiseks ning kohustada avaliku sektori asutusi ja elutähtsate teenuste osutajaid rakendama seda metoodikat nende IKT tarneahelate hindamisel. Selleks tuleb luua sektoriülene töögrupp, mille töösse tuleb kaasata eksperte erinevatest sektoritest. Metoodika väljatöötamisel võib võtta aluseks rahvusvahelisi standardeid ja parimaid tavasid (nt tarkvara materjalide loend). Näitena võib välja tuua NIST SP 800-161r1 „Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations“ või MITRE poolt 2017. aastal avaldatud „Supply Chain Attacks and Resiliency Mitigations. Guidance for System Security Engineers“. On oluline neid mitte

kopeerida, vaid luua uus Eesti huvisid silmas pidav, siinse õigusruumi ja spetsiifikaga sobiv raamistik. Sarnaselt tehti Eesti infoturbestandardi loomisel, kus aluseks võeti BSI IT-Grundschutz etalonturbe meetod. Kuna sellise metoodika välja töötamine eeldab riigiülest koordineerimist ning erasektori kaasamist, siis sobivaks asutuseks võib olla Majandus- ja Kommunikatsiooniministeerium, kelle ülesannete hulka kuulub muuhulgas riigi infosüsteemide arendamise koordineerimine, tehnoloogiline arendustegevus ja innovatsioon või Riigikantselei, kes muuhulgas vastutab kriisireguleerimispoliitika väljatöötamise eest.

2. Ekspert intervjuudest selgus, et täna vastutab iga asutus ise tarneahela usaldusväärsuse kontrolli eest. Olukorras, kus kaks avaliku sektori asutust ostavad täpselt sama teenust või toodet (võib juhtuda, et isegi sama tarnija käest), peavad mõlemad asutused viima läbi tarneahela usaldusväärsuse kontrolli, mis tähendab aja- ja inimressurssi raiskamist. Võttes arvesse avaliku sektori piiratud ressurssi, siis tasub kaaluda erinevate teenuste IKT tarneahela hindamisega seotud ülesannete riigiülest konsolideerimist kompetensikeskuse(te)sse. Selle tulemusel on määratud vastutavad asutused, kelle ülesandeks on teatud baasteenuste või toodete tarneahelate usaldusvääruse kontroll. See võimaldab nii rahalise kui ka inim- ja ajaressurssi optimeerimist mitmes asutustes korraga. Selline lähenemine on juba osaliselt rakendatud serveri baasteenuse ja arvutitöökohateenuse puhul, mille eest vastutab 2021. aastal loodud Riigi IT Keskus. Selle jätkuks tuleb analüüsida, milliseid teenuseid (nt tarkavaraarendus, turvaline mobiil-, satelliit, telefoni-, andmeside jne) on täiendavalt võimalik riigiüleselt konsolideerida.

3. Empiirilise analüüsi tulemused näitavad, et on vajalik muuta isikute taustakontrolli puudutavat õigusraamistiku. Sellest tulenevalt tuleb kaaluda vastava õigusanalüüsi läbi viimist ning õigusaktide muutmist selliselt, et saaks vajalikku taustakontrolli teostada. Õigusanalüüsi eesmärgiks on tuvastada kitsaskohad IKT tarneahelas osalevate füüsiliste- ja juriidiliste isikute taustakontrolli läbiviimises ning pakkuda välja lahendused. Sellega tagatakse, et IKT tarneaheala juhtimise eest vastutaval asutusel oleks õiguslik alus piisavas mahus taustakontrolli läbiviimiseks. Samuti tuleb koostöös pädevate asutustega analüüsida, milliseid IKT lahendusi on võimalik selleks kasutada.

4. Empiirilise uuringu tulemused näitasid, et täna kehtivas riigihangete protsessis on puudujäägid. Sellest tulenevalt teeb magistritöö autor ettepaneku analüüsida riigihangete protsessi ning vajadusel muuta seda selliselt, et IKT tarneahela juhtimise eest vastutaval asutusel oleks õiguslik alus ebausaldusväärse tarnija hankeprotsessist välistamiseks. On oluline, et selle raames ei oleks takistatud vabaturu konkurents ja tagatud oleks hankeprotsessis osalejate võrdne kohtlemine.

5. Tuginedes ekspertintervjuus tehtud soovitusele luua sobivat mehhanismi partneri usaldusväärsuse hindamiseks, teeb magistritöö autor ettepaneku kaaluda koostöös erasektoriga ettevõttete usaldusväärsuse indeksi loomist. Indeksi kujunemist võivad mõjutada sellised aspektid nagu ettevõttes rakendatud riskijuhtimise- ja infoturbepoliitikad, toimunud intsidendid ja muud asjassepuutuvad näitajad. Sellise tööriista loomine võib potentsiaalselt aidata kaasa IKT tarneahelas osalevate partnerite usaldusväärsuse kontrollimiseks. Autor juhib tähelepanu, et usaldusväärsuse indeksi loomine ja indeksi kujundamine peavad olema läbipaistvad nii kliendile kui ettevõttele. Juhul, kui Eesti kogemus osutub edukaks, siis laiendada seda Euroopa Liidu tasandile. See oleks kooskõlas Euroopa Liidu algatustega ja õigusaktidega.

KOKKUVÕTE

Teeoriast ja empiirilisest analüüsist tuli selgelt välja, et küberrünnakud IKT tarneahela vastu on tõusev trend kübermaailmas. Rünnakuobjektiks valitakse kõige nõrgem tarneahela lüli ehk ettevõtte kelle toode või teenus kõige vähem kaitstud. Lõppeesmärgiks on enamasti valitsusasutus või elutähtsa teenuse osutaja mistõttu eduka rünnaku tagajärjeks võib olla sensitiivsete andmete vargus või kriitilise teenuse katkestus, mis avaldab suurt mõju rünnaku alla sattunud riigi julgeolekule. Tarneahela rünnakud on keerulised, nende ettevalmistus on aeganõudev protsess ning vajab paju ressursse. Töö teoreetilises osas kirjeldatud tarneahelarünnakud nagu SolarWinds ja NotPetya tõestavad, et IKT tarneahelarünnaku taga võivad olla vaenulikud riigid nagu Venemaa ja Hiina või nende rahastatud küberrühmitused. Sellest tulenevalt tuleb veenduda, et Eesti avaliku sektori asutuste ja elutähtsate teenuste osutajate IKT tarneahelad on usaldusväärsed ning ei ohusta Eesti julgeolekut.

Magistritöö eesmärk oli hinnata riigi IKT valdkonna tarneahela usaldusväärsuse kontrollimise protsessi tõhusust ning teha ettepanekud selle täiendamiseks. Magistritöö uurimisprobleem oli püstitatud küsimusena „Kuidas tõhustada IKT valdkonna tarneahela kontroll Eesti avalikus sektoris?“. Probleemi lahendamiseks püstitati neli uurimusküsimust. Eesmärgi saavutamiseks ja uurimisküsimustele vastamiseks püstitati neli uurimisülesannet: välja selgitada IKT tarneahela olemuse ja neid ohustavad aspektid; kaardistada teiste riikide IKT tarneahela kontrolli ja usaldusvääruse hindamise parimad praktikad ning Eesti hetkeolukord; kaardistada Eesti avaliku- ja erasektori küber/IKT valdkonna ekspertide seiskohad ja ettepanekud tarneahela usaldusväärsuse hindamiseks ning töötada välja ettepanekud tarneahela kontrollimise protsessi loomiseks Eesti avaliku sektori IKT tarbeks.

Esimene uurimisküsimus puudutas IKT tarneahela ohte, mis tulenevad neljast riskivektorist (riist-ja tarkvara, haldus, alltöövõtja, inimfaktor). Teooria ja empiirilise analüüsi tulemus näitas, et peamised ohud on seotud inimfaktoriga, mis omakorda mõjutab ka teisi vektoreid. Lisaks inimfaktorile tuleb erilist tähelepanu pöörata riist-ja tarkvara soetamisele ja arendamisele ning veenduda, et selles puuduvad nõrkused ja võimalikud tagauksed. Kolmandaks ohuvektoriks on koostööpartnerid (haldus, alltöövõtja), kes on kaasatud IKT tarneahela protsessi. Täiendavalt, avastati teooria ja empiirilise uuringu raames, et IKT tarneahela turvalisust võivad mõjutada geopoliitilised tegurid, milleks on Venemaa ja Hiina küberüksused või nende riikide poolt toetatud küberrühmitused.

Teine uurimisküsimus uuris kuidas on võimalik hinnata ja kontrollida partnerite ja nende pakutud riist-ja tarkvara usaldusväärust. Empiirilise uuringu raames selgus, et riist-ja tarkvara usaldusväärsuse kontrollimiseks tuleb asutusetel luua ja rakendada põhjalik testimise protseduur. Selle raames veendutakse komponentide vastavuses turbestandartidele ja parimatele praktikatele. Vajadusel tuleb kaasata sõltumatu osapooli, kes teostab kontrolli kliendi eest.

Kolmanda uurimisküsimuse fookuses oli personali usaldusväärsuse kontrolli teostamise võimalikkus. Dokumendianalüüsi ja ekspertintervjuu tulemusel selgus, et inimfaktoriga on seotud koge suuremad riskid, mistõttu personali taustakontrolli läbiviimine on hädavalik. Ekspertintervjuu raames saadud vastustest tuli välja, et kehtiv õigusraamistik ei võimalda riigi IKT asutustel teostada põhjaliku taustakontrolli IKT tarneahelas osalevate osapoolte personali üle. See tähendab, et partneri või IKT asutuse võtmeisikuks võib saada ebausaldusväärne isik. Probleemi lahendamiseks tuleb luua toimiv taustakontrolli mehhanism, mida IT-majad saaksid rakendada võtmepositsioonidel töötavate isikute usaldusväärsuse hindamisel.

Viimane küsimuse fookuses olid kriteeriumid, mille alusel on võimalik välistada riigihangetest ebausaldusväärseid pakkujaid. Pakkujate hindamise vajadus on tulnud välja nii teooriast, kui ka empiirilisest uuringust. See on eriti relevantne Hiina tehnoloogia puhul, sest tänu riigiabile Hiina tehnoloogia on teiste konkurentidega võrreldes odavam. Ekspertintervjuudes selgus, et täna riigi tasandil ei ole tõhusat meetodit ebausaldusväärsete pakkujate välistamiseks riigihankemenetluse raames. Dokumendianalüüs ja teoreetiline käsitlus ei andnud vastust uurimisküsimusele, kuigi mõlemas osas on juhitud tähelepanu välistamise olulisusele. Ekspertide sõnul koostatakse probleemi leevendamiseks võimalikult detailsed hankedokumendid, kuid see ei võimalda täielikult välistada ebausaldusväärseid pakkujaid ning esineb vajadus tõhusama tööriista järgi.

Uuringutulemustele saadud vastustele tuginedes tehti neli **järeldust**:

1. IKT tarneahela turvalisust ohustavad riist-ja tarkvara, inimesed, partnerid ning geopoliitilised tegurid.
2. IKT tarneahela usaldusväärsust on võimalik tagada läbi tarneahela juhtimise, mille oluliseks osaks on tarneahela neljast komponentidest (riist-ja tarkvara, inimene, partnerid) tulenevate riskide maandamiseprotsess.

3. Tarneahelas osalevate osapoolte personali taustakontrolli protsess vajab täiendamist.
4. Puuduvad selged kriteeriumid ebausaldusväärsete pakkujate välistamiseks riigihangetest.

Magistritöös esitati viis ettepanekut, mis võimaldavad tõsta IKT tarneahela usaldusväärsuse. Pakutakse nimetada IKT tarneahela juhtimise eest vastutavad asutused ning töötada välja tarneahela juhtimise metoodikat, mille abil oleks võimalik vastutaval asutusel tagada tarneahela ja selle komponentide turvalisust. Samuti tehti ettepanekud tööriistakasti loomiseks, mis aitaks ebausaldusväärsete pakkujate välistamist riigihangetest ning tõhustada isikute taustakontrolli läbiviimist. Kõik ettepanekud on suunatud avaliku sektori asutustele ja elutähtsate teenuste osutajatele ning neid on võimalik rakendada praktikas.

Eeltoodust lähtuvalt uurimisprobleem „Kuidas tõhustada IKT valdkonna tarneahela kontroll Eesti avalikus sektoris?“ on saanud vastuse. Seega on magistritöö eesmärk täidetud.

Magistritöö tulemusi on võimalik kasutada jätkuuringute tegemiseks. Potentsiaalsed uuringuteemad võivad olla seotud IKT tarneahela hindamise metoodika väljatöötamisega, riiklike kompetentsikeskuste loomise ja rollide jaotamisega ning IKT tarneahela hindamisega seotud õigusraamistiku analüüsiga.

SUMMARY

The aim of the thesis was to assess the effectiveness of the national ICT supply chain integrity verification process and to make suggestions for its improvement. The research problem of the thesis was formulated as the question "How to improve the effectiveness of ICT supply chain control in the Estonian public sector?". Four research questions were set to address the problem. In order to achieve the objective and to answer the research questions, four research tasks were set: to identify the nature of the ICT supply chain and the aspects that threaten it; to map the best practices of ICT supply chain control and reliability assessment in other countries and the current situation in Estonia; to map the current situation of experts in the field of cyber/ICT in the Estonian public and private sectors and to develop proposals for the establishment of a supply chain control process for ICT in the Estonian public sector.

The first research question concerned the risks in the ICT supply chain arising from four risk vectors (hardware and software, administration, subcontractor, human factor). The result of the theoretical and empirical analysis showed that the main risks are related to the human factor. In addition to the human factor, particular attention needs to be paid to the acquisition and development of hardware and software, and to make sure that it is free of weaknesses and potential backdoors. The third risk vector is the partners (administration, subcontractor) involved in the ICT supply chain process. In addition, the theory and empirical study discovered that the security of the ICT supply chain can be influenced by geopolitical factors.

The second research question explored how the reliability of partners and the hardware and software they provide can be assessed and verified. The empirical study revealed that to verify the reliability of hardware and software, institutions need to establish and implement a thorough testing procedure. This involves verifying that components comply with security standards and best practices. Where appropriate, an independent party should be involved to perform the verification on behalf of the customer.

The third research question focused on the feasibility of carrying out staff reliability checks. The documentary analysis and the expert interviews revealed that the human factor is associated with higher risks than the other factors, making it essential to carry out background checks on staff. The responses to the expert interviews revealed that the current legal framework does not allow national ICT authorities to carry out thorough background checks on the personnel of the

parties involved in the ICT supply chain. To address this problem, an effective background check mechanism needs to be put in place.

The last question focused on the criteria for excluding unreliable bidders from public procurement. The documentary analysis and the theoretical approach did not provide an answer to the research question, although both parts draw attention to the importance of exclusion. According to the experts, drafting the most detailed tender documents possible will mitigate the problem, but it will not fully exclude unreliable bidders and there is a need for a more effective tool.

Based on the responses to the survey, four conclusions were drawn:
1. The security of the ICT supply chain is threatened by hardware and software, people, partners, and geopolitical factors.
2. The integrity of the ICT supply chain can be ensured through supply chain management, an essential part of which is the process of mitigating the risks arising from the four components of the supply chain (hardware and software, people, partners).
3. The process of background checks of supply chain actors' personnel needs to be improved.
4. There are no clear criteria for excluding unreliable bidders from public procurement.

The thesis put forward five proposals to improve the credibility of the ICT supply chain. It is proposed to designate the authorities responsible for the management of the ICT supply chain and to develop a methodology for supply chain management to enable the responsible authority to ensure the security of the supply chain and its components. Proposals are also made to create a toolbox to help exclude unreliable bidders from public procurement and to improve the performance of background checks on individuals. All the proposals are aimed at public authorities and critical service providers and can be implemented in practice.

In the light of the above, the research problem "How to improve the effectiveness of ICT supply chain controls in the Estonian public sector". has been answered. Thus, the objective of the thesis has been fulfilled.

The results of the thesis can be used for further research. Potential research topics could be related to the development of a methodology for ICT supply chain assessment, the

establishment of national competence centres and the allocation of roles, and the analysis of the legal framework for ICT supply chain assessment.

KASUTATUD ALLIKATE LOETELU

Alawida, M., Omolara, A., Abiodun, O. & Al-Rajab, M., 2022. A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University*, 34, pp. 8176–8206.

America's Cyber Defense Agency, 2018. *Petya Ransomware. Alert.* [Võrgumaterjal] Leitav: https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware [Kasutatud 23. 11. 2022].

[*Anon.*] 2023. *Advanced Persistent Threats (APTs).* [Võrgumaterjal] Leitav: https://www.mandiant.com/resources/insights/apt-groups [Kasutatud 26. 03. 2023].

Arnek, J., 2021. *Improving cybersecurity level of Estonian small and medium sized enterprises through coordination with national level*. *Magistritöö.* Tallinn: Tallinn University of Technology.

Balzacq, T., 2005. The Three Faces of Securitization: Political Agency, Audience and Context. *European Journal of International Relations*, 11(2), pp. 171–201.

Balzacq, T., 2011. *Securitization Theory*. Oxon: Routledge.

Bendiek, A. & Kettemann, M., 2021. *Revisiting the EU Cybersecurity Strategy: A Call for EU Cyber Diplomacy.* [Võrgumaterjal] Leitav: https://www.swp-berlin.org/publications/products/comments/2021C16_EUCyberDiplomacy.pdf [Kasutatud 11. 02. 2023].

Biener, C., Eling, M. & Wirfs, J., 2015. *Insurability of Cyber Risk: An Empirical Analysis.* [Võrgumaterjal] Leitav: https://www.ivw.unisg.ch/~/media/internet/content/dateien/instituteundcenters/ivw/wps/wp151.pdf [Kasutatud 29. 01. 2023].

Blank, S., 2008. Threats to and from Russia: An Assessment. *Journal of Slavic Military Studies*, 21(3), pp. 491–526.

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A. & Fallon, M., 2022. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.* [Võrgumaterjal] Leitav: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf [Kasutatud 23. 04. 2023].

Buzan, B., Wæver, O. & de Wilde, J., 1998. *Security: A New Framework for Analysis.* London: Lynne Rienner Publishers.

Crowe, S., Kathrin Cresswell, K., Robertson, A., Huby, G., Avery, A., Sheikh, A. , 2011. The case study approach. *BMC Medical Research Methodology*, Issue 100, pp. 1-9.

de Bruijne, M., van Eeten, M., Ganan, C.-H. & Pieters, W., 2017. *Towards a new cyber threat actor typology. A hybrid method for the NCSC cyber security assessment.* Delft: Delft University of Technology.

Demidov, O. & Paoli, G., 2020. *Supply chain security in the cyber age sector trends, current threats and multi-stakeholder responses.* Geneva: United Nations Institue for Disarmament Research.

Eesti Vabariigi põhiseadus (1992) RT 1992, 26, 349.

Eggers, S., 2021. A novel approach for analyzing the nuclear supply chain cyber-attack surface. *Nuclear Engineering and Technology*, 53(3), pp. 879–887.

Ettevõtlus- ja infotehnoloogiaminister, 2022. *Eesti infoturbestandard.* [Võrgumaterjal]
Leitav: https://www.riigiteataja.ee/aktilisa/1211/2202/2034/MKM_m101_lisa.pdf#
[Kasutatud 27. 04. 2023].

Euroopa Komisjon, 2019. *KOMISJONI SOOVITUS (EL) 2019/534,.* [Võrgumaterjal]
Leitav: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32019H0534&from=GA
[Kasutatud 21. 04. 2023].

Euroopa Komisjon, 2020. *The EU's Cybersecurity Strategy for the Digital Decade.* [Võrgumaterjal]
Leitav: https://digital-strategy.ec.europa.eu/et/node/435
[Kasutatud 01. 02. 2023].

Euroopa Komisjon, 2022. *ELi küberkaitsepoliitika.* [Võrgumaterjal]
Leitav: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52022JC0049&qid=1679517899576&from=ET
[Kasutatud 02. 01. 2023].

Euroopa Liidu Nõukogu, 2013. *Otsus (2013/488/EL).* [Võrgumaterjal]
Leitav: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32013D0488&from=ET
[Kasutatud 19. 04. 2023].

Euroopa Liidu Nõukogu, 2022. *Nõukogu järeldused IKT tarneahela turvalisuse kohta.* [Võrgumaterjal]
Leitav: https://data.consilium.europa.eu/doc/document/ST-13664-2022-INIT/et/pdf
[Kasutatud 19. 05. 2023].

Euroopa Parlament, 2022. *Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2557.* [Võrgumaterjal]
Leitav: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32022L2557&qid=1679517899576&from=ET
[Kasutatud 14. 04. 2023].

Euroopa Parlament, 2019. *Euroopa Parlamendi ja nõukogu määrus (EL) 2019/881.* [Võrgumaterjal]

Leitav: https://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:32019R0881 [Kasutatud 19. 04. 2023].

Euroopa Parlament, 2022. *Euroopa Parlamendi ja nõukogu direktiiv (EL) 2022/2555.* [Võrgumaterjal]
Leitav: https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32022L2555 [Kasutatud 08 03 2023].

European Union Agency for Cybersecurity, 2021. *Threat Landscape for Supply Chain Attacks.* [Võrgumaterjal]
Leitav: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks [Kasutatud 17. 02 2023].

European Union Agency for Cybersecurity, 2022. *5G Cybersecurity Standards.* [Võrgumaterjal]
Leitav: https://www.enisa.europa.eu/publications/5g-cybersecurity-standards [Kasutatud 24. 04. 2023].

European Union Agency for Cybersecurity, 2022. *ENISA Cybersecurity Market Analysis Framework (ECSMAF).* [Võrgumaterjal]
Leitav: https://www.enisa.europa.eu/publications/enisa-cybersecurity-market-analysis-framework-ecsmaf
[Kasutatud 29. 04. 2023].

European Union Agency for Cybersecurity, 2022. *ENISA Threat Landscape Methodology.* [Võrgumaterjal]
Leitav: https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology [Kasutatud 28. 04. 2023].

European Union Agency for Cybersecurity, 2022. *Risk Management Standards.* [Võrgumaterjal]
Leitav: https://www.enisa.europa.eu/publications/risk-management-standards [Kasutatud 30. 04. 2023].

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi-Psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y. & Marin, S., 2022. A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. *Healthcare,* 2(10), pp. 1–19.

Goldman, D., 2020. *You Will Be Assimilated: China´s Plan to Sino-form the World.* New York:Post Hill Press.

Gredzens, L., 2017. *Ohutajumise mõõtmine poliitilises diskursuses julgeoleku- ja poliitiliste debattide näitel Läti seimis. Magistritöö.* Tartu: Tartu Ülikool.

Greenberg, A., 2018. *The Untold Story of NotPetya, the Most Devastating Cyberattack in History.* [Võrgumaterjal]
Leitav: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hansen, L., Nissenbaum, H., 2009. Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly,* 53, pp 1155-1175.

Heinbockel, W., Laderman, E. & Serrao, G., 2017. *Supply Chain Attacks and Resiliency Mitigations. Guidance for System Security Engineers.* [Võrgumaterjal]
Leitav: https://www.mitre.org/sites/default/files/2021-11/pr-18-0854-supply-chain-cyber-resiliency-mitigations.pdf
[Kasutatud 19. 01. 2023].

Hoffman, S. K. E., 2018. *Huawei and the ambiguity of China's intelligence and counter-espionage laws.* [Võrgumaterjal]
Leitav: https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/
[Kasutatud 22. 03. 2023].

International Telecommunication Union, 2021. *Guide to Developing a National Cybersecurity Strategy 2nd Edition.* [Võrgumaterjal]
Leitav: https://ncsguide.org/wp-content/uploads/2021/11/2021-NCS-Guide.pdf
[Kasutatud 14. 04. 2023].

Jüris, F., 2020. Arctic Connect ja digitaalne Siiditee Arktikas. *Riigikogu Toimetised*, 41, pp. 145–163.

Jüris, F., 2021. Chinese Security Interests in the Arctic: From Sea Lanes to Scientific Cooperation. Rmt: B. Gaens, F. Jüris & K. Raik, toim-d. *Nordic-Baltic connectivity with Asia via the Arctic: Assessing opportunities and risks.* Tallinn: International Centre for Defence and Security, pp. 126–148.

Kaitsepolitseamet, 2022. *Kaitsepolitsei aastaraamat 2021-2022.* [Võrgumaterjal]
Leitav: https://kapo.ee/et/aastaraamatud/
[Kasutatud 06. 03. 2023].

Kaitsepolitseiamet, 2023. *Kaitsepolitsei aastaraamat 2022-2023.* [Võrgumaterjal]
Leitav: https://kapo.ee/et/aastaraamatud/
[Kasutatud 07. 04. 2023].

Kalmus, V., Masso, A., Linno, M., 2015. *Kvalitatiivne sisuanalüüs. K. Rootalu, V. Kalmus, A. Masso, ja T. Vihalemm (toim), Sotsiaalse analüüsi meetodite ja metodoloogia õpibaas.* [Võrgumaterjal]
Leitav: https://samm.ut.ee/kvalitatiivne-sisuanalyys
[Kasutatud 08. 05. 2023].

Kaska, K., Beckvard, H. & Minarik, T., 2019. *Huawei, 5g and China as a Security Threat.* [Võrgumaterjal]
Leitav: http://195.222.11.251/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf
[Kasutatud 26 01 2023].

Kaska, K. & Tolppa, M., 2020. *Hiina interneti valitsemine ja suveräänsus.* [Võrgumaterjal]
Leitav: https://icds.ee/wp-content/uploads/2020/06/RKK_EVI_-Lu%CC%88hidalt_Hiina_interneti_valitsemine_ja_suvera%CC%88a%CC%88nsus_Kadri_Kaska-_Maria_Tolppa_juuni_2020-1.pdf
[Kasutatud 18 02 2023].

Kidron, A., 2007. *Uurija käsiraamat.* Tallinn: Mondo.

Klimburg, A., 2011. Mobilising Cyber Power. *Survival,* 53(1), pp. 41–60.

Kont, K.-R., 2023. *Eesti elanikkonna teadlikkus küberturvalisusest: ülevaade uuringutest ja võimalikest edasistest suundadest.* Tallinn: Sisekaitseakadeemia.

Koort, E. & Piip, T., 2021. *Hiina mõju Eesti turvalisusele ja julgeolekule.* Tallinn: Sisekaitseakadeemia.

Krekel, B., 2009. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation.* [Võrgumaterjal]
Leitav: https://apps.dtic.mil/sti/pdfs/ADA509000.pdf
[Kasutatud 02. 03. 2023].

Ladisa, P., Plate, H., Martinez, M. & Barais, O., 2022. *Taxonomy of Attacks on Open-Source Software Supply Chains.* [Võrgumaterjal]
Leitav: https://arxiv.org/abs/2204.04008
[Kasutatud 23. 04. 2023].

Laherand, M.-L., 2010. *Kvalitatiivne uurimisviis.* Teine trükk toim. Tallinn: Sulesepp.

Lehto, M., Hummelholm, A., Katsuyoshi, I., Jakstas, T., Karim M., Minami, H., Ohnishi, F. & Saunavaara, J., 2019. Arctic Connect Project and cyber security control, ARCY. *Informaatioteknologian tiedekunnan julkaisuja,* 78, pp. 1–86.

Lindsay, J., 2015. The Impact of China on Cybersecurity: Fiction and Friction. *International Security,* 39(3), pp. 7–47.

Lukinskiy, V., Lukinskiy, Vl. & Churilov, R., 2014. Problems of the supply chain reliability evaluation. *Transport and Telecommunication,* 15(2), pp. 120–129.

Läänemets, M., 2021. Kõrgtehnoloogia ja koonduslaagrid. *Sirp,* [Võrgumaterjal]
Leitav: https://www.sirp.ee/s1-artiklid/c9-sotsiaalia/korgtehnoloogia-ja-koonduslaagrid/
[Kasutatud 29. 11. 2022].

Majandus ja Kommunikatsiooniministeerium, 2021. *Eesti digiühiskond 2030.*
[Võrgumaterjal]
Leitav: https://www.mkm.ee/digiriik-ja-uhenduvus/digiuhiskonna-arengukava-2030
[Kasutatud 01.04. 2023].

Majandus-ja Kommuniikatsiooniministeerium, 2019. *Küberturvalisuse strateegia 2019-2022.*
[Võrgumaterjal]
Leitav: https://www.mkm.ee/media/700/download
[Kasutatud 19. 04. 2023].

Majandus-ja Kommunikatsiooniministeerium, 2022. *Välisinvesteeringu usaldusväärsuse hindamise seaduse eelnõu seletuskiri.* [Võrgumaterjal]
Leitav: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/a37b7d26-d0b7-44a1-8325-b15d3d424b5f
[Kasutatud 08. 03. 2023].

Martinez, J. & Duran, J., 2021. Software Supply Chain Attacks, a Threat to Global Cybersecurity: SolarWinds' Case Study. *International Journal of Safety and Security Engineering,* 11(5), pp. 537–545.

Masip-Bruin, X., Marín-Tordera, E., Ruiz, J., Jukan, A., Trakadas, P., Cernivec, A., Lioy, A., Lopez, S., Santos, H., Gonos, A., Silva, A., Soriano., Kalogiannis, G., 2021. Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture. *Sensors,* Köide 21, pp. 1-24.

Matney, A. & Fannin, B., 2014. *The Challenges of Third-Party Data Protection.* [Võrgumaterjal]
Leitav: http://www.rmmagazine.com/articles/article/2014/12/02/-The-Challenges-of-Third-Party-Data-Protection-
[Kasutatud 27. 04. 2023].

McDaniel, E., 2013. Securing the Information and Communications Technology Global Supply Chain from Exploitation: Developing a Strategy for Education, Training, and Awareness. *Informing Science and Information Technology,* Köide 13, pp. 313-324.

National Institute of Standards and Technology, 2021. *Key Practices in Cyber Supply Chain Risk Management: Observations from Industry.*. [Online]
Leitav: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf
[Kasutatud 25. 04. 2023].

North Atlantic Council, 2020. *SECURITY WITHIN THE NORTH ATLANTIC TREATY ORGANIZATION (NATO).* [Võrgumaterjal]
Leitav: https://valisluureamet.ee/doc/infosec/C-M_2002_49_REV1.pdf
[Kasutatud 19. 04. 2023].

OECD, 2020. *Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation.* [Võrgumaterjal]
Leitav: https://www.oecd.org/finance/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf
[Kasutatud 16. 12. 2022].

Oksaar, K., 2014. *Küberjulgeolekustamine Kopenhaageni koolkonna teooria järgi Eesti Vabariigi diskursuse näitel. Magistrtitöö.* Tartu: Tartu Ülikool.

Pernik P., Jančárková T., Kaska K., Ruuto U., Gheorghevici C. & Beckvard H., 2021. *Supply Chain and Network Security for Military 5G Networks,* Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Pilichos, G., 2017. *Securitization of Cyberspace. Magistritöö.* Tallinn: Tallinn University.

Pomfret, J. & Koper, A., 2019. Huawei sacks employee arrested in Poland on spying charges. *Reuters,* [Võrgumaterjal]
Leitav: https://www.reuters.com/article/us-huawei-poland-security-idUSKCN1P60E8
[Kasutatud 23. 03. 2023].

Raponi, S., Caprolu, M. & Di Pietro, R., 2021. *Beyond SolarWinds: The Systemic Risks of Critical Infrastructures, State of Play, and Future Directions.* [Võrgumaterjal]
Leitav: https://ceur-ws.org/Vol-2940/paper33.pdf
[Kasutatud 25. 01. 2023].

Raud, M., 2016. *China and Cyber: Attitude, Strategies, Organisation.* [Võrgumaterjal]
Leitav: https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf
[Kasutatud 19. 02. 2023].

Reichert, C., 2018. *Huawei denies foreign network hack reports.* [Võrgumaterjal]
Leitav: https://www.zdnet.com/article/huawei-denies-foreign-network-hack-reports/
[Kasutatud 20. 03. 2023.].

Schwandt, T., and Gates, E., 2018. Case Study Methodology. Rmt: E. Denzin, toim. *The SAGE Handbook of Qualitative Research.* 5th Edition toim. Thousand Oaks: SAGE, pp. 600-631.

Sailio, M., Latvala, O-M. & Szanto, A., 2020. Cyber Threat Actors for the Factory of the Future. *Applied Sciences*, 10(12), pp. 1–25.

Salu, M., 2023. Eesti politsei suunas riigihanke kahtlase kuulsusega Hiina firmale.*Eesti Ekspress*, [Võrgumaterjal]
Leitav: https://ekspress.delfi.ee/artikkel/92718953/eesti-politsei-suunas-riigihanke-kahtlase-kuulsusega-hiina-firmale?fbclid=IwAR2SUcS67inhHVaG9t52qW5ZLdbGVAfKV2ChV
[Kasutatud 18. 03. 2023].

Sazonov, V., Koort, E., Heinsoo, P. & Paas, K., 2020. *Sisejulgeoleku hübriidohtude tutvustamine.* Tallinn: Sisekaitseakadeemia.

Shafique, K., Khawaja, B., Sabir, F., Qazi, S.& Mustaquim, M., 2020. Internet of Things (IoT) for Next-Generation Smart Systems: A Review of Current Challenges, Future Trends and Prospects for Emerging 5G-IoT Scenarios. *IEEE*, 8, pp. 1–19.

Shakarian, P., 2011. The 2008 Russian Cyber Campaign Against Georgia. *Military Review*, pp. 63–68.

Shehod, A., 2016. *Ukraine Power Grid Cyberattack and US Susceptibility: Cybersecurity Implications of Smart Grid Advancements in the US.* Cambridge: Massachusetts Institute of Technology.

Shuya, M., 2018. Russian Cyber Aggression and the New Cold War. *Journal of Strategic Security*, 11(1), pp. 1–18.

Singh, G., 2020. *Analysing the effect of internet of things to supply chain management in e-commerce industry in India. Magistritöö.* Tallinn: Tallinn Univeristy of Tehcnology.

Siseministeerium, 2020. *Siseturvalisuse arengukava 2020-2030.* [Võrgumaterjal]
Leitav: https://www.siseministeerium.ee/stak2030
[Kasutatud 19 04. 2023].

Stake, R., 1995. *The Art of Case Study research.* Thousand Oaks: Sage Publications.

Stritzel, H., 2007. Towards a Theory of Securitization: Copenhagen and Beyond. *European Journal of International Relations*, 13(3), pp. 357–383.

Strömpl, J., 2014. *Juhtumiuurimus. K. Rootalu, V. Kalmus, A. Masso, ja T. Vihalemm (toim), Sotsiaalse analüüsi meetodite ja metodoloogia õpibaas.* [Võrgumaterjal]

Leitav: https://samm.ut.ee/juhtumiuurimus
[Kasutatud 08. 05. 2023].

Zdanavičius, L., 2021. Russia, China and the Baltic connectivity. Rmt: B. Gaens, F. Jüris & K. Raik, toim-d. *Nordic-Baltic connectivity with Asia via the Arctic: Assessing opportunities and risks.* Tallinn: International Centre for Defence and Security, pp. 252–328.

Thomas, T., 2000. The Russian view of information war. Rmt: M. H. Crucher, toim. *The russian armed forces at the dawn of the millennium.* Carlisle, PA: Center for Strategic Leadership, U.S. Army War College, pp. 335–361.

Teddlie, C., & Yu, F., 2007. Mixed methods sampling: A typology with examples. *Journal of Mixed Methods Research,* 1(1), pp. 77-100.

Telia Eesti AS, 2022. *Telia Company turvadirektiivid.* [Võrgumaterjal]
Leitav: https://www.telia.ee/images/documents/juhendid/est/tarnija_turvadirektiivid.pdf
[Kasutatud 04. 04. 2023].

Tikk, E., Kaska, K. & Vihul, L., 2010. *International Cyber Incidents: Legal Considerations.* Tallinn: Cooperative Cyber Defence Centre of Excellence.

Tran, C., 2021. *The SolarWinds Attack and Its Lessons.* [Võrgumaterjal]
Leitav: https://www.e-ir.info/2021/06/17/the-solarwinds-attack-and-its-lessons/
[Kasutatud 19. 02. 2023].

Täri, T., 2017. *Sisserände julgeolekustamine Eestis poliitiliste kõneaktide põhjal 2014-2016, Magistritöö,* Tallinn: Sisekaitseakadeemia.

U.S. Department of Commerce, U.S. Department of Homeland Security, 2022. *Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry.* [Võrgumaterjal]
Leitav: https://www.dhs.gov/publication/assessment-critical-supply-chains-supporting-us-ict-industry
[Kasutatud 26. 04. 2023].

Urciuoli, L., Männistö, T., Hintsa, J., Khan, T., 2013. Supply chain Cyber Security - Potential Threats. *Information & Security,* 29(1), pp. 51- 69.

Urciuoli, L., 2015. Cyber-Resilience: A Strategic Approach for Supply Chain Management. *Technology Innovation Management Review,* 5(4), pp. 13-18.

Vabariigi Valitsus, 2023. *Eesti julgeolekupoliitika alused.* [Võrgumaterjal]
Leitav:
https://www.kaitseministeerium.ee/sites/default/files/eesti_julgeolekupoliitika_alused_est_22.02.pdf
[Kasutatud 26. 03. 2023].

Valk, B., 2022. NATO Cyber Policies in Relation to the International Stability Framework. Analüüs: P. Pernik: C, toim. . *Cyberspace Strategic Outlook 2030 Horizon Scanning and Analysis.* Tallinn: NATO CCDCOE Publications, pp. 66–82.

Weitz, R., 2016. NATO Varssavi tippkohtumine: hinnang. *Diplomaatia,* September (157), pp. 8–11.

Villalón-Huerta, A., Ripoll-Ripoll, I. & Marco-Gisbert, H., 2022. A Taxonomy for Threat Actors' Delivery Techniques. *Applied Sciences,* 12(8), pp. 1–23.

Willett, M., 2021. Lessons of the SolarWinds Hack. *Survival,* 2(63), pp. 7–26.

Wills, M., 2021. *Official (ISC)2 Student Guide. Volume 2.* 6th edition. London: (ISC)2 Publications .

Wu, X., 2007. *Chinese Cyber Nationalism. Evolution, Characteristics, and Implications.* Lanham: Lexington Books.

Välisluureamet, 2022. *Eesti rahvusvahelises julgeolekeskkonnas 2022.* [Võrgumaterjal] Leitav: https://valisluureamet.ee/hinnang.html
[Kasutatud 06 11 2022].

Õunapuu, M., 2014. *Kvalitatiivne ja kvantitatiivne uurimisviis sotsiaalteadustes.* Tartu: Tartu Ülikool.

Yeng, P. K., Fauszi, M. A. & Yang. B., 2021. *Assessing the effect of human factors in healthcare cyber security practice: An empirical study.*. s.l., 25th Pan-Hellenic Conference on Informatics, pp. 472–476.

Lisa 1. Intervjuu küsimuste seos uurimisküsimustega

Uurimisküsimus	Intervjuu küsimused
Millised on võimalikud riist-ja tarkvarast ning selle haldamisest, alltöövõtjatest ning ettevõtte ja avaliku sektori asutuse personalist tulenevad ohud riigi IKT tarneahelale?	1. Kui kõrgeks Te hindade riske seoses IKT tarneahela küberrünnakutega? 2. Kas riik pöörab piisavalt tähelepanu probleemile? 3. Millised on võimalikud tagajärjed Teie asutusele? 4. Millised on potentsiaalsed ja kõige tõenäolisemad ründevektorid (riist-ja tarkvara, haldus, alltöövõtjad, inimfaktor, muu)?
Kuidas ja milliste kriteeriumite alusel oleks riigi IKT asutustel võimalik hinnata ja kontrollida kasutatava riist- ja tarkvara, riiklike ja riigi seisukohast oluliste infosüsteemide arendus- ja hooldusfirmade usaldusväärsust?	5. Kuidas teie hinnangul saaks riske maandada/ennetada? 6. Kas täna on selleks olemas tõhusad tööriistad? 7. Kuidas saaks teie arvates muuta tööriistad tõhusamaks, ehk turvalisemaks?
Kuidas ja millistel alustel oleks riigi IT-majadel (RIT, SMIT, RMIT, RIA, RIKS jne) võimalik teostada usaldusväärsuse kontrolli alltöövõtjate ja nende personali üle?	
Kuidas ja milliste kriteeriumite alusel oleks riigiasutustel ja nende valitsemisalas olevatel juriidilistel isikutel võimalik välistada riigihangetest ebausaldusväärseid pakkujaid?	8. Kas Teie asustuses on olemas reeglid, mis võimaldavad kontrollida hankes osalevate ettevõttete usaldusväärsust?

Lisa 2. Dokumendianalüüsi koodipuu (NVivo faili põhjal autori koostatud).

Name	Files	References
Küberrünnakud		
Hiina	4	17
küberrünnak	5	19
Küberrünnaku tagajärg	9	22
Küberrünnakud süsteemide vastu	2	3
Küberrünnakud tarneahela vastu	3	12
NotPetya	3	5
SolarWinds	2	3
Venemaa	5	12
Soovitused riskide maandamiseks		
alltöövõtja	7	24
haldus	6	23
partner	8	27
personal	5	17
riistvara	5	10
riskianalüüs	10	31
tarkvara	6	17
Küberturvalisuse tagamise eesmärk ja vajadus		
Küberohud	6	15
Küberriskid	18	64
küberturvalisuse olulisus	10	19
Kübertuvalisuse eesmärk	3	4
Kübertuvalisuse mõiste	3	6
Tarneahela olemus ja selle kaitse vajadus		
alltöövõtja	2	4
haldus	6	20
partnerid	6	18
personal	7	18
riistvara	8	22
rünnaku vektorid	12	41
Tarahela riskid	14	64
tarkvara	10	34
Tarneahela mõiste	5	16
Tarneahela mõju	7	17

Lisa 3. Turvanõuded teenuseosutajale (koostatud Telia Eesti AS turvadirektiivide alusel)

Turvariskide juhtimine
Teenuseosutaja peab perioodiliselt tuvastama, analüüsima, hindama ja kõrvaldama turvariske.

Infoturbepoliitikad
Teenuseosutajal on määratletud ja dokumenteeritud infoturbe juhtimissüsteem (information security management system, ISMS), sealhulgas kehtestatud ja kinnitatud infoturbepoliitika ja rotseduurid.

Infoturbe korraldamine
Teenuseosutajal on oma organisatsioonis määratletud ja dokumenteeritud turvarollid ja -vastuused.

Personaliga seotud turve
Teenuseosutaja tagab, et kõik lepingu alusel ülesandeid täitvad töötajad on usaldusväärsed ja vastavad mis tahes kehtestatud turvalisuse kriteeriumidele. Teenuseosutajal on sätestatud ja dokumenteeritud varahaldussüsteem ning ta peab ajakohastatud registreid kõigi asjakohaste varade ja nende omanike kohta. Varade hulka kuuluvad muu hulgas teave, IT-süsteemid, teavet sisaldavad varukoopiad ja/või eemaldatavad andmekandjad, juurdepääsuõigused, tarkvara ja konfiguratsioon.

Andmed
Teenuseosutaja rakendab meetmeid, et tagada kaitse juhusliku, volitamata või ebaseadusliku kadumise, hävitamise, muutmise või kahjustamise eest seoses ostja edastatud, salvestatud või muul viisil töödeldud andmetega.
Teenuseosutaja tagastab või hävitab kõik andmed ja nende koopiad lepingu lõppemisel või nõudmisel. Teenuseosutaja kinnitab kirjalikult, et teenuseosutaja on selle nõude täitnud.

Juurdepääsu kontroll
Teenuseosutajal peab olema määratletud ja dokumenteeritud juurdepääsukontrolli poliitika rajatiste, tegevuskohtade, võrgu, süsteemi, rakenduste ja teabe/andmete juurdepääsu jaoks (sealhulgas füüsilise, loogilise ja kaugjuurdepääsu kontroll).
Teenuseosutaja peab kehtestama kasutajate juurdepääsu ja privileegide autoriseerimise protsessi, juurdepääsuõiguste tühistamise korra ja personali juurdepääsuõiguste aktsepteeritava kasutamise korra.
Teenuseosutaja määrab kõik juurdepääsuõigused teadmisvajaduse ja vähimate privileegide põhimõtte alusel.

Krüpteerimine
Vajadusel kasutatakse krüpteerimismeetodeid, mida peetakse turvaliseks vastavalt parimatele praktikatele.

Füüsiline ja keskkonnaturve
Teenuseosutaja kaitseb oma andmetöötlusrajatisi väliste ja keskkonnaohtude ja ohtude eest, sealhulgas elektri-/kaabeldamishäirete ja muude häirete eest, mis võivad põhjustada rikkeid pakutavates teenustes. See hõlmab füüsilist perimeetri ja juurdepääsu kaitsmist.

Talitluskindlus
Teenuseosutaja rakendab pahavara kaitset, tagamaks, et tarkvara, mida teenuseosutaja kasutab tarnitavate toodete tarnimiseks, on kaitstud pahavara eest.
Teenuseosutaja rakendab operatiivseid ja tehnilisi turvakontrolle, nagu logihaldus, tulemüürid, viirusetõrje ja krüpteerimine vastavalt tööstusharu parimatele tavadele.
Teenuseosutaja teeb kriitilisest teabest varukoopiaid ja testib varukoopiaid, et tagada teabe taastamine vastavalt ostjaga sõlmitud kokkuleppele.

Suhe partneritega
Teenuseosutaja peab kajastama tarnijate käesoleva dokumendi sisu oma lepingutes partneritega, kes täidavad lepingu alusel määratud ülesandeid.
Vajadusel teenuseosutaja esitab tõendid selle kohta, et partner täidab dokumendis sätestatud nõudeid.

Turvaintsidentide haldamine
Teenuseosutaja peab kehtestama turvaintsidentide haldamise korra.
Igast turvaintsidendist teavitatakse viivitamata pärast turvaintsidendi tuvastamist.

Äritegevuse järjepidevuse juhtimine
Teenuseosutajal peavad olema dokumenteeritud protsessid ja kord talitluspidevuse, sealhulgas avariitaastekava järgimiseks.
Teenuseosutaja peab regulaarselt tuvastama, analüüsima ja hindama talitluspidevuse riske ning võtma vajalikke meetmeid selliste riskide kontrollimiseks ja leevendamiseks.

Vastavus
Teenuseosutaja järgib kõiki asjakohaseid õigusaktidest ja lepingutest tulenevaid nõudeid, sealhulgas neid, mis on seotud Isikuandmete kaitsega.
Teenuseosutaja esitab aruande turvanõuete täitmise kohta.
Teenuseosutaja esitab vajalikud sertifikaadid, kui nad on olemas.
Teenuseosutaja teavitab sellest, kuidas ta täidab turvanõudeid ja milliseid meetmeid ta on võtnud turvanõuete täitmiseks.
Teenuseosutaja jälgib ja auditeerib regulaarselt partnerite vastavust turvanõuetele.
Teenusesaajal on õigus kontrollida, kuidas teenuseosutaja ja tema partnerid täidavad turvanõudeid või vastavaid nõudeid.