Sisekaitseakadeemia
Sisejulgeoleku instituut

Hendrik Pillmann

ASJADE INTERNETI TEHNOLOOGIA KASUTUSEGA SEONDUVAD TURVALISUSE RISKID NING NENDE MAANDAMINE INIMESTE TAVAKASUTUSES OLEVATE TEHNOLOOGIATE NÄITEL

Magistritöö

Juhendaja:
Jaanika Puusalu, PhD

Kaasjuhendaja:
Ester Pukk, MA

Tallinn 2021

MAGISTRITÖÖ ANNOTATSIOON

Instituut: Sisejulgeoleku instituut	Kaitsmise kuu ja aasta: Juuni 2021
Töö pealkiri eesti keeles: Asjade interneti tehnoloogia kasutusega seonduvad turvalisuse riskid ning nende maandamine inimeste tavakasutuses olevate tehnoloogiate näitel.	
Töö pealkiri võõrkeeles: *Security risks related to the use of Internet of Things and risk mitigation: a case study of common technologies.* Uurimistöö keskendub asjade interneti kasutuselevõtust tulenevate turvalisuse riskide kaardistamisele inimeste tavakasutuses olevate seadmete näitel. Töös kaardistatakse, kuidas asjade interneti seadmete riskide tekkimine võib mõjutada küberintsidente ja küberkuritegevust uurivate asutuste igapäevast tööd. Uuriimistöö eesmärk on välja selgitada asjade interneti tehnoloogia arengust tulenevad riskid tehnoloogia kasutajaskonna ning avaliku sektori ameti- ja haldusasutuste jaoks. Töö on kvalitatiivne empiirline uuring, mille uurimisstrateegiaks on fenomenograafia.Töö teoreetiline raamistik tugineb interneti ajaloo ja asjade interneti käsitlusele ning tehnoloogia riske vaadeldakse turvaelementide ning asjade interneti ehitusliku arhitektuuri kaudu, mille kaudu tuvastatakse erinevad ründed, mida annab asjade interneti seadmetele suunata. Asjade interneti seadmete näidetena minnakse süvitsi Amazon Echo tootesarja nutikõlaritega, mida kõrvutatakse turvaelementide ja asjade interneti kolmekihilise arhitektuurilise plaaniga. Töö tuvastas, kuidas kohalikud- ja rahvusvahelised kübervaldkonna dokumendid defineerivad asjade interneti mõistet üldiste tehnoloogiast tulenevate probleemide keskel ning milliseid probleeme toob kaasa asjade interneti seadmete laialdane kasutamine avalikule sektorile nii kübervaldkonna dokumentide kui ka ekspertide hinnangul. Uurimistöö tulemusena esitas autor soovitused tavakasutajatele asjade interneti seadmete turvaliseks kasutamiseks ning ettepanekud poliitikakujundajatele. Töös on 93 lehekülge, millest põhiosa on 73 leheküljel. Töö sisaldab 1 joonist, 7 tabelit ja 6 lisa. Töö on kirjutatud eesti keeles, ingliskeelsena on kirjutatud töö resümee.	
Lisad (nt CD, DVD jms): Puuduvad.	
Võtmesõnad: Asjade internet, digitaliseerumine, internet, digitehnoloogia, küberturvalisus	
Võõrkeelsed võtmesõnad: Internet of Things, Cyber security, IoT, Connected devices, smart home devices	
Säilitamise koht: Sisekaitseakadeemia raamatukogu	
Töö autor: Hendrik Pillmann Allkiri: *(allkirjastatud digitaalselt)*	
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.	
Vastab magistritöö nõuetele	
Juhendaja: Jaanika Puusalu Allkiri: *(allkirjastatud digitaalselt)*	
Kaasjuhendaja: Ester Pukk Allkiri: *(allkirjastatud digitaalselt)*	
Kaitsmisele lubatud	
Instituudi juhataja: Anne Valk (instituudi juhataja Erkki Koorti ülesannetes) Allkiri:	

SISUKORD

TERMINITE JA LÜHENDITE LOETELU

IoT – *Internet of Things* (ingl), asjade internet

RIA – Riigi Infosüsteemide Amet

RFID – *Radio-frequency identification* (ingl), raadiosagedustuvastus

ENISA – European Union Agency for Cybersecurity (ingl), Euroopa Liidu Küberturvalisuse Amet

TalTech – Tallinna Tehnikaülikool

IKT – Info- ja kommunikatsioonitehnoloogia

SMIT – Siseministeeriumi infotehnoloogia- ja arenduskeskus

ISKE – Infosüsteemide kolmeastmeline etalonturbe süsteem, mille eesmärk on süsteemides töötlemisele kuuluvate andmete jaoks piisava turvalisuse tagamine

Nutistu – asjade interneti sünonüüm

Värkvõrk – asjade interneti sünonüüm

CERT – Computer Emergency Response Team ehk organisatsioon, mis tegeleb küberkaitse probleemide uurimise ja lahendamisega

CERT-EE – ehk CERT Eesti, RIA intsidentide käsitlemise osakond

ARPA - *Department of Defence Advanced Research Projects Agancy* - USA Kaitseministeeriumi Teadusuuringute Projektide Agentuur.

SISSEJUHATUS

Inimeste igapäevast elukorraldust määrab aina enam digitaalne info- ja kommunikatsioonitehnoloogia. Arvuti, nutitelefon, targad mõõdikud ja tehisintellekti süsteemidega võimestatud tööstustehnoloogia soodustavad inimeste tõhusamat toimetulekut ühiskonnas (Bejtkovský *et al*., 2018, p. 60). Digitaliseerumise ehk digitaalsete tehnoloogiate kasutamise ning tehnoloogia abil väärtust loovate võimalustega keskendutakse tehnoloogia olulisusele toodete ja igapäevaste teenuste pakkumisel, kasutades uute lahendustena näiteks andmeanalüüsi ja häältuvastust (Parida, 2018, pp. 23–24).

Digitaliseerumist kui tänapäeva ühte olulisemat mõistet on 21. sajandi kahe esimese kümnendi jooksul käsitletud tehnoloogia arengust kantud suundumusena, mis ühiskonda ning inimeste elu nii lähitulevikus kui ka pikemas perspektiivis muudab (Parviainen, *et al*., 2016, p. 64). Digitehnoloogia mõjuvõimule aitab suuresti kaasa internet, mis võimaldab kergesti tehnoloogia ja rakenduste omavahelist suhtlemist. Internet on protokollide abil toimiv võrgustik, kus arvutid ja sarnase võimekusega tehnoloogia on omavahel ühendatud. See võrgustik võimaldab andmevahetust ja tagab nii tehnoloogia kui ka tarkvara koostoimimise. Miljardid inimesed kasutavad internetti kommunikatsiooni, meelelahutuse ja muude rakenduste ning teenuste tööriistana. E-post, pangandus, e-kaubandus, tervishoiuteabe ja uudiste otsimine ning üle maailma populaarsete saitide, näiteks Youtube'i, Facebooki ja Google'i kasutamine on vähesed näited, mida interneti abil on võimalik teha. Teenustel, mida interneti vahendusel kasutada saab, on võime mõjutada sotsiaalseid suhteid, kultuuri, poliitikat ja inimeste sotsiaalseid tegevusi, sest arvutite teel ühendatavus pakub üha enam võimalusi füüsilise maailma digitaalsesse ruumi ülekandmiseks (Warf, 2011, p. 1).

Interneti kasutajate arv maailmas kasvab jõudsalt. Maailmas oli 2019. aastal interneti kasutajaid 4,388 miljardit. Võrreldes 2018. aastaga kasvas interneti kasutajate arv 9,8% (We Are Social, 2019). Interneti kasutus on populaarne ka Eestis. Riigi Infosüsteemide Ameti (2020, lk 5) andmete järgi kasutab 91,6% Eesti elanikest aktiivselt internetti. Märkimisväärne koguarv eestlastest, kuid lisaks ka suur osa maailma kogupopulatsioonist omab seega interneti teel võimalust ühenduda teiste sarnaselt võrku ühendatud asjadega üle terve maailma.

Internetiga ühendumise vahend on traditsiooniliselt olnud arvuti. 2020. aasta aastaraamatus toob Riigi Infosüsteemide Ameti (2020, lk 5) välja statistika, et 87% majapidamistest Eestis on arvuti. Siiski on aja jooksul traditsiooniliste laua- ja sülearvutite kõrvale tulnud ka teisi võrku ühenduvaid seadmeid. Üks selliseid seadmeid on nutitelefon, mis on püsiva võrguühendusega pihuarvuti, kus saab kasutada eri rakendusi (Oulasvirta, *et al*., 2012, p. 105). Statista (2021) andmetel kasutas 2020. aastal

nutitelefone 3,5 miljardit inimest maailma kogupopulatsioonist. See näitab, et ligi pool maailma elanikkonnast kasutab ühte kindlat liiki seadet, millel on sisuliselt üle terve maailma võimalus ühilduda inimesele sobival ajal võrku. Peale nutitelefonide on internetiga ühilduvaid seadmeid teisigi ja ka need koguvad laiemalt populaarsust. Kõrget võrku ühenduvate seadmete kasutamise trendi näitavad ka eestlased, kellest 2017. aasta seisuga omab 848 000 (69%) võimalust kasutada nutiseadmeid, näiteks nutitelefone ja tahvelarvuteid. 2014. aastal omas nutiseadmeid 60% kogurahvastikust, seega kasvas nutiseadmete omamine Eestis kolme aastaga 9% võrra (Kantar Emor, 2017, lk 4).

Maailma statistika kõrval näitab ainuüksi Eesti majapidamistes kasutuses olevate arvutite ning võrku ühilduvate nutiseadmete hulk seda, et digitehnoloogia on saanud inimeste igapäevaelu lahutamatuks osaks. Tehnoloogia arenguga on ka interneti kasutamine saanud iseenesest mõistetavaks tänu kõikidele ühenduvatele seadmetele. Aastal 2000 oli internetikasutajate osatähtsus Eestis alla 30%, samas kui 2016. aastaks oli see kasvanud tervelt 86 protsendini ning 2018. aastaks 90 protsendini (Statista, 2020). Suur põhjus selles on inimeste soov teha igapäevaseid toimetusi võimalikult kiiresti ja mugavalt. Seadmed ja internet suudavad just seda inimesele pakkuda. Riigi Infosüsteemide Amet (2020, lk 14) toob oma 2020. aasta aastaraamatus välja, et seadmete abil internetis tehtud toimingud säästavad keskmiselt 15 minutit toimetuste kohta ning hoidsid 2019. aastal hinnanguliselt kokku 1100 aasta jagu Eesti inimeste tööaega. Võrgustatud digitehnoloogia kasutamine on laialt levinud ning seadmete arv kasvab pidevalt. Tänu tehnoloogia arenemisele on ka paljud kodused seadmed nüüdseks arvuti võimekusega ning kogu aeg võrku ühendatud, et koostoime abil optimaalsemalt ülesandeid täita. Nii võib kodudest leida tarku kodumasinaid, näiteks külmkappe ja tolmuimejaid, mis lisaks otstarbest tulenevatele ülesannetele vahetavad omavahel andmeid täiendamaks üksteise tegevust.

Arvutite, nutiseadmete ja interneti omavahelist suhet aitab lahti seletada 2020. aastal maailma tabanud epidemioloogiline kriis, mille tõttu on tõusnud interneti ning digitehnoloogia kasutamise hulk. Maailmas aset leiduvate üleriigiliste sulgemiste ja sotsiaalse ning füüsilise distantsi hoidmise vajadusest sõltuvad inimesed digitehnoloogiast rohkem kui iial varem. Märkimisväärselt on kasvanud videokonverentsideks vajalike seadmete kasutamine, sest inimesed töötavad pandeemia tõttu järjest rohkem kodukontorites, kus töö, kuid lisaks ka õppetöö korraldamiseks on vajalik videovõimalusega seadmete ning internetiühenduse olemasolu (De *et al*., 2020, pp. 1–2). Arvutid ja nutiseadmed ning nende võimalus omavahel interneti kaudu ühendust saada on andnud inimestele võimaluse pandeemia mõjusid leevendada. Distantsilt suhtlemine ning muutused töö-, õppe- ja ka tarbimisharjumustes on andnud hoogu digitaaltehnoloogia arengule, esile on kerkinud ka teabe jagamise ning platvormi ja jagamisviisi turvalisuse küsimus. Näitena saab tuua videokonverentside keskkonna Zoom, mille kasutamine kasvas suuresti seetõttu, et koroonaviiruse pandeemia sundis 2020. aastal miljoneid

inimesi koju jääma. Platvorm võimaldab lihtsasti videopildis inimeste vahel ühendust saada, kuid paralleelselt kasutajate arvukuse kasvuga suurenesid 2020. aastal keskkonnaga ka probleemid. Zoomis, näiteks, leidsid aset lekked, kus tumeveebi sattusid müügiks 500 000 Zoomi kasutaja kontoandmed (Secara, 2020, pp. 13–15).

Arvutite ning nutiseadmete laialdase kasutamise ja koostoimega on hakatud kasutama mõistet „asjade internet'' (ingl *Internet of Things,* lühidalt ka IoT), mida eesti keeles nimetatakse ka värkvõrguks või nutistuks. Andrew Guthrie Fergusoni ilukirjanduslik paralleel aitab selgitada asjade interneti ehk võrgustatud seadmete koostoime uudset olemust: „Ameerika Ühendriikide asutamise ajal olid kõik asjad käega katsutavad. Raamatud ei elanud pilves. Hobuste veetud vankreid ei jälitanud GPS-seadmed" (Ferguson, 2016, p. 805). Asjade internetti, mida nimetatakse ka kõikide asjade internetiks, saab digitaliseerumise kontekstis käsitleda globaalse võrgustikuna, kus masinad ja seadmed on võimelised omavahel interneti abil suhtlema (Lee & Lee, 2015, p. 431). Masinate omavahelise suhtlemise all mõeldakse seadmete kogutavat informatsiooni, näiteks tervisenäitajate vahetamist eri seadmete vahel ning asjade internetis käib see andmevahetus automatiseeritult. Sisuliselt on tegemist info vahetamise võimekusega, mis varem oli olemas arvutil ja nutitelefonil, kuid nüüd võib eksisteerida kõikidel seadmetel. Nii on ka andmete jagamise turvalisuse probleem tänasel päeval kõikidele seadmetele laienenud, sest lisaks traditsioonilistele seadmetele on ohud üle kandunud ka näiteks igapäevases kasutuses olevatele kodutehnikale.

Oleme jõudnud ajajärku, kus kõik võib olla ühtaegu nutikas ja digitaalne. Eelpool välja toodud tehnoloogilised lahendused on spetsiifilised näited, kuid üldjoontes tavainimese kasutuses olevate seadmete internetiga ühildatavuse tõttu tekitanud olukorra, kus suurel osal inimestel ja asjadel on olemas digitaalne identiteet. Digitaalne identiteet kujutab endast hulka andmeid, millega on võimalik inimesi või asju unikaalselt kirjeldada, kuid mis lisaks sisaldab ka informatsiooni inimese või asja suhete kohta teiste osalistega (Windley, 2005, p. 8). Asjade interneti seadmete kasutamine on pidevalt kasvutrendi näitav. 2009. aastal oli internetti ühendatud 900 miljonit seadet (Lee & Lee, 2015, p. 431). 2014. aastal ennustas Gartner Research 2020. aastaks 26 miljardit internetti ühildatud asjade interneti seadet. Laialdasem seadmete kasutamine suurendab ka inimeste ja asjade digitaalset jalajälge. Igapäevakasutuses on paljud ühendamisvõimekusega nutikad seadmed, mida tervikuna võib pidada andurite ja ajamite võrguühenduseks, millel on ainulaadne raamistik teabe jagamiseks (Adat & Gubta, 2018, p. 423).

Kasvav seadmete ning ühtlasi ka võrku ühilduvate seadmete arv põhjustab aga turvariske. Hsu & Lin (2016. p. 49) toovad oma artiklis välja Ameerika Ühendriikide Riikliku Luurenõukogu 2008. aastal mainitud kuus "häirivat tsiviiltehnoloogiat", mis oma olemusega Ameerika Ühendriikidele ohtlikeks

võivad osutuda. Ühe tehnoloogiana on välja toodud asjade interneti seadmed, mille probleemkohad seisnevad lisaks tuvastuse ning jälgimisega seonduvas võimekuses ja kaugjuhtimises (National Intelligence Council, 2008, pp. 1–31). Seadmed on varustatud anduritega, mis on võimelised pidevalt teavet koguma ning omavad seetõttu infoturberiske (Hsu & Lin, 2016, p. 49).

Võrku ühendatud seadmete näol eksisteerivad positiivsete ilmingute kõrval ka ohud. Seadmete kaudu mitte üksnes ei talletata, vaid ka jagatakse isiklikku kontaktinformatsiooni ja privaatseid sõnumeid, mis sisaldavad nii pilte, audio- ja videofaile ning tundliku sisuga materjali. Võrku ehk internetti ühilduvate seadmetega kaasneb konkreetne oht kasutajatega seotud informatsioonile – varjatud jälgimine, identiteedivargused, andmepüük, viirused ja nuhkvara on vaid vähesed näited, kuidas pahatahtlikud kolmandad osapooled võivad interneti kaudu teistele internetikasutajatele ligi pääseda (Rocha Flores *et al*., 2014, pp. 403-404). Näiteks lekkis 1. jaanuaril 2019 "*Collection #1*" (ingl) nime all tuntud andmekogu meiliaadressidest ja paroolidest, millele häkkerid ligi olid saanud. Esmajoones lekkis tumeveebi üle 770 miljoni meiliaadressi ning 21 miljoni unikaalse parooli. Leke oli üks osa suuremast andmelekete seeriast, mõjutades ka näiteks kommertslennukite tootja Airbusi tegevust, mille infosüsteem andmelekke all kannatas (Check Point Research, 2020, p. 8). Kõik lekkinud andmekogud sisaldasid inimeste andmeid, mille valedesse kätesse sattumise korral on võimalik pääseda ligi veelgi detailsematele andmetele. Teine juhtum, näitlikustamaks asjade interneti turvalisuse probleeme, on Ringi turvakaameratele tehtud rünnakud. Häkkerid pääsesid otsevaates Ringi klientide kodu ümbritsevatesse kaameratesse ning suutsid seadmetega ühendatud mikrofonide ja kõlarite kaudu suhelda inimestega eemalt. Teadete järgi olid häkkerid mitte üksnes visuaalselt inimesi jälginud, vaid ka verbaalselt seadmeid kasutanud inimeste tegevust häirinud (Conosco, 2021).

Digitehnoloogia ja interneti ohte on tarvis ühiskonnas kaardistada ning ohtude ennetusega tegeleda. Internetis aktiivsed inimesed saavad teha palju, et nende sealne tegevus oleks turvaline, sest kui turvalisuse eest hoolt ei kanta, saab sellest korrakaitseasutuste ja julgeoleku küsimus. Euroopa Liidu Võrgu- ja Infoturbeamet (2020, pp. 7–9) toob välja, et 2019. aastal olid Euroopas aset leidnud juhtumid valdavalt seotud rünnakutega digitaalteenuste, panganduse, tehnoloogia- ja tervishoiusektori vastu. Eestis registreeriti 2019. aastal kokku 965 arvutikuritegu, millest 768 olid arvutikelmused ning 197 arvutiandmete ja -süsteemi kuriteod (Justiitsministeerium, 2020). 2020. aasta statistika näitab tõusutrendi – arvutikuritegusid registreeriti kokku 1079, millest arvutikelmuseid oli 82 ning arvutiandmete ja -süsteemi kuritegusid 254 (Justiitsministeerium, 2021). Kasvava intsidentide arvu tõttu on olulisel kohal riigi roll kaitsemehhanismide ja juhiste loomisel. Sisendi juhistesse annavad korrakaitse- ja julgeolekuasutused, mis iga päev kübervaldkonna probleemidega silmitsi seisavad. Eesti arvutivõrkude küberintsidentide tuvastamise, jälgimise, lahendamise ning ennetustööga tegeleb CERT-EE, kelle ülesanne on aidata peaasjalikult asutusi

küberintsidentide asjus (Riigi Infosüsteemide Amet, 2021). Arvutikuritegude menetlemisega tegeleb Politsei- ja Piirivalveamet, mille jaoks mõjutab arvutikuritegevuse tõus otseselt menetluseks vajalikke toiminguid (Politsei- ja Piirivalveamet, 2021). Lisaks on oluline koht ka Küberväejuhatusel, mille ülesanne on tegeleda riigikaitse küsimustega ning spetsiifilisemalt küberoperatsioonidega Kaitseministeeriumi vastutusalas (Eesti Kaitsevägi, 2020).

Asjade interneti seadmete paljusus on riske suurendanud, kuid ametlikku juhist riskide maandamiseks ei eksisteeri, mistõttu on magistritöö keskendunud seadmete riskidele tavakasutajate jaoks. Nimelt on asjade interneti seadmete rohkus aktuaalne mitte üksnes tulevikus, vaid juba praegu. Inimeste tavakasutuses on palju nutikat tehnoloogiat, mis on võimelised võrku ühendatuna jagama andmeid ja muutma seadmete kasutajate elu mitte üksnes informatiivsemaks, vaid ka mugavamaks ja kiiremaks. Andmete jagamise võimekus võib ühendatud seadmetega olla ohtlik. Kuritahtlikel osalistel on võimalik kasutada mõjutamise eesmärgil ära nii üksikseadmeid kui ka seadmete kogumit, et saavutada loodetud tulemus. Arvestades, et asjade interneti tehnoloogia seadmeid tuleb kogu aeg juurde, lisandub ka ohte, millega peavad tegelema hakkama korrakaitseasutused. Magistritöö on kasvava seadmete hulga ja sellega seotud ohtude tõttu **aktuaalne**, sest asjade interneti seadmetega kaasnevad ohud on miski, mida tuleb täpsemalt uurida ning võimalike ohte silmas pidades keskenduda nende maandamisele. Magistritöö keskendub ministeeriumitele ja riigiasutustele (peaasjalikult Politsei- ja Piirivalveamet ja RIA CERT-EE), kes peavad intsidentide ning kuritegevuse menetlemise seisukohalt ees seisvate probleemidega, k.a võimalik intsidentide arvu kasvu ja vajalike kompetentside olemasoluga silmitsi seisma. Töö on oluline ministeeriumitele ja riigiasutustele soovituste pakkumise seisukohalt, kuidas asjade interneti tehnoloogia paremini ning turvalisemalt integreerida ühiskonda nii riigi kui ka tavakasutaja vaatest.

Magistritöö on uudne, sest asjade interneti tehnoloogiaga seonduvaid turvariske pole turvalisuse ja üksikisikute vaatest Eestis varem uuritud. Varem on uuritud küberturvalisusealast ettevalmistust haridussektoris, mille raames Piret Pernik (2019, p. 97) toob välja madalad teadmised infosüsteemide ja andmeedastatuse kohta Sisekaitseakadeemia õpilaste hulgas. Sisekaitseakadeemia vaade on oluline, sest just akadeemia kadetid võiksid digiteadmistega täiendada oluliselt näiteks Politsei- ja Piirivalveameti ridu. Spetsialistide vajalikkust digivaldkonnas on uurinud poliitikauuringute keskus Praxis (2019, lk 4), mis toob välja, et 2023. aastaks vajab Eesti küberturbe valdkond juurde 270–870 spetsialisti, kes aitaksid kaasa kestliku ja digitaalselt pädeva süsteemi toimimisse. Digitehnoloogia ja turvalisuse vahel on seos, mida asjade interneti näitel magistritöö selgelt välja toob, sest annab ainest avaliku sektori metiasutustele asjade interneti seadmetega seonduvate korralduslike ja ennetuslike aspektide loomiseks. Oluline on kaitsta seadmete kasutajaid aktuaalsete tehnoloogiaga seotud ohtude eest ning leevendada valdkonnas eksisteerivat tööjõupuudust.

Magistritöö uurimisprobleem tuleneb asjade interneti kiirest ja globaalsest arengust ning kasutajate arvu hüppelisest kasvust ning on püstitatud küsimusena ,,Missugused on asjade interneti seadmete kasutuselevõtust tulenevad turvalisuse riskid inimeste tavakasutuses olevate seadmete näitel seda kasutava kasutajaskonna jaoks ning kuidas nende riskide tekkimine võib mõjutada küberintsidente ja küberkuritegevust uurivate asutuste tööd?''.

Uurimisprobleemist lähtuvalt on püstitatud järgnevad uurimisküsimused:

1. Kuidas defineerivad kohalikud ja rahvusvahelised dokumendid ning Eesti eksperdid *Internet of Things* (ingl) mõistet ning kuidas suhestub asjade interneti tehnoloogia üldiste IKT-tehnoloogiatega?

2. Missuguseid probleeme toob kaasa asjade interneti tehnoloogia avalikule sektorile, sealhulgas küberkuritegusid ning küberintsidente lahendavate ametiasutuste jaoks kuritegude olemusest ning nende lahendamiseks vajaminevast kompetentsist lähtuvalt?

3. Milliseid probleeme toovad olemasolevad kohalikud ja rahvusvahelised kübervaldkonna dokumendid ning Eesti eksperdid välja asjade interneti ja IKT-seadmeid silmas pidades?

4. Mida peavad poliitikakujundajad ja seadmete kasutajad asjade interneti seadmeid silmas pidades tegema, et maandada nende kasutamisega ilmnevaid riske?

Magistritöö eesmärk on välja selgitada asjade interneti tehnoloogia arengust tulenevad riskid tehnoloogia kasutajaskonna ning avaliku sektori ameti- ja haldusasutuste jaoks. Oluline on tööga kaardistada kasutamisega kaasnevad ohud inimeste jaoks ning välja tuua probleemid, millele peavad avaliku sektori ameti- ja haldusasutused, mis tehnoloogiliste aspektidega kokku puutuvad, tulevikus olukordade ennetamise ja menetlemise ning kompetentsivajaduse tõttu keskenduma hakkama.

Eesmärgi saavutamiseks on seatud järgmised uurimisülesanded:

1. Tuvastada teoreetilistele allikatele tuginedes asjade internetiga kaasnevad turvalisuse riskid, mis aitavad asjade interneti tehnoloogia ohtudest paremini aru saada ning hinnata Eesti Vabariigi ametiasutuste võimekust asjade internetiga seonduvate probleemide vastu võitlemisel.

2. Analüüsida tehnoloogia arengust tulenevate probleemide ennetuse ja tõkestamise meetmeid, sooritades selleks dokumendianalüüs strateegia- ja visioonidokumentide ning rahvusvahelise praktika kohta ja viies läbi ekspertintervjuud Eesti IKT-ekspertidega.

3. Teoreetiliste lähtekohtade ning kogutud andmete põhjal teha ettepanekud avaliku sektori ameti- ja haldusasutustele eesmärgiga luua parem teavitustöö platvorm ja arutelu strateegilise lähenemise muutmiseks.

Magistritöö on kvalitatiivne empiiriline uuring, mille eesmärk on vastata nähtusega kaasnevatele küsimustele (Green & Thorogood, 2014). Töös uuritav nähtus on asjade interneti tehnoloogia areng ning uurimisküsimused tulenevad tehnoloogia turvalisuse riskidest. Nähtusega kaasnevatele küsimustele vastamiseks on andmekogumismeetoditena magistritöös kasutatud dokumendianalüüsi ja poolstruktureeritud intervjuusid. Kvalitatiivse lähenemise kasuks otsustati, kuna andmete kogumine on kvalitatiivse meetodi korral avatum ning see annab võimaluse koostada teema kohta üksikasjaliku ja täpse analüüsi, milles osalejatel on suurem vabadus otsustada, mis on nende jaoks asjakohane ning mis sobitub teemasse kõige paremini (Flick, 2011, pp. 12–14).

Magistritöö koosneb kahest peatükist. Esimeses peatükis selgitatakse teoreetilise materjali põhjal asjade interneti olemust ja võimalikke ohte. Teises peatükis viiakse läbi kahest osast koosnev empiiriline uuring dokumentide ja ekspertidega. Teoreetiline kirjandus keskendub eelretsenseeritud teadusartiklites ning raamatutes kajastatud interneti ja võrgustatuse ajaloole, asjade interneti kontseptsioonile kui osale selle ajaloost, tehnoloogia turvaelementidele ja selle mitmekihilisele arhitektuurile. Näitlikustamaks asjade interneti tehnoloogiat ja selle ohtu tavakasutajatele on välja toodud Amazon Echo nutikõlari tootesarja kuuluvad seadmed ning nendele seadmetele omased küberrünnakute liigid. Empiirilise uuringu käigus selgitatakse, kas ja kuidas ollakse Eestis asjade interneti vaatest ohtudeks valmis ning millele peaks tulevikus tähelepanu pöörama. Teoreetiline kirjandus keskendub eelretsenseeritud teadusartiklites ning raamatutes kajastatud interneti ja võrgustatuse ajaloole, asjade interneti kontseptsioonile kui osale selle ajaloost, tehnoloogia turvaelementidele ja selle mitmekihilisele arhitektuurile. Näitlikustamaks asjade interneti tehnoloogiat ja selle ohtu tavakasutajatele on välja toodud Amazon Echo nutikõlari tootesarja kuuluvad seadmed ning nendele seadmetele omased küberrünnakute liigid. Analüüsis kõrvutatakse teoreetiline materjal empiirilise uuringu tulemustega, mille põhjal esitatakse soovitused ametiasutustele, integreerimaks asjade interneti tehnoloogia paremini ja turvalisemalt ühiskonnaga. Tavakasutajatele esitatakse seadmete turvaliseks kasutamiseks soovitused, mille järgmisel maandada tekkivaid riske.

1. ASJADE INTERNETI TEHNOLOOGIA TEOORIA

Esimene peatükk on keskendunud asjade interneti tehnoloogia teoreetilisele käsitlusele. Peatüki eesmärk on näidata, kuidas on asjade interneti seadmed arenenud, milline on selle seos arvutite ja internetiühendusega ning miks võivad võrku ühendatud seadmed asjade interneti olemusest lähtuvalt kujutada selle kasutajale turvariske. Asjade interneti tehnoloogia teoreetiline käsitlus on jaotatud kolmeks osaks. Esimene alapeatükk esitab arvutite ja interneti kui algtehnoloogiate olemuse ning toob välja peamised etapid tehnoloogia arengus, milleta asjade interneti tehnoloogiat tänapäeval olemas ei saaks olla. Ajaloolises ülevaates tuuakse välja turvariskide järk-järguline suurenemine, mis on tingitud võrgustatud tehnoloogia võimekuse kasvuga.

Teises alapeatükis selgitatakse asjade interneti tehnoloogia mõistet ning tuuakse näidete kaudu välja selle tehnoloogia toimimine ja potentsiaalsed kasutusvõimalused ühiskonnas. Kolmandas alapeatükis esitatakse asjade interneti tehnoloogiaga seonduvad probleemid, küberrünnakute näited, asjade interneti seadmete turvaelemendid ning võimalike probleemide ennetusmeetmed. Turvaelementide näitel tuuakse välja virtuaalse koduabilise Amazon Echo tehnoloogia potentsiaalsed turvariskid tavakasutajatele. Kolmas alapeatükk aitab lahti mõtestada asjade interneti tehnoloogia seadmete üldised murekohad ning ohtlikkuse.

Peatüki eesmärk on näidata, kuidas on asjade interneti seadmed arenenud, milline on selle seos arvutite ja internetiühendusega ning miks võivad võrku ühendatud seadmed asjade interneti olemusest lähtuvalt kujutada selle kasutajatele turvariske.

1.1. Asjade interneti eellugu: Arvuti ja interneti turvariskide tuvastamine

Mõistmaks paremini asjade interneti kui tehnoloogia olemust, tuleb vaadata interneti ja arvutitega seonduva tehnoloogia ajalugu. Tänapäevase internetitehnoloogia idee on komplitseeritud, sest arenguprotsessi keerukus ei ole kinni ühes konkreetses sündmuses, vaid arengut on mõjutanud nii kultuurilised, poliitilised, majanduslikud, sotsiaalsed kui ka julgeoleku- ja militaarvaldkonda kuuluvad küsimused. Kõik need aspektid aitavad nii internetti, tehnoloogiaid kui ka tänapäeva digitaliseerumist oluliselt paremini mõista. Algtehnoloogiate ajalugu aitab detailsemalt lahti mõtestada asjade interneti olulisuse inimeste, riigi ja ühiskonna julgeolekus.

Asjade interneti puhul on keskne teema võrgustatus – see tähendab seadmete võimekust olla omavahel autonoomselt ühenduses ja jagada andmeid. Tehnoloogia arengu saab võrgustatusest lähtuvalt jagada kolmeks etapiks. **Esimese etapi** puhul nähakse arvutite ja veebi ideed kui tulevikku

mõjutavat suundmust, kus kontseptsioon (Memexi näitel) suudab oluliselt kokku hoida info talletamiseks mõeldud ruumi raamatute ja muude sarnasel alusel info säilitamiseks mõeldud materjalide jaoks. **Teise etapiga** saab alguse arvutite ja sidesüsteemide sidumine julgeolekuga, sest maailmasõdade järel proovisid riigid üksteise relvasüsteemidele ja mõjutustegevusele vastu hakata. **Kolmas etapp** näitab, kuidas ARPANET-i näitel informatsiooni tähtsustava ning seda kiiresti vahetava ühiskonna poole liikuma hakati. Selles etapis näidati esimesi ilminguid võrgust kui ebaturvalisest infovahetuse keskkonnast, mille abil on võimalik pääseda privaatsete andmeteni. Selles alapeatükis välja toodavad etapid on üks viis läheneda võrgustatuse teemale, kuid paralleelselt on olemas ka alternatiivseid narratiive. Siin on pearõhk etappide sotsiaal-poliitilisel lahti mõtestamisel ning see lähenemine on valitud alternatiivina rakenduste arendajate ja arvutiinseneride visioonidele. Arvutiinsenerid on omaks võetud näiteks kolmest etapist koosneva võrgustatuse narratiivi *Web 1.0*, *Web 2.0* ja *Web 3.0* (ingl) näitel (Barassi & Treré, 2012, pp. 1270, 1281–1282).

Esimeseks etapiks võib pidada 20. sajandi esimest poolt, mil ehitati esimene analoogarvuti ning 1937. aastal Howard Aikeni ehitatud Mark I nime kandev elektro-mehhaaniline arvuti (Hedges, 1976, p. 44). Eelpool välja toodud tehnoloogiad on olulised II maailmasõja kontekstis, mil Ameerika Ühendriikide president Franklin D. Roosevelti teadusnõunik ning Ühendriikide Teadusuuringute ja Arenduse Bürood (OSRD) juhtinud Vannevar Bush hakkas mõtlema sõjajärgse tähtsaima teadusliku probleemi, **infoplahvatuse** peale (Campell-Kelly & Garcia-Swartz, 2013, p. 19). OSRD oli loodud teadustegevuse mobiliseerimiseks sõja ajal ning agentuur oli Ameerika Ühendriikide jaoks sõjategevuses kesksel kohal, sest toetas valitsuse ettevõtteid arvutite väljatöötamisega, et tõhustada relvade juhtimissüsteeme, krüptograafiat, radarisüsteeme ning aatompommi projektina tuntud Manhattani Projekti (Mills & Mills, 2020, p. 20). Maailmasõdade periood süvendas riikidevahelist võistlusvaimu rahvusvahelisel areenil ning arvutites ja tehnoloogia arendustöödes nähti võimalust teistele riikidele konkurentsi pakkuda. Informatsiooni hakkas pärast sõdu liigselt kogunema ning selle üleküllus oli Bushi arvates probleem. 1945. aastal avaldas Bush artikli pealkirjaga "As We May Think", kus kirjeldas teabe salvestamise ja otsimise põhimõttel töötavat masinat nimega Memex (Campell-Kelly & Garcia-Swartz, 2013, p. 20). **Memexit** saab sisuliselt pidada tänapäevase ülemaailmse veebi (ingl *World Wide Web*), lauaarvuti ning "digitaalse mõtlemise" paberil olevaks prototüübiks. Memex ei jõudnud küll teoreetilisest kontseptsioonist paberil reaalse füüsilise objekti ehitamiseni, kuid eriliseks teeb selle idee detailne kirjeldus. Bush leidis, et Memex oleks seade, milles üksikisik saab salvestada kõik oma raamatud, dokumentatsiooni ning infovahetuse, tehes seda kõike seadme kiirust ja võimekust arvestades (Bush, 1995, p. 6). Bush toob oma kontseptsioonis välja ka kirjavahetuse ning pildistamisrežiimi olemasolu kui Memexi ühe osa. Seadet kujutab ta tekstis kirjutuslauana, mis oma viltuste pooleldi läbipaistvate ekraanidega annaks võimaluse sellele materjali

projitseerida. Olulisel kohal on ka tänapäeva tehnoloogia lisaseadmetena tuntud vahendite nimetamine – klaviatuur, nupud ja kangid on need, mida Bush Memexi puhul esile toob. Need peaksid tekitama võimaluse informatsiooniga navigeerida ja seda nii-öelda töödelda, seda kõike distantsilt (Traub & Lipkin, 1998, p. 365).

Memexi detailse kirjelduse järgi saab öelda, et sisuliselt esitas Bush idee multimeediasüsteemi loomiseks (Kennedy, 1995, p. 4). Ühelt poolt tuleb rääkida Bushi tööst Memexi kontseptsiooni tõttu, mis on tänapäeva seadmete puhulgi olulisel kohal, kuid teisalt peab temast rääkima, sest tema kirjutistes oli juba 20. sajandi I poolel võtmekohal tehnoloogiline metafoor "veeb". Selle terminiga kirjeldas ta metalset ämblikuvõrku (ingl *spider web*), mis klaasist läbipaistvas anumas ühes raadiolainetega võimaldab luua eri osapoolte vahel ühenduse (Bory, 2020, p. 10). Esimest etappi iseloomustab iseloomustab idee olemasolu, mis asjade interneti tehnoloogia juures olulist rolli mängib.

Teiseks etapiks saab Campel-Kelly & Garcia-Swartzi (2013, p. 20) järgi pidada 20. sajandi keskperioodi aastaid, mil 1949. aasta augustis katsetas Venemaa oma esimest aatompommi ning Külma sõja nime all tuntuks saanud poliitilis-majanduslik konflikt vallandas laialdase arvutivõrkude arendustöö rahastamise. Õhutõrjesüsteem vajas Külma sõja ajal Ameerika Ühendriikide näitel täiustamist ning sealne valitsus investeeris selle tehnoloogia uuendamiseks kokku 8 miljardit dollarit, mis viis õhutõrjesüsteemi SAGE loomiseni 1962. aastal. SAGE puhul oli tegemist esimese digitaalse andmesidesüsteemiga, mis oli võimeline analüüsima andmeid reaalajas (Flamm, 1988, p. 89). Tehnoloogiline areng aga jätkus, sest Bushi visioonide ning SAGE tehnoloogia andis ainest arvutite ja võrgustiku süsteemi ideed edasi arendada. Joseph C. R. Licklider nägi vaeva MEMEX-i kontseptsiooni edasiarenduste nimel ning 1960. aastal avaldas artikli pealkirjaga ''Man Computer Symbiosis", kus pooldas arvuti kasutamist igapäevatöö vahendina (Licklider, 1960, pp. 4–11). Teine tehnoloogia arenguetapp on oluline, sest Licklideri visioon sarnanes tänapäeva arvuti ning interneti ideega. See annab arvuti ja interneti arengule ning esimeses etapis välja toodud idee olemasolule tuge julgeoleku kontekstist lähtuvalt. Tehnoloogiat võib pidada selles etapis kui julgeolekustamise ühte aspekti.

Tehnoloogia julgeoleku seisukohalt ja sellest tuleneva seadmete turvalisuse vaatest on oluline välja tuua ka kolmas etapp, milleks saab pidada 1969. aastal ARPANET-iks kutsutud võrgu loomist, millega prooviti ühendada nelja Ameerika Ühendriikide ülikooli (Stanfordi Ülikooli, Los Angelese California Ülikooli, Santa Barbara California Ülikooli ning Utah' Ülikooli) suurarvutit. ARPANET kujutas endast USA Kaitseministeeriumi Teadusuuringute Projektide Agentuuri (ingl

Advanced Research Projects Agency, ARPA) loodud arvutitevahelist suhtlust võimaldavat võrku (Crispen, 1994, p. 18). Kuigi võrguside arvutite vahel toimis, ei jõutud esimese testiga kuigi kaugele. Tegelikkuses reaalselt toimiv võrk sai töökorda poolteist aastat pärast esimest suurarvutite ühendamise testi (Crocker, 2019, p. 14). ARPANET pidi olema usaldusväärne võrk, mida rahastatakse militaarvaldkonna uuringute tegemiseks ja mis oleks siduv osapool Ameerika Ühendriikide Kaitseministeeriumi, sõjatööstuse ning ülikoolide vahel. ARPANET-iga ühinesid 1970ndatel ka teised Põhja-Ameerika ülikoolid ning nii sai sellest ka akadeemilist ringkonda siduv osapool. Kuigi elektronpost ei olnud ARPANET-i eesmärkide hulgas, moodustas juba 1971. aastaks enamiku ARPANET-i võrguliiklusest just elektronpost, mida peeti kolleegidega suhtlemise viisiks ning toeks koostöö tegemisel (Denning, 1989, p. 530). On ka oluline lisada, et Washington Posti 2015. aastal ARPANET-i loojatega korraldatud intervjuus tuuakse välja, et 1973. aastaks moodustas 75% ARPANET-i võrguliiklusest elektronpost (Washington Post, 2015), mis näitab selgelt võrgu sotsiaalset mõju ning informatsiooni kiire ja mugava levimise võimekust.

ARPANET-i areng oli agentuuri jaoks prioriteet, kuid arendustööde käigus hakkasid ilmnema ka lahenduse kitsaskohad. Steve Crocker, üks ARPANET-i loomisprotsessis osalenutest, toob näite turvalisuse kohta 1980ndatel. Proovides süsteemi sisse logida, andis süsteem Crockerile veateate, et keegi oli tema personaalkontole proovinud sisse logida. Sisselogija suudeti tol ajal kindlaks teha, kuid ARPANET-i loojad tunnistavad, et see oli üks esimesi hetki, mil nad said aru võrgu varjukülgedest. Niisiis toovad Crocker ja teised ARPANET-i loojad selge paralleeli tänapäeva võrgu varjukülgedega (ingl *dark side of networks*) (Crocker, 2019, p.18).

Beraneki (2000, p. 72) informatsiooni järgi omas ARPANET 1983. aastaks 562 ühenduslüli, mistõttu otsustas Ameerika Ühendriikide valitsus selle turvalisuse kaalutustel kaheks teha. Kuna militaarstruktuurid soovisid süsteemi, mis suudaks tagada suurarvutite vahel jagatavate andmete ohutu transpordi, eraldus üldsüsteemist MilNeti-nimeline võrgusüsteem, mis jäi valitsusasutuste kasutusalasse. Sellest eraldi jäänud ARPANET jäi akadeemilise ringkonna kasutusse (Crispen, 1994, p. 18). ARPANET oli loodud võrguna, mis oma idee järgi pidanuks olema üksainus omalaadne võrk terves maailmas (Kahn *et al*., 1997, p. 134). ARPANET-i jagunemisega akadeemiliseks ja sõjaväe turvatud võrguks oli aga tekkinud juba kaks paralleelselt toimivat võrku. Lisaks tekkisid ka väiksemad paralleelvõrgud ning nende loojate hulgas oli nii suuri riikliku taustaga ameti- ja julgeolekuasutusi kui ka eraettevõtteid. Nende seas võis näha ka riikliku taustaga NASA-t ning eraettevõtetest suurimaid nimesid IBM-i ja Bell Laboratoriest.

Eraldiseisvate võrkude keskel sai oluliseks võrkude kombinatsioonide loomine, mis sai reaalsuseks tänu Vint Cergi ja Bob Kahni arendatud edastusjuhtimis- (TCP) ja internetiprotokollile (IP). TCP ja IP on aktuaalsed veel tänapäevalgi ning tegemist on protokollidega, mis määravad aadressid võrkude omavahelise ühenduse korral, interneti andmepakettide vormingu ja tõrkeotsingu protsessid (Greenstein, 2020, p. 194). Protokollide idee ja tähtsus sai alguse tänu Tim Berners-Lee välja käidud ideele veebist. Veebitehnoloogia on see, mille pärast 1989. aastal ARPANET-i kontseptsioon Ameerika Ühendriikide poolt ära lõpetati, sest telekommunikatsiooni- ja arvutitööstuse partnerlus tagas võrguühendusele paremad tingimused (Crispen, 1994, p. 18). Tehnoloogia areng ning võimekus näitasid Ameerika Ühendriikidele, et ARPANET-i süsteemi sulgemisega suudetakse kokku hoida 14 miljonit dollarit aastas (Beranek, 2000, p. 72).

ARPANET-i sulgemisele ning tänapäeva informatsiooni jagamise viisidele aitas aluse panna Berners Lee, kes proovis 1980ndatel leida võimalused füüsikute vahel võimalikult kiiresti informatsiooni vahetada. Loodi idee veebist, mis kasutab interneti globaalset võrku, kuid seda spetsiifilisemate protokollide abiga. Protokollid võimaldavad veebiga ühendatud arvutitel kuvada ekraanidele pildi-, heli- ja filmifaile, lisaks võimaldatakse kasutajatel ühelt veebisaidilt kiiresti teistele liikuda (O'Malley & Rosenzweig, 1997, p. 132). Veebikeskkonda loodi 1993. aastal esimene veebibrauser Mosaic. Samal aastal muutus veeb ka avalikuks, kuid kommertslikul eesmärgil kasutatavaks alles 1995. aastal (Bory, 2020, p. 40). Veebitehnoloogia näitas juba alguses enda laialdast levikut. Kui 1993. aastal oli olemas 130 veebisaiti, siis 1995. aasta juunis oli neid juba 23 500 ning 1996. aasta juunis 200 000 (O'Malley & Rosenzweig, 1997, p. 133). Üldpilt on tänapäevaks muutunud: 2020. aasta seisuga on maailmas ligikaudu 2 miljardit veebisaiti, millest vähem kui 400 miljonit on kogu aeg aktiivsed (Hosting Tribunal, 2020). Interneti kasutuse võimekusega tehnoloogia areng on ka interneti kasutusele, sealhulgas saitide ja rakenduste arengule kaasa aidanud.

Tänapäeva saame lugeda traditsioonilise arvuti järgseks ajastuks, kus meie käsutuses olevad nutitelefonid ning muud nutikad seadmed muudavad keskkonna interaktiivsemaks ja informatiivsemaks (Tweneboah-Koduah *et al*. 2017, p. 169). Tehnoloogiata oleks inimeste elu raskem ning teatud küsimustes on selle kasutamine hädavajalik. Selle töö sissejuhatuses (vt lk 5) välja toodud arvutite vahendusel kasutatava interneti kasutusalad on ühed vähesed näited, kuidas algne idee võrgustatusest on inimeste kasuks tööle pandud. Internet, mis on muidu olnud omane üksnes traditsioonilistele arvutitele, liigub enam inimeste igapäevaeluga seonduvatesse valdkondadesse, mille hulka kuuluvad ka asjade interneti seadmed.

Seega saab **neljanda etapina** välja tuua magistritöö fookuses käsitletava asjade interneti tehnoloogia. Eelpool kirjeldatud kolm etappi näitavad arvuti- ja interneti ajaloo taustal tehnoloogia mõju ja rolli maailmas aset leidvatele muudatustele. 21. sajandi kolmanda kümnendi alguseks on tehnoloogia areng jõudnud seisu, kus internetti ei saa tunnistada enam üksnes arvutite pakutava teenusena, vaid inimest ümbritseva igapäevase keskkonnana (Adat & Gubta, 2018, p. 423) Maailmas näitab selget kasvutrendi sisse ehitatud sensoritega seadmete laialdasem kasutamine. Sellised seadmed on võimelised koguma andmeid meid ümbritsevast keskkonnast ja neid kasutavatelt inimestelt. Taolisi andmeid koguvaid seadmeid saab kutsuda asjade interneti seadmeteks (Williams, 2016, p. 14). Järgmises alapeatükis käsitletakse potentsiaalse neljanda etapina asjade interneti tehnoloogia mõistet, toimimist ning kasutusvõimalusi.

1.2. Asjade interneti definitsioon, toimimine ja kasutusvõimalused

Asjade internet on võrk, kus seadmed koosnevad elektroonilistest, tarkvaralistest ning anduritega täiustatud osadest, mis võimaldavad objektidel üksteist distantsilt tajuda ning ühtlasi üksteist ka võrguinfrastruktuuri kaudu juhtida (Zhou, *et. al*., 2017, p. 26). Asjade interneti mõiste tõi esimest korda välja Kevin Ashton 1999. aastal ning see mõiste pidi tähistama uue tehnoloogiaajastu algust, ühe suurima mõiste teket peale interneti laialdast kasutuselevõttu (Adat & Gubta, 2018, p. 425). Asjade internet on esmakordse selgitamise hetkest paljuski muutunud, kuid põhieesmärk on sel visioonil sama – panna arvuti mõistma teavet ilma inimese sekkumiseta (Gubbi *et al*., 2013, p. 1646). Das *et al*. (2018, p. 110) hinnangul saab asjade interneti seadmeid jagada laias laastus kahte kategooriasse: **füüsilised** (mille hulka kuuluvad näiteks nutitelefon, kaamerad, sensorid, sõidukid ja droonid) ning **virtuaalsed objektid** (mille hulka kuuluvad näiteks elektroonilised piletid, raamatud ja rahakotid). Selle idee edasiarendusena leiavad Chanal ja Kakkasageri (2020, p. 1667), et asjade internet on füüsiliste või virtuaalsete objektide arvutus- ja sidevõimalustega varustatud võrk, mis võimaldab seadmetel omavahel ühendust luua ja ülemaailmse interneti kaudu andmeid vahetada.

Nord *et al*., (2019, p. 98) rõhutab, et kui internet kujunes välja inimeste loodud andmete põhjal, siis asjade internet toetub eri seadmete ja asjade loodud andmetele. Asjade interneti seadmete puhul vahetatakse informatsiooni inimeselt inimesele või inimeselt arvutile ülesandeid jagamata ehk inimese sekkumiseta (Williams, 2016, p. 14).

Jamie Lee Williams (2016, p. 14) toob välja, et asjade internet võib paljudele olla seotud futuristliku pildiga kodus olevatest tarkadest külmkappidest, kohvimasinatest, valgustehnikast ning paljudest teistest seadmetest, sealjuures teadmata, et mitmed eelpool nimetatud tehnoloogilised seadmed on juba igapäevaselt kättesaadavad. Asjade interneti tehnoloogiat kasutavad suurettevõtted, näiteks Ericsson, Bosch, Siemens ning BBC, kes on asjade interneti enda tulevikuplaanidesse liitnud (Bassi

et al., 2013, p. 1). Asjade interneti toimimist kirjeldades saab toetuda juba praeguseks ühiskonnas olemas olevatele näidetele, mis ühtlasi näitavad, et tehnoloogia on keskkonnas levinum, kui arvata võiks. 2014. aastal ennustas Gartner Research 2020. aastaks 26 miljardit internetti ühildatud seadet, 2009. aastal oli internetiga ühildatud objekte aga 900 miljonit (Lee & Lee, 2015, p. 431). Seadmete hulk ajas kasvab, sest asjade interneti mõiste kätkeb seadmeid, mis pole lihtsalt traditsioonilised arvutid või mobiilseadmed, vaid ka näiteks igapäevases kasutuses olevad vahendid, linnapildis ja ühiskonnas leiduvad tehnoloogiad tervikuna. Seadmeid puudutav statistika, mis näitab, et internetti ühilduvate seadmete arv kasvab, toob välja, et tegemist ei ole mitte kodude tulevikuga, vaid maailma tulevikuga, mis kogu ühiskonda puudutab (Williams, 2016, p. 14).

Asjade interneti tehnoloogiat võib leida näiteks järgmistes rakendusvaldkondades:

1) **Tööstuses**, kus on andurite kogutava informatsiooni teel võimalik vähendada tootmisprotsesside kadusid ning muuta tõhusamaks tootmisüksuste juhtimissüsteem, tehes ettevõtted konkurentsivõimelisemaks ning nende tooted kvaliteetsemaks (Nižetic *et al*., 2020, p. 3).

2) **Linnalahendustes**, mille peamine eesmärk on teedele, hoonetesse, autodesse ning linnapilti paigutatud anduritega suurendada linnapildi jaoks investeeritavate ressursside ökonoomset kasutamist ning ühtlasi tõsta kodanikele osutatavate teenuste kvaliteeti, kontrollides selleks näiteks anduritega varustatud liiklus- ja valgustus-, pääste- ning häiresüsteeme (Kouicem *et al*., 2018, p. 203).
3) **Põllumajanduses**, kus on näiteks mulla niiskuse, pH-taseme, atmosfääritingimuste ja niisutussüsteemide, kariloomade käitumise ja heaolu ning saagi üldise seisukorra jälgimisega võimalik suurendada põllukultuuride tootlikkust ja säästa valdkonda rahalistest kahjudest (Mahbub, 2020, p. 10).

4) **Jäätmekäitluses**, kus on eesmärk pakkuda tõhusamat jäätmekäitlust kindlates piirkondades, koordineerides jäätmeveokite marsruutide ning jäätmekäitluse tõhusust anduritega, mis suudavad tuvastada prügikastide täitetaset, jäätmete temperatuuri, niiskust ja GPS-asukohta (Nižetic *et al*., 2020, p. 5).

5) **Tervishoiusüsteemis**, kus tehnoloogia kaudu on võimalik koguda tervishoiuteenustega seotud teavet korralduslikest aspektidest (logistika, juhtimine, rahandus) ja meditsiinilistest aspektidest (ravi, taastumisprotsess, ravimid) ning seeläbi parandada tervishoiusüsteemi tervikuna. Näiteks saab anduritega jälgida patsientide olukorda ning muuta arstide tööd efektiivsemaks, andes arstidele võimaluse reageerida äärmisel vajadusel (Tewari & Gupta, 2020, p. 917).

6) **Transpordis**, kus on transpordi infrastruktuuri paigaldatud andurid, millega proovitakse süsteemi muuta kvaliteetsemaks, tõhusamaks ja kättesaadavamaks (Mahbub, 2020, p. 8). Üks näide, mis transpordivaldkonda paremaks ja efektiivsemalt toimivamaks aitab muuta, on nutikas auto, mis näitlikustab asjade interneti olemust. Selle kontseptsioon võtab arvesse autos olevate ning asjade interneti tehnoloogiale toetuvate sisemiste funktsioonide kasutamist. Sõidu ajal kogutakse kindlaid andmeid, seostades need peamiste tööparameetritega, milleks auto puhul võivad olla näiteks rehvirõhk, kütusetase ja rikete tuvastamine. Nii parandatakse asjade interneti tehnoloogia abil juhikogemust, muutes sõitmise mugavamaks ja turvalisemaks (Nižetic *et al*., 2020, p. 7).

Seega aitab asjade internet igapäevaseid tegemisi lihtsustada. Sellest on saanud ühiskonna jaoks tehnoloogiliselt oluline arengusuund, kus nutikate seadmete, kodu- ja isegi linnasüsteemide võrku ühildamise tulemusena on sel potentsiaal kasvada inimeste elu lihtsamaks, protsesse kiiremaks ning tegemisi ressursi poolest optimaalsemaks muutvaks tehnoloogiaks. Tänu säärasele tehnoloogiale ning kogutavatele andmetele võib öelda, et seadmeid kasutavate inimeste elukvaliteet on paranenud, sest inimesed on muutunud teadlikumaks sellest, kuidas nad elavad, reisivad, suhtlevad, õpivad, end ravivad ja enda elu tervikuna juhivad. Asjade interneti seadmed on võimelised seega iseseisvalt andmeid koguma, neid sünteesima ning andmetega ka vajalikke ülesandeid sooritama. Täielikust autonoomsusest lahutab teda siiski inimese võimalus sekkuda selle tehnoloogia otsustusprotsessidesse (Brous *et al*., 2020, p. 2). Teisisõnu ei ole tegemist laia tehisintellektiga (ingl *artificial intelligence*), mis tehnoloogiale toetudes suudaks masinõppe tulemusena iseseisvalt ilma inimeseta masinat.

1.3. Asjade interneti tehnoloogia probleemid, turvaelemendid ning potentsiaalsed rünnakute näited Amazon Echo tehnoloogia vaatest lähtuvalt

1.3.1. Asjade interneti tehnoloogia probleemid

Selles alapeatükis leiavad selgitamist asjade internetiga seonduvad probleemid ning akadeemilises kirjanduses tuvastatud värkvõrgu seadmete probleemid ja turvaelemendid, sest turvaelemendid on üks konkreetne viis, kuidas seadme turvalisust hinnata saab. Mõistmaks paremini tehnoloogia olemust, tuuakse probleemidele ning turvaelementidele tuginedes välja Amazon Echo tehnoloogiasarja toodete näited, mille kaudu seletatakse lahti asjade interneti seadmete idee ning ohukohad probleemide, turvaelementide ning küberrünnete näitel.

Peamise probleemina saab asjade interneti seadmete puhul välja tuua varasema võrguseadmete ehitamise kogemuseta tootjate laialdase eksisteerimise turul. Asjade interneti tehnoloogia ning seadmete omavahelises ühildamises nähakse tulevikutehnoloogiana võimalust kasu teenida – seadmete võimalikult kiire turule viimine, nende täiustamine uuemate ja tarbija jaoks

atraktiivsete lahendustega on saanud omaette eesmärgiks, sealjuures keskendutakse vähem riist- ja tarkvara turvaelementide kujundamisele (Furfaro *et al.*, 2017, p. 44). Asjade interneti tehnoloogia arendusprotsessis on aga ülitähtis seada julgeolek esmatähtsaks, vastasel juhul võib hüppeliselt kasvada turvariskide arv, mis tooksid kaasa nii tootjale kui ka kasutajale riskantseid olukordi.

Teise probleemina on võimalik välja tuua andurite kogutavate andmete edastamiseks võrku ühendatud seadmete suur hulk, mille tõttu suureneb küberrünnete rünnakupind märgatavalt. Julgeolekuprobleemide lahendamata jätmise korral oleks asjade interneti tehnoloogia laialdasem kasutuselevõtt oluliselt raskendatud. Võttes näiteks eelpool välja toodud rakendusvaldkonnad, kus on esindatud ka tervishoiuteenused, on mõistetav, et hädavajalik on kaitsta süsteemis liikuvat tundlikku teavet ja süsteemi olulisi komponente. Tavalisele lauaarvutile lisaks on võimalik kasutada näiteks viirusetõrjeprogrammi, mis võib kaitsta arvutit ohtude eest. Asjade interneti seadmete ressursid on aga olemasolevate tehnoloogiate näitel piiratud ning sageli ei ole neile võimalik lisada uusi võimalusi, näiteks viirusetõrjet (Furfaro *et al.*, 2017, p. 45).

Kolmanda probleemina on võimalik näha, et seadmete ning ühtlasi ka võrku ühilduvate seadmete arv suurendab turvariske. Seadme internetiühenduse kaudu andmete jagamine ning teabe kogumine on need aspektid, mis on loodud seadmete kasutajate elukvaliteedi parandamise eesmärgiga. Rohkemate internetti ühendatud seadmete korral tuleb ette rohkem haavatavusi, mida pahatahtlikud osapooled võivad ära kasutada. Arvestades, et suhtluseks seadmete vahel kasutab asjade interneti seade traadita tehnoloogiaid, näiteks Bluetoothi, raadiosagedustuvastust (RFID), Wi-Fit ja andmesideteenuseid (Gubbi *et al*., 2013, p. 1646), võib tehnoloogia kasutamisel katkeda signaal või signaali edastusele vahele segada keegi, kelle tegevus võib kahjustada kasutajate privaatsust. Selle tulemusena võib kolmandate osapoolte kätte jõuda teave, kellel selleks tegelikult ligipääsu olla ei tohiks (Alaba, *et al.,* 2017, p. 10). Furfaro *et al.* (2017, p. 44) leiab, et asjade interneti tehnoloogia võib hakata käima sama teed, mida internet juba oma evolutsiooni käigus tegi – peaasjalikult keskendutakse seadmete soovitud funktsionaalsuste saavutamisele, jättes tähelepanuta tulevaste turvaküsimuste järelmõjud. Kui asjade interneti lahendustel pole turvalisuse küsimustes head lahendust, piirab see suuresti selle tehnoloogia edasist arengut.

Tehnoloogiata oleks inimeste elu raskem ning teatud küsimustes on selle kasutamine hädavajalik. **Neljanda probleemina on võimalik esile tuua seesama vajalikkus**, mis äratab huvi nende seas, kes üritavad ebaseaduslikult oma eesmärkide saavutamiseks saada juurdepääsu isikute ning ettevõtete andmetele, tuues rünnaku alla sattunutele kaasa kergemad või isegi elu muutvad tagajärjed (Sardar *et al.*, 2018, p. 4987). Seega kerkib asjade interneti seadmete eriilmelisuse ja nutikuse tõttu esile

mitmeid probleeme, mis puudutavad seadme andmetöötluse küsimusi ja seadmete turvalisust laiemalt. Andmete haldamise või seadmete turvalisusega seonduvad probleemid võivad esile tuua aga suuremad probleemid seadmete kasutajatele – raskematel juhtudel võib see tervishoiusüsteemis kasutatavate seadmete rünnakute näitel tuua esile ka elu ja surma küsimuse, sest ohtu võivad sattuda patsiendid. Traadita tehnoloogiat kasutavad näiteks insuliinipumbad ja südamestimulaatorid, mis on võimelised ühilduma suure hulga asjade interneti seadmetega ning rünnakute korral tekitama tervisekahjustusi nendele, kes neid seadmeid kasutavad (Sethuraman *et al.*, 2020, pp. 1–2).

1.3.2. Asjade interneti turvaelemendid

Probleemide lahendamiseks ja rünnete ennetamiseks tuleb mõista asjade interneti seadmete elemente, sest eelpool käsitlemist leidnud eluvaldkondadesse integreeritud nutikus võib häkkerite sekkumisel tuua kaasa negatiivsete juhtumite kasvutrendi. Peamiste asjade interneti tehnoloogiaseadmete murekohtade ning turvaelementidena tuuakse välja:

1) **Konfidentsiaalsus** (ingl *confidentiality*), mis Lin *et al.* (2017, p. 1132) ja Kouicem *et al*. (2018, p. 201) definitsioonide järgi tagab andmete kättesaadavuse ainult selleks volitatud osalistele, välistades kolmandate isikute pealtkuulamise ja sekkumise seadmete ning juhtimissüsteemide vahel vahetatud andmetele ja päringutele. Teenused võivad sisaldada tundlikke andmeid, mistõttu peaksid asjade interneti seadmed olema turvalised ja kindlad. Alam *et al*. (2011, pp. 571–572) toob välja, et konfidentsiaalsuse saab asjade interneti seadmete puhul saavutada krüpteerimisega, mis tagab, et ainult selleks volitatud ja selle ligipääsuks vajalikku võtit omavad inimesed saavad vajalikul hetkel andmeid lugeda

2) **Terviklikkus** (ingl *integrity*), mis Lin *et al.* (2017, p. 1132) järgi tagab selle, et võrgus olles andmete edastamise ajal ei saa andmetele ligi kolmandad osapooled. Asjade interneti seadmed vahetavad andmeid teistega, näiteks ametiasutuste, teenuseosutajate ja juhtimiskeskustega, kes esitavad rangeid nõudmisi, et informatsioon valedesse kätesse ei satuks (Alam *et al*., 2011, pp. 571–572). Kouicem *et al*. (2018, p. 201) toob terviklikkuse raames välja, et pearõhk seisneb selle korral seadmete ja juhtimissüsteemide vahel vahetatavate andmete kompaktsuses, mis on andmete edastamise energia optimeerimise seisukohalt oluline. Kokkuvõtlikult on selles punktis tähtis teabe täpsuse ja usaldusväärsuse säilitamine kogu selle elutsükli vältel. Siinkohal on oluline ennetada ja tõrjuda ka süsteemirünnakuid, mis üritavad süsteemi sisestada valeandmeid ning mis võivad süsteemi otsuste tegemist häirida.

3) **Käideldavus** (ingl *availability*), mis Lin *et al.* (2017, p. 1132) hinnangu järgi tagab andmete ning seadmete kättesaadavuse selleks volitatud osapooltele ja teenustele igal hetkel, kui andmeid soovitakse saada. Kouicem *et al*. (2018, p. 201) hinnangul seisneb idee võrgu infrastruktuuris – nutikate arvestite ja pidevate päringute optimeerimise ja juhtkäskudega tegeleva juhtimiskeskuse "saadaval" või "aktiivne" olemises. Pearõhk on kaitsta volitatud osapooli volitamata kasutajate eest.

4) **Privaatsus** (ingl *privacy*), mis Lin *et al.* (2017, p. 1132) järgi tagab andmete kontrollitavuse ainult kindlate osapoolte kaudu, mis omakorda tagab selle, et kolmandad osapooled ei pääse andmetele ligi ning ei saa neid töödelda. Teisisõnu seisneb privaatsus eraandmete kaitsmises (näiteks inimeste tegevuse kohta hoonetes, ettevõtetes jne) – andmete kaitsmine ja nende privaatsuse tagamine ehk jälgimatuks muutmine on süsteemi loojatele ning haldajatele kohustuslik (Kouicem *et al*., 2018, p. 201).

5) **Identifitseerimine ja autentimine** (ingl *identification and authentication*) ehk objektide identiteedi kinnitamise ja kindlustamise protsess, mis Lin *et al.* (2017, p. 1132) hinnangul tagab loata seadmete või rakenduste ühendamatuse asjade internetiga ja autentimine kontrollib võrkudes edastavate andmete ning andmeid taotlevate seadmete ja rakenduste seaduspärasuse. See tähendab, et kõik seadmed peaksid olema võimelised tuvastama ja autentima süsteemis olevaid objekte.

6) **Usaldus** (ingl *trust*), mis tagab turvalisuse ja privaatsuseesmärkide säilitamise (Lin *et al.*, 2017, p. 1132).

7) **Salgamatus** (ingl *non-repudiation*), mis seisneb kindluse tagamises, et andmeid või juhtkäske pole tegelikult vastu võetud (Kouicem *et al.*, 2018, p 201). Teisisõnu on siin oluline pakkuda viis, kuidas saaks näidata ülesannete või sündmuste omaduste teket eesmärgiga hiljem neid mitte eitada – kui on registreeritud ülesanne ja sündmus, siis see registreeritakse ning sellest ei ole võimalik hiljem taganeda.

Eelpool välja toodud turvaelementide loetelule lisaks saab välja tuua Sicari *et al*. (2015, p. 147) artiklis välja toodud analüüsi, kus nimetatakse kolm turvaelementi: **autentimine**, **konfidentsiaalsus** ning **juurdepääsu kontroll** (ingl *access control*). Lisatakse, et asjade interneti seadmete jagamisvõrgustikus on turvalise suhtluse aluseks autentimine, autoriseerimine ja juurdepääsu

kontroll. Nord *et al*. (2019, p. 103) toob oma artiklis välja kolm peamist elementi: privaatsuse, turvalisuse ning usalduse. Jing *et al.* (2014, pp. 2483–2485) toovad peamiste asjade interneti tehnoloogia väljakutsetena esile **turvaküsimused privaatsuses, kontrollmehhanismides, süsteemi seadistuses ning teabe salvestamises ja haldamises.**

Turvaelemendid on vaid üks osa tervikust, mis aitavad mõista asjade interneti tehnoloogiaseadmetega kaasnevaid ohte. Lisaks turvaelementidele tuleb vaadata ka seda, mille kaudu ja kuidas on võimalik seadmetele ligi pääseda. Asjade interneti seadmetel puudub standardne arhitektuur, kuid akadeemilises kirjanduses on olemas erinevaid mitmetasemelisi visioone, millest kõige traditsioonilisem asjade interneti seadmete arhitektuur on määratletud kolmekihilisena (Tewari & Gupta, 2020, pp. 909–910). **Tewari & Gupta toovad seda iseloomustades välja järgmised kihid:**

1) **Tajuvuskihi/andurikihi**, mille eesmärk on tuvastada asjade interneti süsteemi objektid ainulaadselt ja koguda nende kohta teavet. Konkreetne kiht on tehtud anduritest, mis võtavad keskkonnast vastu andmeid ning saadavad need töötlemiseks ülemistesse kihtidesse. Li *et al*. (2015, p. 1) järgi kuuluvad siia andurid, raadiosagedustuvastus (RFID) ja asjade interneti kliendikomponendid (ingl *client components of IoT*).

2) **Vahevara kihi**, mille eesmärk on pakkuda asjade interneti seadmetele võrgutuge. Arhitektuuriliselt on seda kihti jaotatud kaheks: töötluskihis (ingl *processing layer*) ja transpordikihiks (ingl *transport layer*). Esimeses analüüsitakse andmekihi kogutud teavet ning teises kasutatakse selliseid tehnoloogiaid nagu Bluetooth ja Wi-Fi – viimane võtab tajuvuskihist vastu andmeid. Seega on tegemist interneti ja muude seadmetega ühendust loova infrastruktuuriga.

3) **Rakenduskiht**, mille eesmärk on teostada rakenduse spetsiifilisi funktsioone. Kihis hallatakse rakendusi ning tegeletakse privaatsuse ja turvalisusega. Siin pakutakse ja hallatakse teenuseid kasutajale või muudele rakendustele ning pakutakse kasutajatele liidest ja muid teenuseid.

Tehnoloogilise poole pealt saab vaadata ennetuslikku vaatenurka, mida silmas pidades on Bayuk (2013, p. 155) välja pakkunud, et tänapäeva turbemõõdikud põhinevad valdavalt kahel eeldusel, mille järgi on süsteemide konfigureerimiseks olemas turvalised viisid ja turvakorralduste ülesanne on seda konfiguratsiooni säilitada. Bayuki hinnangul ei kasutata küberrünnete korral ära mitte auke konfiguratsioonis, vaid hoopis rakenduste või süsteemi funktsionaalsuses. Seega on töö autori hinnangul üks praktiline ennetusmeede turvaelemendid. Akadeemilises kirjanduses on välja toodud

asjade interneti seadmete turvaelemendid, mille abil analüüsida seda, kui turvaline on mingi tehnoloogia.

Tehnoloogiaajastule omaselt kasvab seadmete ning ühtlasi ka võrku ühilduvate seadmete arv tunduvalt ning teeb aktuaalseks internetitehnoloogia turvariskid. Seadmete internetiühenduse kaudu andmete jagamine ning teabe laialdasem kogumine on see, mis hoolimata elukvaliteedi parandamisest võivad tekitada probleeme, kui seadmete kiire turule viimise eesmärgiga keskendutakse vähem riist- ja tarkvara turvaelementidele. Sedasi seatakse ohtu inimeste personaalandmete privaatsus. Asjade interneti tehnoloogia rakendusvaldkondade näitel võib tehnoloogia turvalisuse tagamiseta eksisteerida ka oht inimeste elule.

1.3.3. Virtuaalne koduabiline Amazon Echo ning temas peituv assistent Alexa

Selles alapeatükis kirjeldatakse asjade interneti tehnoloogia toimimine spetsiifilisemalt lahti virtuaalse koduabilise Amazon Echo ja temas peituva assistendi Alexa näitel, et mõista paremini eelnevates alapeatükkides välja toodud turvaelementidega seotud riskide määratlemist. Osutatud probleemid ja turvaelemendid saavad järgnevaga täiendust näidetega rünnetest, millega asjade interneti süsteemi ja selle seadmeid on võimalik mõjutada.

Asjade interneti tehnoloogia üks tooteid on nutikõlar ehk traadita seade, mille saab aktiveerida häälkäskluste abil. Esimesed sellisel kujul virtuaalsed koduabilised said inimestele kättesaadavaks 2014. aastal, mil e-kaubandusega tegelev ettevõte Amazon tutvustas esimesena hääle teel juhitavat nutikõlarit (Smith, 2020, pp. 350–351). Sellest ajast peale on olnud nutikõlarite soetamine aktiivne ning kasvutrendi näitav tegevus. Juba 2018. aastaks omas virtuaalseid koduabilisi 24% Ameerika Ühendriikide leibkondadest ning 2019. aastaks 20% Suurbritannia leibkondadest (Brause & Blank, 2020, p. 751). 2018. aastaks oli Amazon juhtivate nutikõlarite tootjate turuliider, nende turuosa oli üle 70% (Smith, 2020, p. 351). Eelpool välja toodud statistika tõendab, et nutikõlarite kasutamine on hoogustunud.

Turuliidri tootevalikus on olemas Amazon Echo nime kandev riistvaraseadmete tootesari, mille esindajate hulka kuuluvad näiteks Echo Dot, Echo Tap ja Echo Show. Kõik eelpool nimetatud seadmed on internetti ühenduvad ning täidavad kõlari, mikrofoni ja kaamera ülesannet. Konkreetse riistvaraga käib kaasas ka pilvepõhine tarkvaraprogramm Alexa, mis on loodud täitma isikliku assistendi ülesandeid (Ford & Palmer, 2018, p. 68). Nutikõlarid on juhitavad häälkäsklustega ning seadmed on võimelised vastama samaväärselt inimestega (Brause & Blank, 2020, p. 751).

Mõistmaks paremini Amazon Echo tootevalikus olevate seadmete omadusi, on tabelis (Tabel 1) välja toodud Amazon Echo tootevalik, nende assistent ja seadmete eriomadused.

Tabel 1. Amazon Echo tootevalik, assistent ja seadme eriomadused (Smith, 2020, p. 351).

Seadme nimi	**Assistent**	**Omadused**
Amazon Echo	Alexa	Hääljuhitav ja võimeline häälega suhtlema. Mängib muusikat, taskuhäälingu saateid, audioraamatuid ja mänge. Seade võimaldab kuulata uudiseid, ilmateadet ning reaalajas vastuseid küsimustele. Säilitab loendeid, kalendreid, alarme ja taimereid.
Amazon Echo Plus	Alexa	Echo funktsioon, kuid samuti kasutatav kui nutikas kodukeskus (ingl *home pod*).
Amazon Echo Look	Alexa	Echo funktsioon, kuid sellel on ka kaamera, mis võimaldab teha fotosid ning 360-kraadiseid videoid. Seade on tehisintellekt moenõuete ja rõivaste soovituse jaoks. Seade sisestab kasutaja riided loodavasse kataloogi ning hindab teie välimust, lähtudes masinõppe algoritmidest koos moespetsialistide nõuannetega.
Amazon Echo Show	Alexa	Echo funktsioon, kuid seadmel on lisaks 7-tolline LCD puuteekraan, mida saab kasutada meediakanalite esitamiseks, videokõnede tegemiseks.
Amazon Echo Spot	Alexa	Echo funktsioon, mis on poolkerakujuline, 2,5-tollise ekraaniga.
Amazon Dot	Alexa	Echo funktsioon, mis ühendatakse teiste väliste kõlaritega.
Amazon Tap	Alexa	Echo väiksem, kaasaskantav versioon, mis on akutoitega.

Amazon Echo ja Alexa süsteemi arhitektuuri ilmestab kõige paremini Joonis 1 (vt lk 26), kus on spetsiifilisemalt lahti visualiseeritud Amazon Echo ja Alexa toimimine. Pilvepõhine tarkvaraprogramm Alexa täidab intelligentse isikliku assistendi ülesandeid, samas kui Amazon Echo tootesarja kuuluvad tooted on käsitletavad kui internetti ühendatav riistvara kõlari, mikrofoni või kaamerana (Ford & Palmer, 2018, p. 69).

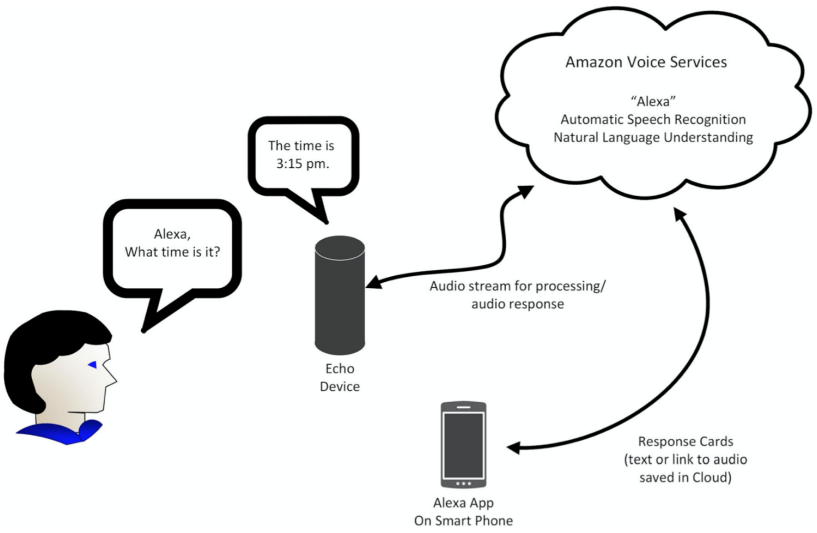

Fig. 1 Alexa system architecture

Joonis 1. Amazon Echo ja Alexa süsteemi arhitektuur – Kuidas seade ning virtuaalne assistent toimivad? (Ford & Palmer, 2018, p. 69).

Echo, kuid ka teised nutikõlarid on võimelised ühilduma majapidamises olevate kodumasinatega ning võimaldavad kasutajatel juhtida kõlari kaudu näiteks termostaate, lambipirne, televiisorit, turvakaameraid ja lukke (Brause & Blank, 2020, p. 751).

Akadeemilises kirjanduses tuuakse Amazon Echo tehnoloogia positiivsete ning mugavusele suunatud kasutegurite kõrval välja kasutajaskonnale turvalisuse ja privaatsuse probleeme põhjustavaid tegureid, mille aluseks peavad Jackson & Orebaugh (2018, p. 92) "vastastikust usaldust", mis nõuab tähelepanelikkust, kuidas ja kuhu kõlarile esitatavate päringute andmed liiguvad, kuidas seadmed kasutajate elu jälgivad ning mil viisil lähevad need vastavusse turvalisuse ja andmekaitse põhimõtetega. Sellest tulenevalt on võimalik analüüsida Amazon Echo tehnoloogia turvaküsimusi eelnevas peatükis välja toodud turvaelementide näitel, mõistmaks paremini seda, mis võib asjade interneti seadmed teha haavatavaks ning inimeste jaoks ohtlikuks.

Ainuüksi nutikõlarite süsteemi mõtestamisel toovad Ford ja Palmer (2019, pp. 67–68) enda artiklis välja, et ka ettevõtted on Amazon Echo taolise süsteemi ning selles peituva abilise Alexa ning teiste virtuaalsete koduabiliste oma võrku ühildamisest huvitatud, kuid siiski pööratakse tähelepanu mitmele turvalisusega seotud küsimusele, mis võivad pikemas plaanis olla takistuseks intelligentse asjade interneti tehnoloogia kasutusele võtmisel. Artiklis tuuakse välja, et tarbijad on mures isikuandmete privaatsuse, isikuandmete elutsükli (näiteks kui pikalt andmeid andmetöötlusprotsessides kasutatakse), kontrolli ning üldlevinud andmetöötluse riskide pärast. Võib öelda, et kui ettevõtted näevad murekohti tehnoloogia kasutamises, rakenduvad need ka

tavainimestele. Toetudes eelmises alapeatükis välja toodud turvaelementidele, saab esile tuua Lei *et al*., (2019, p. 1–3) artikli, milles on Amazon Echo toote näitel tuvastatud kolm turvaauku, millega on kindlaks tehtud, et inimeste jaoks võib see tähendada ohtu kodu turvalisusele (ingl *home security breach*) ning võltskorralduste (ingl *fake order*) rünnakuid. Probleem seisneb selles, et Alexa teenus kasutab ühefaktorilist autentimismeetodit, mis põhineb paroolilaadsel sõnal, mida esitatakse hääle abil – õige audentimissõna kasutamise korral võib Alexa seega esitatava käsu aktsepteerida, sealjuures hoolimata sellest, kas läheduses ka reaalselt inimesi viibib.

Amazon Echos peitub virtuaalne koduabiline Amazon Alexa, kuid lisaks võib näitena tuua teistes seadmetes olevaid Microsofti Cortanat ja Apple'i Sirit, kus saab kõigest häälkäsklustega hallata kalendrisündmusi, ülesandeloendite koostamist, muusika voogedastust ning ka ilmaennustuste teatamist. Need on vaid vähesed näited, kuidas konkreetne seade võib inimestele kasulik olla. Need ning teoreetilises raamistikus välja toodud näited annavad selgesti edasi arusaama, kui suur, laialivalguv ning inimesi mõjutav valdkond on asjade internet.

Kolme mainitud asjade interneti süsteemi arhitektuurilise kihi kaudu on võimalik teha ründeid asjade interneti seadmete vastu. Akadeemilistele allikatele toetudes on selle töö Lisas 1 (vt lk 86-87) välja toodud eelpool nimetatud kihtidega seostatavad küberrünnete liigid. Lisa 1 tabelis olevad ründed võivad saatuslikuks saada kõikidele asjade interneti süsteemi ühilduvatele seadmetele. Arvestades 2021. aasta seisuga seadmete levimust maailmas, võib see mitmete uute tehnoloogiate kasutuselevõtu korral saada märkimisväärselt hoogu juurde ning seda just negatiivses mõttes. Võttes arvesse Amazon Echo tootevalikus olevaid seadmeid, saab öelda, et õige ründe korral võib pahatahtlik osapool ligi pääseda andmetele, mis ei ole üksnes lihtsakoelised muusika- ja retseptisoovitused, vaid ka eluliselt vajalikud mehhanismid, näiteks elekter, vesi ning ka kodude turvasüsteemid jne.

Tehnoloogia areng on kogu aeg koostoime võimekuse poole pürginud ning internet on aidanud selle võimalikuks teha. Tehnoloogia on kiiresti arenenud ja paljudel seadmetel on praeguseks teatav arvutivõimekus. Ühed sellised on inimeste igapäevases kasutuses olevad asjade interneti seadmed, mis on aina enam seotud elu eri valdkondadega. Seadmed, nende võrgus olemine ning andmevahetus võivad kasutajatele, teistele seadmetele ja neid läbivate andmete osas ohtlikuks osutuda.

2. ASJADE INTERNETI TEHNOLOOGIA RISKIDE MAANDAMISE VÕIMALUSED TAVAKASUTAJA JA AVALIKU SEKTORI AMETI- JA HALDUS-ASUTUSTE VAATES

Magistritöö teine, empiirilise uuringu peatükk, jaotub neljaks alapeatükiks. Esimene alapeatükk kirjeldab empiirilise analüüsi metoodikat, teises ja kolmandas alapeatükis viiakse läbi dokumendianalüüs ning ekspertintervjuud, sealjuures analüüsitakse saadud tulemusi püstitatud uurimisküsimustest tulenevalt. Neljandas alapeatükis tuuakse läbi viidud uuringutest tulenevalt välja järeldused ja ettepanekud.

2.1. Uurimismetoodika ja valim

Uurimistöö uurimisstrateegia on fenomenograafia, mille abil on võimalik seletada viise ümbritseva reaalsuse mõistmiseks (Laherand, 2008, lk 143–144). Teisisõnu kasutatakse fenomenograafiat, et kvalitatiivselt selgitada, kuidas inimesed ühiskonda mõtestavad, vahetult kogevad, tajuvad ja mõistavad (Õunapuu, 2014, lk 160).

Syrjälä *et al.* (1994, pp. 114–160) toob fenomenograafilise uuringu puhul välja neli etappi. **Esimene etapp** sisaldab huvi mõiste vastu, mida on võimalik mitmeti mõista ning mille kohta on levinud erinevaid seisukohti. **Teises etapis** tutvutakse teoreetiliste materjalidega ja tuuakse välja mõiste esialgne liigitus ning **kolmandas** viiakse teisele punktile toetudes läbi intervjuud, et selgitada välja eri osapoolte arusaam käsitletavast mõistest. Pärast intervjuusid annab uurija **neljandas etapis** käsitlustele tähendusklassid. Syrjälä *et al.* välja toodud fenomenograafilise uuringu käik sobitub ka selle magistritöö konteksti. Nimelt huvitutakse selles töös kahest teemast: asjade internetist ning selle mõjust ühiskonnale seadmete turvalisuse riskide kaudu. Riskid ja probleemid vajavad asjade interneti juures määratlemist tehnoloogia kasutajaskonna ning avaliku sektori ameti- ja haldusasutuste vaatest lähtuvalt ning kuna nii mõiste, riskid kui ka probleemid on raskesti piiratletavad, on kasulik uurimisstrateegia fenomenograafia.

Uurimisprobleemi lahendamiseks käsitletakse teoorias võrku ühendatud tehnoloogia arengut ja tänapäevase võrku ühendatud tehnoloogia turvaelemente, mis on võimalikud ründevektorid ja selgitavad seadmete haavatavust. Amazon Echo näitab, et haavatavad seadmed võivad olla ka lihtsad kodudes leiduvad kõlarid.

Teoreetilises osas esitatu najal tehakse edasise informatsiooni ning mõiste defineerimise jaoks ekspertintervjuud. Ekspertintervjuud annavad andmekogumismeetodina võimaluse uurida väikest

arvu inimesi ja nähtuseid, tõstes osalised võtmeisiku staatusesse (Laherand, 2008, lk 179). Kõik eksperdid, kes magistritöös vastuseid annavad, on eksperdid oma valdkonnas – see eristab ekspertintervjuud biograafilisest intervjuust. Terviklik huvi inimeste hoiakute vastu on ekspertintervjuude käigus asendunud teatud rühma esindajatega, kelle infoulatus on piiratud ning suunavama funktsiooniga (Laherand, 2008, lk 199). Ekspertintervjuu juures on oluline roll nii asjade interneti teoreetilisel käsitlusel kui ka teisel andmekogumismeetodil. Ekspertide vastuste põhjal on võimalik analüüsida teoreetilist mastaapi Eesti Vabariigi ja rahvusvaheliste visiooni-, strateegia- ja raamdokumentides määratletuga ning lisada sinna ekspertide arvamuse, mis aitab paremini asjade interneti tehnoloogiast tervikpildi saada.

Intervjuu on sobilik andmekogumismeetod, sest ühe laia mõiste defineerimisel ning mõtestamisel on vajalikud pikemad ja põhjalikumad vastused. Laherand (2008, lk 179) toob välja, et intervjuus on kesksel kohal tähenduse sügav mõistmine. Asjade internet on mõistena mitmekülgne, kuid uurimise ja uurimisküsimuste seisukohalt vaadatuna on mõiste seotud siiski spetsiifiliste valdkondadega, mistõttu on intervjuude tegemisel oluline teatud valdkonna inimeste ehk ekspertide arvamus. Ekspertintervjuud on Laheranna (2008, lk 199) järgi üks poolstruktureeritud intervjuu vorme. Poolstruktureeritud intervjuud on osaliselt reglementeeritud vestlused uurija ja intervjueeritava vahel (Õunapuu, 2014, lk 171). Sellises intervjuus on küsimused esitatavad küll kindlas järjekorras, kuid neile vastamine on vaba (Lagerspetz, 2017, lk 140).

Dokumendianalüüs on samuti andmekogumismeetod, sest tekstid ja dokumendid on ühiskondliku elu tähtsad osad, mis loovad ja muudavad nii norme kui ka fakte, kinnitades nähtuste definitsioone ning tuues välja nähtuste head ja halvad küljed (Lagerspetz, 2017, lk 183–184). Dokumendianalüüsi saab kindlamalt kasutada teiste andmekogumismeetodite täiendusena, sest dokumentide kasutamine iseseisva meetodina võib olla inimeste kogemusele lähenemiseks piiratud (Flick, 2006, lk 251 tsit Laherand, 2008, lk 261). Dokumendianalüüsi juures on oluline koht töö teoreetilises kirjanduses esitatud turvaelementidel, mida saab edukalt tervikpildi loomiseks kasutada. Esmalt tuvastati dokumendianalüüsi käigus asjade interneti tehnoloogia määratlus kübervaldkonna strateegia- ning raamdokumentides. Hiljem kaardistati ekspertintervjuude ning dokumendianalüüsi najal Eesti asjade interneti kui tehnoloogia praegune olukord ning tehnoloogia suurimad turvariskid. Dokumendianalüüsi mõte on uurida, kuidas on asjade interneti kasutamine ning turvalahendused Eesti Vabariigi ja rahvusvahelistes visiooni-, strateegia- ning raamdokumentides siiani paika pandud ning millised võivad olla kitsaskohad tehnoloogiaga seonduvate turvariskide käsitlemisel. Dokumendianalüüs annab parema võimaluse ekspertintervjuude tegemiseks, sest sedasi saab formuleerida intervjuus kasutatavad küsimused pärast dokumendianalüüsi.

Ekspertintervjuudes on rakendatud strateegilist valimit, mis on moodustatud otstarbekuse alusel. Kalmus *et al*. (2015) järgi on selle puhul valitud uuritavad heterogeensete ja homogeensete omaduste kombineerimise teel. Valimis on võimalik määratleda inimesed, kes teemaga mingisugusel viisil kokku on puutunud (Lagerspetz, 2017, lk 175). Kalmus *et al*. (2015) definitsiooni järgi omavad need eksperdid siiski ka erisust, sest tagavad hilisemas vaates uurimisobjektide võrreldavuse ning materjali tähendusliku mitmekesisuse. Kasutatud on ka lumepallivalimit (Lagerspetz, 2017, lk 171–173), mille järgi kasutatakse uute vastajate leidmiseks teiste vastajate abi.

Uuringus tehti ekspertintervjuud 13 oma ala eksperdiga Politsei- ja Piirivalveametist, Majandus- ja Kommunikatsiooniministeeriumist, Siseministeeriumist, Riigi Infosüsteemide Ametist, Siseministeeriumi infotehnoloogia- ja arenduskeskusest, Euroopa Liidu IT-agentuurist (eu-LISA), Andmekaitse Inspektsioonist ja riigisektorist. Eksperdiks saab magistritöö koostaja hinnangul pidada neid isikuid, kes omavad töökogemust tehnoloogia küberturbeprobleemide, dokumentide ja muu seadusandluse koostamisel ja probleemide menetlemisel ning kellel on olemas vahetu, pikaaegne praktiline kokkupuude ja seotus valdkonnaga. Spetsialistide kompetentsus on oluline, sest see aitab säilitada magistritöö fookuse ning jõuda täpsemate ja asjakohasemate järelduste ning ettepanekuteni.

Intervjuud viidi 2021. aasta alguses epidemioloogilist olukorda arvestades läbi videokonverentside keskkondades Zoom, Microsoft Teams ja Skype for Business. Intervjuudes osalenud eksperdid on välja toodud magistritöö Lisas 2 (vt lk 88).

Kõigi ekspertide intervjuud salvestati ekspertide nõusolekul digitaalselt, kasutades selleks digitaalseid abivahendeid. Salvestatud intervjuude helifailid transkribeeriti ning transkriptsioonide analüüsimiseks kasutati andmetöötlusprogrammi Nvivo.

Ekspertintervjuude täiendamise eesmärgiga tegi autor ka dokumendianalüüsi, et kaardistada asjade interneti mõistet, määratlust, innovaatilisust ja probleemsust Eesti ja rahvusvaheliste visiooni-, strateegia- ja raamdokumentides. Dokumendianalüüsi saab käsitleda kui andmekogumismeetodit, millega on võimalik täiendada teisi meetodeid (Flick, 2006, lk 245–246), mille hulka kuuluvad ka eelpool lahti seletatud ekspertintervjuud. Lagerspetz (2017, lk. 183–184) toob välja, et tänapäeva ühiskonnas toodavad inimesed ja asutused palju andmeid, mida on võimalik kasutada, kuna kirjalikud allikad on ühiskondliku elu tähtis osa. Hulk ekspertide hinnanguid, otsuseid ja muid määratlusi tekib asutustes iga päev ning seda saab ära kasutada uurimismaterjalina kvalitatiivses uurimistöös (Laherand, 2008, lk 258).

Dokumendianalüüsi valimi puhul on tegemist samuti strateegilise valimiga. Dokumendianalüüsiga töötati läbi Eesti Vabariigi ning rahvusvaheliste visiooni-, strateegia- ning raamdokumendid, mis on seotud digitaliseerumise, tehnoloogia ning peaasjalikult IT-sektoriga. Eelpool välja toodud valdkondade dokumendid aitavad ekspertintervjuude vastuseid hiljem parematel alustel analüüsida (kõik töös analüüsitud dokumendid on avalikult kättesaadavad ning välja toodud töö Lisas 3, vt lk 89).

Dokumentide analüüsimiseks tehti **kvalitatiivne sisuanalüüs**, mis annab võimaluse keskenduda teksti sisule ja konteksti tähendusele (Laherand, 2008, lk 290). Kvalitatiivse sisuanalüüsiga jõutakse materjali seesmiste mustriteni ning olulise ja ebaolulise eristamiseni (Lagerspetz, 2017, lk 201). Tekstide analüüsimiseks kasutatakse **suunatud kodeerimist**, kus kasutatakse teoreetilisest käsitlusest tulenevaid märksõnu ja uurimisküsimuste osi, kus dokumentidest otsitakse varem määratletud teemasid (Linno, 2020). Dokumentide analüüsimiseks kasutati andmetöötlusprogrammi Nvivo.

2.2. Asjade interneti tehnoloogia vaatest digiarenguga seotud Eesti Vabariigi ja rahvusvaheliste visiooni-, strateegia- ja raamdokumentide analüüs

Esitatud analüüsitulemused toetuvad kolme tüüpi dokumentidele. Esimesena leiavad käsitlemist digiarenguga seotud kohaliku taseme eesti- ja ingliskeelsed dokumendid (kokkuvõtlikult kood KD), teisena rahvusvahelised digiarengu ja asjade interneti tehnoloogiaga seotud dokumendid (kood RD) ning kolmandana rahvusvahelised asjade interneti turvalist kasutamist propageerivad näitedokumendid (kood RND). Dokumendianalüüsi käigus moodustus viis kategooriat, mis käsitlevad asjade interneti mõistet, sellest tulenevaid probleeme nii tehnoloogia enda kui ka üldiste digiarengu probleemide, asjade interneti turvaelementide ning esitatud soovitustest lähtuvalt (detailsem sõnastus on välja toodud magistritöö Lisas 4, vt lk 90).

Asjade interneti süsteemi ning sellega ühilduvaid seadmeid võib nimetada erinevalt, mistõttu on dokumendianalüüsi esimese kategooria eesmärk näidata, kuidas tehnoloogia on erinevates asutustes välja toodud. Lisaks defineerimisele saab vaadelda ka mõiste esinevust digiarengu dokumentides nii kohalikul kui ka rahvusvahelisel tasandil, mis annab informatsiooni selle kohta, kui palju sellele teemale dokumentides keskendutakse. Mõistele annavad tuge nimetatavad kasutusvaldkonnad, mida toetavad näited seadmete arvukuse kohta, et näitlikustada asjade interneti tehnoloogia jõulist arengut. Esimese kategooriana sai sellest tulenevalt määratletud **asjade interneti mõiste ning määratlus dokumentides**, mille alla moodustus kolm koodi. Esimene kood keskendub mõiste *Internet of Things* (ingl) defineerimisele Eesti dokumentides ja teine kood mõiste defineerimisele rahvusvaheliste

digiarenguga seotud dokumentides. Kolmas kood keskendub tehnoloogia kasutusvaldkondade, näidete ning seadmete arvukuse välja toomisele ühiskonnas.

Kood **asjade interneti mõiste ja määratlus Eesti digiarenguga seotud dokumentides**, kus prooviti leida ingliskeelsele mõistele *Internet of Things* (ingl) eestikeelsed vasted, tuvastati kahest allikast (KD1 ja KD2) kõige enam mõiste eestikeelse vastena fraasi **„asjade internet"**, mida paljuski seostatakse **ühendatavusega**, mida asjade interneti seadmetele omistatakse. Dokumentide (KD1 ja KD2) näitel saab öelda, et riigi definitsiooni (Majandus- ja Kommunikatsiooniministeeriumi ning Vabariigi Valitsuse dokumendid) järgi on tegemist võrku ühendatud seadmetega, mis on iseseisvalt suutelised omavahel suhtlema ning anduritega koguma ümbritsevast keskkonnast vajalikku informatsiooni (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 7; Vabariigi Valitsus, 2018, lk 17). KD6 lisab asjade interneti seadmete mõtestamisel seotuse pilve- ja mobiilsidetehnoloogiatega, tuues välja, et lisaks andmete kogumisele ja edastamisele on seadmed võimelised ka andmeid töötlema (TalTech, 2019, p. 19).

IoT defineerimisel on oluline koht ka teisel koodil **asjade interneti mõiste ja määratlus rahvusvahelistes digiarenguga seotud dokumentides**, mille abil tehti kindlaks viis allikat (RD7, RD8, RD9, RND10 ja RND11), mis aitavad asjade interneti ideed paremini mõista ning annavad informatsiooni, kuidas ingliskeelsed dokumendid mõistet defineerivad. Ühendatavuse (ingl *connectivity*) definitsioon on sarnane esimese koodiga, mis toob välja seadmete võimekuse internetti ühendatuna omavahel suhelda. Innovaatilisust nähakse inimeste elu lihtsamaks tegemises (UK Government, 2018, p. 1). Samas problemaatilisust nähakse rünnakutes, mida asjade interneti seadmete abil ellu saab viia (Rand Coroporation, 2020, p. 6). Oluline on eraldi välja tuua Euroopa Liidu küberturvalisuse strateegia, mis asjade interneti mõistet edasi arendades kasutab tulevikku suunatult mõistet *Internet of Secured Things* (ingl), mis tõlgituna tähendab turvalist asjade internetti ning mis viitab seadmete turvaliseks tegemisele kui Euroopa Liidu ühele tulevikku suunatud visioonile (European Commission, 2020, p. 9).

Turvalisus on oluline, sest koodi **asjade interneti kasutusvaldkonnad, seadmete näited ning arvukus** raames sai üheksa dokumendi (KD1, KD2, KD6, RD7, RD8, RD9, RND10, RND11 ja RND12) abil täheldatud **seadmetega seotud valdkonnad, seadmete näited ning seadmete arvukus**. Valdkondlikult toovad dokumendid (KD2, KD6, RD7 ja RD8) välja asjade interneti seadmete kasutusvaldkondadena energeetika, telekommunikatsiooni, tööstuse, arhitektuuri, olme, transpordi, turvalahendused, tervishoiu ja rahanduse, mis näitavad mitte üksnes tehnoloogia sobivust eri valdkondadega, vaid ka nende kasutamiseks mõeldud laia pilti. Spetsiifilisemate näidete tasemel tõid kuus dokumenti (KD1, RD8, RD9, RND10, RND11, RND12) välja nutikad koduabilised, autod,

nutitelerid, külmikud, pesumasinad, alarmsüsteemid, kaamerad, kõlarid, suitsuandurid ja ukselukusüsteemid (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 7; ENISA, 2019, p. 7; Rand Coroporation, 2020, p. 6; Government of Canada, 2020; UK Government, 2018, p. 5). Eraldi peab välja tooma, et võrreldes teiste dokumentidega ei pea RND12 asjade interneti seadmeteks mobiiltelefone (nutitelefonid), sest nende arhitektuur on keerukam ning dokumendi hinnangul toimivad need teisiti (Australian Government, 2020, p. 8). Teised dokumendid liigitavad asjade interneti seadmete alla ka mobiiltelefonid. See, mida dokumentides asjade interneti seadmeteks peetakse, kandub edasi ka **seadmete arvukuse** registreerimise juures täheldatavate faktideni, sest välja toodud arvukus dokumentides varieerub. Dokumentides (KD1, RD7 ja RND12) kirjeldatud andmed näitlikustavad tehnoloogia laialdase kasutamise ning laia levimuse vaatenurka. KD1 tõi 2020. aastat silmas pidades välja seadmete arvu tõusu 20–50 miljardi seadmeni (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 7), RD7 seadmete arvu tõusu 25 miljardini aastaks 2025 (European Commission, 2020, p.1) ning RND12 seadmete 64 miljardi seadme piiri ületamise aastaks 2030 (Australian Government, 2020, p. 1). Erinevatest vaatenurkadest hoolimata annab arvuline kontseptsioon informatsiooni asjade interneti kohta, et seadmete arv on kindlalt ületamas inimeste arvukust maailmas.

Teise kategooriana sai dokumendianalüüsi käigus määratletud **IKT ja asjade interneti põhjustatud digiarengu probleemid,** mille all on omakorda kinnitatud kaks koodi: **peamised digiarengust tulenevad probleemid** ja **asjade interneti seadmetest ja selle tehnoloogia arengust tulenevad probleemid**. Esimese koodi määratlemine on tarvilik hilisemate asjade interneti seadmete ja tehnoloogia arenguga kaasnevate probleemide kaardistamisel. See aitab mõista, kuhu teine kood asjade interneti seadmetega seonduvate probleemidega liigitub.

Esimese alamkoodina on viies dokumendis esile toodud (KD1, KD2, KD5, RD7 ja RD9) **probleemid tavainimestele**, mille alla registreeriti **küberkuritegevus, tehnoloogiasõltuvus, vähesed oskused ning teadlikkus** ja **välismaised lahendused**. Küberkuritegevus tuuakse keskmesse kahes Eesti digiarengu seisukohast olulises dokumendis (KD1 ja KD2) ning selle keskmes viidatakse asjaolule, et tehnoloogiast ja küberruumist sõltuvuse suurenedes tõuseb ka küberruumis toime pandavate süütegude arv (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 8; Vabariigi Valitsus, 2018, lk 18). Tehnoloogiasõltuvuse kohta toovad dokumendid (KD2, RD7 ja RD9) välja sõltuvuse riigivalitsemise, majanduse ja üldisemalt kõigi eluvaldkondade näitel, viidates rohkem nendele elualadele, kus tehnoloogia on aja jooksul väikest rolli mänginud (Vabariigi Valitsus, 2018, lk 16; European Commission, 2020, p. 1; Rand Coroporation, 2020, p. 1). Suur seotus digitehnoloogia kasutamisega viib olukorrateadlikkuse ja oskuste juurde tehnoloogiat õigesti vallata. Kolmes dokumendis (KD1, KD2 ja KD5) leidis märkimist vähene küberteadlikkus ning oskus tehnoloogiaid

õigesti kasutada, mis tõstab küberprobleemide ning küberkuritegevuse ohvriks langemise riski (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 20; Vabariigi Valitsus, 2018, lk 13; E-riigi Akadeemia, 2020, lk 9). Eraldi toob välja KD1 välismaiste IT-lahenduse kasutamise, viidates riistvara tootjatele – Aasia riikidest Hiinale ning tarkvaralahenduste poolelt Ameerika Ühendriikidele. Probleem seisneb nii nende seadmete riistvara kui ka tarkvaralahenduste vastu suunatud rünnetes ning turvanõrkustes, mis võivad otseselt kasutajat mõjutada (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 9).

Tavainimeste elu korraldamine on seotud aga mitmete ametiasutustega, kes iga päev poliitika kujundamise kaudu korraldavad ühiskonnaelu, mis puudutavad ja mõjutavad laiemat üldsust. Seetõttu on oluline määratleda ka üldised probleemid riigile tervikuna ja ametiasutuste vaatest lähtuvalt. Teise kategooria teise koodi teise alamkoodiga registreeriti ära seitsme dokumendi (KD1, KD2, KD3, KD5, KD6, RD7 ja RD9) ulatuses välja toodud probleemid.

Esimesena leidsid registreerimist **teadmised ja oskused**, kus dokumentides (KD1, KD2 ja KD3) tuuakse ametiasutuste probleemkohtade hulgas välja ebapiisav küberteadlikkus, vähese küberkompetentsi olemasolu ning puudulikud täiend- ja koolitusprogrammid, millega sektori kompetents tagada. Probleemide tuum on oskustekeskne ja ei käi ainult tavainimeste, vaid ka ametnike ning juhtide kohta (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 12, 20–23; Vabariigi Valitsus, 2018, lk 13-16; Siseministeerium, 2020, lk 122).

Rahvusvahelise koostöö all tuuakse dokumentides (KD1, KD2 ja RD7) välja pidevalt muutuv julgeolekuolukord nii Eestis kui ka Euroopas ning kogu maailmas tervikuna. Probleem on koostöö rahvusvahelistes organisatsioonides, kus suhtlus käib väheste initsiatiivil ning on üles ehitatud ebaühtlaselt. Rahvusvaheline koostöö on ära märgitud kui oluline Eesti mainet ja digiarengut kujundav valdkond, mille hoidmise nimel tuleb kogu aeg näha vaeva (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 20, 31; Vabariigi Valitsus, 2018, lk 18; European Commission, 2020, p. 15). Lisaks välistele probleemidele on dokumentides (KD1, KD2 ja KD6) välja toodud **poliitika kujundamist** puudutavad probleemid. Puudulik tervikjuhtimine ning kübervaldkonna ühtne koordinatsioon, ebapiisav arusaam küberintsidentide ja -ohtude mõjudest, puudulik ülevaade süsteemide omavahelisest sõltuvusest, ebapiisav küberteadlikkus ning valdkonna alahindamine, vähene koostöö teadusasutustega ning puudulik IKT-vahendite kasutamine poliitikakujundamisel (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 12, 20, 25, 29, 36, 39; Vabariigi Valitsus, 2018, lk 15–19; TalTech, 2019, pp. 24–25). Riiklikult sai registreeritud kood **IT-lahendused**, kus KD1 toob välja, et Eesti tihe seotus digitaalse keskkonnaga võib olla lisaks tavainimesele ohtlik ka riigile tervikuna – teistest riikidest pärit riist- ja tarkvara lahenduste

kasutamine paneb riigi süsteemi sõltuma teiste turvanõrkustest ning nende vastu suunatud rünnetest (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 9).

Riiklikus plaanis on oluline nimetada **sisejulgeoleku asutuste ja küberkuritegevusega** seotud probleemid, kus dokumentides (KD1, KD2, KD3, KD5, KD6, RD7 ja RD9) toodi välja uute tehnoloogiate ja digitaalse sõltuvuse kasvu juures küberruumi rolli taseme tõus ning ka sellega seotud süütegude arvukuse kasv (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 36; Vabariigi Valitsus, 2018, lk 18; E-riigi Akadeemia, 2020, lk 9; TalTech, 2019, p. 6; Rand Coroporation, 2020, p. 1). Politseisüsteemile (KD3) on süütegude kõrval peamine probleem kompetentse ametnikkonna leidmine. Näiteks on digikriminalistika ning IKT-teadmiste strateegias kirjeldatud täiendkoolituste visioone, mis viitavad kompetentse töötajaskonna puudusele politseisüsteemis (Siseministeerium, 2020, lk 73–74). RD7 toob välja, et digitehnoloogiast sõltumise juures on oluline mõista, et võrgulahendused ja infotehnoloogia on seotud valdkondadega, mis omakorda tõstavad riske mitte üksnes tavainimestele, vaid ka probleeme lahendavatele asutustele. Dokumendid keskenduvad küberturvalisusele ning toovad välja, et tänu digitehnoloogia arengule ja selle laienemisele eri valdkondadesse on tõusnud ka küberkuritegevuse sooritamiseks sobivate elualade arv, mis teeb kübervaldkonnast inimestele mõju avaldava teema. RD7-s on välja toodud fakt, et pea kõigi kuritegude uurimisel on sees digitaalne komponent (European Commission, 2020, pp. 1–3).

Problemaatilisena nähakse ka **teadus- ja arendustegevuse praegust seisu**, mis dokumentides (KD1 ja KD6) tuuakse välja Eesti tööturu vajadustega kooskõlas olevate küberturbe õppekavade puuduse, ebapiisava teadus- ja arendustegevuse mahu; riigi, ettevõtluse ning teadusasutuste omavahelise koostöö puudulikkuse, digioskuste vajalikkuse määratluse ja esile tõstmise probleemide ning ekspertide ning ressursside piiratuse kaudu (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 12, 25, 29; TalTech, 2019, pp. 24–25). Ekspertide puudus ei ole mure üksnes teaduses, vaid määratletav kui valdkonnaülene probleem, mistõttu sai see defineeritud **tööjõu** probleemina. Dokumentides (KD1, KD2 ja KD3) tuuakse välja piiratud spetsialiseerumisvõime riigi-, teadus- ja erasektoris; spetsialistide puuduse ning nende ebapiisava juurdekasvu. Kaardistatud probleemi hulgas on olemas ka eelpool osutatud sisejulgeoleku asutuste (peaasjalikult politseisüsteemi) puudused, eelkõige küberkuritegevusi lahendavate vähene juurdekasv (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 26-27, 35–36; Vabariigi Valitsus, 2018, lk 14; Siseministeerium, 2020, lk. 73–74). Paljuski on probleemi juured **ressursi** leidmises. Dokumendid (KD1 ja KD6) toovad välja, et ressursside suunamine süsteemide arendamisele ja haldamisele on jäänud üldises digiarengus väikseks. Ressursi puudumise tõttu kannatab nii spetsialistide koolitamine kui ka teadus- ja arendustegevus (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 12, 39; TalTech, 2019, pp. 24–25), mis tegelikult võiksid aidata koodidena välja toodud probleeme pikemas

perspektiivis mitte üksnes lahendada, vaid ka ennetada. Hinnanguliselt võiks oluline roll ressursi leidmisel olla erasektoril ning selles tegutsevatel ettevõtetel, kuid **ettevõtlus** on samuti probleem digiarengus. Dokumentides (KD1 ja KD2) on probleemne väheste edukate IT-ettevõtete hulk sektoris ning koostöövõime puudulikkus erasektori ja avaliku sektori ning teadusasutuste vahel. Võib öelda, et kõikide valdkondade probleemide tõttu on tekkinud puudulik pilt küberruumi arengust ning selle tulemusena puudub tervikpilt ka küberruumi olukorrast (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 9–12; Vabariigi Valitsus, 2018, lk 13–15).

Vastavalt töö spetsiifikale on võimalik vaadata probleeme ka asjade interneti seadmete kaudu, mistõttu sai see dokumendianalüüsis märgitud koodiga **asjade interneti seadmetest ja selle tehnoloogia arengust tulenevad probleemid**. Koodiga registreeritud kaheksa dokumendiga (KD1, KD6, RD7, RD8, RD9, RND10, RND11 ja RND12) sai registreeritud ka kaks alamkoodi: **küberründed** ja **seadmed**. **Küberrünnete** peetakse silmas (dokumentides KD1, RD7, RD8, RD9 ja RND11), et asjade interneti seadmete kasutamine ning arvukus ei mitmekesista mitte üksnes potentsiaalsete sihtmärkide arvu, vaid annab kurjategijatele laiemad võimalused kuritegevusega tegeleda. Asjade interneti seadmete turvanõrkuste seas on välja toodud teenusetõkestusründed (DDoS), lunavararünded ja krüptokaevandusega (ingl *cryptojacking*) seotud ründed ning nende arvu kasv (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 8; ENISA, 2019, p. 43; UK Government, 2018, p. 20). Euroopa Komisjon (2020, p. 1) osutab, et seadmed jõuavad kasutajateni tihtipeale juba teada nõrkustega, mis tegelikult tähendavad ka seadet kasutavale inimesele pahatahtliku kübertegevuse osaks langemise riski. Asjade interneti seadmete andmekogude osas näeb RD8, et seadmetes olevate andmete valguses ähvardavad kasutajaid vargused, väljapressimine ning andmete hävitamine kolmandate osapooltepoolt (Rand Coroporation, 2020, p. 6). Dokumendid näitavad, et asjade interneti seadmeid on kuritegeliku eesmärgiga isikutel võimalik kasutada seadmete kasutajate igapäevaelu häirimiseks ning laialdasemate häirete tekitamiseks ühiskonnas.

Lisaks küberrünnetele on oluline mõista **seadmete tausta**. Dokumentides (KD1, KD6, RD7, RND10, RND11 ja RND12), nagu ka eelmises punktis, tuuakse välja, et seadmed jõuavad inimesteni juba teada olevate nõrkustega ning paljud turul olevad seadmed ei oma elementaarseid ja vajalikke turvalahendusi. Võrku ühendatuna on nad turvanõuete eiramise korral sisuliselt kõigile ligipääsetavad (TalTech, 2019, p. 29; European Commission, 2020, p. 1). Majandus- ja Kommunikatsiooniministeeriumi loodud Küberturvalisuse strateegias (KD1) nimetatud sõltuvus teiste riikide riist- ja tarkvaralahendustest on seega üks suuri probleeme. RND10 ja RND12 toovad välja, et tihti on probleem inimeste teadmatuses – seadme funktsioonide ja mugavuse kõrval ei pruugi toote tarbija isegi teada, et tema kohta andmeid kogutakse ja jagatakse ning et need võivad saada saatuslikuks ka rünnakute puhul (Government of Canada, 2020; Australian Government, 2020, p. 1).

Näiteks toob RND11 välja, et paljud asjade interneti seadmed müüakse universaalsete vaikesätetega, mille puhul eeldatakse, et kasutaja need kasutuselevõtu korral kohe muudab (UK Government, 2018, p. 2).

Kolmanda kategooria raames otsiti nii asjade interneti kui ka IKT-tehnoloogiatega seotud **konfidentsiaalsuse, terviklikkuse ja käideldavuse määratlust dokumentides**. See kategooria on oluline välja tuua, et näidata, mil moel on need dokumentides mainimist leidnud ning milline tähtsus on neil turvaelementidel nii IKT-tehnoloogia kui ka asjade interneti seadmetes. Et otsida kategooriale omaseid vasteid, kasutati otsingul märksõnu „konfidentsiaalsus“, „terviklikkus“, „käideldavus“ ning ingliskeelseid märksõnu *confidentiality*, *integrity* ja *availability*. Kokku leidsid eelpool välja toodud mõisted käsitlemist kuues dokumendis (KD1, KD2, KD5, RD8, RND11 ja RND12).

IKT-tehnoloogia turvaelementidena leidsid konfidentsiaalsus, terviklikkus ja käideldavus käsitlemist dokumendis KD2, kus toodi välja riigi infosüsteemile ja tehnoloogia kiirele arengule toetudes süsteemide ning nende komponentide ajakohastamisele keskendumine. Ajakohastades süsteeme on võimalik tagada taristu komponentide toimimiseks vajalik vastavus konfidentsiaalsuse, terviklikkuse ja käideldavuse nõuetele (Vabariigi Valitsus, 2018, lk 12). KD5 tõi eestikeelsed mõisted välja turvameetmete kohta ning rõhutas, et turvameetmete valik ja nende rakendamine on olulised andmete konfidentsiaalsuse, terviklikkuse ja käideldavuse tagamisel (E-riigi Akadeemia, 2020, lk 19). KD1 tõi elementidest välja üksnes käideldavuse ning seda riigipilve ja andmesaatkonna lahendustele tuginevalt, reaalajas andmete kasutamise ja teenuste opereerimise näitel (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 24). Kolm turvaelementi registreeriti asjade interneti valguses kolmes rahvusvahelises dokumentides (RD8, RND11 ja RND12). RD8 toob välja, et asjade interneti turvaarhitektuur toetub küll peamiselt CIA triaadile, kuid oluline oleks keskenduda eraldi ka juurdepääsu kontrollile (ingl *access control*), poliitika seadistamisele (ingl *policy configuration*) ja turvalisuse elutsüklile (ingl *security lifecycle*) (ENISA, 2019, p. 14). RND11 toob välja, et asjade interneti seadmetega tuleks keskenduda tarkvara terviklikkuse kindlustamisele ning volitamata juurdepääsu korral tuleks seadet kasutavale inimesele tekitada teatav hoiatussüsteem (UK Government, 2018, p. 11). RND12 toob välja turvalisuse kõrval nimelt terviklikkuse, rõhutades, et asjade interneti seadmete turvalisusele ja terviklikkusele keskendudes paraneb inimeste elukvaliteet ning igapäevane töö. Samuti toob dokument välja, et konfidentsiaalsuse või terviklikkuse kaitset vajavad andmed tuleks krüpteerida ning juurdepääsud logida, et oleks näha kuupäev, kellaaeg ning juurdepääsu allikas (Australian Government, 2020, pp. 1, 5–6).

Neljanda kategooriana sai dokumendianalüüsis määratletud **soovitused asjade interneti seadmete turvaliseks kasutamiseks**, mille käigus registreeriti kolm koodi: **soovitused tavakasutajale, riiklikult seotud osapooltele** ning **seadmete ja teenuste tootjatele**.

Tavakasutajatele antavad soovitused registreeriti ära kahes dokumendis (RND10 ja RND12). RND10 [Internet of Things (IoT) Checklist for Consumers, Government of Canada, 2020] keskendub tavakasutaja turvalisusele ja privaatsusele. Näiteks toob RND10 esile, et asjade interneti seadmed peaksid vastama kodukeskkonna privaatsuse ja turvalisuse ootustele. Lisaks nähakse, et kasutajad võiksid teada, kui pikk on seadme eeldatav eluiga ning kas see on võimeline töötama ilma võrguühenduseta. Kahele välja toodud soovitusele tuginedes on RND10 esitanud hulga küsimusi, mida asjade interneti seadmete kasutajad endalt küsida võiksid. Esiteks on oluline enne seadmete ostu küsida, kas ja kuidas seade kasutaja andmeid kogub, kasutab ning kellega ja kuidas neid andmeid jagab. Teisena on oluline endalt küsida, kas seade kogub andmeid, mida kasutaja tegelikkuses ei soovi, et seade koguks. Vaja on läbi mõelda, kas kasutajal on võimalik loobuda seadme andmete kogumisest, jagamisest ja nende kasutamisest, sealjuures loobumata turvauuendustest (ingl *security updates*). Kolmandaks on seadme kohta tarvis küsida, kas ja kui kaua on toote jaoks saadaval turvapaikamine (ingl *patching*) ning uuendused (ingl *updates*), tagamaks toote turvalisus kasutaja jaoks pika aja vältel. Neljandaks on tarvis teada, millised asjade interneti seadme funktsioonid töötavad ilma võrguühenduseta ning kas seade lakkab töötamast, kui tootja lakkab olemast? Samuti on kasutajatugi ning selle olemasolu üks neid aspekte, mille üle seadme kasutaja enne seadme ostu mõelda võiks. Tootja kohta võiksid küsimused laieneda ka tootja privaatsuse ja turvalisuse kaitsmise kogemustele. Oluline oleks enda jaoks selgeks teha, kas seadmega on olnud probleeme ning milline on olnud nende probleemide mõju tarbijale ning milliste meetmetega on tootja probleemid likvideerinud. RND10 toob välja, et paljudele küsimustele aitavad vastused leida sõlltumatute kasutajate ülevaated ja hinnangud seadme kohta, millega tasuks enne seadme soetamist tutvuda. Asjade interneti seadme ostmine võiks olla läbi mõeldud tegevus, kus esitatud küsimused aitavad paremini mõista, kuidas seade kasutaja privaatsuse ja turvalisusega suhestub.

RND10 juhib tähelepanu, et seadme peab seadistama turvaliselt ning seda kasutades jälgima, et see saaks regulaarselt turvavärskendusi, mis aitab privaatsuse ja turvalisuse tagamisele oluliselt kaasa. Ei soovitata vanu seadmeid ära visata, vaid tootja antud juhiste järgi seadmest andmed eemaldada ning seaded lähtestada. Turvaliselt ning vastutustundlikult asjadest lahti saamiseks on võimalik näiteks Kanadas elavatel inimestel kasutada valitsuse loodud seadmete äraviskamiseks loodud e-jäätmete likvideerimise keskkonda.

RND12 (Code of Practice – Securing the Internet of Things for Consumers, Australian Government, 2020, pp. 3–7) toob kasutajatele välja spetsiifilised soovitused. Tavakasutaja ei tohiks omada RND12 järgi asjade interneti seadmetes teiste keskkondadega samu ega ka üldiselt nõrku paroole. Paroolid peaksid olema kordumatud, ettearvamatud, keerulised ja kolmandatele osapooltele mõeldamatud. Lisa-turvalisust aitab luua mitmefaktoriline autentimine ning seadme tarkvara uuendatuna hoidmine. Tavakasutaja peab olema veendunud, et tema isikuandmed on kaitstud ning keeruliste paroolide, mitmeastmelise tuvastamise ning uuenduste tegemine on üks võimalikke viise, kuidas tavakasutajad asjade interneti seadmeid turvaliseks saavad muuta.

Riiklikult seotud osapooltele antavates soovitustes saab välja tuua kolm dokumenti (KD2, KD6 ja RND11). KD2 soovitab Eesti riigisisese dokumendina hakata korraldama uute tehnoloogiate katseprojekte riigi infosüsteemiga seotud lahenduste arendamiseks. Ühe tehnoloogiana toob KD2 välja ka asjade interneti, mille turvalisuse ning riskide kohta annaksid informatsiooni katsed (Vabariigi Valitsus, 2018, lk 27). Sarnaselt katsetega toob KD6 välja, et asjade interneti seadmete ja nendega seonduva informatsiooni uurimine ja analüüsimine võib pikemas plaanis parandada ametiasutuste võimekust nii küberkuritegevuste lahendamisel kui ka digikriminalistika valdkonnas (TalTech, 2019, p. 29). RND11 jaoks on oluline, et vaikesätete ja ka tehase väljastatud kasutajanimede ja paroolide muutmine oleks riigi poolt rohkem probleemina välja toodud ning sellega peaks seadmete kasutamisel alguses kohe arvestama (UK Government, 2018, p. 6). Peaasjalikult soovitatakse riiklikult seotud osapooltele teha rohkem katseid, samuti õppida seadmeid ja nende võimalusi rohkem tundma, et saadud informatsiooni najal probleemidele paremaid lahendusi leida.

Tavainimeste ja riiklike asutuste kõrval antakse soovitusi ka seadmete ja teenuste tootjatele (dokumendid RD7, RD8, RND11 ja RND12). Turvanõrkuste avastamise ning likvideerimisvõimekuse tõstmine, tarkvara- ja turvavärskenduste pakkumise pidev jätkamine ning toote eluea lõppedes andmete kustutamise tagamine on ühed soovitused, millele tähelepanu pööratakse. Eriliselt soovitatakse keskenduda arendusprotsessis turvalise süsteemi ehitamisele (European Commission, 2020, p. 9; ENISA, 2019, pp. 12, 15, 50). Just turvalisus on kõige enam registreeritud soovituslik suund – see on asjade interneti seadmete puhul möödapääsmatu ning sellele peab keskenduma seadmete kasutajaskonna privaatsuse tagamiseks. Eraldi saab välja tuua ka dokumentides esinenud soovituse, et tootja peaks vaikeparoolide kasutamise võimaluse likvideerima, andes kasutajale kohustuse toote kasutamist alustades panna paika enda loodud kasutajanimi ning parool. Lisaks peaks toote paigaldus- ja hooldusprotsess olema kasutaja jaoks lihtne (UK Government, 2018, pp. 18–20; Australian Government, 2020, pp. 3–7).

Asjade interneti soovitused on aga spetsiifilised ning mitme osapoole jaoks võivad eelpool välja toodud kategoorias registreeritud punktid olla ebapiisavad selleks, et tehnoloogiat turvaliselt kasutada. Seetõttu on oluline vaadelda ka dokumendianalüüsi viiendat kategooriat, mis sai registreeritud kui **soovitused digiarengust tulenevate probleemide lahendamiseks**. Kategooria avab digiarengutega tekkinud muredele (välja toodud teises kategoorias) välja pakutud lahendusi, millel võib olla ühisosa asjade interneti seadmetega. Viienda kategooria all sai registreeritud koodidena teises kategoorias välja toodud koodid: **ettevõtlus, IT-lahendused, poliitika kujundamine, rahvusvaheline koostöö, ressurss, sisejulgeoleku asutused ja küberkuritegevus, teadmised ja oskused, teadus- ja arendustegevus** ning **tööjõud.**

Teadmiste ja oskuste koodi all tuuakse kolmes dokumendis (KD1, KD2 ja KD5) välja vajadus korraldada laiemale avalikkusele suunatud tegevusi, suurendada haridusasutuste ja täiendõppeprogrammide, kuid ka muude tegevuste kaudu riigi- ja erasektori küberturbeteadmisi (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 36–37; Vabariigi Valitsus, 2018, lk 33, 39). Lisaks õppeasutustele on võimalik tõsta teadlikkust kübervaldkonna kohta näiteks õppuste kaudu, kus saab lisaks meeskonna testimisele ja olukordade lahendamisele harjutada ka koostööd teiste osapooltega (E-riigi Akadeemia, 2020, lk 23–24). Dokumentide ühtne sõnum on tegeleda inimeste teadmiste edendamisega, teavitustöö ning probleemide kaardistamisega.

Rahvusvahelise koostöö juures andsid soovitusi viis dokumenti (KD1, KD2, KD3, KD5 ja RD7) ning nendes toodi kokkuvõtlikult välja suurem koostöövajadus strateegiliste partneritega, sealhulgas Euroopa Liidu, NATO ja ÜRO staadiumil (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 22–23, 28–29; Vabariigi Valitsus, 2018, lk. 34, 37–38; European Commission, 2020, p. 6–7, 17). Rahvusvahelised projektid on üks võimalus koostöö elavdamiseks, teisalt ka õppustel osalemine, mis aitab tagada kestlikuma kübervõime. Toimima peab rahvusvaheline koostöö küberkuritegude uurimisel ning Euroopa Liidu tasandil peaks looma küberturvalisusele keskenduvad koostöörühmad. Tuleb mõista, et kuna küberkuritegevus riigipiire ei tunnista, on küberkuritegevuse vastane võitlus rahvusvaheliselt fundamentaalne ja oluline (Siseministeerium, 2020, lk 63; E-riigi Akadeemia, 2020, lk 23–24; 27).

Poliitika kujundamine on üks koodidest, millele soovituslikke vasteid oli dokumentides (KD1, KD2, KD5, KD6 ja RD9) nimetatud kõige rohkem. Lahendustena nähakse spetsialistide taseme- ja täiendõppe kvaliteedi tõstmist ning kübervaldkonna iduettevõtete tekkeks ja toimimiseks toetava keskkonna tagamist. Tähtis on teadusasutuste, erasektori ning avaliku sektori vahel toimiva koostöö propageerimine ja soodustamine (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 28–30, 39; TalTech, 2019, p. 26). Koostöö on probleemide lahendamisel vajalik ning lahendusena tuuakse välja

ka riigi selge töökorralduse määratlemine ning kiire ja kvaliteetse teabevahetuse korraldamine osapoolte vahel. Seejuures tuleks jälgida infoühiskonna arenguseisu Eestis ja maailmas, sest see aitab paremini informatsioonil liikuda ning infosüsteeme arenema ja koosvõimelisena toimima (Vabariigi Valitsus, 2018, lk 7; E-riigi Akadeemia, 2020, lk 41). Eraldi toob RD9 välja programmi loomise, mis aitaks kaasa küberkuritegevuse alasele teadlikkusele ja seisaks vastu küberkuritegevuse probleemidele (Rand Coroporation, 2020, pp. 10-11). Riigiga on seotud ka **IT-lahenduste** koodi all registreeritud soovitused. Kahes dokumendis (KD1 ja KD2) tuuakse välja, et riik peaks infoturbe ja andmekaitse põhimõtteid kindlamalt ja tugevamalt järgima just riigi infosüsteemide puhul ning tehnoloogiliselt tõhustama enda vastupanuvõimet. Andmekogude turvalisuse tagamine ning riigi infosüsteemide komponentide arendamine on riigi jaoks elutähtsalt vajalikud (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 22–23; Vabariigi Valitsus, 2018, lk 25, 29).

Sisejulgeleku asutuste ja küberkuritegevuse koodi juures toodi dokumentides (KD1, KD3 ja KD5) esile ühtse küberjulgeoleku kogukonna kujundamine ning tehniliste spetsialistide olemasolu, et saada paremini aru küberkuritegude sisust ning tehnilisest poolest (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 27; E-riigi Akadeemia, 2020, lk 27). Täpsemalt toob visioonid välja KD3 ning seda just politseisüsteemi vaatest lähtuvalt. IKT arengu ja küberkuritegevuse tulevikutrendide pidev analüüs, koostöö soodustamine strateegiliste partneritega ennetusliku tegevuskava koostamiseks, täiendusõppe koolituskavade koostamine ning õppekavadesse küberteadmiste sidumine on vaid vähesed, kuid kesksed lahendused, kuidas sisejulgeoleku valdkond proovib digiarenguga hakkama saada. Spetsialistide tehniliste teadmiste tõstmine ning spetsialistide leidmine on eesmärk omaette, mistõttu on tarvis küberkuritegude uurijate lisavajadust silmas pidades teha analüüs (Siseministeerium, 2020, lk 73–74). Digiarengute keskel on tarvis arvestada ning tegutseda suunal, mis tagaks, et julgeolekuga tegeleksid spetsialistid, kelle võimekus küberkuritegusid avastada ning menetleda on võimalikult kõrge. Üks võimalikke viise panustada oskustega spetsialistide järelkasvu on keskenduda ka **teadus- ja arendustegevusele**. Dokumendid (KD1, KD2, KD3 ja KD6) toovad välja, et lisaks erasektori, riigi ja teadusasutuste vahelise koostöö võimendamisele peab tähelepanu pöörama ka tehnoloogiaga seotud riskide paremale hindamisele ja haldamisele, teadustöö mahu suurendamisele ning spetsialistide taseme- ja täiendõppe kvaliteedi tõstmisele ja hoidmisele (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 24, 27–28; Vabariigi Valitsus, 2018, lk 27, 33, 36, 40; Siseministeerium, 2020, lk 63). Olulisteks suundadeks, millele peaks teadus- ja arendustegevuse raames tähelepanu pöörama, on kvanttehnoloogia, krüptograafia, küberkuritegevus, tehisintellekt, masinõpe ning privaatsusega seonduvad ohud (TalTech, 2019, p. 5).

Kaalukas on arendustegevuse juures **ressurss**, millele toetudes muutuvas ühiskonnas probleeme lahendada. KD5 toob välja, et mitte üksnes inimressurss ei ole selles küsimuses oluline, vaid tähtis on ka arendusressursi olemasolu, mille najal endale vajalikud tööriistad ise välja arendada, vähendades sedasi sõltuvust kolmandatest osapooltest. Nii oleks ka riiklikult olukordade lahendamine tõhusam. Arendusressurssi ei saaks aga kasutada ilma spetsialistide ning teadlikult tegutseva tööjõuta, sest näiteks küberkuritegevuse üksuse töös on vajalik spetsialistide olemasolu, et saada aru küberkuritegude spetsiifikast (E-riigi Akadeemia. 2020, lk 23, 27). Seega on tarvis ressurssi nii spetsialistide leidmiseks kui ka arendusprotsesside algatamiseks ning töös hoidmiseks. Eelpool välja toodud probleemid ressursi, aga ka tööjõu ja spetsialistidega on olnud seotud ka teiste eelpool esitatud koodidega. Peaasjalikult on just nende jaoks ressursi- ja tööjõuküsimused seotud poliitika kujundamise, teadmiste ja oskuste ning teadus- ja arendustegevusega.

Dokumentides (KD1, KD2, KD3, KD5 ja KD6) sai registreeritud ka kood **ettevõtlus**. Selleski tuuakse välja koostöö võimendamine erasektori, riigi ja teadusasutuste vahel, mis on läbivalt viies dokumendis just ettevõtluse kaudu kesksele kohale jõudnud (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 28–29; Vabariigi Valitsus, 2018, lk 33–34; Siseministeerium, 2020, lk 63; TalTech, 2019, p. 26). KD4 toob välja, et ühiskondlikult vajalike IT-teenuste toimimine sõltub tugevalt erasektoris tegutsevatest ettevõtetest, mis annavad keskkonnamuutuste kohta kiiresti vajalikku informatsiooni, tagavad informatsiooni vahetuse ning annavad võimaluse analüüsida kübervaldkonna olukorda (E-riigi Akadeemia, 2020, lk 23).

2.3. Ekspertintervjuude analüüs

Selles alapeatükis analüüsitakse ekspertintervjuusid. Autor viis läbi poolstruktureeritud intervjuud, millega sai kolmeteistkümne spetsialisti (**koodid E1 kuni E13**) arvamused andmetöötlusprogrammi NVivo abil viide kategooriasse koondatud. Esimesele uurimisküsimusele vastuse leidmiseks moodustati **esimene kategooria – asjade interneti mõiste ning määratlus ekspertintervjuudes**. Koodi alla moodustus kolm koodi, kus määratleti asjade interneti definitsioon, seadmete näited ning asjade internet digiarengu dokumentide ja käimasolevate tegevuste valguses (koodid nähtavad käesoleva töö Lisas 5, vt lk 91).

Esimese kategooria **esimese koodi, asjade interneti definitsiooni** kohta tõid eksperdid välja nende arusaama mõistest *Internet of Things* (ingl) ning selle eestikeelse vaste. Sai tuvastatud, et terminoloogias kasutatakse tehnoloogilise idee identifitseerimiseks eestikeelset vastet „asjade internet“ (E1, E5, E6, E7, E8, E10, E11, E13). Endine CERT-EE juht, praegune Cyber4Dew küberturbe ekspert Klaid Mägi (E1, 2021) ütles:

„*Kui me räägime asjadest, mis on internetti ühendatud, siis mina lähtun väga filoloogiliselt ehk asjade internet ehk asjad, mis on ühendatud internetti*.“ (E1, 2021)

Ingliskeelset väljendit *Internet of Things*, mida seostatakse ka lühendiga IoT, eelistavad kasutada viis eksperti (E2, E3, E4, E9, E12). Eestikeelse termini kõrval tuuakse välja valdavalt ingliskeelsete materjalide ning töökeskkonna olemasolu, mistõttu on ingliskeelse mõiste ja lühendi kasutamine osa ekspertide jaoks lihtsam. Politsei- ja Piirivalveameti arendus-, innovatsiooni- ja teaduskoostöögrupi juht Elari Kasemets (E2, 2021) toob ekspertide hinnangu kokkuvõtvalt välja:

„Rääkides majaväliselt konkreetsete koostööpartneritega, on ikkagi Internet of Things ehk IoT, sest see on ikkagi kõige lihtsam ja kõigile nagu üheselt arusaadav.“ (E2, 2021)

Hoolimata erinevatest võimalustest uuritavat subjekti nimetada näevad eksperdid asjade interneti tehnoloogias internetiga ühendatud seadmeid, mis on võimelised informatsiooni ümbritsevast keskkonnast koguma ning seda teiste sarnaselt võrku ühendatud seadmetega jagama. Võrguühendusele lisaks märgitakse definitsioonis ära andurid (E7 ja E12) ja sensorid (E4 ja E7), mille abil on seadmed võimelised informatsiooni talletama. Üks ekspertidest, Euroopa Liidu Küberturvalisuse Ameti IT-agentuuri tugiüksuse juht Uku Särekanno (E11, 2021) juhib tähelepanu ka iseseisvuse mõistele:

„Me räägime asjadest või esemetest, mis on võimelised suhtlema interneti vahendusel, edastama infot ja seda infot koguma ning mingil määral töötlema /.../ pikas perspektiivis seadmed suhtlevad omavahel ja oluline on see iseseisvuse mõiste seal juures ehk kolmandad osapooled vahele nii-öelda ei sega.“ (E11, 2021)

Oluline on välja tuua, et eksperdid näevad mõistet kahest vaatest lähtuvalt: seda on võimalik käsitleda ühe osana suuremast teemast, kus asjade internetile tuleb keskenduda nagu ka teistele IKT-seadmetele. Lisaks üldiste IKT-seadmete alla liigitamisele nähakse võimalust seadmed ka eraldi tööstusharuna ära nimetada tööstusrevolutsiooni 4.0 (täisautomaatne tootmine) osana, kus asjade internetil on täita ekspertide sõnul tähtis roll. Siiski leiavad eksperdid, et asjade internetile tasub anda mõõde, mis seostuks üldiste IKT-seadmetega, sest see annaks näiteks avalikule sektorile paremad viisid tegeleda tehnoloogiaprobleemidega üldiselt ning tuua sisse perspektiivikas teema, asjade internet, üldiste IKT-seadmete keskel (ekspertintervjuude analüüsi 4. Kategooria, vt lk 91).

Teise koodi, ekspertide välja toodud asjade interneti seadmete näited, eesmärk oli esimese koodi ehk definitsiooni kinnistamine, mille käigus eksperdid nimetasid nende arvamuse järgi tehnoloogia alla liigituvad seadmed. Seadmete nimetamine annab võimaluse paremini mõista, mida asjade interneti seadmeteks pidada. Seadmetena tõid eksperdid välja näiteks mängukonsooli, nutikaalu, robottolmuimeja, nutika rösteri ja kohvimasina, saunakerise, ukseluugi, targa kaamera, televiisori, nutitelefoni, sülearvutid, külmkapi ja ahju. Oluline on esile tuua, et eksperdid (E4, E7 ja E9) osutavad ka komplitseeritusele mõiste defineerimisel, sest näiteks nutitelefonide ja sülearvutite ning taoliste seadmete käsitlemine asjade interneti seadmetena võib olla küsitav ning määratlemist vajav. Majandus- ja Kommunikatsiooniministeeriumi Riigi Infosüsteemide osakonna küberturvalisuse tehnoloogia nõunik Rein Põdra (E7, 2021) rõhutab defineerimise keerukust:

„*Mis seadmed need IoT seadmed on? Keeruline küsimus, sest ega meil see täpselt ei ole ju defineeritud, mis ta tegelikult on, et kust maalt see piir jookseb, et kas näiteks nutikell on IoT seade või ei ole? Tal on ju iseseisev andmetalletus ja töötlemisvõimekus, seega…"* (E7, 2021)

Kolmanda koodina toodi välja asjade internet digiarengu dokumentide ja käimasolevate tegevuste valguses, milles sai registreeritud ekspertidele (E1, E2, E3, E4, E5, E6, E7, E8, E9, E11) teadaoleva mõiste esinemine ning sellele keskendumine dokumentides ja programmilistes tegevustes. Kood annab aimu sellest, kui perspektiivikaks võib teemat näiteks otsustustasandil pidada. Ekspertide hinnangul on asjade interneti teema asutustes loodud ja olemas loodavates visioonidokumentides (E1, E3, E4, E6, E7, E8, E9, E11), kuid eraldi dokumente selle kohta ekspertidele teadaolevalt Eestis ei ole. Välja tuuakse, et asutuste sees keskendutakse tehnoloogiale seadmete sertifitseerimise (E7 ja E9) ja standardiseerimise (E1 ja E4) võtmes ning ainsa konkreetselt asjade internetile keskenduva dokumendina toovad eksperdid (E4, E11) välja ENISA "Good Practices for Securing IoT".

Eksperdid leiavad, et kuna asjade internetil on suur ühisosa üldiste infotehnoloogia seadmetega, on neil sellest tulenevalt seos ka üldiselt seadmetele kehtestatud raamistikega, mis panevad paika tehnoloogiale seatud tingimused ning turvalisuse algprintsiibid. Tehnoloogiaga seostuvate määruste juures tõid eksperdid intervjuudes ühisosana välja infosüsteemide turvameetmete süsteemi ISKE (E3, E4 ja E9) ja isikuandmete kaitse üldmääruse (GDPR) (E6, E7 ja E13). Asjade interneti seadmeid reguleerivaid määruseid nähakse küll vajalikena, kuid öeldakse, et infotehnoloogia seadmete põhimõttelised regulatsioonid juba eksisteerivad ning ka nendega saab läheneda asjade interneti seadmete paremale määratlemisele. Politsei- ja Piirivalveameti infoturbetalituse juhataja Priit Kleemann (E4, 2021) ning Elari Kasemets (E2, 2021) viitavad olemasolevatele reeglitele:

„Meil on ISKE-s olemas ju nõuded, et meil on turvameetmete süsteem ISKE, kus meil on nutiseadmete kohta eraldi peatükid, et kohe ta seal IoT-seadet nii ei anna, aga muidu ta seal olla võiks /.../ seos on ju olemas." (E4, 2021)

„IoT-le keskenduvaid dokumente eeldatavasti võiks ju olla, aga praegusel hetkel ma arvan, et sellised üldised põhimõttelised raamid või kasutuspõhimõtted on hetkel juba piisav." (E2)

Teisele uurimisküsimusele vastuse leidmiseks moodustati **teine kategooria, IKT kui keskse tehnoloogia vaatest probleemsed aspektid**, mille alla moodustus viis koodi – registreerimist leidsid probleemid, mis viitavad ebapiisavale ennetustööle, inimeste madalale teadlikkusele, inimeste puudulikele oskustele, avaliku sektori korralduslikele puudujääkidele ning seadmete ebakvaliteetsele taustale (koodid välja toodud käesoleva töö Lisas 5, vt lk 91).

Esimese koodina sai registreeritud **ebapiisav ennetustöö**, mille käigus tõid eksperdid (E1, E3, E5, E7, E8, E10 ja E13) välja tõhusama ennetustöö vajalikkuse. Ennetustöös tuuakse positiivsena välja RIA, kes erinevate kampaaniatega (näiteks RIA korraldatud ennetuskampaania "IT-vaatlik") keskenduvad inimeste teadlikkuse kasvatamisele nii tehnoloogia kui ka selles peituvate ohtude kohta. Siiski toovad eksperdid esile puuduliku ennetustöö nooremates eagruppides, sest see toob pikemas perspektiivis esile probleemid vanemates eagruppides, kus ennetustöö avaldab suuremat ja efektiivsemat mõju inimestele vähem. Ennetustöö võiks toimida ka üksnes spetsiifilise tehnoloogia näitel, kuid üldises vaates on seda kasumlikum teha tehnoloogiaüleselt, sest probleem on pigem üldise teadlikkuse kasvatamises ning informatsiooni edastamises inimesteni sedasi, et see neid ka huvitaks. Majandus- ja Kommunikatsiooniministeeriumi Riikliku Küberturvalisuse osakonna küberriskide halduse juht Martin Sepp (E3, 2021) ja Klaid Mägi (E1, 2021) viitavad ennetuslikule vaatele:

„Küber on üldse selline, et vastupanuvõimest ja turvalisusest rääkimine ei ole atraktiivne inimeste jaoks, et tavakodanikku see ei kõneta, sest tema soovib saada kiiresti, mõnusalt mingit teenust kasutada ja teda ei huvita see turvalisuse ja turbe pool." (E3, 2021)

„RIA teeb erinevaid kampaaniaid /.../ tehakse blogisid ja reklaame siin ja kolmandas kohas /.../ politsei teeb ennetust, veebikonstaablid ennetavad, aga sellega peab tegelema oluliselt laiemale sihtgrupile ja sellega peaks alustama pihta oluliselt madalamas eas kui praegu." (E1, 2021)

Lisaks toob RIA intsidentide käsitlemise osakonna osakonnajuhataja, CERT-EE juht Tõnu Tammer (E5, 2021) välja, et ennetustegevusega võidakse olla juba hiljaks jäänud:

„Üle-eelmise aastani ei olnud meil mitte mingisugust internetisuunalist ennetamist /.../ Arvestades seda, et internetist tulenevad võimalused antakse piltlikult öeldes inimesele kätte juba siis, kui nad lasteaeda lähevad või isegi varem, ja ma ei anna kaasa seda teadmist, et mis ohud varitsevad ja kuidas mõelda, siis ega hilisemas ennetuses tegeleme sellise tulekahju kustutamise, mitte sisulise ennetustööga." (E5, 2021)

Murekohad ennetustöös viivad **inimeste ebapiisava teadlikkuseni**, mis sai registreeritud teise kategooria **teise koodina.** Probleem seisneb lihtsamate teadmiste puudujäägis. Eksperdid toovad välja, et ründevektorid võivad olla lihtsad ja labased ning tihti süüdistatakse probleemide korral seadmeid ja tehnoloogiat, kuigi probleemi juures võivad olla inimeste enda teadmistes ning lähenemistes, mis ei ole piisavalt läbi mõeldud. Politsei- ja Piirivalveameti anonüümistatud spetsialist (E10, 2021) toob välja ka inimese haavatavuse ja manipuleeritavuse, mida võrku ühendatud seadmed võimaldavad:

„Me tajume digitaalset ruumi teistmoodi kui füüsilist, millest tulenevalt on edukad ka ründevektorid, mis on seotud inimeste sotsiaalse manipuleerimisega. Keeruline on esile tuua nii-öelda ,,kõige probleemsemat aspekti, kuna need asjad töötavad kogumis." (E10, 2021)

Eelpool välja toodud eksperdi arvamus on otseses seoses teadlikkusega, sest ründevektorite lihtsus, inimeste teadlikkus ning digitaalse ja füüsilise ruumi tajuvuse erinevused teevad kasutajatest kerged sihtmärgid, millele viitavad ka teised eksperdid. Üks ekspertidest (E7, 2021) ütleb, et inimesed soetavad asjade interneti seadmeid nende kasutust läbi mõtlemata ja seavad ennast sellega ohtu:

„Kõige peamisem on teadlikkus /.../, et kui mingid asjad võetakse läbimõtlemata kasutusele, sealhulgas ka seda, et turvaseadmeid ei rakendata või ühendatakse ja kasutatakse neid seal, kus ei peaks neid kasutama ja ei ole nad selle jaoks mõeldud, siis kõik see toetub teadmatusele." (E7, 2021)

Inimeste puudulikud oskused, mis sai registreeritud kolmanda koodina, on eksperdid (E1, E2, E10, E12 ja E13) välja toonud, et inimeste oskused on ebapiisavad nii tavalise arvuti kui ka nutikate seadmete käsitsemises. Peaasjalikult toovad eksperdid välja oskused seadmete turvaliseks tegemises. Tavakasutuses elementaarseks saanud seadmetele, näiteks arvutitele, televiisoritele, digiboksidele ja nutitelefonidele on sätetele ligipääs ning uuenduste tegemine kasutajale tehtud lihtsaks ja visuaalselt kättesaadavaks, seega saab enamik kasutajaid seadmete turvaliseks tegemisega hakkama, kuid asjade interneti seadmete uuendamisega võib tavainimesel probleeme tekkida. Seadmete uuendused võivad käia teiste seadmete kaudu ning sellega võib toiming komplitseeritumaks muutuda. Oskamatus juba

üldisi infotehnoloogilisi seadmeid kasutada näitab, et asjade interneti seadmete turvaline kasutamine võib samuti kasutajaskonna jaoks paljuski oskuste taha kinni jääda ning oskamatust üksnes süvendada. Seadme kasutamine võib sealjuures olla üks kõige lihtsamaid ning õpitavamaid punkte, kuid seadmete kaitsmine on see, mis puudulike oskuste all on probleem. Eksperdid ütlevad, et kui üldlevinud tehnoloogia ühendatavuse puhul saab kasutaja mingil määral kindel olla selles, kuidas seadmed võrku on ühendatud, siis asjade interneti seadmete puhul ei pruugi kasutajad ühendatavusest või selle välja lülitamise võimalustest teadlikud olla. Anonüümistatud Politsei- ja Piirivalveameti spetsialist (E10, 2021) ja ekspert Klaid Mägi (E1, 2021) toovad välja:

„Minu meelest on peamine risk asjade internetiga see, et paljude seadmete puhul inimesed isegi ei pruugi teada, et nad internetis on ja teiselt poolt ei oska nad neid ise turvaliseks konfigureerida." (E10, 2021)

„Kui arvutile ja telefonile, televiisorile ja digiboksile ma oskan teha tarkvarauuendusi ja ma tean, kuidas neid kaitsta, siis andke andeks, IoT-kaalu, -tolmuimejat ja -hambaharja ma tõesti kaitsta ei oska." (E1, 2021)

Teadmiste ning oskuste edendamine on üks suurimaid tehnoloogiaprobleeme. Eestile omistatud tehnoloogiliselt pädeva ja tugeva riigi kuvand ei saa toetuda vaid üksikute tehnoloogiliselt innovaatiliste ideede loomisele, vaid olulisel kohal on ka selle süsteemi turvalisena hoidmine ning selle igakülgne arendamine nii süsteemi kui ka elanikkonna jaoks. Tõnu Tammer (E5, 2021) toob tulevikku vaatavalt välja olevikupildi:

„Me ei ole tähelepanu pööranud ja meil on kaks generatsiooni vähemalt, kes on selles maailmas, kus nad ei oska adekvaatselt toimetada ning siin läheb 15–30 aastat enne, kui see uus generatsioon kasvab peale, kes oskab. Loomulikult eeldusel, et me hakkame süstemaatiliselt seda tööd ka tegema." (E5, 2021)

Eksperdina määratletud Siseministeeriumi anonüümistatud ametnik (E8, 2021) toob välja, et innovatsiooniretoorika kõrval on turvalisuse teema käsitlustes jäänud vajaka:

„Digiriigi digitiigri kuvand, mis meile nii-öelda omistatud on, ma tahaksin öelda, et võrreldes sellega, kui tugevad me millalgi olime, siis me ei ole küberturvalisuse vaatest asjadele tähelepanu piisavalt pööranud." (E8, 2021)

Neljanda koodina sai registreeritud **avaliku sektori korralduslikud puudujäägid**, mille raames tõid eksperdid (E1, E3, E5, E7, E8, E9, E11) välja riigiasutuste korraldusliku poole probleemid. Lisaks ennetustöö ning elanikkonna harimisele, mis toodi välja eelnevate koodide juures, lisavad eksperdid võimalike riskianalüüside puudulikkuse. Lisaks oleks tarvis turul müüdavate toodete regulatsiooni, mis seaks kriteeriumid turul müüdavatele seadmetele. Tuuakse esile ka avaliku sektori toimingute kiiruse ja efektiivsuse madal tase, mis ei ole vastavuses tehnoloogia kiire arenguga. Tehnoloogia areng nõuab ekspertide hinnangul võimekust olukordadele kiiresti reageerida ning vajaduse korral otsuseid etteulatuvalt teha. Seotus on sealjuures ka õigusruumi olemuses, sest intervjueeritud ekspertide järgi ei toeta see piisavalt intsidentide ja kuritegevuse lahendamist ning peaasjalikult ei ole arvesta lahenduse soosimise juures kübervaldkonna globaalset mõõdet. Üks ekspertidest (E7, 2021) ütleb riigisektori toimimiskiiruse kohta nii:

„Tegeleme küll, aga erasektorist tulnuna ei ole see riigiasutuste liikumise kiirus kõige suuremat optimismi tekitav. Kui kiiresti muu maailm, eriti erasektor seal kõrval liigub? Tihti ei tegele me mitte probleemi ennetamisega või võimalike regulatsioonide loomisega, vaid enamjaolt asja lahendamisega, sest kuskil on miskit juhtunud ja me peame seda lahendama." (E7, 2021)

On olemas üks suurem ja laiem küberdomeen, mis ei ole üksnes Eesti Vabariigi keskne, vaid omab laialdasi mõjusid ka väljaspool Euroopat, üle terve maailma. Globaalne mõõde on see, mis ekspertide hinnangul võiks avalikule sektorile näidata teema tõsidust ning atraktiivsust. Kiirus ja lähedus on küberruumis saanud uue tähenduse, mida kirjeldab hästi CERT-EE juht Tõnu Tammer (E5, 2021):

„Pole mingit vahet, kas Tallinna ja Piiteri vahe on 400 km või Piiteri ja Pariisi vahe on 3000 km – mõlemal juhul liigub pakett alla sekundiga. Küberruumis oleme kõik üksteise naabrid ja seda meil väga ei arvestata, meie õiguskeskkond seda tüüpi maailmas esile tulnud probleemide lahendamist ei toeta." (E5, 2021)

Regulatsioonide ning globaalsuse mõõdet aitab paremini lahti seletada **viiendana registreeritud kood seadmete ebakvaliteetsusele viitava tausta** kohta, kus eksperdid (E1, E3, E4, E5, E6, E7, E8, E9, E11, E13) osutavad kolmandatest riikidest pärinevale tehnoloogiale. Kuna turul müüdavad turvalisema taustaga seadmed on tihti kallimad, kuid valdavalt Hiina päritolu seadmed odavamad ning sarnaste kui mitte kallimate toodetega võrreldes sama heade või isegi paremate tehniliste näitajatega, otsustavad inimesed tihti odavamate seadmete kasuks. Odavamatele Aasia turult pärinevatele seadmetele viidates toovad eksperdid välja järgmised probleemid

1) Seadmete ebakindla tarkvara, mis võib olla eelnevalt testimata. Mure kerkib esile kiiresti arendatud seadmete puhul, millel testperioodile tähelepanu ei pöörata.
2) Võimaluse turva- ja vaikesätteid mitte muuta – seadmete seaded on sellised, mida muuta ei ole võimalik ning mis kõikidel seadmetel on tehasest tulnuna samasugused.
3) Seadmete avatus rünnetele, mis kerkivad esile nõrkade ja testimata süsteemide tõttu.
4) Uuendusi seadmetele ei pakuta või tekitatakse kasutajates vaikimisi rahulolu, kuvades uuenduste informatsiooni seda tegelikkuses mitte võimaldades.
5) Mis andmeid seadmed koguvad ning kuhu nad neid andmeid jagavad? Andmeid võidakse koguda kasutajate teadmata.

Kolmanda kategooriana sai moodustatud **asjade interneti tehnoloogiast tulenevad probleemid**, mille alla moodustus kolm koodi, mis keskenduvad asjade internetiga seotud üldistele probleemidele, probleemidele turvaelementide vaatest ning seadmete ära kasutamisele ja sellega seonduvatele rünnakutele (koodid välja toodud käesoleva töö Lisas 5, vt lk 91).

Kolmanda kategooria esimese koodina sai registreeritud **peamised asjade interneti tehnoloogia probleemid**, milles registreeriti ekspertide nimetatud asjade interneti tehnoloogiaga seonduvad mured. Peamine probleem, mida eksperdid (E1, E3, E6, E8, E9, E10, E11 ja E12) koodi all välja toovad, seonduvad seadmete arvukusega. Öeldakse, et seadmete arvu kasv tõstab potentsiaalselt rünnatavate objektide hulka ning seega suureneb ka üldine haavatavus. Nähakse, et asjade interneti seadmete madal hind Aasia turul võib tõsta seadmete arvu veelgi ja see avaldaks otsest mõju ka halduskoormusele. Asjade interneti seotust küberkuritegevusega on hästi välja toonud Klaid Mägi (E1, 2021):

„Kurjategija jaoks on see mitukümmend miljardit potentsiaalset asja, mida rünnata ja potentsiaalset asja, mille kaudu rünnata." (E1, 2021)

Üks ekspert tuletab meelde, et tehnoloogiline areng on muutnud kõik seadmed viimase 30 aastaga meie ümber nutikaks: *„Ühest perekonna lauaarvutist 1990ndatel on saanud kolm sülearvutit, kaks tahvlit, paar telekat, külmkapp ja ahi, mis on internetti ühendatud ja sellest mahust tulenevalt on ka riskid kasvanud.*" (E10, 2021).

Seadmete kaheldav taust on ka asjade interneti ohtude juures intervjuudes välja toodud, sest odavamate kolmandatest riikidest pärit ning vähem turvatumate asjade interneti seadmete puhul ei

pruugi kasutajad teadlikud olla, millal ja kuidas nende seadmed on internetiga ühendatud. Üldises plaanis võib see tähendada seda, et asjade interneti tehnoloogia alla liigituvad kaamerad, mikrofonid ning muud seadmed võivad koguda kasutajate kohta materjali, mida saab hiljem nende vastu ära kasutada. Pealtnäha kattuvad ekspertide nimetatud probleemid koodi all tavaliste infotehnoloogia seadmetega seotud probleemidega, kuid puuduste tõsidust annab juurde asjade interneti seadmete globaalne mõõde. Seadmed on seotud nimelt pilvetehnoloogiaga, mille suuremaid pakkujaid Eestis ei ole ning ekspertide hinnangul võib see tekitada olukorra, kus teistest riikidest pärit tehnoloogia ja inimeste vahele tulevad veel kolmandad osapooled, kes pakuvad teenuseid, mis seotud osapoolte arvu tõstab ning omakorda tõuseb selle tulemusena ka riskide mastaap. Tõnu Tammer (E5, 2021) ütleb internetiseadmete kogutava info kohta nii:

„Need asjade interneti asjad, kuna nad oma toimimiseks koguvad tükk maad rohkem infot /.../, siis see info annab palju parema pildi, kui mõni politsei profileerija suudaks inimest väliste tunnuste najal kirjeldada. See on ohtlik!” (E5, 2021)

Täpsemad probleemid tuvastatakse asjade interneti teoreetilises käsitluses kajastatud turvaelementidele tuginedes. Teisena registreeriti kood, **asjade interneti turvaelementidega seotud probleemid**, mille juures tõid eksperdid (E3, E4, E6, E7, E9, E10, E11 ja E12) välja peamised probleemid infoturbe põhikomponentide ehk konfidentsiaalsuse, terviklikkuse ja käideldavuse kohta, lisasid sinna viite privaatsusele (E1, E2, E3, E4, E7, E8, E9, E11 ja E13) ning väiksemal määral ka identifitseerimise ja audentimise (E5 ja E8).

Konfidentsiaalsuse puhul tuuakse esile, et asjade interneti seadmetega, mis ei ole sertifitseeritud, mis ei vasta standarditele või mis pole ehitatud neid silmas pidades, on risk, et kasutajate andmed võivad lekkida. Kuna asjade interneti hulka kuuluvad ka seadmed, mis üldjoontes kasutaja kohta andmeid suures koguses ei oma, peitub ekspertide hinnangul probleem ühendatavuses. Vähemal määral andmeid koguvad ja omavad seadmed võivad olla ühendatud võrku selliste seadmetega, mis omavad kasutajate kohta privaatseid andmeid. Seega võivad pealtnäha vähem tähtsad seadmed olla oht ning juurdepääsuvõimalus mitte üksnes üksikutele seadmetele ega ka kasutajate andmetele, vaid süsteemile tervikuna. Andmeid nähakse toetumas mitte üksnes seadmete sisemälule või kodustele võrgulahendustele, vaid välja tuuakse ka seos teenusepakkujate serveritega, mis võivad rünnete korral olla seadmete talletatud kasutajaandmetele allikaks. Üks ekspertidest selgitab, et niinimetatud „rumal nutiseade” võib olla ohu looja:

„Pesumasinast või külmkapist ei ole andmete osas midagi võtta, kuid see võimaldab siiski minna sisse kuskilt mujalt ja ohustada inimese privaatseid andmeid /.../ sotsiaalmeedia kontodel või kusagil mujal, sest tihti kasutatakse täpselt samu autentimisviise, paroole, kasutajanimesid, mis on ka inimlik." (E11, 2021)

Terviklikkuse kui turvaelemendi kohta tuuakse esile selle probleemi sisukus ning riskantsus. Terviklikkust nähakse andmekooslustega manipuleerivana. See on teema, mis on ekspertide arvates seotud eelkõige seadmetega, mis inimeste igapäevatoiminguid jälgivad ning tegevuste kohta andmeid talletavad. Terviklikkuse juures näevad eksperdid probleemi siis, kui kogutavatele andmetele ligi saades hakkavad pahatahtlikud osapooled neid ära kasutama ning ümber koordineerima. Terviklikkust tuleks mõne eksperdi arvates vaadata läbi kasutajate silmade – eeldatakse, et mingisugune seade töötab ühte kindlat moodi, kuid ei arvestata, et võib eksisteerida võimalusi, kus keegi suudab seadmete tegevust häirida, parameetreid andmete najal muuta ning sellega kahju tekitada. Ekspert Uku Särekanno (E11, 2021) ütleb:

„Sellest aru saamiseks ei pea üldse kaugele vaatama, sest meil on väga suur hulk seadmeid, mis jälgivad inimeste igapäevast terviseseisundit, palju nad samme teevad ja palju nende süda lööb /.../ kõik see on ühendatud telefoni või käekella health monitoring'uga ning kui nende andmetega hakatakse manipuleerima kellegi poolt, mängides näiteks ümber andmete terviklikkust, mängides ümber näiteks sinu südame rütmiga seotud häired ja nii, siis sellel võivad olla valusad tagajärjed." (E11, 2021)

Käideldavuse kohta toovad eksperdid esile teenuste rivist välja viimise võimalikkuse. Arvestades seda, et võrgus olevate seadmete maht kasvab pidevalt, suureneb ka võimalus rohkemaid seadmeid üle võtta, kasutada neid bottidena, teostada nende suunal teenusetõkestusrünnakuid ning mõjutada seeläbi andmete käideldavust. Kui kolmandad osapooled suudavad seadme välja lülitada või häirida rünnakutega seadmete tööd, ei saaks asjade interneti seadmete kasutajad enda informatsioonile ligi ning nende kättesaadavus oleks komplitseeritud. Ekspert Markko Künnapu (E9, 2021) ütleb käideldavuse kohta nii:

„Käideldavus on samamoodi probleemiks, et kui keegi kuskilt väljastpoolt suudab selle masina välja lülitada või panna ta kuidagi teistmoodi tööle või muul viisil seda häirida, siis ka see on oluline, sest andmete saadavus on ju kannatamas." (E9, 2021)

Eksperdid näevad, et eelpool nimetatud kolm turvaelementi (konfidentsiaalsus, terviklikkus ja käideldavus) on infoturbe alustalad ning need sobituvad ka asjade interneti seadmete konteksti. Oluline on välja tuua, et turvaelemente nähakse läbivate ja fundamentaalsetena ning nende alla koonduvad asjade interneti spetsiifilisemad mured, mille juures on välja toodud näiteks seadmete automaathäälestus, hajus ummistusrünne, hajustatud teenusetõkestusrünne, seadmete turvanõuete määramine, autentimine, regulaarne ajakohastamine ja võrkpääsu piiramine. Eksperdid rõhutavad intervjuudes, et kolm turvaelementi on kõik omavahel tihedalt seotud:

„Konfidentsiaalsus, käideldavus ja terviklikkus – need on nagu kolme jalaga taburet, et kui sa ühte väga lühikeseks või teist väga pikaks ajad, siis ta kukub ümber ning sama on IoT-ga, et ei saa ühtegi välja neist kolmest jätta, sest nad on võrdselt olulised." (E7, 2021)

„Kolm tugisammast on reaalsed, kuna asjade internetis kehtivad samad reeglid nagu teistes arvutivõrkudes. Reaalsed on need ainuüksi seetõttu, et väga lihtsate seadmete puhul me kipume unustama, et need on samamoodi arvutid nagu kõik teised ning sellest tulenevalt ei pruugi nende turvalisuse peale üldse mõelda, kuigi peaksime." (E10, 2021)

„Konfidentsiaalsus, käideldavus ja terviklikkus, et /.../ võttes CERT-EE statistika näiteks intsidentide kohta, siis nemad löövadki intsidente nagu selle kolme jaotuse põhjal laiali ja kokku." (E11, 2021)

Kolmest tugisambast rääkides võib ohtudele keskendudes tavakasutaja tähelepanu hajuda ning seetõttu tuuakse välja privaatsus kui turvaelement. Suur hulk seadmetest ei vasta turvastandarditele ning asjade interneti seadmete puhul ei peeta neid kõige olulisemateks, sest tähtsam on toote innovatsiooni käigus võimalikult kiire turule jõudmine. Sellisel juhul ei pöörata tähelepanu andmevahetuse krüpteeritusele, infovahetuse haldamisele, andmete ja sätete haldamisele, serverivahelisele vahetusele ning süsteemi turvamisele. Keskselt tuuakse välja, et tegelikult ei teata, mida seadmed teevad, kuidas nad andmeid koguvad ning kuidas on kasutajate andmete turvalisus aktsepteeritaval tasemel kaitstud. Öeldakse, et seadmeid kasutatakse tihti ilma neid kasutajatega otseselt seostamata, isikustamata, kuid tänapäeval on võimalik koguda ka näiliselt unikaalse konto kohta informatsiooni, mida saab kokku koondades luua profiiliks, mis annab siiski kasutaja kohta informatsiooni. Privaatsus on tihedalt seotud terviklikkusega, kuid spetsialistide hinnangul piisavalt oluline, et see eraldi kolme peamise turvaelemendi kõrval esile tuua. Eksperdid ütlevad, et inimestele ei ole seadmeid kasutades arusaama andmekasutusest ning ollakse eksiarvamusel, et andmete kogumine ja vahetus on privaatne:

„Privaatsus, hästi lihtne näide – ostad omale kaamerad, paned need igale poole ümber maja ning eeldad, et sa kaitsed sellega oma vara, oma privaatsust. Aga kuna pool maailma saab su kaamerale ligi, siis tegelikult avalikustab see kõik, mis sul kodus on ja selliseid kaameraid on meil Eestiski tuhandeid." (E1, 2021)

„Kasutajad ei tea, millist teavet see seade välja kuvab ja tihti ekslikult arvatakse, et kui seadmest ei lähe nii-öelda isiku või nime tasemel teavet välja, siis ei olegi probleemi, kuigi seal võivad taga olla kogutavad „küpsised", mille taga on unikaalne kasutaja ja selle analüüsimisel võib siiski üht-teist teada saada. Ka privaatsed protsessid selles keskkonnas ei pruugi olla nii privaatsed, kui me arvame." (E13, 2021)

Kolmanda koodina registreeriti **asjade interneti seadmete ärakasutamine ja sellega seonduvad ründed**, mille juures tõid eksperdid esile täpsemad näited asjade internetiga seonduvatest seadmete ärakasutamistest, rünnete näidetest ning seadmetega üles kerkivatest küsimustest. Eksperdid ütlevad, et asjade interneti seadmete kaudu on võimalik saada ligipääs teistele võrgus olevatele seadmetele ning samuti nähakse, et sarnased seadmed langevad ka sama tüüpi rünnakute ohvriks. Tihti ei peeta seadmete võrku ühendamisel turvalisust kõige prioriteetsemaks, sest seadmeid nähakse pisemate asjadena, mis ei pruugi kasutajale suurt mõju avaldada, kuigi tegelikult võivad need olla teeks süsteemi ja selles olevatesse seadmetesse. Üks ekspertidest (E1, 2021) ütleb nii:

„Ma ei muretse selle pärast, et keegi häkiks mu robottolmuimejasse sisse ja sellega teeb mu kodus olevale kassile midagi, et see ei ole kuigivõrd realistlik, kuid kuna mu tolmuimeja on ühendatud mu telefoniga ning selle kaudu on võimalik saada ligi mu telefonile, siis see on reaalne asi /.../ need värkvõrgu seadmed on selline hüppelaud kusagile väärtuslikumasse kohta." (E1, 2021)

Eksperdid (E1, E2, E3, E4, E5, E6, E9, E10, E11, E13) toovad asjade interneti seadmete võimalike ärakasutamise viisidena välja andmete kogumisega seonduvad probleemid, kus näiteks mikrofonide ja kaamerate kaudu koguvad pahatahtlikud inimesed tundlikku informatsiooni. Levinud rünnakuna nimetatakse teenusetõkestusrünnakud ehk DDoS-rünnakud, mida eksperdid seostavad rünnetega kolmandate osapoolte vastu. Teisisõnu kasutatakse asjade interneti seadet varjuseadmena suuremate süsteemide rivist välja löömiseks. Sellisel puhul võivad lihtsakoelisena tunduvad võrku ühilduvad kodumasinad asetuda *botnet*'i konteksti ning selle kaudu rünnatakse kolmandaid osapooli. Eksperdid juhivad tähelepanu, et sisuliselt on võimalik seadmetesse häkkimisel seadmete ülekoormusest tingitud osade kuumenemine selliselt, et seade lõpuks pahatahtlike osapoolte soovi järgi süttiks ning sellisel juhul võivad olla kahjud suuremad, kui seni arvatud. Ründed mitte üksnes andmetele, vaid

varale laiemalt võivad ekspertide hinnangul saada värkvõrgu seadmete puhul reaalsuseks, alustades andmeleketest ja DDoS-rünnetest ja lõpetades küberseadmete abil teostatavate terrorirünnakutega. Räägitakse globaalsetest rünnakutest ehk korraga erinevates asukohtades olevate hoonete ja asutuste ründamisest, tekitades sedasi ka rahvusvahelist kahju. Ohu tõsidustest rääkides toovad eksperdid välja:

„Potentsiaalselt võib isegi terrorirünnaku nende seadmete abil ellu viia, et kui keegi suudab seadmetesse sisse häkkida ja massides need enda kasuks tööle panna nii, et kõik seadmed lähevad lolliks ja hakkavad võrku häirima, kõik asjad kukuvad kokku." (E4, 2021)

„Lihtne ja tavaline viis on sooritada nende seadmete vastu DDoS-rünne, kus koduühendust kasutatakse potentsiaalsete haiglate ründamiseks /.../ võidakse rünnata lastehaiglat Eestis ja New Yorkis ja Sidneys. Globaalne värk." (E5, 2021)

Esile tuuakse (E4, E7, E9 ja E13), et seadmete kasutajad ei küsi enne seadmete soetamist, mida asjade interneti seadmed teevad, kuidas nad andmeid koguvad ning millised on andmete kogumise sihtkohad. Teisisõnu ei tea kasutajad, kus on asjade interneti seadmete kasutamise korral „teine ots", kes neid andmeid täpselt samamoodi näeb ning nendega opereerib. Lisaks ei keskenduta piisavalt õiguspärasusele. Selle tulemusena ei tea kasutaja tihti, kellega seadmete kogutavad andmed jagamisele kuuluvad ning mis tingimustel on need kolmandatele osapooltele kättesaadavad. Inimesed ei küsi endalt seadmete kohta piisavalt küsimusi, mis teeb aga seadmete kasutamise probleemseks just hilisemas kasutusfaasis. Eksperdid esitavad retoorilisi küsimusi, mida kasutaja endalt seadet soetades küsima peaks:

„Kus andmekeskused ja serverid asuvad /.../ järjest rohkem tekib küsimusi, et kuhu need andmed lähevad. Kellel nendele juurdepääs on ja kas neid andmeid võidakse kuritarvitada?" (E9, 2021)

„Kas see teenusepakkuja ise on jätkusuutlik? Kui kuu aja pärast teda ei ole enam, mis siis andmetega saab? Kas andmeid müüakse kellelegi teisele? Kuidas kolmandatel osapooltel andmetele ligipääs on? Kõik need on olulised küsimused kasutaja jaoks." (E7, 2021)

Neljanda kategooria, **IKT ja asjade interneti tehnoloogiast tulenevad probleemid avalikule sektorile** all sai registreeritud kolm koodi, mis keskenduvad kompetentsi, koostöö ja ressursi probleemidele (koodid välja toodud käesoleva töö Lisas 5, vt lk 91).

Vastava kategooria esimese koodina registreeriti **kompetentsi probleemid**, mille juures tõid eksperdid (E3, E4, E5, E6, E7, E8, E9, E12 ja E13) välja avaliku sektori IKT taustaga tööjõu problemaatilised kohad. Tööturul on täna avaliku sektori asutustel raske konkureerida erasektoris tegutsevate ettevõtetega, sest tihti pakutakse just seal IKT valdkonna spetsialistidele märgatavalt kõrgemat palgataset kui avalikus sektoris. Avalikus sektoris näevad intervjueeritavad ekspertide leidmise nimel palju vaeva ning tuuakse välja, et nii Siseministeeriumis, Politsei- ja Piirivalveametis kui ka Siseministeeriumi infotehnoloogia- ja arenduskeskuses võib olla kompetents mingisuguses ulatuses hetkel kaetud, kuid kuna tehnoloogia on tulevikuga seotud, võivad probleemid eri tehnoloogiate kasutuselevõtuga laieneda. Lisaks toovad eksperdid välja, et spetsialistide teadmised vajavad pidevalt täiendamist ning kuna tegemist on ka valdkonnaga, mis ise pidevalt areneb, peab keskenduma olemasolevate töötajate teadmiste edendamisele. Teisisõnu tuleb keskenduda uute töötajate leidmisele, nende hoidmisele ning arendamisele. Eksperdid rõhutavad kübervaldkonna teemade ja küberoskuste ajakriitilisemaks muutmist:

„Probleem on selles, et küberteema olulisus ajas kasvab ja meil kui ühiskonnal ei ole lihtsalt võtta neid inimesi sellises mahus, et see probleem ära katta." (E12, 2021)

„Inglise keeles on hea terminoloogia, et alati räägitakse "capacity-st", aga tegelikult seda aetakse segi "capability-ga" /.../ Kui meil on see capability horisontaalselt nagu olemas, siis see capacity, et minna igas kohas asjaga süvitsi, tegeleda mahuga, see on see nüanss, mida me kasvatame ja kuhu on abi juurde tarvis." (E5, 2021)

Kompetentsi juures võib esile kerkida ka **koostöö tegemise** küsimus, mis on kategooria all määratletud teise koodina. Eksperdid (E1, E5, E6, E7, E8 ja E9) ütlevad, et koostöö operatiivtasandil võiks olla eri asutuste raames Eestis kübervaldkonda puudutavates küsimustes parem. Intsidentide ja kuritegude lahendamise ning lisaks ka poliitika kujundamise juures on välja toodud asutuste tegevuste erinevus, kindlatele reeglitele toetumine ning lisaks madal teadlikkus teiste asutuste võimetest ja võimalustest. Rahvusvaheline koostöö on rahvusvaheliselt keeruka olukorra tõttu komplitseeritud ning kõik ei sõltu mitte üksnes Eestist, vaid ka teiste osapoolte võimekusest ja soovist koostööd teha. Koostöö võimalikkust nähakse siiski võimalikuna ning peamise suunana nähakse küberhügieeni taseme tõstmist, mis vajab toimiva süsteemi loomiseks ühisosa leidmist. Rahvusvahelise koostöö võimekus võiks ekspertide hinnangul olla Eestis parem, sest vaadates värkvõrgu seadmeteid ja nende globaalset haaret, võib eri asutustel olla vajalik teha koostööd teiste riikide eri asutustega. Näiteks tuuakse menetlustoimingute läbiviijatena politseiasutused, kes kriminaalmenetluses võivad

rahvusvahelist koostööd teha. Koostöö toimib ka täna, aga seadmete mastaapi arvestades tuleb ka sellele rohkem keskenduda. Tsitaadid illustreerivad ekspertide hinnangut praegusele seisule:

„Probleeme on näiteks kriminaalpoliitika ehk siis karistusõiguse ja kriminaalmenetluse osas, sest kui intsidendid on enamasti kõik piiriülesed, siis ega üksi neid asju lahendada ei ole võimalik /.../ ründed suvalises riigis meie asjade suunas, see on juba rahvusvahelise koostöö küsimus." (E9, 2021)

„Kui panna asjad näiteks menetluse võtmesse, kus kõik on hästi jäik, uurija peab paljud asjad läbi rääkima prokuratuuriga ja see ei toeta eriti sellist kiiret lähenemist asjale /.../ paljudel juhtudel oleks otstarbekas see, et me hoiaks ära edasiselt tekkivat jama, kuid riigina me ei kasuta ära neid võimalusi tervikuna /.../ ühel omad mängureeglid, teisel teised mängureeglid ja koostöö ei suju." (E5, 2021)

Eksperdid leiavad, et kompetents on eri asutustel mingil määral küll olemas, kuid prioriteetseks tuleb seada nende valdkondade rahastamise küsimus. Selle kategooria all ära registreeritud kolmas kood, **ressursiprobleemid**, mille kohta tõid eksperdid (E1, E2, E3, E4, E6, E7, E8, E9, E11 ja E12) välja meie asutuste peamise probleemi, mis seostub suuresti kategooria esimese koodi juures osutatud kompetentsi küsimusega. Kompetents on otseses seoses rahaga – kompetentsed inimesed lahkuvad avalikust sektorist erasektoris olevate kõrgemate palkade tõttu.

Leitakse, et probleem on ka avaliku sektori asutustele, ministeeriumitele, politseile ja RIA-le kübervaldkonna analüüsimiseks vajaliku riistvara ning tarkvara pakkumises, mis on tehnoloogia kiiret arengut arvestades kallis. Kallis on nii seadmete uuendamine, koolitamine kui ka süsteemide hooldamine ja haldamine, mis seadmete arvu juures ning eeldusel, et eri seadmete ja tehnoloogia kasutamise arv ka avaliku sektori asutustes kasvab, nõuab rohkem ressurssi. Eksperdid toovad siin välja järgmist:

„Selleks, et näiteks prefektuurides ja C3-l oleks vajalik tarkvara-riistvara ja ruumispetsiifika digitaalkuritegude menetlemiseks olemas, on vaja raha. Selleks, et litsentse, tarkvara ja kõike muud uuenada, on vaja raha. See ei ole odav lõbu. Kogusumma, mis riigis oleks vaja välja käia, on ikkagi miljonitesse ulatuv." (E8, 2021)

„Ma arvan, et probleem on meil selles, et turu pealt küberturbega tegelevate inimeste leidmine, põhimõtteliselt on hästi hapu seis nendega või on nad kinni makstud selles osas, et me riigina ei jaksa maksta seda palgataset, mida startup jaksab inglirahade eest maksta." (E12, 2021)

Viienda kategooriana sai registreeritud **soovitused asjade interneti tehnoloogia valguses** ning kategooria alla moodustus kaks koodi – asjade interneti seadmeid puudutavatest aspektidest tulenevad **soovitused ametiasutustele** ning **kasutajaskonnale (**koodid välja toodud käesoleva töö Lisas 5, vt lk 91).

Spetsialistid soovitavad avalikul sektoril keskenduda nii ametkondadel kui ka avalikul sektoril turbeteenuste automatiseerimisele, mis võiks leevendada IKT-spetsialistide puudust. Veel soovitatakse keskenduda koolitustele, et tagada olemasoleva tööjõu head teadmised digitaalselt kiiresti muutuvas keskkonnas. Paika tuleks panna IKT-põhimõtete ja toimimise üldformaat. Kindlaks peab määrama suhtluskanalid ning näiteks asjade interneti puhul tasuks määratleda, millega on tegemist, et kõik ametkonnad sellest ühtmoodi aru saaksid ning tulevikus oleks töö efektiivsem. Ennetusele peab avalik sektor rohkem tähelepanu pöörama ning keskenduma selle baashügieenile – selgitada elanikkonnale ohte ning seda, kuidas end nende keskel seadmete, sealjuures ka asjade interneti seadmete kasutamisel kaitsta. Üks ekspertidest väljendab, et digiteadlikkusega ühiskonnas oleks vaja alustada uuesti põhitõdede selgitamisega ning ütleb nii:

„Selles mõttes peaksime tegema täieliku restardi või alustama sellist Tiigrihüpe 2.0-i, et mitte üksteist õpetama, et see on arvuti ja vajuta siia ja ilmuvad tähed, vaid pigem näitama, et selle taga on mingisugused riskid. Toome tähelepanelikkuse küberpoolele või näiteks siis asjade interneti poolele ja õpetame lisaks sellele plusspoolele ka asjade suhtes kriitilised olema ja küsima neid küsimusi, et miks nii." (E5, 2021)

Eksperdid peavad oluliseks, et seadmetele kehtestataks kindlad standardid ehk turule tulevate seadmete puhul peaksid ekspertide hinnangul seadmed vastama ette kirjutatud kriteeriumitele ning selles osas saab ka riik omapoolse panuse anda. Kindlate standardite seadmine aitaks turule tuua kindlatel alustel töötavad seadmed, mis turvaelementide abil kujutaksid seadmete kasutajatele, kes omakorda reegleid peaksid järgima, vähem riske ning nendest põhjustatud probleeme. Poliitilisel tasandil on välja vaja töötada reeglistik ning erinevate tehnoloogiate, sealhulgas asjade interneti kohta koostada riskianalüüs, mis aitaks reeglistiku loomisele kaasa. Kui asjade internetile mitte eraldi teemana keskenduda, soovitavad spetsialistid teema defineerida üldiste IKT teemade all eraldi peatükina. Nähakse, et ISKE all võiks olla asjade internet välja toodud eraldi sektsioonina, mis aitaks tehnoloogia defineerimisele ning raamitlemisele kaasa ka riigi ja kohalike omavalitsuste andmekogude jaoks. Riskianalüüside koostamise ning teema kinnitamise järel saaks riik hakata mõtlema asjade interneti seadmete kasutamisele ka erinevates asutustes, kuid see tähendaks vajaliku kasutuspoliitika välja töötamist ning põhimõtete paika seadmist.

Leitakse, et riik võiks kehtestada üldpõhimõtted esmajoones enda asutustele ning seejärel liikuda tavainimeste igapäevaelu puudutavaid seadmeid reguleerima, andes sellega suuna, et ka riigiasutused ise pööravad piisavalt tähelepanu turvalisusele. Kui aga peaksid ilmnema asjade interneti seadmetega seotud probleemid, siis nähakse, et kuritarvitamise ning selle käsitlemise puhul tuleb reguleerida ka seaduseid. Võimaliku muudatuse saab teha kriminaalseaduses, kus tulevikus tuleb osa ekspertide hinnangul määratleda ka tulevikutehnoloogiate mastaap, sealhulgas asjade interneti oma. Asjade interneti seadmete määratlemine reeglistikes on aga keeruline. Seda arvestades toob üks ekspertidest iseloomustavalt välja nii:

„Igasugused kuritarvitamised ja nende käsitlemine peab olema eelnevalt reguleeritud ning juba enne seda, kui mingisugune jama juhtub. Hiljem tagantjärgi ei saa kedagi vastutusele võtta /.../ aga samas jällegi ülereguleerimine ei ole samamoodi mõistlik tegevus ning seal on see koht, kus riigil tuleb leida kompromiss." (E7, 2021)

Intsidentide ja küberkuritegevuse kohta leitakse, et arendama peaks valmisolekut ööpäev ringi problemaatilistele olukordadele reageerida. Kuivõrd täna on reageering RIA näitel juba olemas, öeldakse, et sarnast süsteemi tuleks rakendada laiemalt, sest tehnoloogiavõimaluste avardudes muutuvad ka probleemid aktuaalsemaks ning sagedasemaks. Valmisolek eeldab ka rahvusvahelise koostöö tegemise võimekust, kus nähakse ministeeriumite tasandilt, et koostööd tuleb teha suurriikidega, kes ise soovivad ja saavad koostööd teha ning on võimelised tulemusliku eesmärgi nimel koostööd tegema. Turvaliste asjade turule toomises nähakse võimalust teiste riikidega koostööd teha, kuid välja tuuakse ka see, et Eesti Vabariik on väike ning resultatiivne rahvusvaheline koostöö saab peaasjalikult võimalik olla Euroopa Liidu või selle liikmesriikide tasandil, mis võimaldab probleemide korral anda ühise lähenemise abil asjadele tõsidust juurde. Koostöö ei ole aga võimalik ilma riigisiseste ametiasutuste läbikäimiseta ning seetõttu leitakse, et ka riigi sees tuleks mõistete mõtestamisel leppida kokku suund, kus igal ametkonnal on roll tervikpildi ja eesmärgi täitmisel. Ministeeriumite jaoks ei ole küsimus ainult omavahelise koostöö tegemises, vaid oluline oleks kaasata ka nende haldusalasse kuuluvate osapoolte visioonid, et tervikpildi loomisele veelgi enam kaasa aidata. Ekspert (E6, 2021) ütleb, et haldusalaülene ühine vaade on kaardistamisel oluline:

„Kaardistamised oleks nagu tore asi, millest alustada, aga tegelikult tuleks peaasjalikult kokku leppida omavahel see suund, kuhu me täna läheme, ministeeriumi vaatest kindlasti peab kõikide ametitega maha istuma ja selle paika panema, et koostööd ka mujal suurendada ..." (E6, 2021)

Teise koodina tõid eksperdid välja **soovitused asjade interneti seadmete kasutajatele** ning selles said registreeritud järgmised nõuanded:

*Tasub mõelda, kas asjade interneti seadet on inimesel üldse vaja***.** See ekspertide soovitus kehtib nendele inimestele, kes pole veel toodet soetada jõudnud. Oluline on enda jaoks vastata järgmistele küsimustele: Mida see seade võrku ühendatuna teeb? Milliseid andmeid see seade kogub? Millistel tingimustel jagab see seade kasutaja kohta käivaid andmeid kolmandate osapooltega? Kas seadme kasutaja on valmis, et keegi võib neid andmeid näha?

*Uurida enne asjade interneti seadme ostmist tootja ja toote kohta informatsiooni***.** See soovitus on esile toodud selleks, et seadme tulevased kasutajad hindaksid seadme turvalisust ning tootja tausta. Seadme kasutusaeg on eeldatavasti pikk ning oluline on teada, kas tootja on piisavalt usaldusväärne ning võimeline pakkuma seadmele uuendusi ka tulevikus. Seadme puhul on oluline teada, milliste näitajatega ta kasutusse tuleb ehk millised võimalused on seda ise seadistada. Soovituslikult võiksid kasutajad vaadata, kas sellega käib kaasas ka turvasertifikaat. Läbi tasub lugeda tootja poolt seadmele väljastatud manuaalid ning privaatsussätted, mis annavad parema pildi selle kohta, kuidas ja mis alustel seade kasutaja valduses potentsiaalselt töötada võiks. Internetist on võimalik leida tagasisidet turvariskide, näidete, toote ja tootja kohta.

Seadme soetamise järel mõelda, kuidas ning mis tingimustel seade võrku ühendatakse. Seadme ostmise järel tasub ekspertide hinnangul vaadata, kuhu seade ühendatakse ning kuidas ta võrgus seadistatakse. Võimaluse korral tasub mõelda asjade interneti seadmetele eraldi võrgu loomisele.

*Seadme soetamise järel tuleb muuta tehase määratud kasutajanimi ja vaikeparool.*Oluline on meeles pidada, et mitmes seadmes ei tasu kasutada samu kasutajanimesid ja paroole. Järgima peab soovitusi, mis on antud paroolidele ja autentimisele laiemalt. Tehase määratud kasutajanime ja vaikeparooli muutmine aitab muuta kasutatava seadme turvalisemaks.

Teha asjade interneti seadmetele regulaarselt uuendusi. Seadmetele tuleb regulaarselt teha uuendusi. Sõltuvalt seadme iseloomust tuleb kriitilisema tähtsusega seadmete tarkvarauuenduste pakkumistele reageerida kohese, vähem tähtsate toodete korral tuleb uuendusi kontrollida regulaarselt mingisuguse kindla ajaperioodi jooksul (näiteks kord kuus). Oluline on, et seade ei oleks võrgus „ühendan ja unustan" põhimõttel ehk algselt ühendatud seade peaks saama teatud aja jooksul seadme omaniku tähelepanu, et võimalikud turvariskid välistada.

Kohandada seadme konfiguratsioonisätteid. Sätete alt on seadmetel tihti võimalik valida, millistes olukordades võib seade töötada ning kuidas ja millal informatsiooni koguda. Konfiguratsioonisätetega tutvumine annab kasutajale võimaluse olla kursis kasutuses oleva seadme spetsiifikaga ning soovi korral panna seade tööle enda jaoks turvaliselt.

Arvestama peab seadme omadusi ning selle kasutamise konteksti. Asjade interneti seadmetega on seotud andmete jagamine ning oluline on lahti mõtestada, millised seadmete kogutavad andmed millisesse konteksti sobituvad. Teisisõnu on igal andmel jagamiseks oma aeg ja koht.

Kui seade on seotud andmetega, tasub andmetest teha teatud aja tagant tagavarakoopiad. Andmete varundamine kõvakettale on üks viisidest, kuidas oma seadmega seonduvaid andmekogusid hävimise või kolmandate osapoolte eest kaitsta. Andmete varundamine võib käia nii pilvetehnoloogia kui ka andmekandjate kaudu.

Juhul, kui seadmele on võimalik paigaldada viirusetõrje tarkvara, tuleks seda võimalusel kasutada. Viirusetõrje tarkvara hoiatab ja kaitseb seadet pahatahtlike osapoolte eest.

Üks ekspert (E7, 2021) toob välja, et tavainimesed võiksid lähtuda sarnasest õpetusest nagu ka küberturvalisuse eksperdid:

„Turvainimeste küberturvalisuse nii-öelda kolm käsku: ära näpi, ära kliki, ära topi!" (E7, 2021)

2.4. Dokumendianalüüsi ja ekspertintervjuude tulemuste analüüs

Esimese uurimisküsimuse eesmärk oli välja selgitada, kuidas defineerivad kohalikud ja rahvusvahelised digitaliseerumise ja julgeolekuga seotud dokumendid ja Eesti infotehnoloogia-, küberturbe- ja julgeolekueksperdid mõistet *Internet of Things* (ingl) ning kuidas suhestub asjade internet IKT-tehnoloogiatega.

Eestikeelsetes dokumentides nimetati *Internet of Things* (ingl) vastena mõistet „asjade internet", mida on seostatud ühendatavusega. Majandus- ja Kommunikatsiooniministeeriumi eestvedamisel on asjade internet riiklikult defineeritud võrku ühendatud seadmeteks, mis on iseseisvalt suutelised omavahel suhtlema ning anduritega ümbritsevast keskkonnast vajalikku informatsiooni koguma. Ingliskeelsetes dokumentides sai nagu eestikeelseteski dokumentides registreeritud mõiste ,,ühendatavus'' (ingl *connectivity*), mida on seletatud kui asjade võimekust internetti ühendatuna omavahel suhelda. Nende kõrval on asjade interneti tehnoloogiat kirjeldatud kui innovaatilist

tehnoloogilist lahendust, mis inimeste elu lihtsamaks teeb, ja teisest küljest kui problemaatilist lahendust, mis seostub rünnakutega, mida asjade interneti seadmete abil ellu saab viia. See kinnitab esimeses peatükis osutatud asjade interneti definitsiooni nii positiivsest kui negatiivsest küljest (käesolev töö, lk 17-19).

Eksperdid eelistavad kasutada mõiste *Internet of Things* definitsioonina kas ingliskeelset algväljendit, selle mõistega seonduvat tähekombinatsioonidest moodustunud lühendit IoT või mõiste eestikeelset vastet ,,asjade internet''. Eksperdid kinnitasid, et ingliskeelne mõiste on universaalne ning seda kasutatakse aktiivselt rahvusvahelistes dokumentides. Suusõnaliselt saavat ingliskeelsest mõistest üldjoontes aru kõik, kes selle tehnoloogiaga on kokku puutunud. Eestikeelne versioon „asjade internet" on ekspertide jaoks seotud mõiste definitsiooniga, mis lihtsustatult käsitleb asju, mis on ühendatud võrku. Eksperdid leiavad, et tegemist on seadmetega, mis on varustatud andurite või sensoritega ning mis võrku ühendatuna on võimelised ümbritsevast keskkonnast koguma informatsiooni ning seda sarnastel alustel võrku ühendatud teiste seadmetega jagama. Asjade interneti teooria (käesolev töö, lk 17–19) toetab ekspertide pakutud asjade interneti definitsiooni, kuid ei anna edasi intervjuudes välja toodud ideed, mille järgi on asjade internetti võimalik käsitleda ühe osana suuremast ja eraldiseisvast teemast IKT valdkonna all. Ekspertintervjuude tulemusena leiti, et avaliku sektori jaoks on oluline asjade internet defineerida laiema valdkonna ühe osana, sest see võib tagada probleemide parema ning kiirema lahendamise.

Mõistet aitasid dokumentides selgitada nimetatud kasutusvaldkonnad, millega toodi esile energeetika, telekommunikatsioon, tööstus, arhitektuur, olme, transport, turvalahendused, tervishoid ja rahandus. Dokumendid näitavad, et tehnoloogiat on võimalik kasutada kõikides eluvaldkondades. **Spetsiifiliste näidetena** toodi dokumentides välja nutikad koduabilised, autod, nutitelerid, külmikud, pesumasinad, alarmsüsteemid, kaamerad, kõlarid, suitsuandurid ja ukselukusüsteemid – asjad, mida leidub kõikides kodudes üle terve maailma. Üks käsitluse all olevatest dokumentidest keskendus pikemalt mobiiltelefonide liigitamisele asjade interneti alla ning tõi välja, et seadmete arhitektuuri keerukuse tõttu ei ole võimalik seadet asjade interneti seadmete alla liigitada. Eksperdid tõid spetsiifiliste asjade interneti seadmete näidetena välja mängukonsooli, nutikaalu, robottolmuimeja, nutika rösteri ja kohvimasina, nutika saunakerise, ukselingid, targa kaamera, nutiteleri, nutitelefoni, sülearvutid, nutika külmkapi ja ahju. Kolm eksperti kolmeteistkümnest ütlesid, et seadmete liigitamine sõltub sellest, kuidas mõistet defineerida ning seetõttu on nutitelefonide ja sülearvutite kategooriasse liigitamine raske. Dokumendianalüüs kinnitab ekspertintervjuudes püstitunud küsimust nii mobiiltelefonide tehnoloogia alla liigitamise kui ka mitteliigitamise kohta.

Mõiste kasutamise ning selle esinevuse ja perspektiivikuse kohta, mis annab informatsiooni ka mõistest endast, arvavad eksperdid, et Eesti ametiasutuste sisestes (peamiselt Siseministeeriumi ning Majandus- ja Kommunikatsiooniministeeriumi haldusalas) dokumentides on asjade internet leidnud määratlemist kui üks innovaatilistest digilahendustest, mis pakub võimalusi erinevates eluvaldkondades ning on seotud suure seadmete arvuga. Eraldi dokumente, mis keskenduksid asjade internetile, ei ole Eestis loodud, kuid asutuste sees on kesksel kohal seadmete sertifitseerimise ja standardiseerimise küsimused, mille üle arutelud praegu käivad. Kaks eksperti toovad olulise näitena välja Euroopa küberagentuuri ENISA loodud dokumendi "Good Practices for Securing IoT", mis on ka magistritöö dokumendianalüüsi üks allikas (välja toodud käesoleva töö Lisas 3, vt lk 89). Eksperdid tõid välja, et asjade interneti seadmete reeglistikke ja määrusi võib käsitleda vajalikena, kuid IKT-seadmete määratlus eksisteerib loodud kujul ning selle najal on võimalik käsitleda ka antud tehnoloogiat ja selle alla liigituvaid seadmeid. Eksperdid näevad seega, et asjade interneti tehnoloogial on seos IKT-vahendeid puudutavate reeglitega, mis panevad paika tehnoloogiale seatud tingimused ning seadmete turvalisuse algprintsiibid. Kokkupuutepunkte nähakse intervjuudes infosüsteemide turvameetmete süsteemi ISKE ja isikuandmete kaitse üldmääruses (GDPR).

Eraldi keskenduti dokumentides tehnoloogiaseadmete arvukusele, mille andmed olid allikates erinevad, varieerudes vahemikus 20 miljardit kuni 64 miljardit seadet aastaks 2030. Erinevatest vaatenurkadest hoolimata annab arvuline kontseptsioon informatsiooni selle kohta, et asjade interneti seadmete arv on kindlalt ületamas inimeste arvukust maailmas ning seda saab teoreetilises raamistikus esitatud suurt hulka seadmeid kokku koondavaks tehnoloogiaks pidada (käesolev töö, lk 20). Dokumendianalüüsis ei selgunud, kas dokumendid ning neid loonud asutused liigitaksid asjade interneti seadmed pigem eraldi käsitlemist vajava tehnoloogia hulka või peaks seda käsitlema ühe osana IKT-st, millele kehtivad üldised reeglid ja põhimõtted.

Teise uurimisküsimuse eesmärk oli välja selgitada, missuguseid probleeme toob IKT-tehnoloogia kaasa avalikule sektorile, sealhulgas küberkuritegusid ning küberintsidente lahendavate ametiasutuste jaoks.

Tehnoloogiast sõltuvatena nähakse riigivalitsemist, majandust ja ka kõiki teisi eluvaldkondi ning süütegude spekter on sedavõrd laiem, kui suur on tehnoloogiaga seotud valdkondade haare. Dokumendid toovad välja tehnoloogiate kasutajaskonna vähesed oskused ning madala teadlikkuse, viidates madalale küberteadlikkusele ning oskusele tehnoloogiaid õigesti kasutada, mis tõstab küberkuritegevuse ohvriks langemise riski. Nagu dokumentides, näevad ka eksperdid ebapiisavat teadlikkust probleemina, mille kese peitub ekspertide hinnangul lihtsamate küberteadmiste

puudujäägis ja oskamatuses end kaitsta. Kaitse on aga oluline, sest ründevektorite lihtsus, teadlikkus ning digitaalse ja füüsilise ruumi tajuvuse erinevused teevad kasutajatest kerged sihtmärgid. Teadlikkus on seotud **inimeste puudulike oskustega** – vähesed on nii arvutite kui ka nutikate seadmete kasutamisega seonduvad oskused. Näiteks on üks peamisi ekspertide nimetatud probleeme inimeste oskamatus seadmeid turvaliseks teha ning neid turvaliselt võrku ühendada. Eksperdid on arvamusel, et oskamatusest kasutada juba traditsiooniliseks kujunenud seadmeid, näiteks arvutit ja telefoni, võib juhtuda, et ka asjade interneti seadmete kasutamine võib kasutajaskonna jaoks keeruliseks osutuda. Eksperdid ütlevad, et kui üldlevinud tehnoloogia ühendatavuse puhul saab kasutaja mingil määral kindel olla, kuidas seadmed võrku on ühendatud, siis asjade interneti seadmete puhul ei pruugi kasutajad ühendatavusest või seadmete välja lülitamise võimalustest teadlikud olla. Teadlikkuse ning seadme tundmise juures mängib olulist rolli ka **seadmete madal kvaliteet** ning seda peamiselt kolmandates riikidest pärinevate seadmete puhul, millele on omane ebakindel tarkvara, vaikesätete muutmatus, testimata nõrgad süsteemid, uuenduste puudulikkus ning kaheldavad andmete kogumise ja jagamise aluspõhimõtted. Asjade interneti puhul on ekspertide hinnangul tõusmas ka riskide hulk tavakasutajale võrku ühendatavate seadmete kasutamisel. Dokumentides kirjeldatul ja ekspertide arvamusel on ühisosa magistritöö teoreetilise käsitlusega, kus tuuakse välja kogemuseta tootjate laialdane eksisteerimine turul (käesolev töö, lk 19-20). Oluline on märkida, et seadmete ebakvaliteetne ja kaheldav taust ei ole aktuaalne mitte üksnes tavainimeste jaoks, vaid seda seostatakse dokumentides ka välismaiste tehnoloogiatega. Dokumentides esitatud hinnangu alusel on see riigisüsteemide probleem, sest kolmandatest riikidest pärit riist- ja tarkvara lahenduste kasutamine paneb meie riigi süsteemi sõltuma teiste turvanõrkustest ning nende vastu suunatud rünnetest.

Teadlikkus ja puudulikud oskused, kuid ühtlasi ka ebakvaliteetse taustaga toodete kasutamine on ekspertide hinnangul seotud puuduliku ennetustööga. Positiivseks näiteks tuuakse välja RIA, kes teeb küberteemalist ennetustööd, kuid ennetustöö on puudulik madalamates vanuseastmetes (lapsed, noorukid), mis hiljem tekitab puudujääke ka kõrgemates vanuseastmetes (vanurid, pensionärid). Kuivõrd elanikkond on tehnoloogiast üha suuremas sõltuvuses, võib ebapiisava ennetustöö tulemusena kerkida jõulisemalt esile **küberkuritegevus**, mis omakorda küberruumis toime pandavate süütegude arvu kasvades süvendab kompetentse ametnikkonna puudust.

Tööjõud on määratletud nii dokumentides kui ka ekspertide hinnangus probleemina ning eraldi on välja toodud piiratud spetsialiseerumisvõime riigi-, teadus- ja erasektoris; spetsialistide puudus ning nende ebapiisav juurdekasv. **Kompetentsi** probleem seisneb raskustes konkureerida spetsialistide palkamisel erasektoris tegutsevate ettevõtetega ning selle konkurentsi on tinginud valdkonna avaliku

sektori madalad palgad. Probleemina tuuakse kompetentsi küsimus sisse Siseministeeriumi, Politsei- ja Piirivalveameti ning Siseministeeriumi infotehnoloogia- ja arenduskeskuse näitel, mis tehnoloogia arenemisel vajavad pädevaid inimesi juurde. Probleem ei ole nähtav üksnes uute töötajate puhul, vaid olemasolevate spetsialistide teadmisi tuleb pidevalt arendada – arenev valdkond peab omama arenemiseks valmis olevaid töötajaid, kelle teadmiste edendamine aitab nende kompetentsust tõsta. Kokkuvõttes on tarvis leida tööjõudu, hoida olemasolevaid töötajaid ning panustada inimeste teadmiste arengusse, kuid probleemina nähakse ka siin täiend- ja koolitusprogrammide puudulikkust.

Tööjõud on tihedas seoses teadus- ja arendustegevusega, mille mahtu, teadustööks vajalike ressursside ja ka ettevalmistuse ning uute ohtude teadlikkuse olemasolu peetakse puudulikuks. Ressurss ei ole problemaatiline aga üksnes haridus- ja teadusvaldkonnas, vaid puudulik on ressursside suunamine süsteemide arendamisesse ja haldamisse. Ressurss on otseselt seotud eelpool juba välja toodud probleemidega, näiteks kompetentse tööjõu olemasolu, töötajate koolitamise ja ennetustööga tavakodanikele. Finantsressursi puudumise tõttu on avaliku sektori palgad erasektorist madalamad, mistõttu lahkuvad paljud madalate palkade tõttu erasektorisse. Puudulikuna nähakse ka ametiasutuste analüüsimiseks vajaliku riist- ning tarkvara olemasolu, mis, nagu ka koolitamine, süsteemide hooldamine ja haldamine, vajab samuti lisaressurssi. Arvestades tehnoloogia kiiret arengut ning asjade interneti seadmete olemust, kasvab seadmetega seonduvate juhtumite menetlemiseks vajaminevate ametnike arv veelgi. Kasvavad ka koolituste ja vahendite vajadus, mis süvendavad probleemi veelgi. Ressursiprobleem mõjutab otseselt kõiki eelpool välja toodud punkte, mida nii ekspertide hinnangul kui ka dokumentides on välja toodud. Ressurss on see, mille tõttu kannatab praegu nii ennetustöö, spetsialistide koolitamine kui ka spetsialistide juurdekasv.

Eelpool mainitud probleemid mõjutavad omakorda koostööd, mis kerkib esile operatiivtasandilt, kus võiks asutuste vahel olla kübervaldkonda puudutavates küsimustes parem omavaheline suhtlus. Nii küberintsidentide kui ka kuritegude lahendamise ning poliitika kujundamise kohta toovad nii dokumendid kui ka eksperdid probleemsena välja asutuste tegevuste erinevuse ning madala teadlikkuse teiste asutuste võimetest ja võimalustest. Lisaks riigisisesele koostööle on probleem ka rahvusvahelise koostöö tegemise võimekus. Arvestades asjade interneti seadmete globaalset haaret, on nii dokumendianalüüsi põhjal kui ka ekspertide hinnangul tarvis saada aru rahvusvahelise koostöö tegemise võimalustest ning mingisuguses ulatuses ka vältimatusest. Rahvusvaheliste organisatsioonide staadiumil käib suhtlus väheste initsiatiivil ning riigi sees mõjutab koostöö poliitika kujundamist, kus on puudulik valdkonna tervikjuhtimine ning kübervaldkonna ühtne koordinatsioon, mis tekitab ebapiisava arusaama küberintsidentide ja -ohtude mõjudest. Riigil puuduvad võimalikud hinnangud ja riskianalüüsid uute ja juba praeguseks aktuaalsete tehnoloogiate kohta ning koostöö

puudumine süvendab probleemi üha enam. Piisavalt ei pöörata tähelepanu toodete regulatsioonide kehtestamisele ning avaliku sektori toimingute kiirus ja efektiivsus on tehnoloogia kiiret arengut arvestades madalal tasemel. Ekspertide arvates ei soosi meie õigusruum kübervaldkonna globaalset mõõdet silmas pidades küberintsidentide ja küberkuritegude lahendamist. Kübertemaatika globaalsus on see, mida avalik sektor ja riigiasutused peavad ekspertide hinnangul rohkem arvestama.

Teisest uurimisküsimusest lähtub kolmas uurimisküsimus, mille eesmärk oli välja selgitada, milliseid probleeme toovad olemasolevad kohalikud ja rahvusvahelised kübervaldkonna dokumendid ning Eesti eksperdid välja üldisi IKT- ja asjade interneti seadmeid silmas pidades.

Asjade interneti seadmete kohta on dokumendid ja eksperdid välja toonud viited turul eksisteerivatele seadmetele, inimeste teadmatusele ning teiste riikide riist- ja tarkvaralahendustele, mis võivad pikemas plaanis seadet kasutavale inimesele riske tekitada. Öeldakse, et asjade interneti seadmete kasutamine ning arvukus ei mitmekesista mitte üksnes potentsiaalsete sihtmärkide arvu, vaid annab kurjategijatele laiemad võimalused ja viisid kuritegevusega tegeleda, mis viib seadmete kasutajate haavatavuse suurenemiseni. See on kooskõlas teoreetilises kirjanduses esitatud probleemidega (käesolev töö, lk 20), mis ütleb, et seadmete koguarv ning võrku ühilduvate seadmete arv suurendab turvariske. Lisaks näitab selline vaade asjade interneti seadmetele teise uurimisküsimuse analüüsi tulemuste all välja toodud seotust probleemidega, mis liigitab asjade interneti seadmed probleemide poolest võrdväärseks IKT-tehnoloogiatega.

Asjade interneti teoreetilises kirjanduses turvaelementidele tuginedes leidsid nii üldiste kui ka asjade interneti seadmete puhul dokumentides käsitlemist konfidentsiaalsus, terviklikkus ja käideldavus, millele lisaks tõid eksperdid välja ka privaatsuse. **Konfidentsiaalsust** seostatakse standarditele mitte vastavalt ehitatud seadmetega, mis toovad esile andmete lekkimise võimaluse. Võrkudes olevad kriitilisemad seadmed võivad ekspertide hinnangul olla võrgus vähem tähtsate seadetega ning kui nende seadete sisu on üles ehitatud standardeid järgimata, kujuneb sellest oht kolmandate osapoolte juurdepääsu kaudu mitte üksnes andmetele, vaid kogu süsteemile. See on kooskõlas teoreetilises käsitluses välja toodud asjade interneti turvaelemendina esitletud konfidentsiaalsusega (käesolev töö, lk 21). **Terviklikkus** on andmekooslustega manipuleerimise tõttu probleem ning seda juhul, kui kogutavatele ja jagatavatele andmetele ligi saades hakkavad pahatahtlikud osapooled saadud informatsiooni ära kasutama ning andmeid ümber koordineerima, muutes neid endale sobilikul viisil. Analüüsi käigus selgus ekspertide hinnang tavainimestele. Ekspertide arvates töötavad seadmed teatud viisil ning seetõttu ei arvestata, et võib eksisteerida võimalusi, kus keegi suudab seadmete tegevust häirida, parameetreid andmete abil muuta ning sellega kahju tekitada. Välja toodud

turvaelement on kooskõlas teoreetilises käsitluses kirjeldatud asjade interneti turvaelemendina esitletud terviklikkusega (käesolev töö, lk 21). **Käideldavust** seostavad eksperdid teenuse rivist välja viimise võimalikkusega ning ühe osana näevad eksperdid, et seadmeid on võimalik rivist välja viia teenusetõkestusrünnete abil, mõjutades nii andmete käideldavust, sest seadmele ligipääsu takistamise korral ei pääseks seadme tavakasutaja andmetele ligi ning nende kättesaadavus oleks komplitseeritud. Käideldavuse visioon on kooskõlas teaduskirjanduses esitatud konfidentsiaalsuse turvaelemendiga (käesolev töö, lk 22).

Eraldi tõid eksperdid esile ka privaatsuse, mis analüüsile tuginedes on tootjate jaoks probleem, sest nemad proovivad enda seadmetega võimalikult kiiresti turule tulla. Sellisel puhul on probleem andmevahetuse krüpteeritus, andmete ja sätete seotus serveriga ning süsteemi turvatus. Privaatsuse kui turvaelemendiga seonduva nimetamine on kooskõlas teoreetilises käsitluses kirjeldatud asjade interneti turvaelemendina esitletud privaatsusega (käesolev töö, lk 22). Ekspertide hinnangul on õigusliku poole pealt privaatsuse riive üks keerukamaid ja problemaatilisemaid punkte, millega seadmete kasutajad silmitsi seisavad ning mille turvalisusele peavad tootjad ja haldajad tulevikus kohustuslikult mõtlema.

Eksperdid näevad turvaelementides konfidentsiaalsust, terviklikkust ja käideldavust. Tegemist on infoturbe alustaladena defineeritud kolme turvaelemendiga, mida peetakse asjade interneti seadmete puhul läbivateks ja fundamentaalseteks mõisteteks. Analüüsi tulemusena saab väita, et ekspertide hinnangul koonduvad asjade interneti alla probleemid, mille seas on välja toodud näiteks seadmete automaathäälestus, hajus ummistusrünne, hajustatud teenusetõkestusrünne, seadmete turvanõuete määramine, autentimisküsimused, regulaarne ajakohastamine ja võrkpääsu piiramine. Ekspertide arvamus kolme turvaelemendi kohta on kooskõlas asjade interneti teoorias turvaelementidena välja toodud konfidentsiaalsuse, terviklikkuse ja käideldavusega (käesolev töö, lk 21-22). Asjade interneti seadmete juures leidsid kolm peamist turvaelementi mainimist rahvusvahelistes dokumentides, mille alusel saab öelda, et asjade interneti seadmete puhul tuleks keskenduda tarkvara terviklikkuse kindlustamisele ning volitamata juurdepääsu korral peaks seadet kasutavale inimesele olema olemas teatav hoiatussüsteem. Nähakse, et konfidentsiaalsuse või terviklikkuse kaitset vajavad andmed tuleks krüpteerida ning juurdepääsud logida. Logides võiks näha kuupäeva, kellaaega ning juurdepääsuallikat. Dokumentide määratlus konfidentsiaalsuse, terviklikkuse ning käideldavuse kohta kinnitab samuti magistritöö teoreetilise materjali juures välja toodud turvaelementide käsitlust (käesolev töö, lk 21-22).

Ekspertide hinnangul on seadmete küsitav taust ning andmete kogumise võimekus üks peamisi asjade interneti tehnoloogia probleeme ning sellel on olemas ühisosa magistritöö teoreetilise osaga, kus tuuakse välja kogemuseta tootjate laialdane eksisteerimine turul (käesolev töö, lk 19-20). Eksperdid toovad esile ühisosa üld- ja asjade interneti tehnoloogia seadmete vahel, seega võib üldistavalt öelda, et mitte üksnes asjade interneti seadmete puhul ei ole seadmete taust probleem. Analüüsi käigus selgus, et probleemina näevad eksperdid seadmete seotust pilvetehnoloogiaga ning kuna Eestis pilvetehnoloogia pakkujaid ekspertidele teadaolevalt ei ole, on ka see üks aspektidest, mis võib seadmete kasutamisel probleemiks osutuda, sest sõltutakse välismaistest lahendustest, mille turvalisuses ei saa sada protsenti kindel olla.

Analüüsis viidati probleemile, et võrku ühendatud seadmetele on võimalik ligi saada asjade interneti seadmete kaudu. Võimalike ärakasutamise viisidena tuuakse esile nõrgad seadmed, millel mikrofonidel ja kaameratel on andmete kogumisega seonduvaid probleeme. Eksperdid ütlevad, et kolmandate isikuteni jõudmiseks kasutatakse lihtsasti ligipääsetavaid seadmeid, sooritatakse nende vastu teenusetõkestusrünnakud ning seadme üle kontrolli omades sooritatakse nende abil edasisi rünnakuid. Nii nähakse tavakasutajate seadmetes *botnet*'ide komponente, mis võivad tekitada palju kahju. Asjade interneti seadmete turvanõrkuste kohta on välja toodud teenusetõkestusründed (DDoS), lunavararünded ja krüptokaevandusega (ingl *cryptojacking*) seotud ründed ning nende arvu kasv. Ründed ei ole aktuaalsed mitte üksnes andmetele, vaid ka varale laiemalt, mis võib ekspertide hinnangul andmelekete, DDoS-rünnete ja seadmete abil korraldatavate terrorirünnakute näitel viia suuremate kahjudeni ühiskonnas. Seda toetavad ka teoreetilises käsitluses välja toodud asjade interneti süsteemi ja seadmetega seonduvad ründed (Lisa 1, vt lk 86-87).

Neljanda uurimisküsimuse eesmärk oli välja selgitada, mida peavad poliitikakujundajad ja seadmete kasutajad asjade interneti seadmeid silmas pidades tegema, et maandada kasutusega ilmnevaid riske.

Üldjoontes toovad nii dokumendid kui ka eksperdid asjade interneti seadmeid puudutavate soovitustena tavakasutajatele välja eri sõnastuses, kuid samadele alustele toetuvad soovitused. Dokumentides kirjutatakse, et asjade interneti tehnoloogia seadmed peaksid vastama kodukeskkonna privaatsuse ja turvalisuse ootustele. Seadmete kasutajad saavad palju ise selle jaoks ära teha, alustades lihtsast teadmisest, kui kaua seadmed eeldatavasti kestavad ning kas need on võimelised töötama ka võrguühenduseta. Oluline on seadme turvalisus ning selles on peamine roll seadme turvalisel seadistamisel, mille puhul peab jälgima, et seadmed saaksid regulaarselt uuendusi, mis aitavad privaatsuse ja turvalisuse tagamisele oluliselt kaasa. Seadmetes ei tohiks kasutada nõrku paroole –

kordumatud, ettearvamatud, keerulised ja kolmandatele osapooltele ennustamatud paroolid aitavad seadmete ja süsteemi turvalisusele oluliselt kaasa. Lisaks soovitatakse parooli turvalisusele tuge juurde anda mitmefaktorilise autentimisega. Tavakasutaja peaks soovituste järgi olema veendunud, et tema isikuandmed on kaitstud ning vanu seadmeid ei tasu ära visata, vaid neist andmed eemaldada ning sätted lähtestada.

Dokumentides välja toodud soovitusi täiendavad eksperdid, lisades, et seadmete tulevasel kasutajal tasub mõelda, kas asjade interneti seadet on neil üldse vaja. Enne seadme ostmist tasub uurida tootja ja toote kohta täpsemat informatsiooni. Oluline on, et tavakasutaja mõistaks ja arvestaks seadme omadusi ning selle kasutamise konteksti. Seadmete soetamise järel tasub mõelda, kuidas ning mis tingimustel seade võrku ühendatakse. Ekspertide sõnul jäetakse seadme soetamise järel tehase määratud kasutajanimi ja vaikeparool muutmata, kuid see peaks olema esimesi kohustuslikke seadme turvalisusega seotud tegevusi. Vastutustundlik kasutaja võiks tutvuda seadme konfiguratsioonisätetega ning kohandada neid enda äranägemise järgi. Juhul, kui seade on seotud andmetega, tasub andmetest teha teatud aja tagant tagavarakoopiad ning võimaluse korral paigaldada seadme süsteemile viirusetõrje tarkvara.

Dokumendid ja eksperdid tõid lisaks tavakasutajatele välja ka soovitused riiklikult seotud osapooltele. Töös osutatud tööjõu probleemide leevendamiseks soovitatakse turbeteenuste automatiseerimisele üleminekut, mis aitaks oluliselt töötajate tööülesannete mahtu vähendada. IT-lahendustena nimetatakse ka infoturbe ja andmekaitse põhimõtete kindlam järgimine, tehnoloogilise vastupanuvõime tõhustamine ja andmekogude turvalisuse tagamine ning riigi infosüsteemide komponentide arendamine.

Automatiseerimine on üks viisidest, kuidas **tööjõu ja kompetentsi** probleemi lahendada. Lisaks võiks keskenduda kindla suunitlusega koolitustele, sest inimeste täiendamine nii valdkonnas valitsevate ohtude kui ka seadmete ja tehnoloogiate kasutamise teemal on kiiresti arenevate tehnoloogiate juures oluline. Pikemas perspektiivis on aga õppe- ja koolituskavade ümberhindamine ja täiustamine parematеks lahendusteks vajalik, sest see toob üldhariduskoolide ja järelõppe formaadis paremini sisse kübervaldkonna ning sellega seotud teadmiste omandamise ja nii tagame teadlikuma ja oskuste poolest võimekama tulevase kasutajaskonna. Parema aluse koolitussüsteemi loomisele aitaks luua IKT-põhimõtete ja toimimise üldformaadi paika panemine, mille juures on tarvilik panna paika asutuste suhtluskanalid, mis tagaksid tulevikus efektiivsema koostöö ning ametkondadeülese arusaama, millega ning mis ulatuses tegeletakse ning tegelema peaks. Näiteks

võiks olla üks nendest tehnoloogiatest just asjade interneti tehnoloogia, mille kohta pole asutusteülest ühist visiooni veel loodud.

Asjade internetiga kaasnevate probleemide leevendamiseks peab keskenduma ennetustegevusele ning baashügieeni reeglite loomisele ja nende presenteerimisele laiemale elanikkonnale. Tarvis on selgitada ohtude spetsiifikat ning seda, kuidas on võimalik end näiteks asjade interneti seadmetega kaasnevate ohtude eest kaitsta. Osaliselt langeb see kokku eelpool välja toodud koolitamise punktiga, kuid lisaks ametnike kübervaldkonna teadmiste ja oskuste kasvatamisele peaks ennetavalt seda intensiivsemalt suunama ka tavakasutajatele.

Asjade interneti seadmete puhul on soovituslik kehtestada seadmetele kindlad standardid, et turule tulevad seadmed vastaksid teatud kriteeriumitele ning seeläbi väheneks seadmete kasutajatele kaasnevad riskid. Lisaks tasuks eri tehnoloogiate, kuid käesolevaga peaasjalikult asjade interneti seadmeid puudutavad reeglistikud välja töötada. Üks võimalus on see välja tuua ISKE kriteeriumite nimistus. Standardite ja reeglite loomise jaoks oleks oluline asjade interneti kohta teha riskianalüüs, mille koostamise ning teema kinnitamisese järel saaks riik hakata mõtlema asjade interneti seadmete kasutamisele ka erinevates asutustes, kuid see tähendaks vajaliku kasutuspoliitika väljatöötamist ning põhimõtete paikaseadmist. Mõistagi laieneb riskianalüüside tegemine ka teistele tehnoloogiatele. Eelpool mainimist leidnud suhtluskanalite, üldformaadi ja põhimõtete paikapanemine riigiasutustes annaks tavainimeste regulatsioonidele kindlama aluse asjad omaks võtta, sest ka riigiasutustes endas on asjad reguleeritud.

Intsidentide ja küberkuritegevuse puhul nähakse olulise punktina valmisolekut ööpäev ringi probleemidele reageerida. RIA-ga sarnast reageeringut tuleks rakendada laiemalt, sest tehnoloogiavõimaluste avardumisel muutuvad ka probleemid aktuaalsemaks ning sagedasemaks. Määratledes selgemini ja paremini riigiasutuste töökorraldust ning tagades nende omavahelise kiire ja kvaliteetse teabevahetuse, suudetakse ka problemaatilistele olukordadele kiiresti reageerida. Leitakse, et IKT ja küberkuritegevuse praegusi ja tulevikutrende tuleb pidevalt analüüsida ning koostööd strateegiliste partneritega ennetusliku tegevuskava koostamiseks ning pidevaks täiustamiseks peaks riik soodustama. Ennetusega on oluline luua küberkuritegevuse kohta teadlikkust propageeriv programm. Programm aitaks vastu seista küberkuritegevusega seotud probleemidele, mida toovad esile mitte üksnes tavakasutuses olevad asjade interneti seadmed, vaid ka teised IKT-tehnoloogiad. Digitaliseeruvas ühiskonnas, mille seadmete arvukus näitab kasvutrendi, on oluline mõista, et olukordade sagenedes peab **seadmete kuritarvitamisel ning kuridegude osas**

reguleerima ka seadusi ning nii võib muudatus puudutada just kriminaalseadustikku, kus tulevikus tuleb määratleda ka tekkinud tulevikutehnoloogiate hulk, sealhulgas asjade interneti oma.

Globaliseeruvas maailmas on olulisel kohal **rahvusvaheline koostöö ning selle võimekuse kasvatamine.** Oluline on leida endale rahvusvahelisel areenil aktiivsed koostööpartnerid (näiteks Euroopa Liit, NATO, ÜRO), kellega koos panustada süsteemide turvaliseks muutmisesse nii ametiasutuste kui ka riigi jaoks tervikuna. Rahvusvaheliselt võiks keskenduda küberturvalisusele orienteeritud koostöörühmade loomisele või nendes osalemisele, sest see aitaks oluliselt küberkuritegude uurimisele kaasa. Rahvusvaheline koostöö saab aga toimida, kui ametiasutuste vaheline koostöö riigi sees juba toimib. Riigis tuleks luua toimiv süsteem, kus igal ametkonnal on roll IKT tulevikule suunatud tervikpildi ja eesmärgi täitmisel nii, et kaasatud on kõik osapooled ning kõik on ka teiste tegemistest teadlikud. Toimiv riigisisene mehhanism on alus ka tõhusale rahvusvahelisele koostööle.

Teadus- ja arendustegevuse juures tuuakse dokumentides välja erasektori, riigi- ja teadusasutuste koostöö soodustamine, mis ei aitaks tähelepanu pöörata üksnes tehnoloogia küsimustele, vaid tõstaks tehnoloogiatega seotud riskide hindamise ja haldamise võimekust. Välja tuuakse teadustöö mahu suurendamine ning spetsialistide taseme- ja täiendõppe kvaliteedi tõstmise ja hoidmise vajadus, et tagada tehnoloogia ja turvalisusega tegelevate spetsialistide olemasolu. Soovitatakse tähelepanu pöörata ka kvanttehnoloogia, krüptograafia, küberkuritegevuse, tehisintellekti, masinõppe ning privaatsusega seotud ohtudele ning nende keskendumisele teadustöös.

Olulise lülina nähakse teadus- ja arendustegevuse kõrval koostööd erasektoriga. Teadustöö ja ettevõtluse tihedama koostöö soodustamine, kuid ka näiteks iduettevõtete tekkeks ja toimimiseks toetava keskkonna loomine aitaks mitte üksnes lahendada uurimist vajavaid probleeme, vaid panustaks otseselt ka riigi majanduslikku toimimisse ning teaduse arengusse. Riigil on siinkohal võimalus koostöö tegemist propageerida ning selleks soodsad tingimused luua. Välja tuuakse, et oluline on arendusressursi leidmine, mille najal endale vajalikud tööriistad ise välja arendada, vähendades sedasi sõltuvust kolmandatest osapooltest. Nii oleks erasektoril teadusasutuste ja riigiga koostööks kokkupuutepunkt olemas. Oluline on mõista, et läbi tuleb hakata viima uute tehnoloogiate katseprojekte riigi infosüsteemiga seotud lahenduste arendamiseks, sealhulgas testida asjade interneti tehnoloogiat, mille turvalisuse ning riskide kohta annaksid informatsiooni katsed.

Dokumentides on eristatud ka soovitused seadmete ja teenuste tootjatele, kes peaksid veelgi aktiivsemalt ja sihipärasemalt turvanõrkuste avastamise ning nende likvideerimise võimekuse

tõstmisega tegelema. Olulise komponendina turvaliste süsteemide juures nähakse tarkvara- ja turvavärskenduste veelgi aktiivsemat täiustamist ja kiiret pakkumist ning toote eluea lõppedes kasutajatele kogutud andmete kustutamise võimalikkust. Arhitektuuriliselt tuleb seadmed ja tarkvara ehitada arendusprotsessis turvaliselt, et tagada lõppkasutajatele turvalisus. Lisasoovitusena nimetatakse vaikeparoolide kasutamise võimaluse likvideerimist, mis annab kasutajatele kohustuse toote kasutusele võtmisel panna paika enda loodud kasutajanime ja parooli. Et tagada seadmete turvaline kasutamine, tuleb kasutaja jaoks lihtsustada toote paigaldus- ja hooldusprotsessi.

2.5. Järeldused ja ettepaneku

Selles magistritöös püstitatud küsimus uurimisprobleemile „Missugused on asjade interneti seadmete kasutuselevõtust tulenevad turvalisuse riskid inimeste tavakasutuses olevate seadmete näitel seda kasutava kasutajaskonna jaoks ning kuidas nende riskide tekkimine võib mõjutada küberintsidente ja küberkuritegevust uurivate asutuste tööd?“ lahenduse leidmiseks oli püstitatud neli uurimisküsimust. Teoreetilisele käsitlusele, kübervaldkonna dokumentide ning ekspertintervjuude analüüsile toetudes vastatakse selles alapeatükis uurimisküsimustele. Vastuste järel on välja toodud ettepanekud avaliku sektori ameti- ja haldusasutustele ning asjade interneti seadmete kasutajatele.**Esimesele uurimisküsimusele**, milleks oli „Kuidas defineerivad kohalikud ja rahvusvahelised dokumendid ning Eesti eksperdid mõistet *Internet of Things* (ingl) ning kuhu liigitub mõiste digitehnoloogiast tulenevate probleemide keskel?“ leidis autor vastuse dokumendianalüüsi ning ekspertintervjuude kaudu. Nende põhjal saab öelda, et ingliskeelse mõiste vastena nähakse eesti keeles mõistet ,,asjade internet’’. Kuivõrd mitmed dokumendid on rahvusvahelises kontekstis ingliskeelsed, eelistatakse kasutada ka tehnoloogia ingliskeelset mõistet või selle lühendit IoT, mis tagab erinevates ringkondades mõiste ühese mõistetavuse. Asjade internetti käsitletakse võrku ühendatud seadmete kogumina, mis on iseseisvalt suutelised omavahel suhtlema ning anduritega ümbritsevast keskkonnast vajalikku informatsiooni koguma. Magistritöö kinnitas, et asjade interneti tehnoloogia on liikunud inimeste tavakasutuses olevate seadmete konteksti ning seadmete näited võivad olemas olla praktiliselt kõikides kodudes – alates elutoa meelelahutussüsteemidest köögis eksisteerivate seadmeteni ning tervist jälgivatest seadmetest turvasüsteemi seadmeteni välja.

Magistritöös kogutud andmed ei andnud ühest vastust sellele, kas asjade interneti kui tehnoloogia peaks defineerima ühe suurema ja eraldiseisva teemana IKT valdkonna all. Eraldiseisva teemana näeb seda prioriteetsena teadus- ja arendusvaldkond, kuid **avalikus sektoris on ekspertide hinnangul asjade internet tarvis ära määratleda laiema valdkonna ühe osana, sest see võimaldab tagada tekkivate probleemide tõhusama lahendamise**. Teisisõnu viidatakse sellele, et probleemid eksisteerivad paljudes seadmetes ning tehnoloogia spetsiifikast sõltumata annaks asjade interneti

probleeme lahendada teiste probleemide hulgas. Töös leidis kinnitust levinud arusaam, et asjade interneti definitsioon on tarvis eri ametiasutustes ühiselt kokku leppida, sest see aitaks luua parema arusaama mõiste määratluse kohta.

Teisele uurimisküsimuse, milleks oli „Missuguseid probleeme toob kaasa asjade interneti tehnoloogia avalikule sektorile, sealhulgas küberkuritegusid ning küberintsidente lahendavate ametiasutuste jaoks kuritegude olemusest ning nende lahendamiseks vajaminevast kompetenstist lähtuvalt?“ vastuseks leidis autor, et avaliku sektori ameti- ja haldusasutuste jaoks on probleemne asjade interneti seadmete arvukus, sest sellega tõuseb potentsiaalsete rünnatavate objektide hulk ning seadmete kaudu kasutajaskonna haavatavus. Sarnaselt arvukusega on probleemne ka seadmete päritolu – viidatakse valdavalt Hiinast imporditud testimata seadmetega kaasnevatele riskidele, mis võivad tavakasutaja asetada potentsiaalselt haavatavasse olukorda. Kaheldava ebakvaliteetse taustaga seostatakse asjade interneti turvaelemendina konfidentsiaalsust, millega viidatakse standarditele mittevastavatele seadmetele, mis võivad esile tuua andmete lekkimise. Nõrgalt üles ehitatud seadmete probleem on terviklikkus andmekooslustega manipuleerimise võimalikkuse tõttu, ning käideldavus, mida seostatakse teenuste rivist välja viimise võimalikkusega. Seadmete arvukuse kasv ning nende kaheldav taust on olulised küberintsidentide ja küberkuritegevust lahendavate ametiasutuste jaoks, kelle jaoks tõuseb potentsiaalselt menetlemist vajavate juhtumite hulk, mis tähendab pikas perspektiivis probleeme tööjõu ning vajaliku kompetentsiga. Spetsialistide puudus IKT valdkonnas ei ole mitte üksnes küberintsidente ja küberkuritegevust lahendavate ametiasutuste, vaid terve avaliku sektori probleem. IKT valdkonna eelarve ning eraldatud toetuste maht ei ole vastavuses tehnoloogia kiire arengu ning digitehnoloogiate, sealhulgas asjade interneti kasutuselevõtust tingitud probleemide lahendamisega.

Kolmandale uurimisküsimusele ehk „Milliseid probleeme toovad kohalikud ja rahvusvahelised kübervaldkonna dokumendid ning Eesti eksperdid välja üldisi IKT- ja asjade interneti seadmeid silmas pidades?“ leidis autor vastuseks, et peamised probleemid on seotud tööjõu, koostöö, teadlikkuse ja oskuste, poliitika kujundamise, teadus- ja arendustegevuse ning potentsiaalsete küberrünnete spektri kasvuga. Probleem on IKT-sektori kompetentsivajaduse tagamine, sest lisaks ametikohtade täitmisele tegeletakse vähe ka olemasolevate töötajate koolitamise ning nende teadlikkuse ja oskuste kasvatamisega. Vähesed teadmised ja oskused ei ole üksnes ametnike, vaid peaasjalikult tavainimeste, kuid lisaks ka juhtide probleem. Nähakse, et ennetuskampaaniate ning koolituskavade väljatöötamine võiks olla paremini üles ehitatud, sest praegu on selle tase madal. Riigisisene koostöö on ametiasutuste jaoks probleemne, sest asutused on liigselt enda valdkonna spetsiifikas kinni ning ühisosa leidmine on komplitseeritud. Probleem on ka valdkondlik

tervikjuhtumine ning kübervaldkonna ühtne koordinatsioon, mis tekitab ebapiisava arusaama küberintsidentide ja -ohtude mõjudest. Koostöö on probleemne ka rahvusvahelisel tasandil. Leitakse, et koostöö teiste riikide ja organisatsioonidega käib väheste initsiatiivil.

Sisejulgeoleku asutuste ja küberkuritegevusega seotult nähakse probleemsena süütegude arvu kasvu ning kompetentse ametnikkonna puudust. Asutusi mõjutab ka asjade interneti seadmete seotus ning avatus küberrünnetele. Asjade interneti seadmete kasutamine ning arvukus ei mitmekesista mitte üksnes potentsiaalsete sihtmärkide arvu, vaid annab kurjategijatele laiemad võimalused ja viisid kuritegevusega tegeleda. Lisaks on teadus- ja arendustegevus Eestis puudulik nii mahu, eraettevõtetega koostöö kui ka teadustööks vajalike ressursside olemasolu poolest.

Neljandale uurimisküsimusele ehk „Mida peavad poliitikakujundajad ja seadmete kasutajad asjade interneti seadmeid silmas pidades tegema, et maandada kasutusega ilmnevaid riske?“, sai autor vastuse nii dokumendianalüüsi kui ka ekspertintervjuude põhjal. Dokumentides (käesolev töö, lk 38–42) ning ekspertintervjuudes (käesolev töö, lk 57–60) välja toodud soovituste järgi saab nimetada järgnevad ettepanekud poliitikakujundajatele:

1. Asjade interneti seadmete kohta on vaja koostada riskianalüüs. Analüüs aitaks defineerida tehnoloogiaga seonduvad probleemid ning paremini ette valmistada probleemide ennetuse ning lahendamisega seonduva.

2. Ametiasutustes tuleks koostöös määratleda üldised põhimõtted ja koostada spetsiifiline tegevuskava lähtuvalt ministeeriumite ja nende haldusala vaatest. On oluline, et osapooled näeksid koostöövõimalusi digitehnoloogiatest tulenevate probleemide lahendamisel ning turvalise ühiskonna loomisel. Tuleb mõtestada, et tehnoloogiaprobleeme, sealhulgas asjade internetiga kaasnevaid, saab lahendada ametiasutuste koostöös.

3. Lahendama peab tööjõu ja kompetentsiga seotud probleeme, näiteks looma koolituskavasid, mis tagaksid praeguste töötajate võimekuse digitehnoloogia väljakutsete edukaks lahendamiseks. Kui üldiselt on tööjõuprobleem IKT valdkonna ülene, tasuks erilist tähelepanu pöörata küberkuritegevuse ja küberintsidente lahendavate spetsialistide koolitamisele ning pidada seda seadmete arvukust ning tehnoloogia arengut silmas pidades prioriteetseks.

4. Asjade interneti seadmetele tuleb kehtestada standardid, et tagada kindlatele kriteeriumitele vastava tehnoloogia kättesaadavus ja müük.

5. Lisaks standarditele tuleks välja töötada asjade interneti seadmeid puudutav reeglistik. Asjade interneti seadmed võiks välja tuua ISKE seadmetele püstitatud kriteeriumite nimistus.

6. Rahvusvahelise koostöö võimekust tuleb kasvatada. Rahvusvaheliste koostööpartnerite olemasolu ning suhete hoidmine peab olema üks eesmärkidest nii kuritegude kui ka intsidentide lahendamise ja poliitikakujundajate vaatest lähtuvalt.

7. Laialdase probleemi tuvastamise korral peab riik olema valmis reageerima seadusandluse muudatustega.

8. Oluline on teadus- ja erasektori asutuste vahelise koostöö edendamine, sest sellega on võimalik digitehnoloogiate arenguga paremini kursis olla ning probleemide korral ettenägelikult tegutseda.

9. Keskenduma peab ennetusele ning baashügieeni reeglite loomisele ja tegelema nende presenteerimisega laiemale elanikkonnale. Tavainimestele keskendudes peab saama loodud asjade interneti turvalist kasutamist propageeriv programm, mis suudaks parandada asjade interneti seadmetega seotud teadlikkust ja oskusi. On oluline, et asjade interneti seadmete puhul lähtutaks järgmistest punktidest:

- Seadme tulevasel kasutajal tuleb mõelda, kas asjade interneti seadet on tal üldse vaja.
- Enne seadme ostmist tuleb uurida tootja ja toote kohta lisainformatsiooni.
- Seadme soetamise järel tuleb planeerida, kuidas ning mis tingimustel seade võrku ühendatakse.
- Seadme soetamise järel tuleb muuta tehase määratud kasutajanimi ja vaikeparool.
- Asjade interneti seadmetele tuleb teha regulaarselt uuendusi.
- Tutvuma peaks seadme konfiguratsioonisätetega ning kohandama neid vastavalt vajadusele.
- Arvestama peab seadme omadusi ning selle kasutamise konteksti.
- Kui seade on seotud andmetega, tasub andmetest teha teatud aja tagant võimaluse korral tagavarakoopiad.
- Kasutaja peab tutvuma, kas seadmele on võimalik paigaldada viirusetõrje tarkvara ning võimaluse korral tuleks seda kasutada.

KOKKUVÕTE

Magistritöö keskendub asjade interneti seadmete kasutuselevõtust tulenevate turvalisuse riskidele inimeste tavakasutuses olevate seadmete näitel seda kasutava kasutajaskonna jaoks ning sellele, kuidas nende riskide tekkimine võib mõjutada küberintsidente ja küberkuritegevust uurivate asutuste tööd. Autor tugines uurimisprobleemi lahendamiseks teoreetilises osas interneti ajaloo ja asjade interneti käsitlusele ning vaatles asjade interneti tehnoloogiaga seotud riske turvalementide ning asjade interneti tehnoloogia arhitektuuri kaudu. Asjade interneti seadmetena toodi esile Amazon Echo tootesarja nutikõlarid, mida kõrvutatakse turvaelementide ja asjade interneti kolmekihilise arhitektuurilise plaaniga, mille kaudu tuvastati küberründed, mida annab asjade interneti seadmetele suunata.

Magistritöö eesmärk oli välja selgitada asjade interneti tehnoloogia arengust tulenevad riskid tehnoloogia kasutajaskonna ning avaliku sektori ameti- ja haldusasutuste jaoks. Tööga kaardistati riskid seadmete kasutajate jaoks ning kaardistati probleemid, millega avaliku sektori ameti- ja haldusasutused peavad tulevikus asjade interneti olukordade ennetamisel ja menetlemisel ning kompetentsi vajadusest lähtuvalt keskenduma. Töö eesmärgi saavutamiseks analüüsiti asjade internetti käsitlevaid teoreetilisi lähtekohti, asjade interneti tehnoloogia ja digiarenguga seotud Eesti Vabariigi ja rahvusvahelisi visiooni-, strateegia- ja raamdokumente ning intervjueeriti Eesti kübervaldkonna eksperte. Kvalitatiivse meetodina kasutati fenomenograafilist uurimisstrateegiat ning andmekogumise meetodina kasutati dokumendianalüüsi ja poolstruktureeritud ekspertintervjuusid.

Eesmärgi saavutamiseks oli paika pandud kolm uurimisülesannet. Esiteks tuli **t**uvastada teoreetilistele allikatele tuginedes asjade internetiga kaasnevad turvalisuse riskid, mida kajastab teooriapeatükk arvuti ja interneti turvariskide, asjade interneti tehnoloogia, selle turvaelementide ja rünnakute näidete kohta. Teiseks tuli analüüsida tehnoloogia arengust tulenevate probleemide ennetuse ja tõkestamise meetmeid, milleks viidi läbi dokumendianalüüs strateegia- ja visioonidokumentide ning rahvusvahelise praktika kohta ning ekspertintervjuud Eesti IKT-ekspertidega. Intervjuusid on käsitletud teise peatüki alapeatükkides. Kolmandaks tuli teoreetiliste lähtekohtade ning kogutud andmete põhjal teha ettepanekud avaliku sektori ameti- ja haldusasutustele, et luua parem teavitustöö platvorm ja arutelu strateegilise lähenemise muutmiseks asjade interneti tehnoloogia suunal.

Tehtud uuringust selgus, kuidas kohalikud ja rahvusvahelised kübervaldkonna dokumendid defineerivad asjade interneti mõistet üldiste tehnoloogiast tulenevate probleemide keskel ning

milliseid probleeme toob kaasa asjade interneti seadmete laialdane kasutamine avalikule sektorile nii kübervaldkonna dokumentide kui ka küberekspertide hinnangu järgi. Töös kaardistati küberkuritegevust ja küberintsidente lahendavate ametiasutuste jaoks eksisteerivad probleemid asjade interneti ning üldtehnoloogia kaudu ning lisati sellele kokkuvõtlik visioon poliitikakujundajatele ja seadmete kasutajatele asjade interneti turvaliseks kasutamiseks.

Uuringu tulemusena esitas autor ettepanekud peaasjalikult poliitikakujundajatele, kuid andis lisaks ka seadmete tavakasutajatele alused asjade interneti turvaliseks kasutamiseks. Töö omab praktilist väärtust nii asjade interneti seadmete kasutajate kui ka Eesti ameti- ja haldusasutustele. Asjade interneti käsitlus ei anna tulemust mitte üksnes kindlale tehnoloogiale tuginedes, vaid aitab kinnitada valdkonnaüleseid probleeme ning juhtida tähelepanu tehnoloogiavaldkonna üldistele kitsaskohtadele. Töö tulem on näha autori esitatud ettepanekutes (käesolev töö lk 73–74) ja kokku koondatud asjade interneti seadmete tavakasutajatele ette nähtud soovitustes (käesolev töö, lk 74), mis aitab kaasa mitte üksnes turvalisema ühiskonna ning digitehnoloogiate turvalisele kasutamisele, vaid annab ka sisendi ametiasutuste edaspidisesse töösse.

Edasised uuringud peaksid keskenduma asjade interneti seadmete tehnilisele poolele, et anda veel soovitusi poliitikakujundajatele, seadmete kasutajatele ning seadmete tootjatele. Vajalik on teha täpsem riskianalüüs asjade interneti seadmete kohta, sest see aitaks asutustel paremini ette valmistada ennetusprogramme ning neid ka suuremal määral ellu viia.

SUMMARY

The aim of this thesis is to identify the risks from Internet of Things (IoT) technology devices toward users and public sector administrative institutions. The thesis maps the risks to users as well as the problems that public sector institutions are likely to face in the near future in respect to public use of IoT. The thesis is built around two principal areas of research: (1) An analysis of theoretical frameworks that structure discussion of the Internet and IoT, principally in relation to security features of IoT and IoT device-based cyberattacks. (2) Study of local and international vision and strategy documents related to IoT technology and digital development. This part of the research also includes interviews with local Estonian cyber experts. In carrying out the research contained in the thesis, a phenomenographic research strategy was employed as a qualitative method, and document analysis and semi-structured expert interviews were used as data collection methods.

The thesis identifies and explains the ways in which local and international cyber documents define the concept of the IoT in the midst of general technological challenges, as well as identifying problems that the widespread use of IoT devices will pose for the public sector, according to both cyber documents and cyber experts. Finally the thesis identifies challenges for cybercrime and cyber incident authorities that arise in relation to IoT and general technology, and provides a concise roadmap for policy makers and device users on how to use the IoT technology devices safely.

The recommendations within the thesis are intended mainly for the benefit of policy makers, but also provide a basis for the safe use of devices for ordinary users. Further research should focus on the technical side of IoT devices to provide further guidance to policy makers, device users and device manufacturers. In this light, this research has practical value for IoT technology users and for Estonian agencies and administration institutions.

VIIDATUD ALLIKATE LOETELU

Adat, V. & Gubta, B. B., 2018. Security in Internet of Things: Issues, challenges, taxonomy, and architecture. *Telecommunication Systems*, 67, pp. 423-441.

Alaba, F.A., Othman, M., Hashem, I.A.T., Alotaibi, F., 2017. Internet of Things: A survey. Journal of Network and Computer Applications, 88, pp. 10-28.

Alam, S., Chowdhury, M.M.R., Noll, J., 2011. Interoperability of Security-Enabled Internet of Things. *Wireless Pers Commun*, 61, pp. 567-586.

Australian Government, 2020. Securing the Internet of Things for Consumers. [Võrgumaterjal] Leitav: https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf [Kasutatud 19. 05. 2021].

Barassi, V., Treré, E., 2021. Does Web 3.0 come after Web 2.0? Deconstructing theoretical assumptions through practice. *New Media and Society*, 14(8), pp. 1269-1285.

Bassi, A., Bauer, M., Fiedler, M., Kramp, T., Kranenburg, R., Lange, S., Meissner, S., 2013. *Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model*. Berlin: Springer.

Bayuk, J.L., 2013. Security as theoretical attribute construct. *Computers & Security,* 37, pp. 155-175.

Bejtkovský J., Rózsa Z., Mulyaningsih D.H., 2018. A phenomenon of digitalization and e-recruitment in business environment. *Polish Journal of Management Studies*, 18(1), pp. 58-68.

Beranek, L., 2000. Roots of the Internet. *Massachusetts Historical Review*, 2, pp. 55-75.

Bory, Paolo. *The Internet Myth*. London: University of Westminster Press.

Brause, S.R. & Blank, G., 2020. Externalized domestication: smart speaker assistants, networks and domestication theory. *Information, Communication & Society*, 23(5), pp. 751-763.

Brous, P., Janssen, M., Herder, P., 2020. The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. *International Journal of Information Management*, 51, pp. 1-17.

Bush, Vannevar, 1995. As We May Think (an article that appeared in The Atlantic Monthly in 1945 predicting the electronic revolution). *The Journal of Electronic Pubishing*, 1(2), pp. 1-7.

Campell-Kelly, M. & Garcia-Swartz, Daniel D., 2013. The History of the Internet: The missing narratives. *Journal of Information Technology*, 28, pp. 18-33.

Chanal, P.M. & Kakkasageri, M.S., 2020. Security and Pricacy in IoT: A Survey. *Wireless Personal Communications*, 115, pp. 1667-1693.

Check Point Research, 2020. *Cyber Security Report 2020*. [Võrgumaterjal] Leitav: https://resources.checkpoint.com/cyber-security-resources/cyber-security-report-2020 [Kasutatud 19. 05. 2021].

Conosco, 2021. *IoT Security Breaches: 4 Real-World Examples*. [Võrgumaterjal] Leitav: https://www.conosco.com/blog/iot-security-breaches-4-real-world-examples/ [Kasutatud 19. 05. 2021].

Crispen, Patrick Douglas, 1994. *Roadmap*. MELA Notes, 61, pp. 17-19.

Crocker, S., 2019. The Arpanet and its impact on the State of Networking. *Computer*, 52(10), pp. 14-23.

Das, A.K., Zeadally, S., He, D., 2018. Taxonomy andanalysis of security protocols for Internet of Things. *Future Generation Computer Systems*, 89, pp. 110-125.

De, R., Pandey, N., Pal, A., 2020. Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. *International Journal of Information Management*, 55, pp. 1-5.

Denning, Peter J., 1989. The Science of Computing: The ARPANET after Twenty Years. *American Scientist*, 77(6), pp. 530-534.

E-riigi Akadeemia, 2020. *Riigi küberturvalisuse käsiraamat.* [Võrgumaterjal] Leitav: https://ega.ee/wp-content/uploads/2020/05/Kuberturvalisuse_kasiraamat_EST.pdf?fbclid=IwAR0-AWnhXJq3-bQpyLUsV3w_2IEwQKKkiAScvHuvqpcVjHKPedbiAKzMNGo [Kasutatud 19. 05. 2021].

Eesti Kaitsevägi, 2021. *Küberväejuhatus*. [Võrgumaterjal] Leitav: https://mil.ee/uksused/kubervaejuhatus/ [Kasutatud 19. 05. 2021].

ENISA, 2019. *Good Practices for Security of IoT - Secure Software Development Lifecycle.* [Võrgumaterjal] Leitav: https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1/at_download/fullReport [Kasutatud 19. 05. 2021].ENISA, 2020. *Main incidents in the EU and*

worldwide – ENISA threat Landscape. [Võrgumaterjal] Leitav: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents [Kasutatud 19. 05. 2021].

European Commission, 2020. *The EU's Cybersecurity Strategy for the Digital Decade.* [Võrgumaterjal] Leitav: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164 [Kasutatud 19. 05. 2021].

Ferguson, A. G., 2016. The Internet of Things and the Fourth Amendment of Effects. *California Law Review*, 104(4), pp. 805-880.

Flamm, K., 1988. *Creating the Computer: Government, industry, and high technology*, Washington DC: Brookings Institution Press.

Flick, U., 2006. *An introduction to qualitative research*. London: SAGE.

Flick, U., 2011. *Introducing Research Methodology: A Beginner's Guide to Doing a Research Project.* Los Angeles, London, New Delhi, Singapore, Washington DC: Sage.

Ford, M. & Palmer, W., 2019. Alexa, are you listening to me? An analysis of Alexa voice service net work traffic. *Personal and Ubiquitous Computing*, 23(1), pp. 67-79.

Furfaro, A., Argento, L., Parise, A. & Piccolo A., 2017. Using virtual environmentsfor the assessment ofcybersecurity issues in IoT scenarios. *Simulation Modelling Practice and Theory*, 73, pp. 43-54.

Government of Canada, 2020. *Internet of Things (IOT) Checklist for Consumers.* [Võrgumaterjal] Leitav: http://www.ic.gc.ca/eic/site/oca-bc.nsf/eng/ca03071.html [Kasutatud 19. 05. 2021].

Green, J. & Thorogood, N., 2014. *Qualitative Methods for Health Research,* SAGE.

Greenstein, Shane, 2020. The Basic Economics of Internet Infrastructure. *The Journal of Economic Perspectives*, 34(2), pp. 192-214.

Gubbi, J., Buyya, R., Marusic, S., Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29, pp. 1645-1660.

Hedges, Willam D., 1976. The Computer and Man. *Educational Technology*, 16(1), pp. 44-46.

Hosting Tribunal, 2020. *How Many Websites Are There? How Many Are Active in 2020?* [Võrgumaterjal] Leitav: https://hostingtribunal.com/blog/how-many-websites/#gref [Kasutatud 19. 05. 2021].

Hsu, C.-L. & Lin, J.C.-C., 2016. Exploring Factors Affecting the Adoption of Internet of Things Services. *Journal of Computer Information Systems*, 58(1), pp. 49-57.

Jackson, C. & Orebaugh, A., 2018. A study and privacy issues associated with the Amazon Echo. *Int. J. Internet of Things and Cyber-Assurance*, 1(1), pp. 91-100.

Jing, Q., Vasilakos, A.V., Wan, J., Lu., J., Qiu, D., 2014. Security of the Internet of Things: perspectives and challanges. *Wireless Netowork*, 20, pp. 2481-2501.

Justiitsministeerium, 2020. *Kuritegevus Eestis 2019*. [Võrgumaterjal] Leitav: https://www.kriminaalpoliitika.ee/kuritegevuse-statistika/kuberkuriteod.html [Kasutatud 19. 05. 2021].

Justiitsministeerium, 2021. *Kuritegevus Eestis 2020*. [Võrgumaterjal] Leitav: https://www.kriminaalpoliitika.ee/kuritegevus2020/kuberkuriteod [Kasutatud 19. 05. 2021].

Kalmus, V., Masso, A., Linno, M., 2015. *Kvalitatiivne sisuanalüüs.* [Võrgumaterjal] Leitav: http://samm.ut.ee/kvalitatiivne-sisuanalyys [Kasutatud 19. 05. 2021].

Kantar Emor, 2017. *Nutiseadmete kasutajate turvateadlikkuse ja turvalisuse käitumise uuring.* [Võrgumaterjal] Leitav: https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/nuti-uuring2017_aruanne.pdf [Kasutatud 19. 05. 2021].

Kennedy, B., 1995. Computer Forum. *The Journal of Preservation Technology*, 26(4), pp. 4-5.

Kouicem, D.E., Bouabdallah, A., Lakhlef, H., 2018. Internet of things security: A top-down survey. *Computer Networks*, 141, pp. 199-221.

Lagerspetz, M., 2017. *Ühiskonna uurimise meetodid.* Tallinn: TLÜ Kirjastus.

Laherand, M.-L., 2008. *Kvalitatiivne* uurimisviis. Tallinn: OÜ Infotrükk.

Lee, I. & Lee, K., 2015. The Internet of Things (IoT): Applications, investments, and challanges for enterprises. *Business Horizons*, 58(4), pp. 431-440.

Lei, X., Tu, G.-H., Liu, A.X., Ali, K., Li, C.-Y., Xie, T., 2019. The Insecurity of Home Digital Voice Assistants – Amazon Alexa as a Case Study. *IEEE Security &Privacy,* pp. 1-12.

Li, S., Xu, L.D., Zhao, S., 2015. The internet of things: a survey. *Inf Syst Front*, 17, pp.243-259.

Licklider, J. C. R., 1960. Man Computer Symbiosis. *IRE Transactions on Human Factors in Electronics*, 1, pp. 4-11.

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H. & Zhao W., 2017. A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal*, 4(5), pp. 1125-1142.

Linno, M., 2020. *Kvalitatiivsed uurimismeetodid sotsiaalteadustes: Kodeerimine ja kategoriseerimine*. [Võrgumaterjal] Leitav: https://sisu.ut.ee/kvalitatiivne/kodeerimine-ja-kategoriseerimine [Kasutatud 19. 05. 2021].

Mahbub, M., 2020. Progressive researches on IoT security: An exhaustive analysis from the perspective of protocols, vulnerabilities, and preemptive architectonics. *Journal of Network and Computer Applications*, 168, pp. 1-26.

Majandus- ja Kommunikatsiooniministeerium, 2019. *Küberturvalisuse strateegia 2019-2022*. [Võrgumaterjal] Leitav: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf [Kasutatud 19. 05. 2021].

Mills, M.A & Mills, M.P., 2020. The Science Before the War. *The New Atlantis*, 61, pp. 19-34.

National Intelligence Council, 2008. Disruptive Civil Technologies: Six Technologies With Potential Impacts on US Interests out to 2025. [Võrgumaterjal] Leitav: https://fas.org/irp/nic/disruptive.pdf [Kasutatud 19. 05. 2021].

Nižetic, S., Solic, P., Lopez d I. Gonzalez d. Artaza, D., Patrono, L., 2020. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *Journal of Cleaner Production*, 274, pp. 1-32.

Nord, J. H., Koohang, A. & Paliszkiewicz, J., 2019. The Internet of Things: Review and theoretical framework. *Experts System With Applications*, 133, pp. 97-108.

O'Malley, M. & Rosenzweig, R., 1997. Brave New World or Blind Alley? AmericanHistory on the World Wide Web. *Journal of American History*, 84(1) pp.132–155.

Oulasvirta, A., Rattenbury, T., Ma, L., Raita, E., 2012. Habits make smartphone use more pervasive. *Pers Ubiquit Comput*, 16, pp. 105-116.

Parida, V., 2018. Digitalization. *Addressing Social Challenges*, pp. 23-38.

Parviainen, P., Kääriäinen, J., Teppola, S., Tihinen, M., 2016. Tackling the Digitalisation Challenge: How to Benefit from Digitalisation in Practice? *International Journal of Information Systems and Project Management*, pp. 63-77.

Pernik, Piret, 2019. Cybersecurity education in Estonia: Building competences for internal security personnel. *Proceedings*, 18, pp. 71-108.

Politsei- ja Piirivalveamet, 2021. *IT-kuriteod*. [Võrgumaterjal] Leitav: https://www2.politsei.ee/et/nouanded/it-kuriteod/ [Kasutatud 19. 05. 2021].

Praxis, 2019. Küberturbe valdkonna tööjõuvajaduse ja hariduse uuring. [Võrgumaterjal] Leitav: http://www.praxis.ee/wp-content/uploads/2018/04/Küberturbe-uuring_aruanne-23_04_2019.pdf [Kasutatud 19. 05. 2021].

Rand Europe, 2020. The Future of Cybercrime in Light of Technology Developments. [Võrgumaterjal] Leitav: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA100/RRA137-1/RAND_RRA137-1.pdf [Kasutatud 19. 05. 2021].

Riigi Infosüsteemide Amet, 2020. *Riigi Infosüsteemide Ameti aastaraamat 2020*. [Võrgumaterjal] Leitav: https://www.ria.ee/sites/default/files/ria_aastaraamat_2020_48lk_est_veeb.pdf [Kasutatud 19. 05. 2021].

Riigi Infosüsteemide Amet, 2021. *Küberintsidentide käsitlemine CERT-EE.* [Võrgumaterjal] Leitav: https://www.ria.ee/et/kuberturvalisus/cert-ee.html [Kasutatud 19. 05. 2021].

Riigikantselei, 2017. *Riigikaitse arengukava 2017-2026 arengukava avalik osa.* [Võrgumaterjal] Leitav: https://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/rkak_2017_2026_avalik_osa.pdf [Kasutatud 19. 05. 2021].

Rocha Flores, W., Holm, H., Svensson, G., 2014. Usuing phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management & Computer Security*, 22(4), pp. 393-406.

Sardar, I., Ghafir, I.,Prenosil, V., Saleem, J., Hammoudeh,M., Faour, H., Jabbar, S., Baker, T., 2018. Security threats to critical infrastructure: the human factor. *The Journal of Supercomputing*, 74, pp. 4986-5002.

Secara, I.-A., 2020. Zoombombing – the end-to-end fallacy. *Network Security*, 8, pp. 13-17.

Sethurman, S.C., Vijayakumar, V., Walczak, S., 2020. Cyber Attacks on Healthcare Devices Using Unmanned Aerial Vehicles. *Journal of Medical Systems*, 44(29), pp. 1-10.

Sicari, S., Rizzardi, A., Grieco, L.A., Coen-Porisini, A., 2015. Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, pp. 146-164.

Siseministeerium, 2020. *Siseturvalisuse Arengukava 2020-2030 eelnõu.* [Võrgumaterjal] Leitav: https://www.siseministeerium.ee/sites/default/files/dokumendid/STAK/STAK2/04082020_eelnou_siseturvalisuse_programm_2020-.docx [Kasutatud 19. 05. 2021].

Smith, K. T., 2020. Marketing via smart speakers: what should Alexa say? *Journal of Strategic Marketing*, 28(4), pp. 350-365.

Statista, 2020. *Share of household in selected European countries with internet access in 2020.* [Võrgumaterjal] Leitav: https://www.statista.com/statistics/185663/internet-usage-at-home-european-countries/ [Kasutatud 19. 05. 2021].

Statista, 2021. *Number of smartphone users worldwide from 2016 to 2023 (in billions).* [Võrgumaterjal] Leitav: https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ [Kasutatud 19. 05. 2021].

Syrjälä, L., Ahonen, S., Syrjäläinen, E., Saari, S., 1994. *Laadullisen tutkimuksen työtapoja*. Rauma: Kirjayhtymä.

Zhou, J., Cao, Z., Dong, X. & Vasilakos, A.-V., 2017. Security and Privacy for Cloud-Based IoT: Challanges, Countermeasures, and Future Directions. *IEEE Communications Magazine*, 55(1), pp. 22-36.

TalTech, 2019. *Estonian Cybersecurity R&D Concept*. [Võrgumaterjal] Leitav: https://www.mkm.ee/sites/default/files/content-editors/failid/E_riik/estonian_cybersecurity_rd_concept.pdf [Kasutatud 19. 05. 2021].

Tewari, A. & Gupta, B.B., 2020. Security, privacy and trust of different layers in Internet of Things (IoTs) framework. *Future Generation Computer Systems*, 108, pp. 909-920.

Traub, C.H. & Lipkin J., 1998. If we are digital: Crossing the Boundaries. *Leonardo*, 31(5), pp. 363-366.

Tweneboah-Koduah, S., Skouby, K.E., Tadayoni, R., 2017. Cyber Security Threats to IoT Applications and Service Domains. *Wireless Personal Communications*, 95(1), pp. 169-185.

UK Government, 2018. *Code of Practice for Consumer IoT Security.* [Võrgumaterjal] Leitav: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf [Kasutatud 19. 05. 2021].

Vabariigi Valitsus, 2018. *Eesti Infoühiskonna Arengukava 2020.* [Võrgumaterjal] Leitav: https://www.mkm.ee/sites/default/files/eesti_infouhiskonna_arengukava.pdf [Kasutatud 19. 05. 2021].

Warf, Barney, 2011. Geographies of global Internet censorship. *GeoJournal*, 76(1), pp. 1-23.

Washington Post, 2015. *A Flaw in the Design: The Internet's founders saw its promise but didn't forsee users attacking one another.* [Võrgumaterjal] Leitav: https://www.washingtonpost.com/sf/business/2015/05/30/net-of-insecurity-part-1/ [Kasutatud 19. 05. 2021].

We Are Social, 2019. *Digital 2019: Global Internet Use Accelerates.* [Võrgumaterjal] Leitav: https://wearesocial.com/blog/2019/01/digital-2019-global-internet-use-accelerates [Kasutatud 19. 05. 2021].

Williams, J. L., 2016. Privacy in the Age of the Internet of Things. *Human Rights*, 41(4), pp. 14-16.

Windley, P.J., 2005. *Digital Identity*. Sebastopol, CA: O'Reilly Media,Inc.

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

LISA 1. ASAJDE INTERNETI SÜSTEEMI JA SEADMETEGA SEOSTUVAD RÜNDED.

Tabel. Asjade internet süsteemi ja seadmetega seostatavad ründed (Lin *et al.* 2017, pp. 1132-1134; Tewari & Gupta, 2020, pp. 910-912).

Asjade interneti arhitektuuriline kiht	**Rünnak, mis võib kihi kaudu teoks saada**
Tajuvuskiht/ andurikiht	**Sõlmede hõivamise rünnakud** (ingl n*ode Capture Attacks*), mille raames võib pahatahtlik häkker hõivata ja juhtida asjade interneti süsteemis asuvat konkreetsele ülesandele pühendunud programmi või seadet, asendades kogu programm seadmes ka füüsiliselt või muutes programmi või selle seadme riistvara.
	Pahatahtliku koodi sisestamise rünnakud (ingl *malicious code injection attacks*), mille raames sisestab pahatahtlik häkker programmi või seadmesse koodi, mille abil saab täita seadmes teatud funktsioone. Sellisel juhul lisab häkker olemasolevale süsteemile tülika sõlme, mille kaudu saab häkker pahatahtlikke koode ja teavet võrgus levitada, nakatades nii kogu süsteemi.
	Valeandmete sisestamise rünnakud (ingl *False data injection attacks*), mille raames saab programmi või seadme abil pahatahtlik osapool lisada valeandmeid hõivatud programmi või seadme poolt mõõdetud tavapäraste andmete asemel ja edastada valeandmed asjade interneti rakendustele, tekitades olukorra, kus asjade interneti rakendused võivad anda tagasi valesid käske või pakkuda valesid teenuseid.
	Kordusrünnakud (ingl *replay attacks*) – seadmes saab pahatahtlik häkker korrata eelmist sõnumit sihtprogrammile, et see kahjustaks võrgu usaldus ja autentimisskeeme.
	Krüptoanalüüsi rünnakud ja kõrvalkanalirünnakud (ingl *cryptanalysis attacks and side channel attacks*) – selle rünnaku tulemusena võib pahatahtlik häkker saada krüptoteksti või lihteksti abil järeldada krüpteerimisalgoritmis kasutatavat krüptovõtit.
	Pealtkuulamine ja häired (ingl *eavesdropping and interference*) – asjade interneti seadmed on suhtlemas võrkude kaudu ning nende haavatavus seisneb selles, et juhtmevabades seadmetes edastatud teavet saavad kolmandad osapooled pealt kuulata.
	Unerežiimi rünnakud (ingl *sleep deprivation attacks*) **–** üldjoontes on asjade interneti seadmetel madal energiavõime ning seadmed jälgivad elutsükli pikendamise eesmärgil unerežiimi. Rünnak režiimi toimimise vastu võib lühendada seadme eluiga.
Vahevarakiht	**DDoS-rünnakud** (ingl *DDoS attacks*) – rünnaku korral kasutatakse asjade interneti seadme ressursse selleks, et rünnata võrguprotokolle või tekitada võrgus suur liiklus, muutes sellega asjade interneti süsteemide teenused kättesaamatuks.
	Võltsrünnakud (ingl *spoofing attacks*), mille eesmärk on, et vastane saaks täieliku juurdepääsu asjade interneti süsteemile ning saadaks süsteemi pahatatlikke andmeid.
	Sinkhole rünnakud (ingl *sinkhole attacks*), mille korral nõuab seade suuri võimu-, arvutus- ja sidevõimalusi ning kutsub võrgus asuvaid seadmeid edastama andmeid läbi haavatud seadme.

	Ussiaugu rünnakud (ingl w*ormhole attacks*), mille korral kaks seadet saavad vahetada teavet privaatsete linkide teel.
	"Mees-keskmes-rünnak" (ingl *man in the middle*), mille korral võib pahatahtliku häkkeri seade olla paigutatud võrgus niiöelda kahe seadme vahele, saades sellega ligipääs keskse seadmena andmete salvestamiseks ja edastamiseks.
	Informatsioonirünnakute marsruutimine (ingl *routing information attacks*), mille korral saab pahatahtlik häkker seadme teabega manipuleerida ning tekitada seadmete vahel viivitusi.
	Sybil rünnakud (ingl *Sybil attacks*), mille korral ründaja õõnestab võrguteenuse mainesüsteeme, luues pseudonüümseid identiteete, saades selle teel mõju.
	Volitamata juurdepääs (ingl *unauthorized access*), mille korral RFID-märgendite kaudu on võimalik saada juurde salvestatud teabele.
Rakenduskiht	**Õngitsusrünne** (ingl *phishing attack*), mille korral pääsetakse ligi konfidentsiaalsetele andmetele, näiteks identifitseerimisandmetele ja paroolidele.
	Pahatahtlik viirus (ingl *malicious virus/worm*), mille korral pahatahtlik häkker nakatab asjade interneti seadme ning seeläbi saab juurde konfidentsiaalsetele andmetele või võimalusele neid muuta.
	Pahatahtlikud skriptid (ingl *malicious scripts*), mille korral lisatakse süsteemidesse seadme kahjustamise eesmärgil skriptid.

LISA 2. INTERVJUUDES OSALENUD EKSPERDID

Tabel. Intervjuudes osalenud eksperdid (autori koostatud).

Kood	Nimi	Intervjueeritava organisatsioon, ametipositsioon	Intervjuu läbiviimise keskkond	Intervjuu kestvus
E1	Klaid Mägi	Cyber4Dew, küberturbe ekspert	Zoom	1h 19min
E2	Elari Kasemets	Politsei- ja piirivalveamet, politseinõunik	Zoom	45min
E3	Martin Sepp	Majandus- ja kommunikatsiooni-ministeerium, Riikliku Küberturvalisuse Osakond, Küberriskide halduse juht	Microsoft Teams	1h 7min
E4	Priit Kleemann	Politsei- ja Piirivalveamet, infoturbetalituse juhataja	Skype for Business	1h 6min
E5	Tõnu Tammer	RIA intsidentide käsitlemise osakond, osakonnajuhataja (CERT-EE juht)	Microfoft Teams	58min
E6	Anonümis eeritud	Siseministeerium	Microfoft Teams	45min
E7	Rein Põdra	Majandus- ja Kommunikatsiooniministeerium, nõunik	Microfoft Teams	44min
E8	Anonümis eeritud	Siseministeerium	Skype for Business	1h 3min
E9	Markko Künnapu	Justiitsministeerium, nõunik	Zoom	58min
E10	Anonümis eeritud	Politsei- ja Piirivalveamet	Meilitsi	
E11	Uku Särekanno	Euroopa Liidu Küberturvalisuse Amet, IT Agentuuri tugiüksuse juht	Microsoft Teams	1h 1min
E12	Einar Laagriküll	Siseministeeriumi infotehnoloogia- ja arenduskeskus, peadirektori asetäitja baasteenuste valdkonnas	Microsoft Teams	47min
E13	Urmo Parm	Andmekaitse Inspektsioon, tehnoloogia nõunik	Zoom	1h 1min

LISA 3. DOKUMENDIANALÜÜSIS KASUTATUD MATERJALID.

Tabel. Dokumendianalüüsis kasutatud dokumendid.

Kood	Organisatsioon	Dokumendi nimetus
KD1	Majandus- ja Kommunikatsiooni-ministeerium	Küberturvalisuse Strateegia 2019-2022
KD2	Vabariigi Valitsus	Eesti Infoühiskonna Arengukava 2020
KD3	Siseministeerium	Siseturvalisuse Arengukava 2020-2030 eelnõu
KD4	Kaitseministeerium	Riigikaitse arengukava 2017-2026 avalik osa
KD5	E-riigi Akadeemia	Küberturvalisuse käsiraamat
KD6	TalTech	Estonian Cybersecurity R&D Concept (ingl)
RD7	European Comission	The EU's Cybersecurity Strategy for the Digital Decade (ingl)
RD8	ENISA	Good Practices for Security of IoT (ingl)
RD9	Rand Europe	The Future of Cybercrime in Light of Technology Developments (ingl)
RND10	Government of Canada	Internet of Things (IOT) Checklist for Consumers (ingl)
RND11	Government of the United Kingdom	Guidance: Code of Practice for Consumer IoT Security (ingl)
RND12	Australian Government	Code of Practice: Securing the Internet of Things for Consumers (ingl)

LISA 4. DOKUMENDIANALÜÜSI KOODIPUU.

Name	Files	References
1. Asjade interneti mõiste ning määratlus eri dokumentides.	9	41
1.1 Asjade interneti mõiste ja määratlus Eesti digiarenguga seotud dokumentides.	3	12
1.2 Asjade interneti mõiste ja määratlus rahvusvahelistes digiarenguga seotud dokumentides.	5	13
1.3 Asjade interneti kasutusvaldkonnad, seadmete näited ning arvukus.	9	16
2. IKT ja asjade interneti põhjustatud digiarengu probleemid.	11	142
2.1 Peamised digiarengust tulenevad probleemid.	7	122
2.1.1 Probleemid tavainimestele.	5	15
2.1.2 Probleemid riigile ja ametiasutustele.	7	107
2.2 Asjade interneti seadmetest ja selle tehnoloogia arengust tulenevad probleemid.	8	20
Küberründed	5	13
Seadmed	6	7
3. Konfidentsiaalsuse, terviklikkuse ja käideldavuse määratlus dokumentides.	6	23
Käideldavus asjade interneti tehnoloogia korral	1	3
Käideldavus üldiste IKT tehnoloogiate korral	3	3
Konfidentsiaalsus asjade interneti tehnoloogia korral	2	4
Konfidentsiaalsus üldiste IKT tehnoloogiate korral	2	2
Terviklikkus asjade interneti tehnoloogia korral	3	9
Terviklikkus üldiste IKT tehnoloogiate korral	2	2
4. Soovitused asjade interneti seadmete turvaliseks kasutamiseks.	7	49
Asjade interneti seadmetega seonduvad soovitused seadmete ja teenuste tootjatele.	4	36
Asjade interneti seadmetega seonduvad soovitused tavakasutajatele.	2	10
Asjade interneti seadmetega seonduvalt soovitused riiklikult seotud osapooltele.	3	3
5. Soovitused digiarengust tulenevate probleemide lahendamiseks.	7	126
Ettevõtlus	5	10
IT-lahendused	2	7
Poliitika kujundamine	5	33
Rahvusvaheline koostöö	5	21
Ressurss	1	1
Sisejulgeoleku asutused ja küberkuritegevus	3	28
Teadmised ja oskused	3	6
Teadus- ja arendustegevus	4	19
Tööjõud	1	1

LISA 5. EKSPERTINTERVJUUDE KOODIPUU.

Name	Files	References
1. Asjade interneti mõiste ja määratlus ekspertintervjuudes.	13	89
1.1 Asjade interneti definitsioon.	13	33
1.2 Ekspertide välja toodud asjade interneti seadmete näited.	13	24
1.3 Asjade internet digiarengu dokumentide ja käimasolevate tegevuste valguses.	11	32
2. IKT kui keskse tehnoloogia vaatest probleemsed aspektid.	13	67
2.1 Ebapiisav ennetustöö.	7	8
2.2 Inimeste ebapiisav teadlikkus.	11	22
2.3 Inimeste puudulikud oskused.	5	7
2.4 Avaliku sektori korralduslikud puudujäägid.	7	13
2.5 Seadmete ebakvaliteetsusele viitav taust.	11	17
3. Asjade interneti tehnoloogiast tulenevad probleemid.	13	120
3.1 Peamised asjade interneti tehnoloogia probleemid.	13	41
Seadmete arvukusest tulenevad probleemid	8	12
Üldised probleemid asjade interneti vaatest lähtuvalt.	13	29
3.2 Asjade interneti turvaelementidega seotud probleemid.	12	45
Käideldavusega seonduvad probleemid	8	9
Konfidentsiaalsusega seonduvad probleemid	8	12
Privaatsusega seonduvad probleemid	9	15
Terviklikkusega seonduvad probleemid	8	9
3.3 Asjade interneti seadmete ärakasutamine ja sellega seonduvad ründed.	11	34
Näited asjade interneti seadmete ära kasutamisest	3	5
Rünnete näited	10	19
Seadmetega üles kerkivad konkreetsed küsimused	4	10
4. IKT ja asjade interneti tehnoloogiast tulenevad probleemid avalikule sektorile.	11	40
4.1 Kompetentsi probleemid.	9	11
4.2 Koostöö probleemid.	6	12
4.3 Ressursiprobleemid.	10	17
5. Soovitused asjade interneti tehnoloogia valguses.	13	102
5.1 Soovitused ametiasutustele.	13	71
5.2 Soovitused tehnoloogia kasutajatele.	12	31

LISA 6. EKSPERTINTERVJUUDE ÜLDKÜSIMUSED JA TÄIENDMÄRKMED.

Uurimisküsimus	Ekspertintervjuu küsimus
1. Kuidas defineerivad kohalikud ja rahvusvahelised dokumendid ning Eesti eksperdid mõistet *Internet of Things* (ingl) ning kuhu liigitub mõiste digitehnoloogia probleemide keskel?	Kuidas mõistate mõistet *Internet of Things*?
	Milline võiks olla mõiste eestikeelne tõlge?
	Millised seadmed teile mõistega seonduvad?
	Milline seos on asjade interneti seadmetel teiste tehnoloogiliste lahendustega? Täiend: Ühisosa? Erinevused?
2. Missuguseid probleeme toob kaasa asjade interneti tehnoloogia avalikule sektorile, sealhulgas küberkuritegusid ning küberintsidente lahendavate ametiasutuste jaoks kuritegude olemusest ning nende lahendamiseks vajaminevast kompetenstist lähtuvalt?	**Milline võib olla asjade interneti seadmetega kaasnevate ohtude iseloom?** Täiend: Globaalsus? Lokaalsus? Täiend: Millega peaks globaalsuse raames arvestama?
	Milliseid probleeme võivad asjade interneti seadmed esile tuua küberintsidente ja küberkuritegevust lahendavatele ametiasutustele?
	Kuidas ning mil viisil on Eesti pööranud siiani tähelepanu asjade internetile? Täiend: Asjade internetiga kaasnevatele probleemidele? Täiend: Ennetus? Täiend: Mis on jäänud tegemata? Täiend: Euroopa? Maailm? (Näited)
	Mil viisil mõjutavad asjade interneti seadmetega kaasnevad probleemid küberintsidentide ja küberkuritegevusega tegelevaid ametiasutusi?
3. Milliseid probleeme toovad olemasolevad kohalikud ja rahvusvahelised kübervaldkonna dokumendid ning Eesti eksperdid	**Millised üldised kübervaldkonna ohud ja riskid on täna kõige levinumad?** Täiend: IKT-seadmete korral?
	Millised üldisest vaatest lähtuvad kübervaldkonna ohud ja riskid võivad olla omased ka asjade interneti seadmetele?
	Millised kübervaldkonna ohud ja riskid võivad vaid asjade interneti seadmetele omased olla?

välja üldisi IKT- ja asjade interneti seadmeid silmas pidades?	**Kuidas ning mil viisil on Eesti pööranud siiani tähelepanu üldisi IKT-seadmeid silmas pidades?** Täiend: IKT-seadmetega kaasnevatele probleemidele? Täiend: Ennetus? Täiend: Mis on jäänud tegemata? Täiend: Euroopa? Maailm? Täiend: Positiivsed näited?
4. Mida peavad poliitikakujundajad ja seadmete kasutajad asjade interneti seadmeid silmas pidades tegema, et maandada kasutusega ilmnevaid riske?	**Mida tuleb asjade interneti seadmeid silmas pidades nendega seonduvate riskide maandamiseks tavainimese jaoks teha?**
	Mida tuleb asjade interneti seadmeid silmas pidades nendega seonduvate riskide maandamiseks riigina teha?
	Milliseid soovitusi annaksite asjade interneti seadmete turvaliseks kasutamiseks tavakasutajatele?