TARTU ÜLIKOOL

Majandusteaduskond

Martha Jung

KÜBERTURBE INVESTEERINGUTE PROBLEEMID JA MEETMED TURBEINVESTEERINGUTE SOODUSTAMISEKS EESTI AVALIKU SEKTORI ORGANISATSIOONIDE PÕHJAL

Magistritöö

Juhendaja: professor Kadri Ukrainski

Tartu 2020

Suunan kaitsmisele ……..

(juhendaja allkiri)

Olen koostanud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite tööd, põhimõttelised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

……..

(töö autori allkiri)

SISUKORD

SISSEJUHATUS

Kaasaegse maailma üheks toimimise aluseks võib pidada info- ja kommunikatsioonitehnoloogilisi (IKT) lahendusi. Infotehnoloogialahendusi kasutatakse igapäevaselt nii eraisikute, ettevõtete kui riikide tasandil, aina keerulisem on eristada digitaalset ja n-ö pärismaailma (Riigi Infosüsteemi Amet 2020: 4). Küberruumis valitsevate ohtudega tegelemiseks pööratakse rohkem tähelepanu küberturvalisusele, mille kaudu tagatakse digitaalse informatsiooni konfidentsiaalsus, terviklus ja käideldavus ehk korrektse, täpse ja täieliku informatsiooni õigeaegne kättesaadavus vaid selleks ettenähtud inimestele. Probleemid informatsiooni konfidentsiaalsuse, tervikluse või käideldavusega võivad (ajutiselt) katkestada (äri)tegevuse.

Eesti ühiskond on edukalt lõiminud IT-lahendused oma igapäevatoimimisse, rahvusvaheliselt on Eesti digiriigi ja e-süsteemide maine ning rahva seas usaldus süsteemide suhtes kõrge. Eesti digitaalne riik on toiminud juba üle 20 aasta ning küberturvalisus omab suurt osatähtsust Eesti riigi ja majanduse toimimises ning julgeolekus (Küberturvalisuse strateegia… 2019: 7). Küberturvalisuse strateegia 2019-2022 (2019: 7) alusel on Eesti digiriigi ühe osa, eID ökosüsteemi, majanduslik kogumõju hinnanguliselt ligikaudu 800-1500 miljonit eurot ehk 4-7% SKP-st. Arenenud ökosüsteem, hea tehnoloogiline teadmus ja tugev maine ei kindlusta head positisooni edaspidiseks: küberruumi kiire ja raskesti prognoositav areng eeldab pidevat panust valdkonna arendamisse.

Käesoleva töö eesmärgiks on selgitada välja Eesti avaliku sektori organisatsioonide küberturbeinvesteeringute takistusi ja pakkuda akadeemilises kirjanduses kirjeldatud poliitinstrumentide näol lahendusi, mis sobiksid Eesti konteksti. Töö on fokuseeritud eelkõige sellistele organisatsioonidele, mis tegelevad küberturbe tagamisega kindlas valitsemisalas või valitsemisalade üleselt, kuna nende mõju küberturbele avalikus sektoris on suurim.

Eeltoodud töö eesmärgi täitmiseks on püstitatud järgmised uurimisülesanded:

- selgitada küberturvalisuse olemust, olulisust ning küberturvalisuse valdkonda mõjutavaid turutõrkeid;
- analüüsida küberturbeinvesteeringute otsustusprotsesse organisatsiooni tasandil ning selgitada avaliku ja erasektori otsustusprotsesside erinevusi;
- tuua välja akadeemilises kirjanduses pakutud meetmeid, mis aitaksid lahendada turutõrgetest tekkivaid probleeme küberturbe valdkonnas, sh investeeringute kvaliteeti;
- viia läbi intervjuud Eesti avaliku sektori asutuste esindajatega, kes tegelevad küberturbe tagamisega, kogumaks informatsiooni Eesti küberturvalisuse hetkeolukorra kohta;
- analüüsida avaliku sektori asutuste, mis tegelevad küberturbe tagamisega, turbeinvesteeringute tausta intervjuudest kogutud info põhjal;
- tuua välja Eesti konteksti sobivaid akadeemilises kirjanduses pakutud meetmeid.

Töö teoreetilise tagapõhja moodustavad teadusartiklid ja uuringud küberturbe olemusest, ökonoomikast, organisatsioonide turbeinvesteeringute otsustusprotsessidest ning riiklikest meetmetest küberturvalisuse valdkonna investeeringute stimuleerimiseks. Kuna küberturve on infoturbe osa, mis tegeleb vaid digitaalse informatsiooni turbega ning võrreldes infoturbega on küberturbe näol tegemist uuema uurimisvaldkonnaga, siis on käesolevas töös vaadatud lisaks küberturbe investeeringute olemusele ka infoturbe investeeringute otsustusprotsesse, mõjutajaid ja valitsemist. Samuti on kasutatud teaduskirjandust, mis kirjeldab erinevusi avalikus ja erasektoris, sh IT-investeeringute tegemisel. Küberturbe eelarve kuulub IT-eelarve hulka ning võimaldab seoste loomist kitsama valdkonna kohta. Magistritöö empiirilises osas on kasutatud 2019. a jooksul IKT Arenguprogrammi raames tellitud uuringute tarbeks läbiviidud intervjuusid Eesti avaliku sektori organisatsioonide esindajatega, kes tegelevad küberturbe tagamisega enda valitsusalas või valitsusalade üleselt.

Magistritöö koosneb kahest suuremast peatükist, mis omakorda jagunevad kolmeks alapeatükiks. Esimeses, teoreetilises osas kirjeldatakse esmalt küberturbe olemust ja seoseid IT ning infoturbega ning levinumaid turutõrkeid, mis küberturbe valdkonda

mõjutavad. Seejärel vaadeldakse avaliku ja erasektori eripärasid ning turbeinvesteeringute otsustusprotsesse. Viimaks tutvustatakse teaduskirjanduses enamlevinud poliitinstrumente küberturvalisuse olukorra parandamiseks ning vaadeldakse nende rakendamist kolme riigi (Soome, Prantsusmaa ja Jaapan) põhjal. Töö teises osas kirjeldatakse esmalt täpsemalt kasutatud metoodikat ning seejärel analüüsitakse intervjuude tulemusi, hinnates nii küberturbe hetkeolukorda Eestis laiemalt kui ka asutustes endis. Lõpetuseks hinnatakse teoreetilise osa viimases alapeatükis kirjeldatud poliitinstrumente Eesti kontekstis, kasutades ka intervjueeritute sisendit meetmete hindamiseks.

Käesolevas töös on kasutatud poolstruktureeritud intervjuude meetodit. Poolstruktureeritud intervjuude meetod võimaldab küsida lisaküsimusi ning liikuda vastavalt küsitletava mõttekäigule erinevate teemade vahel. Samas võivad vastused sõltuda kontekstist ning on raskemini üldistatavad. Intervjueeritute nimesid ega asutusi töös ei avalikustata. Esiteks võimaldab anonüümsuse tagamine avatud intervjuu-õhkkonna, mis suurendab tõenäosust saada ausaid vastuseid mh ressursside, probleemide ja riskide kohta. Tulemuste üldistamine toob välja avaliku sektori küberturbe murekohad, ilma süüdistavat õhkkonda loomata. Töö autori soov on analüüsida avaliku sektori küberturbe probleeme ning teadusallikate ja intervjuude põhjal luua seoseid meetmetega, millega kitsaskohtade ulatust vähendada.

Magistritöös kasutatakse intervjuusid, mis on läbi viidud Majandus- ja Kommunikatsiooniministeeriumi IKT Arenguprogrammi (IKT valdkonna … 2018: 19) raames TalTechi küberkriminalistika ja küberjulgeoleku keskuselt tellitud uuringute jaoks. Need uuringud on Eesti küberturvalisuse võime analüüs (TalTech 2019); küberturvalisuse majandusharu kontseptsioon (TalTech 2020a); ja küberturvalisuse teadus- ja arendustegevuse kontseptsioon (TalTech 2020b). Käesoleva töö autor osales Eesti küberturvalisuse võime uuringu töögrupis ühe autorina ning oli majandusharu kontseptsiooni uuringu üks põhilisi autoreid. Autor soovib tänada Majandus- ja Kommunikatsiooniministeeriumi, kõiki intervjueerituid, TalTechi küberkriminalistika ja küberjulgeoleku keskuse uurimisgruppi ning magistritöö juhendajat prof. Kadri Ukrainskit.

Magistritööga seotud märksõnad: riiklik poliitika; avalik sektor; infoturbepoliitika; investeerimiseelarve; IT valitsemine; majandusstiimulid; turutõrge

CERCS: S180

1. KÜBERTURBE OLEMUS JA TURBEINVESTEERINGUTE MÕJUTAJAD

1.1. Küberturbe olemus ja olulisus

Järgnevas alapeatükis antakse ülevaade mõistetest, mis küberturvalisuse valdkonnas enim esinevad ja selgitatakse küberturvalisuse olemust, seejärel kirjeldatakse turutõrkeid, mis küberturbe valdkonda, sh küberturbe investeeringuotsuseid, mõjutavad.

Info- ja kommunikatsioonitehnoloogiad (IKT) on viimastel aastakümnetel moodustanud olulise osa inimeste igapäevaelust ja riikide toimimisest ning on digiühiskonna alustalaks. IT-lahendused suurendavad produktiivsuse kasvu (nt läbi automatiseerimise). Küberturvalisuse kõrge tase suurendab inimeste usaldust elektrooniliste lahenduste vastu ja seeläbi julgustab IT-lahenduste kasutamist. (Bauer, J., van Eeten, M. 2011: 1) Kuigi infotehnoloogia laial kasutusel on positiivseid aspekte, nagu nimetatud produktiivsuse juurdekasv, siis kaasnevad sellega ka uued riskid ja ohud, sh küberründed ja -kuritegevus. Kuna olemasolevad süsteemid vajavad ohtude realiseerumise eest kaitset, on kasvanud küberturvalisuse valdkonna tähtsus (Christou, G. 2016: 1).

ENISA (*European Union Agency for Cybersecurity*) möönab raportis „Definition of Cyber Security – Gaps and overlaps in standardisation“ (2015: 28), et kuna küberruum on niivõrd kiirelt muutuv, siis tähendab see, et ka küberturvalisuse definitsioon on pidevas arengus. Mõistet on raske sõnastada nii, et see kataks kõiki olemasolevaid tahkusid. Ühtse mõiste puudumine võimaldab erinevaid tõlgendusi, mis mõjutavad valdkonna valitsemist (i.k. *governance)*.

Eesti küberturvalisuse strateegias 2019-2022 on defineeritud valdkonna olulisimad terminid. Esmalt defineeriti baasmõistena liide ’küber-’: „eesliide, mis tähistab „võrgu- ja infosüsteeme“ (Küberturvalisuse strateegia … 2019: 40). Küberturvalisust (i.k *cybersecurity*, ka *cyber security*), defineeritakse kui „seisundit, kus võrgu- ja infosüsteemid on kaitstud ohtude realiseerumise eest“ (*Ibid.* 2019: 40).

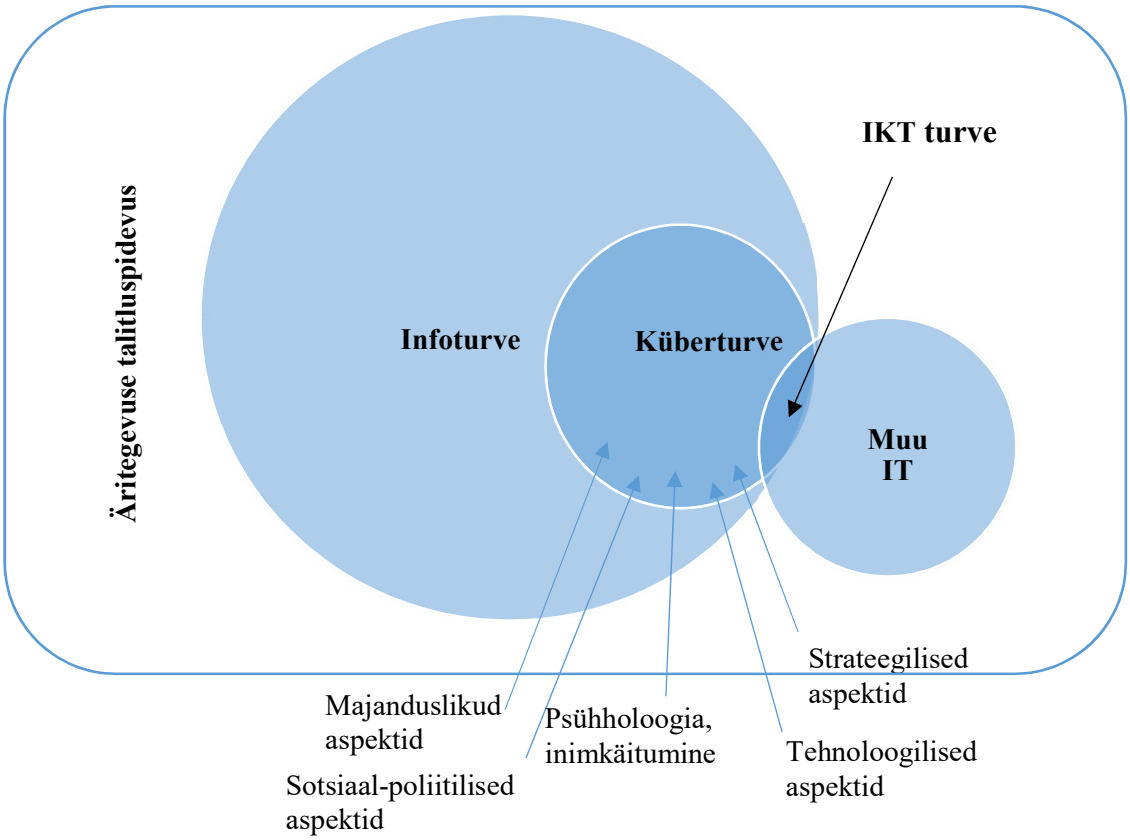
Lisaks eelnimetatud põhilistele mõistetele on käesolevas töös kasutusel veel mõisted ’küberturve’(i.k. samuti *cybersecurity*) ja ’küberkaitse’ (i.k. *cyber defence)*, mida kasutatakse sagedasti samatähenduslikena küberturvalisuse mõistele. Samas esineb mõistete kasutamisel erisusi valitsemisalade lõikes, näiteks riigikaitsevaldkonnas on enam kasutusel terminid küberjulgeolek ja -kaitse ning vähem leiab kasutust -turvalisus, samas esineb valdkondi, kus kõik mõisted on ristkasutuses. Eelnimetatud strateegia (*Ibid.* 2019: 40) järgi on küberturve meetmete rakendamise kaudu turvalisuse tagamine, küberkaitse on „meetmete rakendamine küberrünnakute ennetamiseks ja tõrjumiseks“. Kuna erinevus nimetatud mõistete vahel on marginaalne ning inglisekeelses kirjanduses vähem relevantne, siis käesolevas magistritöös on mõisted kasutusel samatähenduslikena. Strateegias defineeritud terminid on toodud magistritöö lisas 1, et hõlbustada valdkonna mõistete kättesaadavust lugejale.

Lisaks on valdkonnas kasutuses ka infoturbe (i.k. *information security)* ja IKT-turbe (i.k. *ICT security)* mõisted, mis on tihti samuti kasutuses küberturbe mõistega samatähenduslikena, kuid on tegelikult laiema tähendusega (von Solms, B., von Solms, R. 2018: 5). Küberturve on infoturbe osa (vt joonis 1): infoturve tegeleb kogu informatsiooni turvalisuse tagamisega, olenemata selle „asukohast“ või liigist, samas kui küberturve tagab digitaalse informatsiooni konfidentsiaalsuse, tervikluse ja käideldavuse (i.k *confidentiality, integrity, availability,* lühendatult *CIA*) küberruumis (von Solms, R., van Niekerk, J. 2013: 98). *CIA* tingimused on defineeritud järgmiselt (Andress, J. 2014: 6-7):

- konfidentsiaalsus – informatsiooni kättesaadavus vaid selleks autoriseeritud inimestele;
- terviklus – informatsiooni töötlemisel selle õigsuse, täpsuse ja täielikkuse tagamine;
- käideldavus – õigeaegse ligipääsu tagamine informatsioonile selleks autoriseeritud kasutajatele.

Küberturve peab tagama digitaalse informatsiooni konfidentsiaalsuse, tervikluse ja käideldavuse, kuid kõiki kolme tingimust ei saa samaaegselt täielikult täita ning tuleb leida sobiv kombinatsioon. Sobiv kombinatsioon on asutuste, info tüübi jms põhiselt erinev ning tuleb eraldi analüüsides otsustada. (von Solms, R., van Niekerk, J. 2013: 99)

IKT-turve (ka IT-turve) tegeleb riist- ja tarkvara turvalisuse tagamisega (Understanding … 2016). Joonisel 1 toodud parempoolne ring kätkeb ülejäänud IT-tegevusi, mis ei ole turbe-spetsiifilised, näiteks IT-süsteemide ülesehitust ja hooldust. Kõiki joonisel 1 kujutatud turbe tüüpe rakendades tagatakse äritegevuse järjepidevus ehk talitluspidevus. Talitluspidevust defineeritakse nii katkestusteta äritegevuse tagamisena (Finantsinspektsioon 2006: 2) kui ka katkestuse järgselt kokkulepitud tasemel tegevuse jätkamise võimekusena (Eesti Pank 2020). Küberturvalisus võimaldab muid (äri)tegevusi ning ei ole eesmärk omaette (Griffith 2018: 6).



Joonis 1. Info- ja küberturbe seosed, küberturvet mõjutavad aspektid (von Solms, B., von Solms, R. 2018: 5 põhjal autori koostatud). Tegemist on ühe võimaliku käsitlusega omavahelistest seostest.

Küberturvalisuse valdkond on distsipliinide ülene (i.k. *interdisciplinary*), hõlmates endas aspekte infotehnoloogiast, juurast, sotsiaal-poliitikast, majandusest, psühholoogiast ja mujalt (Craigen, D. *et al.*, 2014: 13). Craigen *et al.* (2014:13) väidavad, et erinevate valdkondade mõjusid kirjeldava küberturbe definitsiooni puudumine viib eelkõige küberturbe tehnoloogiakeskse vaateni ja IT probleemide lahendamiseni.

Küberturvet võib omakorda alamkategooriateks jagada. Järgnev põhineb ENISA raportil (ENISA 2015: 11), kuid esineb ka teistsuguseid liigitusi. Küberturve jaguneb:

- kommunikatsioonide turve – IT-süsteemide tehnilise infrastruktuuri kaitsmine pahatahtlikel eesmärkidel selle omaduste muutmise eest;
- operatsioonide turve – töövoogude kaitse turvaintsidentide eest;
- infoturve – digitaalse informatsiooni konfidentsiaalsuse, tervikluse ja käideldavuse kaitse;
- füüsiline turve – IT-süsteemide kaitse füüsiliste turberikkumiste eest;
- riiklik julgeolek – kaitse küberruumist lähtuvate rünnete eest, mis võivad mõjutada poliitilist või sõjalist olukorda.

Eelkõige viimane alagrupp, aga osaliselt ka teised küberturbe kategooriad, kuuluvad sisejulgeoleku- ja kaitsepoliitika valitsemisaladesse. Seega tuleb erinevate riikide küberturbe dokumentide või süsteemide võrdlevanalüüse koostades arvestada, et riigiti võib rõhuasetus olla erinev ning paljud dokumendid ei pruugi olla (täielikult) avalikud (Griffith 2018: 8). Samas võib see ka viia selleni, et samalaadsete murekohtadega tegelevad paralleelselt erinevate valitsusalade asutused ning koostöö puudumisel viib see ressursside raiskamise ja potentsiaalselt konfliktideni.

Küberturbe puhul on oluline rõhutada, et täielik turvalisus ei ole soovitav: eksisteerib riskide optimaalne tase, kus tehingu kasulikkus kaalub üles riski vähendamise, mida saavutaks lisaühiku turbemeetmega (Moore, T. 2010: 106). Turutõrked võivad takistada optimaalse turbetaseme saavutamist (Bauer, J., van Eeten, M. 2011: 4). Jentzsch (2016: 8) on loetlenud küberturbe turu omadused, mis muudavad selle teistest eristuvaks:

- küberturbe toodete ja teenuste immateriaalsus;
- kaitstavate varade (nt informatsiooni) mittemateriaalsus ja keerukus;
- ristsõltuvus erinevate turu osapoolte vahel ehk ühe osapoole turvalisus sõltub teiste otsustest.

Küberturbe valdkonda mõjutavad tugevalt erinevad turutõrked. Turutõrge esineb, kui ressursside jaotus ei toimu osapoolte vahel parimal võimalikul viisil ja see viib heaolukaoni. Turbeteenuste ja -toodete puhul vähendavad turutõrked investeerimisstiimulit ja turbeprotseduuride rakendamist. (Jentzsch, N. 2016: 21)

Küberturvalisusel on nii avaliku kui erahüvise omadusi (Bauer, J., van Eeten, M. 2011: 3). Avalikud hüvised on mitte-eristavad ehk kõigile kättesaadavad ja ei kaota oma väärtust tarbijate arvust hoolimata. Klassikaline näide avalikust hüvisest on puhas õhk, küberturvalisuse vaatenurgast on nii informatsioon kui ka turvalisus avalikud hüvised. Juba avalikustatud informatsiooni jagamist on raske kontrollida. Ühest küljest võivad seda kasutada pahatahtlikud osapooled, teisalt tekitab see ka teistes turu osapooltes „tasuta sõitmise" (i.k. *free riding*) soovi. See võib kaasa tuua ala-investeerimise, näiteks küberturvalisuse valdkonna T&A-tegevusse. Samasugune probleem on ka turvalisusega – ühe osapoole turbeinvesteeringud mõjutavad vähemalt osaliselt ka teisi turuosalisi. (Jentzsch, N. 2016: 24)

Informatsiooni asümmeetria on olukord, kus turuosalised peavad tegutsema mittetäieliku informatsiooniga: ühel osapoolel on selles olukorras teistest kas rohkem informatsiooni või on kõigi turu osapoolte jaoks informatsioon ühtlaselt kättesaamatu. Küberturvalisuse valdkonnas puudub tahe avalikustada intsidente, tuvastatud haavatavuste või turbe rikkumiste (i.k. (*security) breach*) informatsiooni, kuna see toob kaasa mainekahju. Avalikustamist saab motiveerida stiimulitega, millega vähendatakse või tasakaalustatakse tajutavat kahju. Raske on hinnata ka avalikustatud rünnete informatsiooni täielikkust (Aggarwal, V. K., Reddie, A. W. 2018a: 9), näiteks parema mulje jätmiseks võidakse tagajärgi pisendada. Aina enam avalikustavad hoopis kurjategijad väidetavate rünnakute kohta infot: näiteks lunavararünnak ettevõtte LG vastu avalikustati ründajate poolt juunis 2020, kuid ettevõte ei ole ka kuid hiljem avalikult seda rünnakut kommenteerinud (Olukord küberruumis … 2020: 4). Ebapiisav informatsioon võib jätta petliku mulje turvalisusest, mis vähendab organisatsioonide turbeinvesteeringute vajaduse hinnanguid (Jentzsch, N. 2016: 21). Samuti on kvaliteetset informatsiooni vaja õigete turbemeetmete valimiseks ja nende kasulikkuse hindamiseks (Aggarwal, V. K., Reddie, A. W. 2018a: 9).

Informatsiooni asümmeetria ei too tingimata kaasa ala- või üleinvesteerimist, küll aga muudab see riskide õige hindamise raskeks ehk tõenäosus õigesse kohta vajalikus proportsioonis investeerida väheneb (Moore, T. 2010: 106). Juba 2010. a täheldas T. Moore (2010: 106), et vaja on lahendusi, mis muudaksid usaldusväärse informatsiooni

kättesaadavaks. Vastasel juhul ei rakendata vajalikke küberturbe mehhanisme, kuna olemasolevad andmed ei kinnita ohtude tõsidust.

Informatsiooni asümmeetria soodustab moraaliriski (i.k. *moral hazard*) teket. Moraaliriskiga kirjeldatakse suurema riski võtmise motivatsiooni, kui riskiga kaasnevate kulude eest ollakse kaitstud. Moraalirisk on küberturbe valdkonnas tihedalt seotud (negatiivsete) välismõjudega: paljud ettevõtted on teadlikud turbenõrkustest, aga riskiga kaasnevaid kulusid kannavad kasutajad. (Jentzsch, N. 2016: 22) Näiteks Cambridge Analytica kogus Facebooki süsteemide ülesehituse tõttu 87 miljoni Facebooki kasutaja isiklikke andmeid, millega mõjutati poliitilisi protsesse. Facebook sai küll mainekahju osaliseks, kuid kahju kandsid eelkõige kasutajad ja ühiskond, mille protsesse mõjutati. (Vagle, L. 2020: 94)

Suure osa küberturbe tehnoloogiate kasulikkus sõltub kasutajate hulgast: mida suurem see on, seda suuremad on kättesaadavuse ja ühilduvuse kaudu positiivsed välismõjud. Seda kirjeldab kõige efektsemalt sotsiaalvõrgustike fenomen, mille populaarsus sõltub lisaks funktsionaalsusele ka sellest, kui palju inimesi juba sellega liitunud on. (Moore, T. 2010: 107) IKT-tehnoloogiate puhul on kriitiline kasutajate mass väga oluline, kuid võib lisaks positiivsetele välismõjudele kaasa tuua ka negatiivseid (nt võrguliikluse ummistumine) (Jentzsch, N. 2016: 23). Võrgustikuefekt (i.k. *network effect*) ja kasutajate käitumine soodustavad IT-monokultuuride teket, mis pikas perspektiivis viivad loomulike monopolideni (ehk mittetäielik konkurents, mis on omakorda turutõrge). Suurfirmad (nagu Apple, Facebook, Google, Microsoft jt) on ehitanud üles toote- ja teenuskeskkonnad või ostnud üles võimalikud konkurendid, mis ei võimalda uutel tulijatel turule lisanduda ja soodustavad monopoolset hinnapoliitikat. Huvitaval kombel on sellel ka otsesemad mõjud küberturbele: kui konkurents puudub või on minimaalne, puudub ka turvalisuse arendamise konkurents (Aggarwal, V. K., Reddie, A. W. 2018a: 9).

Välismõjude tõttu on küberturbe tehnoloogiate vahel ümberlülitumine tülikas ning tekib tehnoloogiline lukustumine. Lisaks tegelikele ümberlülitumise kuludele nagu ostuhind, rakendamiseks tehtavad kulud jms, on olulised ka tajutavad kulud. Nendeks võivad olla tunnetuslik pingutus (nt ajakulu), et uut süsteemi tundma õppida. Seega võib mõne vana tehnoloogia suur kasutajate hulk muutuda uute tehnoloogiate jaoks sisenemisbarjääriks.

(Jentzsch, N. 2016: 23) IT-valdkonna suurfirmade (vt eelmine lõik) platvormid peavad kasutajamugavuse nimel olema omavahel ühilduvad (i.k. *interoperability*), kuid see suurendab võrgustikuülese nakatumise tõenäosust (Aggarwal, V. K., Reddie, A. W. 2018a: 9). IT-ettevõte teenib partnerite platvormide ühildumise kaudu tulu: kui ettevõte otsustaks suurendada turvanõudeid partnerite suhtes, et need võiksid ühilduda (nt Google platvormiga), siis kaotavad nad nõudeid mittetäitvate partnerite ärakadumise tõttu tulu. Küberturvalisuse tase võrgustikus on alati võrdne nõrgima lüli turvalisuse tasemega, aga eelkirjeldatud olukord ei soosi esimesena turvalisustaseme tõstmist (i.k. *first mover disadvantage)*. (*Ibid*. 2018: 9)

Küberturvalisuse valdkonnas on kasutusel erinevaid mõisteid, mida käesolevas alapeatükis lühidalt kirjeldati, ning arusaamatusi tekitab mõistete ristkasutus ka teaduskirjanduses. ENISA küberturbe definitsioonide kirjeldav väljaanne (ENISA 2015: 10) toob humoorikalt välja, et kui inglise keeles ei suudeta isegi kokku leppida, kas kasutatakse *cyber security* või *cybersecurity*, siis ei ole realistlik leida ühist definitsiooni või defineerida, mis moodustab küberruumi. Küberturbe valdkonnas esinevad kõik peamised turutõrked: avalike hüviste pakkumine, informatsiooni asümmeetria ja moraalirisk ning välismõjud.

1.2. Küberturbeinvesteeringute otsused organisatsiooni tasandil

Alapeatükis antakse ülevaade era- ja avaliku sektori organisatsioonide omadustest ning organisatsioonide küberturbe investeeringu otsuste alustest. Esmalt vaadeldakse avaliku ja erasektori eripärasid ning seejärel kirjeldatakse turbeinvesteeringute otsustusprotsesse.

Joon era- ja avaliku sektori vahel ei ole tingimata enesestmõistetav ja erisusteta. Peamisteks eristavateks teguriteks peetakse eraettevõtte poolt vaadates omanikke (organisatsioon pole riiklikus omanduses) ning kasumile orienteeritust. Avaliku sektori asutused sõltuvad üldiselt valitsuse eelarvelisest jaotusest. Käesolevas töös lähtutakse ülaltoodud lihtsustusest, mööndes, et on olemas erandeid, näiteks mittetulundusühingute või riigiettevõtete näol, mida siinkohal ei vaadelda. (Campbell, J. *et al.* 2009:7)

Alltoodud tabel 1 kirjeldab avaliku ja erasektori asutusi iseloomustavaid tegureid, mis mõjutavad vastavate asutuste otsustusprotsesse.

Tabel 1. Era- ja avaliku sektori eripärad

Eripärad	Erasektori asutus	Avaliku sektori asutus
Eesmärgid	Konkreetsed, materiaalsed	Avaliku hüve pakkumine, tihti immateriaalne
Huvigrupid	Konkreetsed, vähe	Palju, vastandlike soovidega
Riskitundlikkus	Madal	Kõrge
Keskkond	Pigem vähe reguleeritud Turu mõjud	Reguleeritud mitmete juriidiliste ja bürokraatlike piirangutega Poliitilised mõjud
Mõõdikud	Efektiivsus, kasumlikkus	Poliitiline efektiivsus, poliitilise missiooni elluviimine

Allikas: (Campbell *et al.* 2009:10; Winkler, T.J. 2013:3), autori koostatud.

Avaliku sektori organisatsioonide üldine eesmärk on avaliku hüve pakkumine, kuid asutuste spetsiifilisemad eesmärgid võivad olla üsna laiahaardelised ja tihti immateriaalsed (Campbell, J. *et al.* 2009: 9), näiteks „ettevõtlikkust ja innovatsiooni soosiv riik“ või „infoühiskonna areng“ (Ministeeriumi tutvustus … 2020). Eesmärkide saavutamine on keerukam, kui kasumi maksimeerimine, kuna arvesse tuleb võtta ka laiemat poliitilist ja sotsiaalset kasu (Winkler, T.J. 2013: 3). Erasektori ettevõtete eesmärk on omanikele kasumi teenimine. Eelnimetatud eesmärkide erinevusest nähtub ka huvigruppide erinevus: erasektori asutuste puhul on peamiseks huvigrupiks ettevõtte omanik (omanikud) ehk tavaliselt suhteliselt piiratud hulk, samas kui avaliku sektori asutuste puhul on huvigruppe rohkem ning tihti on erinevatel huvigruppidel märkimisväärselt erinevad soovid (*Ibid.* 2013: 3).

Eriti tuleks rõhutada avaliku sektori asutuste puhul just erinevaid poliitilisi huvisid, mis võivad valitsuste vahetuste puhul perioodiliselt muutuda, mõjutades seega eelarve jaotumist ja investeeringuotsuseid (Campbell, J. *et al.* 2009:9). Avaliku sektori asutused peavad mh IT-investeeringute puhul analüüsima nii majanduslikku kui poliitilist väärtust ehk ühest küljest kulude vähendamist, efektiivsuse kasvu ning teisest küljest avalikku vastutust, õiglust jms (Chircu, A.M., Lee, D.H.-D. 2003: 792). Mõõdikud, mille alusel organisatsioonide edukust hinnatakse, on sarnaste omadustega nagu eesmärgid: avaliku sektori asutuste puhul on edukuse hindamine keeruline, kuna mõõdikuteks on poliitiline efektiivsus, poliitilise missiooni elluviimine jm, samas kui erasektori organisatsioonid kasutavad enamasti mõõdikuna kasumlikkust. (Campbell, J. *et al.* 2009: 9)

Avaliku sektori organisatsioone peetakse pigem riskikartlikeks (i.k. *risk averse)* ehk nende riskitundlikkus on kõrge, erasektori asutused on innovaatilisemad ning riskialtimad (riskitundlikkus on madal). Winkler (2013:3) nendib, et avaliku sektori asutused on peamiselt hilised kohanejad (i.k. *late adopter*).

Erasektori organisatsioonide otsuseid suunavad turu signaalid ning keskkond on turumajanduse puhul üsna vähe reguleeritud. Avaliku sektori asutused ei ole nii tugevalt mõjutatud turu signaalidest, suurem mõju on poliitilistel mõjutajatel. (Campbell, J. *et al.* 2009: 9) Samuti on avaliku sektori organisatsioonide puhul keskkond rohkem läbipõimunud erinevate piirangute ja regulatsioonidega, nagu avalike hangete nõuded (Winkler, T.J. 2013: 4).

Winkler (2013: 4) toob välja veel ühe erisuse kahe sektori organisatsioonide vahel: konkurentsi olemasolu. Ta väidab, et avaliku sektori asutused ei koge üldse või kogevad vaid vähesel määral konkurentsi, mis annab võimaluse koostööks ja teadmisevahetuseks. Avalikus sektoris on Winkleri (2013: 4) väitel tihti madalam IT pädevus, kuna ei suudeta konkureerida turul valitsevate palkadega.

Infotehnoloogia arengu ja digitaalsete süsteemide kasutamise jõudsa kasvu mõjul on IT-üldjuhtimine või haldus (i.k. *IT governance*) oluliseks osaks asutuste strateegilistest otsustest (Campbell, J. *et al.* 2009: 6). Organisatsiooni IT-haldus arendab ja kontrollib vastava organisatsiooni IT-strateegia elluviimist ja ressursside jaotamist. Peamiseks eesmärgiks võib lugeda riskide ja kasu tasakaalustamist, suunates seeläbi IT-investeeringuotsuseid. Tegemist on üldjuhul tippjuhtkonna taseme otsustega, kes saavad vajaliku informatsiooni vastavatelt allüksustelt. (*Ibid.* 2009: 5)

Turbeinvesteeringud, mis nagu eelnevalt selgitatud, kuuluvad IT-investeeringute hulka, erinevad otsustusprotsessi poolest paljudest teistest investeeringutüüpidest. Otsuseid tehes kasutatakse harva finantsmõõdikuid nagu kulude-tulude analüüs või investeeringu tootlus (ROI). (Economic Analysis … 2006: 1) Mõõdikute kasutamine aitaks kaasa optimaalsete investeerimisotsuste tegemisele, kuid puuduvad usaldusväärsed andmed kulude, tulude või intsidentide esinemise tõenäosuse kohta (de Vries, J. 2017: 3). Lisaks otsestele kuludele ja tuludele peaks investeerimisotsuse eel arvesse võtma ka kaudseid mõjusid, nagu ülekandeefekt (i.k. *spillover efect*), kus konkurendid saavad

organisatsiooni investeeringust kasu. Samuti ei saa unustada, et piiratud eelarvega organisatsioon peab investeeringuid tehes analüüsima, kas turbeinvesteeringuga potentsiaalselt ärahoitav kahju on väärt rohkem kui investeering otsesemalt mõõdetava kasumlikkusega valdkonda (nt turundusse). (Jentzsch, N. 2016: 11)

Küberturbe investeeringuotsuseid tehakse pahatihti ohu realiseerumise ajal või järgselt *ad hoc* otsustena või eelarves teiste investeeringute ja kulude ülejääki arvestades. Arusaadavalt ei vii selline otsuste tegemine läbimõeldud ja adekvaatse investeerimisstrateegiani ega optimaalse turvalisuse tasemeni. (Economic Analysis … 2006: 4) Investeeringuotsuseid mõjutavad märkimisväärselt ka eelmises alapeatükis mainitud turutõrked, sealjuures näiteks informatsiooni asümmeetria võib viia nii üle- kui alainvesteerimiseni, kuid välismõjud ja avalike hüviste pakkumine viivad alainvesteeringuni (Jentzsch, N. 2016: 24). Kuna turbeinvesteeringute küsimus on 2000. aastatest alates muutunud aina relevantsemaks, on analüüsimiseks vajalike mõõdikute kohta märkimisväärselt akadeemilist kirjandust. Sel teemal on artikleid avaldanud näiteks Gordon, L. A. ja Loeb, M. P. (2002, 2003, 2006), Anderson, R. ja Moore, T. (2006: 611), samuti on turbeinvesteeringute mõõdikuid laiemalt tutvustanud mh ENISA 2012. a väljaandes „Introduction to Return on Security Investment“ (ENISA 2012: 2).

Üldiselt on investeeringute tootluse mõõdikuna kasutusel ROI (i.k. *Return on Investment*):

$$ROI = \frac{eR - I}{I}$$

kus *eR* – oodatav kasum (i.k. *expected return*),

I – investeeringu kulu (i.k. *investment costs)*.

Investeeringud küberturbesse ei ole klassikalised investeeringud, st investeeringuid ei tehta kasumlikkuse eesmärgil, vaid potentsiaalse kahju vältimiseks. Seetõttu ei ole investeeringu tootlikkus sobilik mõõdik turbeinvesteeringute analüüsimiseks. Alternatiivina on välja pakutud turbeinvesteeringu tootlikkuse mõõdikut ROSI (i.k. *Return on Security Investment)*:

$$ROSI = \frac{(RE)(RM) - I}{I}$$

kus *RE* – riskile avatus (i.k. *risk exposure)*,

RM – riski leevendamine (i.k. *risk mitigation),*

I – investeeringu kulusid.

Riskile avatusega samatähenduslikuna esineb mitmetes allikates (nt ENISA 2012: 7 ja Sonnenreich *et al.* 2005: 47) ka aastane kahju ootus (ALE, i.k. *Annual Loss Expectancy)*:

$$RE = ALE = ARO * SLE$$

kus *ARO* – aastane tõenäosus riski realiseerumiseks (i.k. *Annual Rate of Occurance),*

SLE – ühekordne intsidendi realiseerumise kogukulu (i.k. *single loss expectancy)*.

Riskile avatus peab põhinema olemasolevatel andmetel, näiteks rünnete arv ja neist tekkinud rahaline kahju. Riski leevendamine on tänu turbelahenduse rakendamisele tekkinud riski vähenemine (näiteks rünnete sageduse protsentuaalne vähenemine). Siiski tekib ROSI mõõdiku kasutamise puhul probleeme: peamine kirjanduses mainitud murekoht on korrektsete ja sobivate andmete saamine. Andmete saamine ühe organisatsiooni sees ROSI arvutamiseks võib kujuneda keeruliseks. Nii riskile avatus kui riski leevendamine on ligikaudsed väärtused ning hinnangud sõltuvad hindajast. See tähendab, et ROSI mõõdikuga on võimalik üsna kergelt manipuleerida, et õigustada soovitud otsuseid. (ENISA 2012: 7) Kui soovida analüüsida erinevate organisatsioonide turbeinvesteeringute tootlikkust, siis peab esmalt mõistma, mis metoodikaga andmeid kogutud on, et tagada korrektne analüüs (Jentzsch, N. 2016: 14).

Investeerimisstrateegia kõrval on vähemalt sama tähtis ka rakenduskava (Economic analysis … 2006: 3). Erinevalt investeeringustrateegiast pannakse rakenduskava kokku peamiselt IT/küberturbe meeskonna poolt ning analüüsitakse erinevaid turbelahendusi. Rakenduskava puhul on oluline analüüsida reaktiivse ja proaktiivse (ennetava) lähenemise vahekorda. Proaktiivne lähenemine võimaldab üldiselt ennetavalt vältida ründeid, samas on keerulisem ennustada, millistele turbelahendustele peaks enam rõhku panema. Samuti võib proaktiivsete strateegiate positiivseks küljeks lugeda nende mainekujunduslikku külge, mis võivad kaasa aidata rünnete vähenemisele (reputatsioon tugevast turbest vähendab ründaja motivatsiooni katsetamiseks) ning mõjutada seeläbi klientide otsuseid. (Economic analysis … 2006: 4) Reaktiivne strateegia tegeleb juba selgunud nõrkuste või toimunud rünnete tagajärgede parandamisega. Kuna reaktiivse strateegia puhul on haavatavused välja selgitatud (ennetava puhul peab end kaitsma täpseid haavatavusi teadmata), siis võib see olla kuluefektiivsem kui ennetav strateegia.

Optimaalset turvalisuse taset on raske saavutada isegi ideaalse rakendusplaani puhul, kuna küberturbe valdkond ja ohud arenevad väga kiiresti. (*Ibid.* 2006: 4)

Nii investeeringuotsuseid kui rakenduskava otsuseid mõjutab kvaliteetse informatsiooni olemasolu. Turbeotsuste vaatenurgast oluliseks informatsiooniallikaks on erinevad standardid, nõuded ja regulatsioonid, mis annavad soovitusi või kehtestavad reegleid, millest turbeotsustes joonduda. Samuti toetutakse organisatsioonides palju oma valdkonna ekspertide hinnangutele ja kogemustele ning organisatsioonis kogutud andmetele, nagu rünnete arv, liik vms. (*Ibid.* 2006: 6)

Avaliku sektori asutusi mõjutavad üsna laiahaardelised ja immateriaalsed eesmärgid ning erinevate soovidega huvigrupid. Investeeringute puhul peavad avaliku sektori asutused analüüsima nii majanduslikku kui poliitilist väärtust. Valimistega võivad muutuda ka poliitilised huvid ja ümber kujuneda eelarve jaotus. Turbeinvesteeringu otsustele peaks eelnema finantsanalüüs (nt turbeinvesteeringu tootlikkus), kuid olemasolevate mõõdikute kasutamise muudab keeruliseks andmete hinnangulisus. Organisatsiooni turbemeetmed võivad olla nii reaktiivsed kui proaktiivsed, kuid valdkonna kiire arengu tõttu on raske optimaalset turvalisustaset saavutada.

1.3. Küberturbeinvesteeringute tõstmise stiimulid

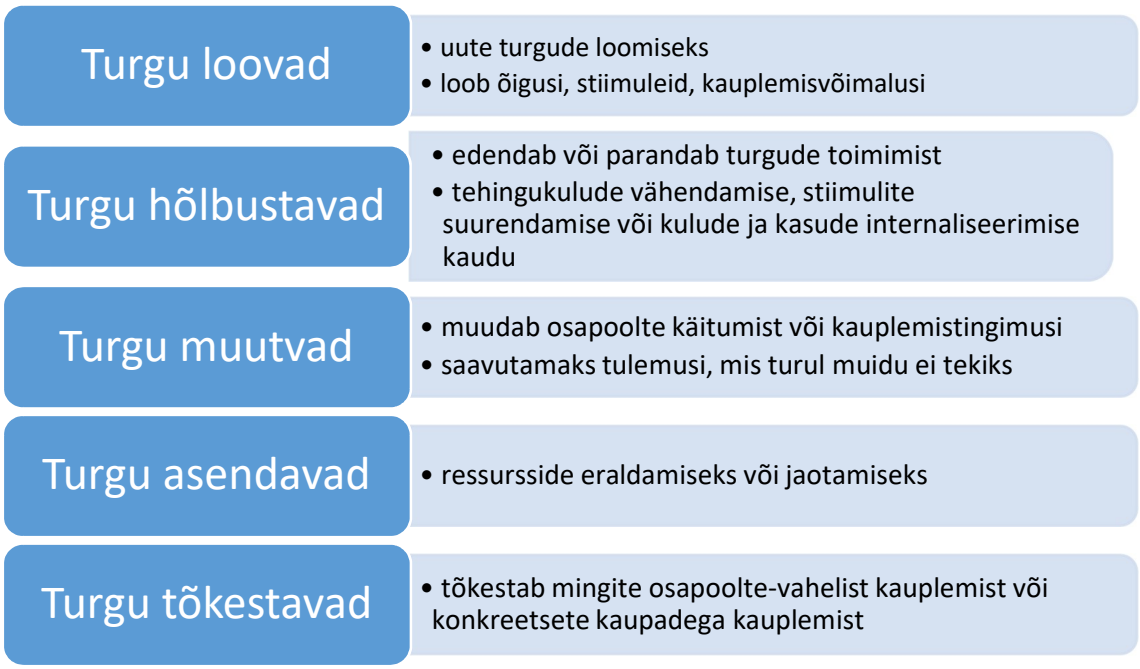
Alapeatükis 1.1. kirjeldatud turutõrked ja neist tekkivad probleemid turuosalistele viitavad riigipoolse sekkumise vajadusele, kuid lisaks turutõrgete mõjude vähendamisele põhjendatakse riigipoolse sekkumise vajalikkust ka julgeoleku tagamisega (Aggawal, V. K., Reddie, A. W. 2018: 6). Kui turutõrgete probleeme saaks leevendada, võiks see turu osapooled viia optimaalse turbeinvesteeringute taseme poole. Selleks kasutatakse poliitinstrumente (i.k. *policy instrument*) ehk positiivse resultaadi kaudu tekitatavat lisamotivatsiooni, mis viib soovitava käitumiseni.

Ühe instrumendi asemel on tõenäoliselt efektiivsem lahendus kasutada erinevate meetmete kombinatsiooni, lisaks tuleb leida sobiv pakutavate stiimulite tase, mis osapooli motiveeriks (Jentzsch, N. 2016: 69). Jentzsch (2016: 71) möönab, et poliitinstrumentide rakendamist lisamotivatsiooni tekitamiseks küberturbe valdkonnas ei ole piisavalt uuritud ning seetõttu ei teata:

- instrumentide paremusjärjestust;

- erinevate instrumentide koostoimet ja milline on parim meetmete kombinatsioon;
- kas ja milliste instrumentide rakendamine peaks olema kohustuslik ja kui kõrgel tasemel;
- võrgustikuefekti mõju meetmete rakendamisel;
- reaalset instrumentide rakendamise kulu.

Robert Harris ja James Carman (1984: 43) esitlesid 1984. a riiklike meetmete tüpoloogiat (vt joonis 2), mille järgi instrumendid jagati turgu loovateks, hõlbustavateks, muutvateks, asendavateks ja tõkestavateks (i.k. vastavalt *market creating, facilitating, modifying, substituting, proscribing)*.

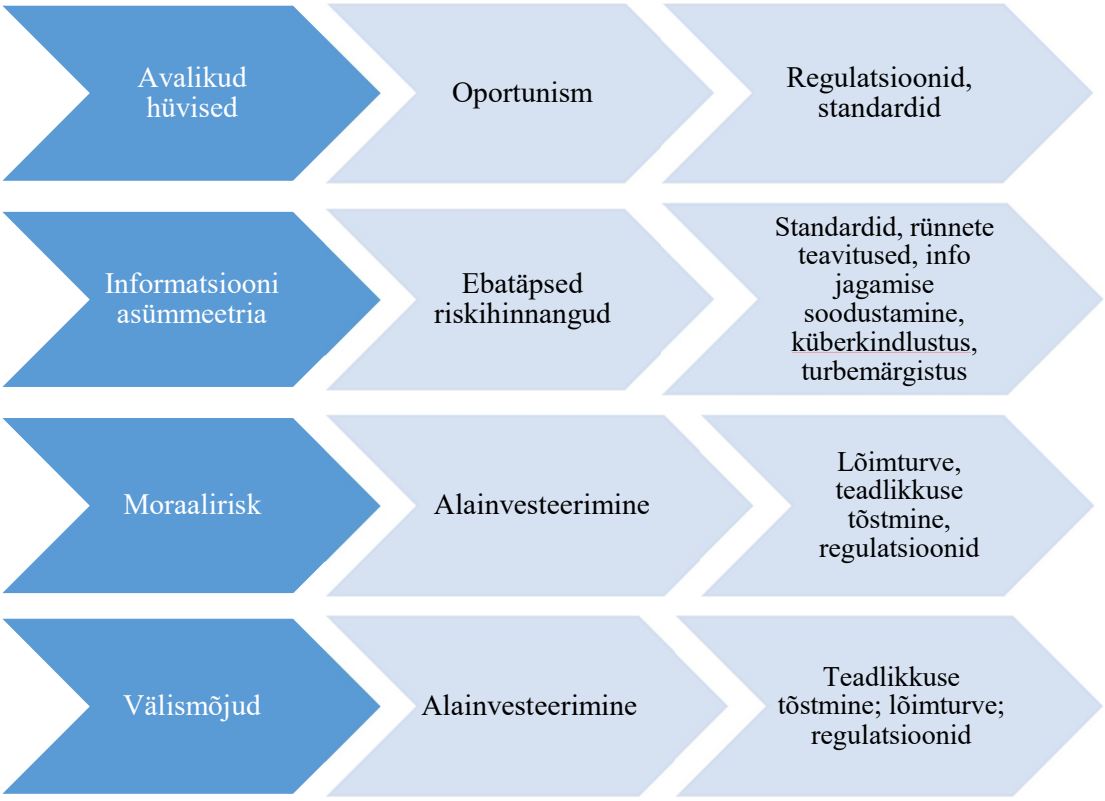


Joonis 2. J. Carman ja R. Harris poliitinstrumentide tüpoloogia (Allikas: Harris, R. G., Carman, J. M. 1984: 43).

Küberturbe instrumendid on kasutusel läbipõimunult, mis tuleneb nii riigipoolse sekkumise loogika ajaloolisest muutumisest (vertikaalsest valdkonnaspetsiifilisest sekkumisest horisontaalse valdkonnaüleste poliitikate poole (Aggawal, V. K., Reddie, A. W. 2018: 5) kui ka küberturvalisuse interdistsiplinaarsusest (Griffith,. M 2018: 11). Küberturbe instrumendid ei ole diskreetsed tunnused ning kuigi Carman ja Harrise tüpoloogiat on kasutatud erinevates allikates riikide meetmete ülevaadetes, siis on sama instrumenti erinevates allikates kategoriseeritud erinevalt. Näiteks Bartlett (2018: 19) on

Jaapanis kasutusel oleva informatsiooni jagamise (JPCERT/CC – *Japan Computer Emergency Response Team Coordination Center*) liigitanud turgu asendavaks meetmeks, samas kui Griffith (2018: 15) on analoogse Soome meetme liigitanud turgu hõlbustavaks meetmeks. Sarnane näide esineb D'Elia (2018: 16) analüüsis, kus Prantsusmaa küberkaitse klaster on liigitatud turgu loovaks ja turgu hõlbustavaks, ent Soome näites (Griffith 2018: 12) on see turgu muutev meede.

Alloleval joonisel 3 on kirjeldatud alapeatükis 1.1. vaadeldud turutõrkeid, nende mõju turu osapooltele ning levinumaid instrumente, millega turutõrgete mõju vähendada.



Joonis 3. Küberturbe valdkonna turutõrked, nende mõju ja meetmed (autori koostatud)

Avalike hüviste pakkumine ja välismõjud tekitavad soovi n-ö tasuta sõitmiseks, näiteks teiste ettevõtete turbeinvesteeringute kaudu tekkiva kasu näol (Jentzsch, N. 2016: 24). Moraalirisk (Vagle, L. 2020: 74) vähendab motivatsiooni investeerida, kuna riskidega kaasnevaid kahjusid kannavad teised osapooled (nt kasutajad). Sisuliselt tekib nende turutõrgete mõjul alainvesteerimine. Vastumeetmena kasutatakse regulatsioonide ja standardite kehtestamist, üldist teadlikkuse tõstmist ühiskonnas ning lõimturbe lähenemist. Informatsiooni asümmeetria puhul ei pruugi tekkida üle- või ala-investeerimist, kuid ebatäpse info põhjal tehtud riskihinnangud võivad põhjustada valede

turbemeetmete kasutamist (Moore, T. 2010: 106). Lahendust toovad meetmed, mis soodustavad informatsiooni jagamist (nt vabatahtlikud organisatsioonid, rünnete teavitused) ja annavad turuosalistele turbeinformatsiooni (nt turbemärgitused, kindlustus) (Bisogni, F. *et al.*, 2011: 116).

Ainuüksi poliitinstrumentide rohkus turul ei määra tekkivat mõju, kriitilise tähtsusega on ka sekkumise intensiivsus (Aggawal, V. K., Reddie, A. W. 2018: 10). Poliitinstrumentide hulgas on neid, mille rakendamisega kaasneb vaid vähene riigipoolne sekkumine (nt informatsiooni jagamise soodustamine) ning sellised, mille rakendamine eeldab riigi aktiivset sekkumist (nt maksusoodustuste pakkumine) (Cordes, J. J. 2011: 11).

Jentzsch (2016: 69) on meetmed jaganud kolme kategooriasse: kohustuslikud, vabatahtlikud/kohustuslikud ning vabatahtlikud stiimulid. Kohustuslike alla kuuluvad siduvad juriidilised regulatsioonid ja piirangud. Keskmisesse kategooriasse kuuluvad instrumendid, mille puhul kasu suureneb osalejate arvu kaudu, nt mida rohkem organisatsioone relevantset ja korrektset ohuteavet jagab, seda kasulikum see on, ülejäänud liigituvad vabatahtlike kategooriasse. (Jentzsch, N. 2016: 69) Allolevas tabelis 2 on levinumad stiimulid jagatud kohustuslikkuse ja sekkumise intensiivsuse põhjal ning sellele järgnevalt kirjeldatakse peamisi kirjanduses kajastatud lahendusi.

Tabel 2. Levinud instrumentide jaotus kohustuslikkuse ja sekkumise intensiivsuse järgi

	Kohustuslikud instrumendid	Kohustuslikud või vabatahtlikud instrumendid	Vabatahtlikud instrumendid
Minimaalne sekkumine	Rünnete teavitused Organisatsiooni vastutus turbe eest	Turbemärgistuste süsteem Informatsiooni jagamine Standardid Vabatahtlikud organisatsioonid	Lõimturve Teadlikkuse tõstmise kampaaniad Hankeprotsesside kujundamine
Keskmine sekkumine		Küberkindlustus	T&A rahastamine PPP
Aktiivne sekkumine	Riiklikud regulatsioonid		Finantsstiimulid (nt maksustuse stiimulid)

Allikas: (Jentzsch, N. 2016: 69 ja Cordes, J. J. 2011:12), autori koostatud.

Riik saab soosida erinevate platvormide ja keskkondade teket, kus eesmärgiks on ohtude, riskide, nõrkuste, rünnete ja parimate praktikate jagamine. Oluline on suurendada osapoolte omavahelist usaldust, väärtusliku info jagamist, erapooletust ja jagatud informatsiooni konfidentsiaalsust. Taolised platvormid võivad olla riigi poolt juhitud või vabatahtlikkuse-põhised, aga formaalselt juhitud platvormid toimivad osapoolte vahel esmaseks usalduse tekkimiseks paremini. (Jentzsch, N. 2016: 70) Osaliselt täidavad taolise informatsiooni levitamise rolli riiklikud CERT (i.k. *Computer Emergency Response Team,* ka CSIRT, i.k. *Computer Security Incident Response Team*) meeskonnad, kelle ülesandeks on koguda ja levitada informatsiooni küberintsidentide ja turvaaukude kohta ning pakkuda tuge teenusepakkujatele (Küberintsidentide … 2020). Samas on see vaid üks samm lahenduse suunas, kuna on formaalne ja esmajoones ühesuunaline info jagamine. Rohkem olemasolevat informatsiooni riskide ja nende maandamise kohta annab andmeid investeeringute tasuvuse analüüsimiseks ja seeläbi võimaluse pädevamaks analüüsiks investeeringuotsuste tegemisel. Jentzsch (2016: 70) rõhutab, et informatsiooni jagamise meetmete kujundamisel peab silmas pidama kahepoolsust. Muidu tekitab see taas motivatsiooni n-ö „tasuta sõita“ (i.k. *free-rider*) ehk olukorda, kus üks osapool jagab ise vähe, kuid saab vastu palju informatsiooni (Gordon 2007: 5). Küberturvalisuse teadlikkuse kampaaniad kuuluvad teataval määral ka informatsiooni asümmeetria probleemi lahendavate meetmete alla. Viies läbi teavituskampaaniaid küberturbest, selle arengutest ja levinumatest ohtudest, soodustab see küberturvalisuse-alast kriitilist mõtlemist (Bayuk, J. L. *et al.* 2012: 188).

PPP ehk era- ja avaliku sektori koostöö (i.k. *private-public partnership*) on küberturbe valdkonnas üsna laialivalguv käsitus ning võib endas sisaldada erinevaid poliitilisi initsiatiive (Bossong, R., Wagner, B. 2016: 269). Siiski rõhutab aina enam strateegiaid ja poliitilisi dokumente PPP tähtsust küberruumis (*Ibid.* 2016: 265). Traditsiooniliselt on PPP projektide puhul tegemist pikaajaliste koostööprojektidega, mille käigus teeb vajalikud investeeringud eraettevõte ning avalik sektor saab kasutusõiguse kokkulepitud tingimustel (nt kasutustasu) (Innopolis … 2008: 3). Küberturvalisuse valdkonnas on PPP projektidena ellu viidud eelmises lõigus kirjeldatud ohuinformatsiooni kogumist, jagamist ja vastastikkust abistamist nende ohtude adresseerimisel (Bossong, R., Wagner, B. 2016: 272), kuid ka T&A-tegevust ja hariduse (sh õppuste) arendamist (Clark, K. *et al.* 2014:33).

Riik saab panustada küberturvalisuse sektori arengusse olles toodete ja teenuste tellija. Lisaks tähendab see, et kasutatakse turul olemasolevaid kompetentse ära, dubleerimata sama võimekust avalikus sektoris. Paljud, eriti väiksemad ettevõtted, ei kvalifitseeru bürokraatlike nõuete tõttu hangetes osalema või ei ole protsessi keerukuse tõttu selleks motiveeritud. Avalik sektor ei pruugi aga ise omada vastavat teadmust või on see (näiteks arendustegevuses) ebaefektiivselt kulukas. (Aggarwal, V. K., Reddie, A. W. 2018b: 297) Hankeprotsesside lihtsustamine avalikus sektoris kergendab koostööd erasektoriga.

Riikidel on võimalik rakendada finantsstiimuleid, nt maksusoodustustena, riistvara ajakohastamiseks või küberturbe-alase T&A-tegevuse koostöö puhul. Instrumenti kasutatakse innovatsiooni soodustamiseks, valdkonna tähtsuse suurendamiseks ja ka koostöö soodustamiseks. *Cyber Security Policy Guidebook* (Bayuk, J. L. *et al.* 2012: 187) toob aga välja, et see võib kaasa tuua vaid näilise muutuse, näiteks teiste investeeringute ümbernimetamise küber-alaseks, ilma et sellega kaasneks reaalset kasu.

Turbemärgistused ja -standardid annavad signaali mingist olemasolevast turbetasemest, mis motiveerib organisatsioone vähemalt minimaalset turbeinvesteeringut tegema (Jentzsch, N. 2016: 70). Enamik riigipoolseid regulatsioone sätestavad vastavustingimused (i.k. *compliance*), mida asutused järgima peavad, enne ohtude realiseerumist (*ex ante)*. Üldiselt üritatakse vältida tehniliste tingimuste regulatsioonidesse kirjutamist, et vältida ajale jalgu jäämist ning lihtsustada vastavuskontrolli tööd (Moore, T. 2010: 107). Samas ka paindlikud standardid võivad uutele turuosalistele olla liiga keerulised või kallid, et neid suuta täita. Poliitikakujundajad peavad standardid ja sertifitseerimise üles ehitama paindlikuna. Standardeid ja sertifitseerimist on pakutud lahenduseks informatsiooni asümmeetria probleemi vähendamiseks, et pakkuda turuosalistele vajalikku infot. Kui turbemärgistuste süsteemi metoodiliselt ei suunata, võib tekkida sildistuste rägastik, mis ei vähenda turutõrget. (Jentzsch, N. 2016: 71) Sertifitseerimine on aga üsna pikk protsess ning kulukas, seetõttu kasutatakse seda enamasti väga konkreetsete turbenõuete täitmise kinnitamiseks. Sertifitseerimisprotsessi tuleb korrata juhul, kui toodet muudetakse või arendatakse edasi. (Fraunhofer ... 2014: 11)

Lisaks *ex ante* regulatsioonidele on ka *ex post* regulatsioone, nt organisatsioonile turberikkumiste (i.k. *breach*) eest (rahalise) vastutuse panemine. Ühest küljest võiks see

vähendada turberikkumisi, kuna turvalisusele pööratakse suuremat tähelepanu, kuid samas võib hoopis kaasa tuua innovaatiliste lahenduste vähenemise, kuna kardetakse turbeprobleemide hilisemat ilmnemist ja sellega kaasnevat vastutust. (Moore 2010: 107) Parema alternatiivina tuuakse välja lõimturvet.

Lõimturvet (i.k. *security by design*) võib defineerida kitsamalt tarkvara arendamise käigus turvalisuse aspekti arvessevõtmisena. Laia definitsiooni järgi on lõimturve raamistik, mida rakendatakse tarkvara kogu elutsükli käigus, näiteks teiste (tootjate/arendajate) komponentide ühildamisel läbiviidav turbeanalüüs (Fraunhofer … 2014: 4). Lõimturbe lähenemine vähendab nõrkuste n-ö paikamisele (i.k. *patching*) kuluvaid ressursse, kuna turbepaikamisega kaasnevad kulud testimisele, levitamisele jms (*Ibid.* 2014: 7). Lõimturve vähendab inimlike vigade läbi tekkivaid turvariske. Kui lõimturvet vaadeldakse laia raamistikuna, mida rakendatakse metoodiliselt läbi kogu elutsükli, siis annab see asjakohast informatsiooni, suurendades mõõdetavust ja kontrollitavust. (*Ibid.* 2014: 10) Ühiskondliku efektina suurendab lõimturve usaldust infotehnoloogia lahenduste ja küberruumis toimuva suhtes (*Ibid* . 2014: 5).

Küberkindlustus on arenev alamvaldkond kindlustuse turul, mis omab suurt kasvupotentsiaali (Wang, S. 2019: 9). Kindlustus võtab teatud hinna eest enda kanda osa küberturbe riskist, mis potentsiaalsete turberikkumistega tekkida võivad (Bodin, L. D. *et al.* 2018: 528). Küberkindlustuse kaudu saab motiveerida investeeringuid, premeerides asutusi läbi sissemakse alandamise. Samuti on kindlustusepakkujal vajalik koguda informatsiooni turbeintsidentide kohta, seeläbi panustades väärtuslike andmete kogumisse. (Moore, T. 2010: 109) Küberkindlustuse valdkond ei ole siiski veel aktiivselt toimima hakanud, Wang (2019: 9) põhjendab seda järgmiselt: esiteks on olemasolevate küberkindlustuse pakkujate sõnastused kindlustatuse ulatuse kohta väga erinevad, mis ei anna kindlustuse ostjale selgust, kas ja mis ulatuses intsidendi aset leidmisel reaalselt kaitstud ollakse. Teiseks, moraaliriski probleem ehk pärast kindlustuse ostmist väheneb kindlustatu motivatsioon investeerida küberturbesse, kuna osa riski kannab kindlustus. Viimasena toob Wang (2019: 9) välja küberturbe intsidentide andmete probleemid, mida käesolevas tööd kirjeldati alapetükis 1.2., ja sellest tingitud küberkindlustuse hinnastamise väljakutse.

Järgnevalt vaadeldakse kolme riigi– Soome, Jaapani ja Prantsusmaa – näitel meetmeid, mis on suunatud küberturvalisuse valdkonna tegevuse soodustamisesse. Ülevaade põhineb kolmele Berkeley APEC *Study Centre* töögrupi artiklile projekti "*Comparative Industrial Policy in the Cyber Security Industry: Policies, Drivers, and International Implications*" raames, mis kirjeldavad nimetatud riikide küberturbe üldolukorda ja meetmeid. Artiklites on meetmeid grupeeritud kasutades Carman ja Harrise tüpoloogiat. Ülevaatlik tabel näiteriikide meetmetest Carman ja Harrise jaotuse järgi, on toodud lisas 1.

Soome ja Prantsusmaa on märkimisväärselt panustanud küberturbe valdkonnas tugevate võrgustike loomisesse, eesmärgiga tekitada valdkonnasisest usaldust ja ühtset arusaama ohtudest ja vastumeetmetest. Soomes on rakendatud erinevaid seadusest tulenevaid nõudeid, regulatsioone ning loodud koostööplatvorme ja -võrgustikke, et soodustada koostööd era- ja avaliku sektori vahel. (Griffith, M. 2018:12; D'Elia, D. 2018: 16-17) Soomes toimib edukalt Soome inforturbe klaster (*Finnish Information Security Cluster*, FISC), kus lisaks Soome küberturbe ettevõtetele (nt F-Secure) on esindatud ka mitmed välismaised ettevõtted (nt Microsoft, Cisco jt) Eriliseks teeb Soome inforturbe klastri mh see, et see hõlmab nii küberturvalisuse kui ka küberkaitse (kui riigikaitse osa) esindajaid. Tihti on need kaks tegelikkuses väga tihedalt seotud valdkonda moodustanud eraldi klastrid (või on osa eraldiseisvatest klastritest), kuid Soomes on suudetud need ajapikku ühte klastrisse liita. (Griffith, M. 2018: 13) Prantsusmaal on loodud küberkaitse klaster, küberkaitse reservväelastide võrgustik ning Prantsusmaa turbejuhtide võrgustik. Samuti on Prantsusmaal loodud töögrupp, mis tegeleb standardite ja regulatsioonide väljatöötamise toetamisega, tagades meetmete asja- ja ajakohasuse. (D'Elia, D. 2018: 14) Sarnaselt eelnimetatule on ka Jaapanis mitmeid töögruppe, mis kaasavad ka erasektori esindajaid, andmaks sisendit avaliku sektori asutustele (Bartlett, B. 2018: 18).

Soomes korraldatavatele, traditsiooniliselt eelkõige militaarse ja riigikaitse fookusega, riigikaitsekursustele on hakatud integreerima enam küberturbe aspekti, millest loodetakse samuti kogukonnatunde tekitamise efekti ning küberturbe olulisuse mõistmise suurenemist. Lisaks on Soomes üldise ajateenistuse raames on võimalik spetsialiseeruda küberajateenistusse. (Griffith, M. 2018: 14) Prantsusmaal korraldatakse aga riiklikke

kriisijuhtimise kursuseid, kuhu on aina enam lisatud ka küberturbe aspekti (D'Elia, D. 2018: 16)

Nii Soome kui Jaapani analüüsides märgiti, et suurt rõhku pannakse küberturvalisuse alasele haridusele, koolitustele ja T&A-tegevuse rahastamisele. Prantsusmaa analüüs neid aspekte otseselt ei rõhutanud. Samas on Prantsusmaa uuringus ära märgitud näiteks Prantsusmaa küberkuritegevusega võitlemise kompetentsikeskus, mis on PPP printsiibil toimiv teadusgrupp (D'Elia, D. 2018: 16). Jaapani ja Prantsusmaa analüüsides mainiti küberturvalisuse teadlikkuse tõstmist ühiskonnas kui ühiskonda üldharivat meedet (Bartlett, B. 2018: 16; D'Elia, D. 2018: 15).

Soome analüüsis tuuakse välja, et riik on küberturvalisuse teenuste ja toodete tellija: Soome hangib nii turul kõigile kättesaadavaid küberturbe tooteid ja teenuseid kui ka tellib hangete kaudu spetsiifilisi lahendusi (Griffith, M. 2018: 15). Prantsusmaa on kehtestanud turbestandardid ja muid juriidilisi meetmeid oma kriitilise infrastruktuuri asutustele, eesmärgiga vähendada küberrünnetest tulenevat riski (D'Elia, D. 2018: 15). Ka Jaapanis kasutatakse regulatiivset võimu, kuid eesmärgiks on turbeinvesteeringute motiveerimine. Lisaks kasutatakse Jaapanis samal eesmärgil ka maksusoodustusi, peamiselt organisatsiooni turbeolukorda parandavate riistvara investeeringute puhul (Bartlett, B. 2018: 23).

Küberintsidentide monitooringut ning ohuteavitust pakuvad kõik kolm vaadeldavat riiki, Soomes NCSC-FI (*National Cybersecurity Centre),* Jaapanis JPCERT/CC ning Prantsusmaal CERT-FR (Griffith, M. 2018: 15; Bartlett, B. 2018: 19; D'Elia, D. 2018: 15). Carman ja Harris tüpoloogia järgi on nii Soomes kui Prantsusmaal liigitatud see meede turgu hõlbustavaks (vt lisa 2 lk 55-56), samas Jaapani puhul turgu asendavaks meetmeks, see liigituse erinevus võib tähendada organisatsioonide toimimise sisulist erinevust.

Eelnimetatule lisaks on Soomes ja Prantsusmaal rakendatud ka Euroopa Liidu regulatsioonid (turgu muutvad instrumendid): isikuandmete kaitse üldmäärus (GDPR, i.k. *General Data Protection Regulation*) ja NIS direktiiv (i.k. *Network and Information Systems Directive*).

Alapeatükis anti esmalt ülevaade meetmetest, millega turutõrgete probleeme lahendatakse. Avalike hüviste, välismõjude ja moraaliriski kaudu tekib küberturbesse alainvesteerimine. Vastumeetmena kasutatakse regulatsioonide ja standardite kehtestamist, üldist teadlikkuse tõstmist ühiskonnas ning lõimturbe lähenemist. Informatsiooni asümmeetria võib põhjustada valede turbemeetmete kasutamist, seega lahendust toovad meetmed, mis soodustavad informatsiooni jagamist (nt vabatahtlikud organisatsioonid, rünnete teavitused) ja annavad turuosalistele turbeinformatsiooni (nt turbemärgitused, kindlustus). Seejärel anti ülevaade, kuidas on neid meetmeid rakendanud Soome, Prantsusmaa ja Jaapan.

2. KÜBERTURBE OLUKORD JA MAJANDUSSTIIMULID EESTIS

2.1. Metoodika

Eesti küberturvalisuse hetkeolukorra hindamiseks ning küberturbe investeeringute otsustusprotsesside ja kitsaskohtade välja selgitamiseks Eesti avaliku sektori asutustes on käesolevas magistritöös kasutatud intervjuusid Eesti avaliku sektori organisatsioonide esindajatega, kes tegelevad küberturbe tagamisega kindlas valitsemisalas või valitsemisalade üleselt. Lisaks intervjuudele on kasutatud olemasolevaid strateegilisi dokumente, regulatsioone ning muud dokumentatsiooni.

Intervjuud viidi läbi 2019. a jooksul Majandus- ja Kommunikatsiooniministeeriumi IKT Arenguprogrammi (IKT valdkonna … 2018: 19) raames TalTechi küberkriminalistika ja küberjulgeoleku keskuselt tellitud Eesti küberturvalisuse võime (TalTech 2019), küberturvalisuse majandusharu kontseptsiooni (TalTech 2020a) ning valdkonna teadus- ja arendustegevuse kontseptsiooni (TalTech 2020b) uuringute tarvis. Eesti küberturvalisuse võime analüüsis hinnati Eesti küberturvalisuse hetkeolukorda; küberturvalisuse majandusharu kontseptsiooni uuringus vaadeldi kübermajandusharu konkurentsivõimet ning riigi võimalusi konkuretsivõime tõstmiseks; ning küberturvalisuse valdkonna T&A-tegevuse uuring hindas küberturbe T&A-tegevuse hetkeolukorda ning tulevikuväljavaateid, sh olulisemaid uurimisvaldkondi. Käesoleva töö autor osales Eesti küberturvalisuse võime uuringu töögrupis ühe autorina ning oli majandusharu kontseptsiooni uuringu üks põhilisi autoreid. Uuringute jaoks läbiviidud intervjuude küsimustikud pandi kokku TalTechi uurimisgrupi liikmete koostöös, käesoleva magistritöö jaoks on erinevate intervjuude küsimustikest valitud teemaga haakuvad küsimused. Esimese küsimuste grupi eesmärk oli Eesti küberturbe üldise hetkeolukorra kaardistamine. Seejärel küsiti küsimusi intervjueeritava asutuse kohta kaardistamaks küberturbe tagamise ülesandeid ja intervjueeritava rolli organisatsioonis. Sellele järgnesid küsimused asutuse infoturbe töötajate, eelarve ning investeeringute

kohta. Viimane grupp küsimusi olid suunatud identifitseeritud probleemidele lahenduste leidmisele ja olemasolevate meetmete üle arutlemisele. Magistritöö jaoks kasutatud küsimused on esitatud käesoleva töö lisas 2.

Antud töös on analüüsitud 15 läbiviidud intervjuud, neist 11 viis läbi käesoleva magistritöö autor. Intervjueeriti poliitikakujundajad ja -elluviijad ning avaliku sektori asutusi, mis mh tegelevad küberturvalisuse tagamisega. Intervjueeritute hulka kuulusid riigi tippjuhid ning infoturbe- ja/või IT-juhid, sõltuvalt sellest, kuidas vastavas organisatsioonis kohustused jagatud on. Mõne asutuse puhul esitati intervjuule järgnevalt täpsustavaid küsimusi. Valdav enamus (11 intervjuud 15-st) intervjuudest salvestati, v.a kui intervjueeritav seda ei soovinud. Salvestatud intervjuudest on autor teinud transkriptsioonid, ülejäänute puhul tehti kirjalikud ülestähendused. Käesolevas magistritöös on läbiviidud intervjuude tulemused esitatud anonümiseeritud kujul. Tulemuste anonüümsus ja seeläbi tekkiv üsna suur üldistatus ning intervjueeritute konfidentsiaalsus on olulised mitmel põhjusel. Ühest küljest ei soovita avalikustada (ka kaudselt) tegevusi, sh investeeringuid, millega küberturvalisust tagatakse. Parafraseerides ühes intervjuus kõlanut: me võime aimata, et maja lukustatakse võtmega ning ukse ees on valvekaamerad, aga avalikult ei soovi keegi kirjeldada, kas on tehtud investeeringuid uue turvalisema ukseluku ostmiseks või et valvekaamera ei pruugi alati salvestada. Viimati nimetatu viib teise põhjuseni, miks tulemusi on vaja üldistada: konkreetsetele asutustele ega avalikule sektorile laiemalt ei ole kasulik üldistamata kitsaskohtade rõhutamine. Muudele ohtudele lisaks võib see tekitada süüdistavat õhkkonda, kuid antud töö eesmärk on läbi intervjuudes identifitseeritud kitsaskohtade parandada üldist avaliku sektori küberturbe olukorda. Anonüümsuse tagamine suurendab avatud õhkkonda, mis suurendab tõenäosust saada ausaid vastuseid ressursside, riskide, turvaprobleemide jpm kohta.

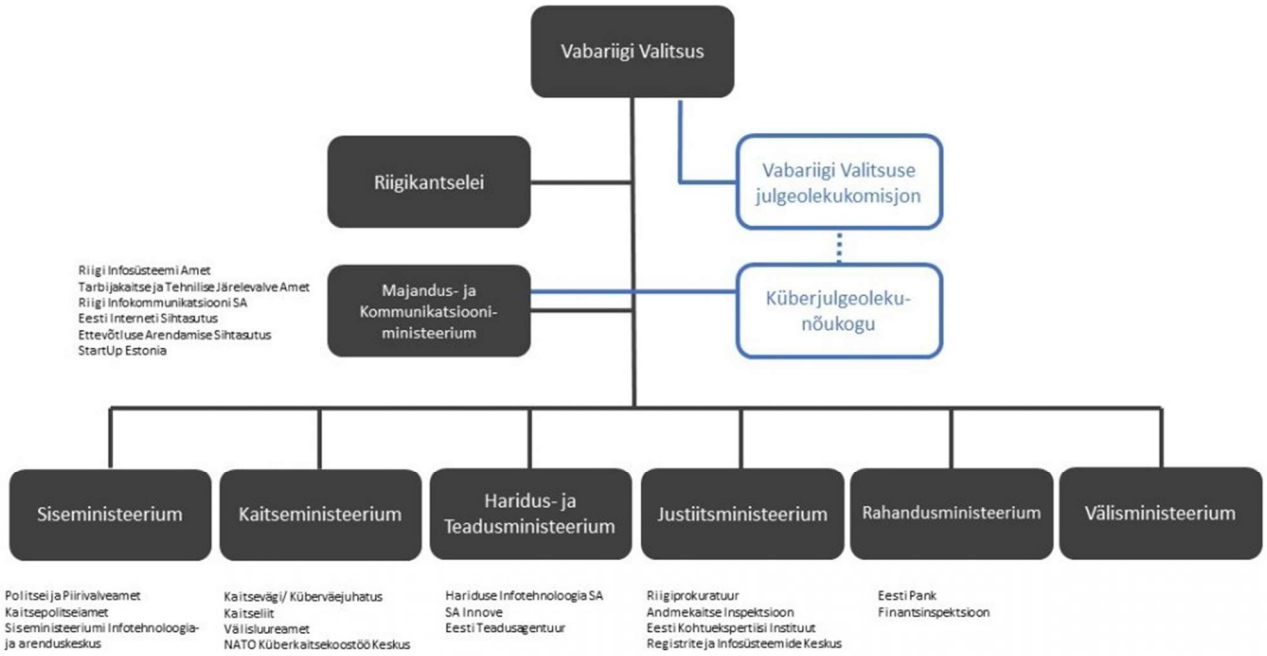
Sisendi saamiseks kasutati poolstruktureeritud intervjuude formaati. Intervjuud viidi läbi näost-näkku kokkusaamistel ning kestsid ligikaudu poolteist tundi. Iga intervjuu alguses selgitati intervjueeritavale, et tulemused anonümiseeritakse, sh ei nimetata nimesid või asutusi. Poolstruktureeritud intervjuumeetodi tugevuseks on võimalus küsida lisaküsimusi ning liikuda intervjuu jooksul vastavalt vajadusele ning intervjueeritava mõttearendustele erinevate teemade vahel. See tagab suurema paindlikkuse ja võimaldab

põhjalikuma arutelu kui struktureeritud küsimustikuga intervjuud. (Moore, T. *et al.* 2015: 3) Poolstruktureeritud intervjuu nõrkuseks on see, et tulemusi on raskem üldistada ning vastused võivad sõltuda kontekstist (*Ibid.* 2015: 3). Arvesse peab võtma, et tegemist on eelkõige intervjueeritava arvamusega ning on võimalik, et küsimustele antaks teiste intervjueeritavate korral erinevad vastused.

2.2. Küberturvalisuse hetkeolukord Eestis ja vaadeldavate asutuste turbeinvesteeringute kontekst

Antud alapeatükis kirjeldatakse Eesti küberturvalisuse valdkonna korraldust avalikus sektoris ning küberturbe üldist hetkeolukorda põhinedes läbiviidud intervjuudele. Seejärel vaadatakse lähemalt asutuste küberturbe olukorda, infoturbe investeeringuotsuseid ning kitsaskohti.

Alljärgneval joonisel 4 on kirjeldatud küberturvalisuse valdkonna juhtimise korraldust Eestis. Riigikantselei on Vabariigi Valitsuse juures olev valitsusasutus, mis mh toetab riigi strateegilist planeerimist, küberturvalisuse vaatenurgast tagab Riigikantselei temaatika lõimimise riigikaitse planeerimisdokumentidesse ehk riigikaitse arengukavasse ning riigikaitsetegevuste kavasse (Riigikantselei … 2020). Majandus- ja Kommunikatsiooniministeerium (MKM) korraldab Eesti küberturvalisuse poliitika kujundamist ning koordineerib riigiasutuste ning laiema kogukonna koostööd. MKM juhib Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu, mille eesmärk on koostöö soodustamine erinevate ametkondade vahel ning järelevalve strateegia rakendamise üle. (Küberturvalisus. Majandus- ja Kommunikatsiooniministeerium 2020) Joonisel toodud teised ministeeriumid (Siseministeerium, Kaitseministeerium, Välisministeerium, Haridus- ja teadusministeerium, Justiitsministeerium ning Rahandusministeerium) tagavad oma valitsusalasiseselt küberturvalisuse strateegia eesmärkide saavutamise (*Ibid.* 2020). Lisaks on joonisel ministeeriumite juures märgitud tähtsamad allasutused, mis tegelevad küberturvalisuse tagamisega Eestis ja valdkonna arendamisega, näiteks Riigi Infosüsteemi Amet, Siseministeeriumi Infotehnoloogia ja Arenduskeskus, Registrite ja Infosüsteemide keskus jt.

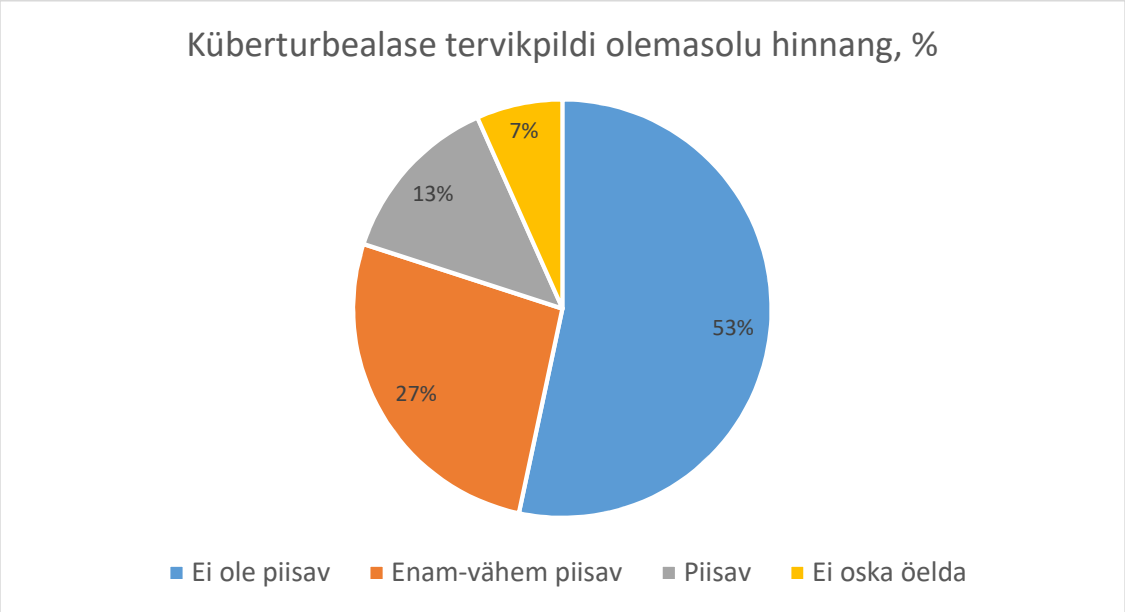


Joonis 4. Eesti küberturvalisuse valdkonna korraldus (Küberturvalisus. Majandus- ja Kommunikatsiooniministeerium 2020).

Eesti küberturvalisuse ja -kaitse valdkonda hakati jõuliselt arendama 2007. a kevadest, mil toimusid ulatuslikud küberründed Eesti riigiasutuste ja ettevõtete vastu (Küberjulgeoleku … 2007: 7) Valdkonnas on sel perioodil toimunud jõudsaid arenguid. Välja on töötatud kolm küberjulgeoleku/-turvalisuse strateegiat: 2008-2013 ning 2014-2017 küberjulgeoleku strateegiad ning 2019-2022 küberturvalisuse strateegia. 2018. a kuulutati välja küberturvalisuse seadus (Küberturvalisuse seadus 2018). Küberturvalisuse valdkonnas tegutsevate Eesti (-põhiste) ettevõtete hulk on kasvanud (nagu näiteks SK ID Solutions, Guardtime, Cybernetica, CybExer Technologies, Clarified Security, RangeForce). Lisaks Eesti ettevõtetele on siin ka rahvusvaheliste küberturbe ettevõtete esindusi ja teiste valdkondade ettevõtete küberturbeosakondi (nt MalwareBytes, Microsoft, Arvato, Kühne&Nagel jt). (TalTech 2019: 6) Eestil on rahvusvaheliselt väga hea maine e-riigi ja digitaalse ühiskonna ning selle toimimiseks vajaliku küberturbe asjatundmuse poolest ning riigis sees on suhteliselt kõrge usaldus digitaalsete süsteemide suhtes (Eesti infoühiskonna … 2019: 9). Võib väita, et kõrge usaldus on mh tõendus

küberturvalisuse heast tasemest. Inimesed ei sooviks IKT-lahendusi kasutada, kui kaasnev risk oleks suurem saadavast lisandväärtusest.

Intervjuudes kinnitati Eesti head rahvusvahelist mainet ja üldist kõrget usaldust rahva seas, kuid mööndi, et valdkonnas on vajaka uutest ja värsketest ideedest. Mitmed intervjueeritud nentisid, et küberturbes rahvusvaheliselt olulise positsiooni säilitamiseks on vajalik ala aktiivselt arendada ja uute lahenduste poole pürgida. Sarnast vaatenurka tõi välja ka Griffith (2018: 5) põhjusena, miks Soome näeb jätkuvat vajadust valdkonna stimuleerimiseks olenemata oma praegusest võrdlemisi heast positsioonist. Üldist riiklikku küberturvalisuse olukorda hinnati pigem heaks, mööndes probleemidena ühtse tervikpildi puudumist (vt joonis 5). See tähendab, vaade erinevate valitsusalade küberturbesse on olemas eelkõige valitsusalasiseselt, aga puudu on strateegilisest vaatest ning tervikjuhtimisest. Üldise juhtimise ja/või poliitilise huvi puudumist küberturbe suhtes mainiti kuues intervjuus (vt ka lk 39). Üldise olukorrapildi olemasolu hindas ebapiisavaks kaheksa intervjueeritut 15-st. Mõningaste mööndustega piisavaks ja piisavaks hindas tervikpildi olemasolu vastavalt neli ja kaks vastanut. Vastust ei osanud anda üks küsitletu.

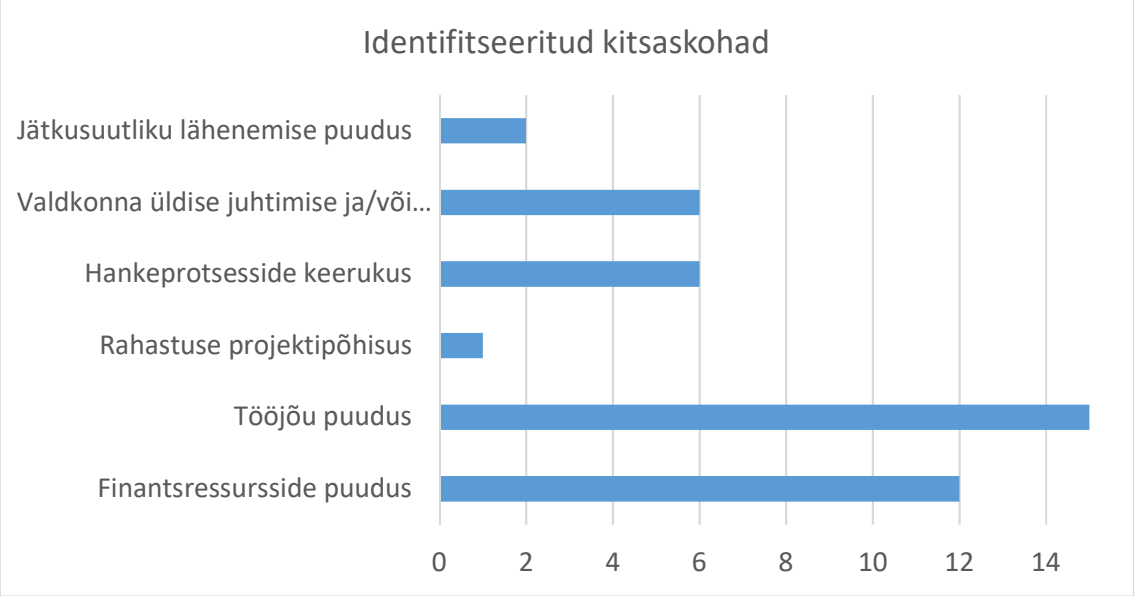


Joonis 5. Intervjueeritute hinnang küberturbealase tervikpildi olemasolule, % (autori koostatud).

Viis intervjueeritavat nentisid lisaks tervikliku ohuolukorrapildi puudumist ja kahes intervjuus toodi välja teadmise puudumist juba väljatöötatud lahenduste ja arenduste

kohta. See võib viia, ning läbiviidud arutelude põhjal on kohati juba viinud, ebamõistliku dubleerimiseni, mis eriti väikese ja piiratud ressurssidega riigi puhul ei ole soovitav. Autori hinnangul oleks oluline tegeleda tervikpildi loomiseks infovahetuse parandamisega. Eraldi tuleks analüüsida samasuguste lahenduste konsolideerimise vajadust. Avaliku sektori sees võib dubleerimine olla kohati õigustatud, näiteks seoses riikliku julgeoleku küsimustega, mille lahendusi ei pruugi konfidentsiaalsuse tõttu saada mujal valdkondades rakendada. Lisaks eelnimetatule mainiti kahes intervjuus asutuste ning ettevõtete kompetentside ülevaate puudulikkust või ei teatud, kust taolist ülevaadet võiks saada. Kõigis 15-s intervjuudes kinnitati, et probleem ei ole koostöötahte puudumises, kuid mööndi, et omavahelist koostoimimist saaks ja tuleks parendada, nii avaliku sektori sees kui ühes erasektori ja teadusasutustega.

Kõigis 15-s intervjuus nimetati ühe kitsaskohana küberturbe ekspertide vähesust (vt joonis 6).



Joonis 6. Avaliku sektori infoturge valdkonnas identifitseeritud kitsaskohad (autori koostatud).

Küberturvalisus on interdistsiplinaarne ja lai valdkond, mis vajab arendamiseks väga laia asjatundjate baasi, alates tehnoloogia spetsialistidest, analüütikutest, lõpetades juura, rahvusvaheliste suhete või riigikaitse eriteadmistega küberturbe ekspertidega. Iga eelnimetatud valdkond jaguneb omakorda erineva spetsiifikaga spetsialistideks. Samuti on puudu n-ö küberturbe valdkonda tundvatest koordinaatoritest, kes valdkonnas sidusust tekitaks (TalTech 2020a: 14). Era- ja avaliku sektori vahel on tööjõu pärast suur

konkurents, mis tekitab avalikus sektoris palgasurvet. Rahvusvaheliselt tegutsevate ettevõtetega, mis pakuvad heatasemelist palka, on riigiasutustel keeruline tööjõu pärast konkureerida. Kolmes intervjuus mööndi kaadrivoolavuse probleemi. Lisaks palga suurusele rõhutati avaliku sektori puudustena erialaste väljakutsete puudust ja liigset bürokraatiat.

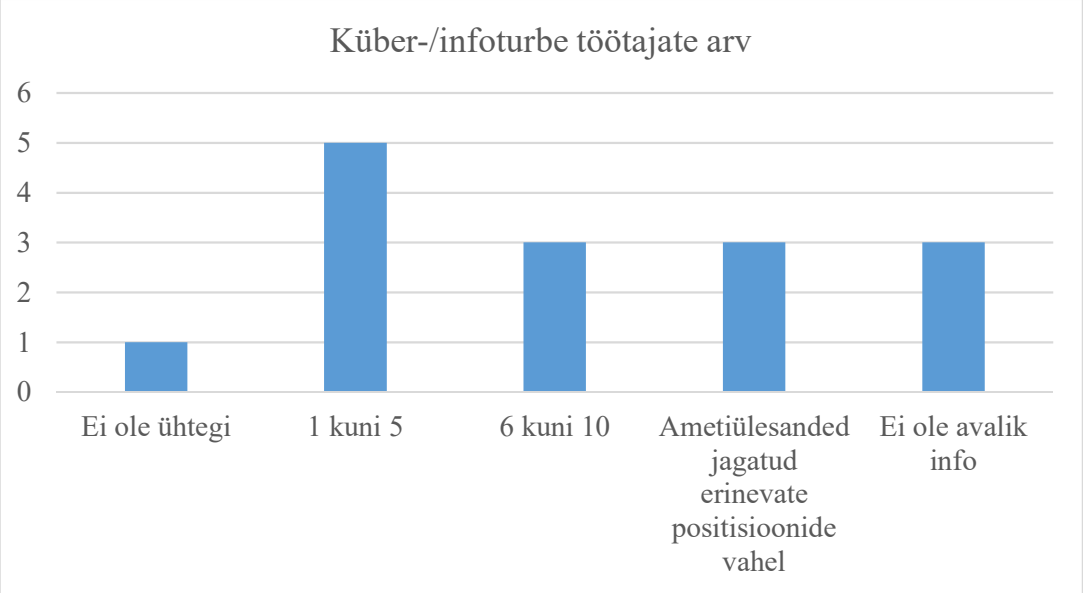
Siiski on suhteliselt väikese kogukonna hea külg tugev kogukonnatunne, mille tähtsus ilmneb eriti suuremate intsidentide (või kriiside) korral. Kaadrivoolavuselgi nähti osades intervjuudes positiivset külge: erinevate asutuste toimimise mõistmine ja arusaam küberturbe erinevatest tahkudest Eestis suureneb. Eestis toimib küberkaitse kriisihaldus üldjoontes hästi, mida illustreerib see, et intsidentidest suudetakse edukalt taastuda ja neist on osatud õppida. Siinkohal on hea näide ka avalikkuses palju tähelepanu saanud ID-kaardi kaasus (TalTech 2018: 33), mille lahendamisse panustasid paljud eksperdid, olenemata nende tolle hetke töökohast. Siiski toodi Eesti väiksust kriiside lahendamise vaatenurgast välja nii edu aluse kui kitsaskohana: ühest küljest on võimalik otsuseid kiirelt teha ja ellu viia, samas on süvaeksperte, keda väga spetsiifiliste intsidentide korral vaja läheb, vähe. Ühe võimalusena inimressursi probleemi lahendamiseks pakuti välja välismaiste turbespetsialistide väljaõpetamist ja värbamist. Välismaalastele võib avalikus sektoris küberturvalisuse valdkonnas töötamine olla tõkestatud julgeoleku ja riigikaitse kaalutlustel. Eestis olemasolevad küberturbe ja -kaitse õppekavad on rahvusvahelise vastuvõtuga, mis võimaldab tööjõu juurdekasvu. Autori arvates oleks vaja hinnata, kus oleks avaliku sektori infoturbes võimalik välismaalastel töötada, et suurendada ekspertide baasi.

Kuues intervjuus nimetati kitsaskohana hankeprotseduuride keerukust, mis pärsib aktiivsemat koostööd erasektoriga. Kolmes intervjuus mööndi, et kohati tekitatakse samaväärne kompetents või lahendus avaliku sektori asutuse juurde, mis on toimiva toote või teenusena erasektoris olemas. Koostöö erasektoriga on pidurdatud nii hankeprotsesside keerukuse kui ka koostöömudelite puudumise tõttu. Viimati nimetatu alla kuuluvad nii andmete konfidentsiaalsuse hoidmine kui näiteks intellektuaalse omandi küsimus. Asutused, kus probleem on teravamalt päevakorral, nentisid, et praegune süsteem, kus vajadusi püütakse rahuldada asutuste-siseste lahenduste väljatöötamisega, ei ole efektiivne. Hankeprotsesside muutmise käiku tajutakse niivõrd komplekssena, et

pigem jäädakse olemasoleva süsteemi juurde. Avaliku sektori sisest ja avaliku ja erasektori vahelist koostöö süsteemi juurutamist nähakse kõrgema juhtkonna ülesandena, kuna see ei ole vaid küberturbe-spetsiifiline murekoht.

Kahes intervjuus muretseti küberturbe valdkonna vähese jätkusuutliku ülesehitamise pärast asutuses. Ühest küljest kirjeldati juba eelnimetatud ekspertide puudusest tingitud olukorda, kus infoturbe osakond koosneb paarist tugevast eksperdist, keda sisulise töökatkestuseta asendada on raske. Teisest küljest peab jätkusuutlikust tagama ka tehnoloogilises aspektis: nii olemasoleva IT hoolduse kui ka uute investeeringute korral (selle tulevased hoolduskulud, ühilduvus olemasolevaga jms).

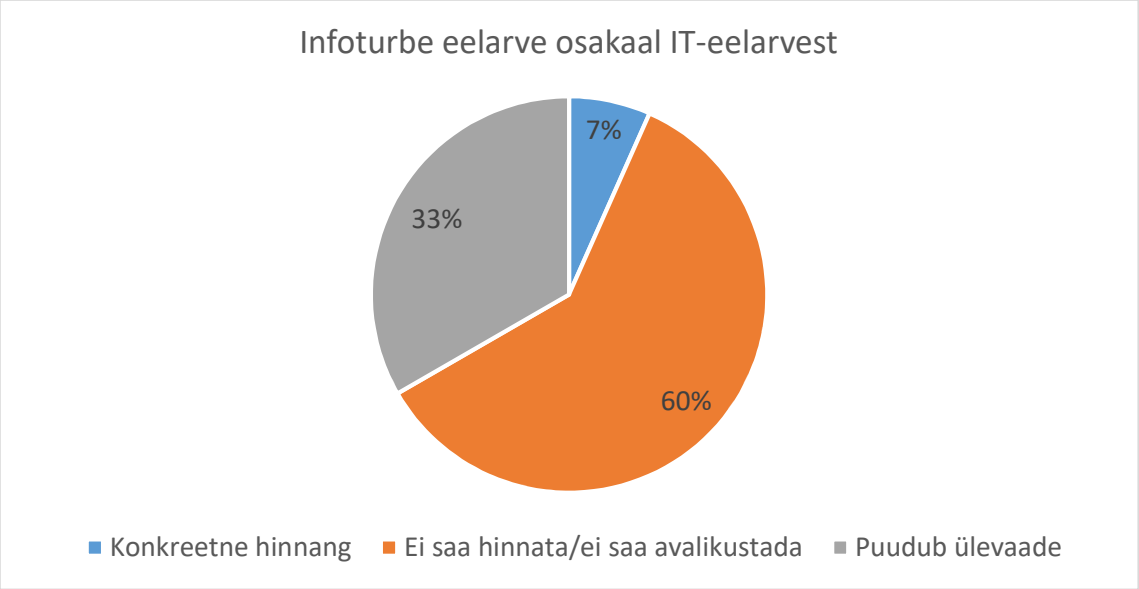
Küsimusele infoturbe ametikohtade arvu kohta vastati konkreetselt üheksal puhul 15-st ning kolmes usutluses mööndi, et olemasolevad ametipositsioonid ei täida ainult turbespetsiifilisi ülesandeid (vt joonis 7). Kolmel puhul ei soovitud antud küsimust kommenteerida, kuna vastavat informatsiooni ei saa avalikustada.



Joonis 7. Infoturbe töötajate arv intervjueeritud asutustes (autori koostatud).

Infoturbetöötajate arvu kommenteerinud üheksast intervjuust ühes mööndi küberturbe töötajate puudumist. Viies asutuses jääb küberturbe töötajate arv vahemikku 1-5 ning kolmes vahemikku 6-10 inimest. Kõik intervjueeritud asutused kinnitasid, et vajaksid küberturbe valdkonda rohkem töötajaid, et täita ettemääratud tööülesandeid.

Küber-/infoturbe eelarve küsimusele suutsid vähesed täpselt vastata (vt joonis 8), vaid ühe asutuse intervjuus öeldi, mitu protsenti üldiselt IT-eelarvest moodustab küberturbe eelarve. Eelnimetatud osakaal on autorile teada, kuid kuna tegemist on ainsa taolise hinnanguga käesolevas töös, siis ei ole seda teiste asutustega võimalik võrrelda.



Joonis 8. Küberturbe eelarve osakaal IT-eelarvest (autori koostatud).

Teised intervjueeritavad ei soovinud ligikaudseid hinnanguid anda, põhjused jagunesid sisuliselt kolmeks: ei ole avalikustatav informatsioon, raske hinnata (turbe eristamise keerukus IT-st) ning eelarve ülevaate puudumine. Kõige enam ehk 13-s intervjuus tõdeti, et infoturbe eelarve kuulub üldise IT-eelarve hulka. IT-eelarvest turbe eristamine on väga hinnanguline, kuna küberturvalisus on valdkonnana täpselt defineerimata ning eelarve võib mõnes asutustes olla vaid investeeringud küberturbetehnoloogiatesse, samas mujal hõlmata ka koolitusi või avalikke kampaaniad. Seetõttu ei pruugiks nende andmete võrdlemine, kui neid Eesti asutuste kohta oleks, osutuda korrektseks: esmalt oleks vajalik teostada ühtse metoodika alusel andmete kogumine.

Kõigis 15-s intervjuus kinnitati, et asutuse küberturbe eelarve põhineb eelmise aasta eelarvel ja kulutustel. Kuues intervjuus tõdeti, et analüüsitakse ka uue eelarve-aasta vajadusi, mis tingimata ei too kaasa vajalikke muutusi eelarves. Eelarvet mõjutava tegurina mainisid viis asutust ka (uute) regulatsioonide rakendamisega kaasnevaid vajadusi. Kõige suuremaid muutusi eelarves toovad kaasa riiki mõjutavad küberintsidendid, eriti, kui need saavad märkimisväärset kajastust meedias ja ühiskonnas.

Kahjuks tõdeti, et sellised muutused ei too kaasa eelarve-olukorra paranemist pikemas perspektiivis. 12-s intervjuus (vt ka joonis 6 lk 34) mööndi läbivat probleemi küberturbe valdkonna rahastusega organisatsioonides: küberturbe osakonnad vaevlevad pidevas baasrahastuse puuduses. Ühe intervjuu kinnitusel püütakse seda tasandada projektipõhise rahastusmudeliga. Seetõttu sõltuvad küberturvalisuse investeeringud muuhulgas Euroopa Liidu rahastusest, mis muudab pikema perspektiivi planeerimise väga ebakindlaks. Valdav enamus intervjueerituid (12) kinnitasid, et küberturbe eelarve ei ole piisav ning seetõttu ei saa kõiki vajalikke investeeringuid teha. Neist kolmes intervjuus väideti, et suudetakse tagada vaid baasturve ning kiirelt arenevas küberruumis ei ole see piisav panus. Teisest vaatenurgast kinnitati kolmes intervjuus, et olukord on arvestades piiratud ressursse (selles asutuses) küberturbes üsna hea: olulisim saab tehtud.

Alapeatükis 1.2. toonitati, et küberturbe investeeringute eesmärgiks ei ole kasu teenimine või kulude vähendamine. Kõigis 15-s läbiviidud intervjuus toodi peamiste eesmärkidena esile vastavusnõuetele kvalifitseerumist ning riskide vähendamist. Intervjuus ei eeldatud eesmärkide tähtsuse järjekorda panemist, see kumb nimetatud kahest olulisemaks osutub, varieerub investeeringute lõikes. Otsuseid mõjutavad nii asutusesisesed kui -välised infoallikad. Asutusesiseste allikatena toodi välja avastatud nõrkusi, auditeid ning töötajate teadmisi ja kogemusi. Viimati nimetatu on intervjuude põhjal asutusesisestest allikatest üheks olulisimaks, kuna on muuhulgas kõige kättesaadavam. Asutuseväliste allikatena rõhutati erinevaid regulatsioone või juhendeid.

Intervjuudes kinnitati paljudes akadeemilistes allikates kirjeldatut, et turbeinvesteeringuotsustele ei eelne üldjuhul finantsanalüüsi. Mitmed (viis intervjuud 15-st) kinnitasid, et mõõdikuid on kasutatud, kuid mõõdikute hinnangulisuse (nt lk 18 riski leevendamise näitaja) tõttu neid enam ei rakendata või kasutatakse harva.

Küsimusele, mis puudutas juhtkonna toetust küberturbe valdkonna suhtes, oli erinevaid reaktsioone (vt tabel 3).

Tabel 3. Kõrgema juhtkonna toetus küberturbe valdkonnale

Asutus	Kõrgema juhtkonna toetus küberturbe valdkonna suhtes	Kommentaar
1	Ebapiisav	
2		Asutusesisene toetus piisav, kõrgemal tasemel pigem madal
3	Piisav	
4		Asutusesisene toetus pigem hea, poliitilisel tasandil huvi olematu
5	Piisav	
6		Poliitiline huvi hinnati väga madalaks
7	Piisav	
8	Ebapiisav	
9	Piisav	
10	Piisav	
11	Ebapiisav	
12	Ebapiisav	
13		Poliitiline toetus ebapiisav
14	Piisav	
15	Ebapiisav	

Allikas: Intervjuude põhjal autori koostatud.

Kuues usutluses 15-st kinnitati, et juhtkonna toetus on piisav, neljas intervjuus toodi välja, et isegi kui asutuse tippjuhtide poolt on toetus küberturbe valdkonna suhtes olemas, siis poliitilisel tasandil ei ole küberturvalisus vajalikku tähelepanu saanud, sh kolmes intervjuus tõdeti lisaks, et poliitilisel tasandil ei peeta turbeinvesteeringuid võrreldes muude investeeringutega piisavalt olulisteks ning neid ei nähta kui investeeringut julgeolekusse. Viies intervjuus nenditi, et juhtkonna toetus ka asutusesiseselt ei ole küberturbe valdkonnale piisav, mööndes, et sellisel juhul on iga investeeringuvajaduse tõestamine keeruline. Seega võib öelda, et neis asutustes on suuremad investeeringuotsused tõenäolisemalt reaktiivsed, otsuseid tehakse *ad hoc* lahenduste kasuks. Intervjuudes mööndi, et selle põhjuseks on *ad hoc* lahenduste vajaduse kerge selgitamine ning turberikkumiste korral kohati suureneb ka poliitiline huvi teema vastu.

Selles alapeatükis kirjeldati Eesti küberturbe valdkonna korraldust avalikus sektoris ning analüüsiti läbiviidud intervjuude vastuseid. Kokkuvõtvalt võib öelda, et kuigi Eesti maine on valdkonnas üsna hea, siis vajatakse positsiooni hoidmiseks n-ö uut hingamist. Kitsaskohtadena toodi intervjuudes välja küberturbele määratud rahaliste vahendite vähesust, mis piirab valikuid ja kohati tuleb teha valikuid hädavajalike investeeringute vahel. Rahaliste vahendite piiratuse tagajärg on ka inimressursi puudus, kuna ei ole võimalik vajalikke küberturbe eksperte palgata. Positiivsena toodi intervjuudes välja tugevat kogukonnatunnet, mis on kergendanud küberintsidentidega toimetulekut ja kõrget üldist usaldust IKT lahenduste suhtes elanikkonnas.

2.3. Võimalikud turbeinvesteeringute suurendamise meetmed Eesti kontekstis

Järgnevalt vaadeldakse 1.3. alapeatükis kirjeldatud küberturbe valdkonna instrumente Eesti kontekstis ning intervjueeritute arvamusi erinevate riiklike meetmete osas. Mitmeid meetmeid on Eestis juba ka rakendatud (vt tabel 4), sh osade puhul võiks kaaluda jõulisemat rakendamist.

Töö jaoks läbiviidud intervjuude käigus uuriti ka organisatsioonide esindajate arvamusi riigipoolsete stiimulite kasutamise kohta küberturbe valdkonna edendamiseks, eelkõige investeeringute soodustamiseks. Kõik intervjueeritud (15) hindasid riigi sekkumist vajalikuks, kuid eelkõige nähti positiivsetena valdkonnaüleseid meetmeid. Kõige ebapopulaarsemate meetmetena nimetati piiranguid (ehk Carman ja Harrise tüpoloogia järgi turgu tõkestavad meetmed). Seitsmes intervjuus hinnati uusi regulatsioone ja vastavusreegleid samuti pigem negatiivsetena. Põhjuseks toodi välja, et enamasti selliseid regulatsioone ja piiranguid ei suudeta kujundada piisavalt paindlikuna ning need jäävad kiirelt ajale jalgu, hakates takistama valdkonna loomulikku arengut. Taoliste regulatsioonide kujundamine ja muutmine on aga pikaajaline protsess, isegi kui vajadus muutmiseks võib olla ilmne.

Intervjuudes mainiti ka, et poliitika kaudu muutuste toomine, eriti käitumise kujundamine, on väga pikk protsess ning seetõttu oleks vaja vaadata pikka perspektiivi ning mitte üritada kujundada praegust hetke. Seitsmes intervjuus nenditi, et Eestis puudub praegu küberturbe pika perspektiivi (10+ aastat) vaade, enne edasiste riiklike meetmete

või intensiivsemate praeguste meetmete kasutamist peaks teadma, mida soovitakse saavutada. Seatud eesmärgi saavutamine eeldaks samas ka poliitilise huvi püsimist küberturbe vastu, valimisperioodidest sõltumata. Eelnevale vastukaaluks nenditi, et pikka perspektiivi on raske planeerida, kuna küberturbe valdkond areneb kiiresti.

Huvitaval kombel vastati küsimusele, kes peaks tegelema küberturvalisuse poliitika, riiklike meetmete kujundamise või intervjuude käigus ilmnenud probleemidega tegelema, enamasti „avalik sektor" või „riik", oskamata või tahtmata täpsustada, milline asutus konkreetsemalt sellega tegelema peaks. Intervjuudest oli selles küsimuses tajutav, et „riik" on ka avaliku sektori asutuste jaoks pigem defineerimata üksus, kuhu hulka ise otseselt ei kuuluta. Samuti ei taheta ise suuremaid muutusi algatada. See on sarnane teoorias kirjeldatule, et n-ö esimese sammu (i.k. *first mover*) tegemine on välismõjude tõttu kahjulik ning selle ületamiseks on vaja riiklikku stiimulit, et kõigis ühtselt motivatsiooni tekitada.

Tabel 4. Tabel 2 (lk 22) meetmed Eesti konteksti üle tooduna

	Eestis olemas, lisasekkumist ei vaja	Eestis olemas, aga vajab jõustamist	Eestis pole, aga vajalik	Eestis pole ja intervjueeritavad ei hinda jõustatavaks
Minimaalne sekkumine	Rünnete teavitused Teadlikkuse tõstmise kampaaniad Standardid	Informatsiooni jagamine Vabatahtlikud organisatsioonid Lõimturve Organisatsiooni vastutus turbe eest	Riik kui tellija → hankeprotsesside ümberkujundamine	Turbemärgistuste süsteem
Keskmine sekkumine		Küberkindlustus T&A-tegevuse rahastamine	PPP	
Aktiivne sekkumine		(Riiklikud) regulatsioonid		Maksusoodustused

Allikas: (Jentzsch, N. 2016: 69 ja Cordes, J. J. 2011:12; läbiviidud intervjuud), autori koostatud.

Mitmed kirjanduses pakutud meetmed on Eestis juba rakendamist leidnud, seetõttu on lk 22 tabelis 2 toodud meetmed ümber jaotatud Eesti kontekstis rakendamise järgi (vt tabel 4). Tumehalli taustaga märgitud meetmed vajaksid autori hinnangul rakendamiseks täiendavat analüüsi. Rünnetest teavitamisega tegeleb Eestis sarnaselt Soome, Jaapani ja Prantsusmaaga CERT-EE, mis jagab ohuinfot ning vajadusel toetab intsidentidega

toimetulemist. Samuti on Eestis kasutusel erinevad infoturbe standardid: 2017. a andis Riigi Infosüsteemi Amet välja „Juhised infoturbe halduse süsteemi loomiseks“ (Juhised infoturbe ... 2017), kust saab täpsemalt lugeda peamiste standardite ja raamistike kohta.

Küberturvalisusealase teadlikkuse üldiseks suurendamiseks on läbi viidud kampaaniaid, üks viimatisi neist „IT-vaatlik“. Mõne läbiviidud intervjuu käigus seati nende kasutegur kahtluse alla, kuid samas tuleb tõdeda, et läbiviidud intervjuudes osalejad ei ole enamasti nende kampaaniate sihtgrupiks. Küberturbe teadlikkuse tõstmiseks juhtkondlikul ja poliitilisel tasandil rõhutati kriisiõppuste olulisust. Paaris intervjuus toodi eraldi välja õppuste stsenaariumi ja läbiviimise usutavuse olulisust, et riskide tõsidus välja kooruks. Õppuseid saab kasutada ka asutuste sees või erinevate asutuste infoturbeosakondade-vaheliselt riskide ja sõltuvuste kaardistamiseks.

Samuti on info jagamise soodustamiseks Eestis juba tööd alustatud: tegutsevad on koostööplatvormid nagu Eesti Infoturbe Assotsiatsioon (EISA … 2020), lisaks Eesti Infotehnoloogia ja Telekommunikatsiooni Liit ehk ITL (Eesti infotehnoloogia … 2020) ja Eesti kaitse- ja julgeolekutööstuse innovatsiooni klaster (Eesti kaitse-…2020), mõlemasse kuuluvad ka küberturbe organisatsioonid. Eesti Infoturbe Assotsiatsioon (EISA) asutati 2018. a ning sinna kuuluvad spetsiifilisemalt küberturbe ettevõtted, riigiasutused ning ülikoolide esindajad. Seni on EISA veel arenemisjärgus, intervjuudes mainiti aktiivse juhirolli täitja leidmise vajadust, kes assotsiatsiooni sisulise käimalükkamisega tegeleks. PPP mudeli kasutamine Eesti küberturbe valdkonnas vajaks sisulisemat analüüsi, nagu lk 23 kirjeldati, on PPP infoturbes üsna abstraktse tähendusega. Kui palju seda Eesti küberturbes teadlikult rakendatakse ja kuidas seda paremini teha, vääriksid täpsemat käsitlust. Intervjuudes kinnitati üsna tugevat kübervaldkonna kogukonnatunnet ja usaldust. Näiteks toimuvad kogukonna seminarid, kus osalevad riigiasutuste turbevaldkonna juhid ja poliitikakujundajad ning valdkonna T&A-asutuste esindajad, samuti mõned eraettevõtete turbejuhid. Kuna Eesti on väike riik, siis paljude erinevate võrgustike ja koostööplatvormide juurde loomine lisakasu ei tooks, pigem oleks vaja olemasolevad platvormid toimima saada ning erinevate platvormide omavahelised rollid ja suhted paika panna, et vähendada dubleerimist.

Üheks allikates välja toodud lahenduseks oli uute regulatsioonide ja vastavusnõuete rakendamine. Valdkonna esindajad, keda intervjueeriti, uute regulatsioonide sätestamist

ei soosinud: üheksas intervjuus mainiti teatavat rahulolematust ka praegu kehtivate nõuete osas. Põhjused olid sealjuures erinevad. Ühest küljest toodi välja asutusi, kus nõudeid täidetakse pinnapealselt ja eelkõige näiliselt korrektselt, et läbida edukalt auditeid. Isegi kui nõudeid täidetakse ka sisuliselt, aga n-ö „linnukese kirjasaamiseks“, siis ei taga see riskide õigesti haldamist. Käesolevas töös kasutatud intervjuudes rõhutati, et auditeid peaks võtma positiivse sisendina edasiseks tööks, mitte kui eksamit, kust peab parima hinde saama. Juba olemasolevate regulatsioonide puhul toodi samuti ühes intervjuus välja, et kui nõudeid ei suudeta täita, siis sellele ei järgne reaalset tagajärge. Autor leiab, et uute nõuete sätestamise asemel tuleks rõhuasetus Eestis panna olemasolevate nõuete sisulise täitmise saavutamisele. See võib tähendada mh ka olemasolevate nõuete realistlikumaks muutmist ja „nõrgemate lülide“ (suuremat) abistamist nõuete täitmisel. Praegu nähtub intervjuudest, et eksisteerib lõhe kõrgema juhtimistasandi, bürokraatia ning valdkonna spetsialistide vahel, kus oleks vaja omavahelist lähenemist.

Viies intervjuus nimetati Eesti asutuste üsna hea küberturbe olukorra põhjusena lõimturbe lähenemise kasutamist, kuid leiti, et vajalik oleks intensiivsem juurutamine. Sealhulgas võiks vaadelda lõimturvet laiema definitsiooni järgi, mille alusel tuleks kogu elutsükli jooksul hinnata arenduste turvalisust, ka koostöös teiste süsteemidega. Üheks võimaluseks on seada turvalisuse aspekt kõigi arenduste nõudeks ja jälgida rakendamist, samas laiema definitsiooni rakendamine on pigem mentaliteedi küsimus. Ka autori hinnangul, toetudes kirjandusallikatele, tuleks lõimturbe lähenemist aktiivsemalt ja elutsüklipõhiselt rakendada, see võiks vähendada ülalpidamiskulusid ja ristsõltuvustest tekkivaid riske.

Peatükis 1.3. kirjeldatud Soome poliitinstrumentidele sarnaselt on Eestiski riik küberturbe lahenduste tellijaks. Selle meetme kitsaskohana toodi välja jäikasid bürokraatlikke (hanke)protsesse. Paljudes intervjuudes kinnitati ebaefektiivset ressursside kasutamist (vt lk 34), mille põhjustajaks hankeprotseduuride keerukuse tõttu erasektoris pakutavate turbelahenduste dubleerimine avalikus sektoris. Autorile kättesaadava informatsiooni alusel ei ole võimalik anda ühest hinnangut, kas saaks lihtsustada avaliku sektori asutuste koostööd eraettevõtetega. On võimalik, et vähemalt osade valdkondade puhul, mis haldavad väga tundlikku julgeoleku või riigikaitse informatsiooni, ei olegi see võimalik.

Antud probleemipüstitus vajab edasist sisulist analüüsi ning kui ilmneb erasektorist turbelahenduste hankimise võimalikkus, siis tuleks koostöö soodustamiseks üle vaadata keerulised hankeprotseduurid.

Üsna hiljuti on Eesti turul pakkuma hakatud ka küberkindlustuse teenust, millega saab maandada organisatsioonide riske rünnete korral. Küberkindlustus võiks teoreetiliselt suurendada asutuste motivatsiooni turbesse panustada, kuid nagu varasemates peatükkides kirjeldatud, võib kahjuks toimida ka vastupidiselt. Küll aga saaks küberkindlustuse pikaajalise rakendamise kaudu koguda asjakohast informatsiooni, mida saab kasutada näiteks turbeinvesteeringu analüüsis. Küberkindlustus muutub küberturvalisuse valdkonna ja digitaalsete süsteemide suure kasutusega ilmselt aina populaarsemaks, muutudes osade autorite (nt Moore, T. 2010: 109) hinnangul samasuguseks normiks kui autokindlustus. Riigil tuleks analüüsida, kas sellele kui ühiskondliku turvalisuse suurendamise meetmele lisatuge pakkuda ning kuidas motiveerida turuosalisi end kindlustama.

Turbemärgistuste süsteemi rakendamist ei hinnanud intervjueeritavad vajalikuks, hinnates, et see muudaks „pildi kirjuks“, aga reaalset kasu ei tooks. Autori hinnangul ei oleks mõistlik luua Eestis oma märgistust, kuna turg on selleks liialt väike. Turbemärgistuste teema vajaks samuti edasist analüüsi, k.a riikidevaheline koostöö turbemärgistuste vallas (sh Euroopa Liidus). Maksusoodustuse meede hinnati kõigis (15-s) intervjuus liiga üht valdkonda soosivaks, mis ei tooks kaasa soovitud investeeringuid. Autori hinnangul tooks see kaasa näilisi muutusi (sh küberturbe investeeringute suurenemise), aga ilmselt peamiselt teisi kulusid küberturbe rahapaigutusena esitledes.

Analüüsides kirjanduses välja toodud meetmeid Eesti kontekstis tuleb tõdeda, et paljud neist on juba kasutusele võetud. Mitme meetme puhul tuleks suurendada rakendamise intensiivsust (nt lõimturbe käsitlus, regulatsioonide rakendamine jm). Mõne meetme rakendamise võimalikkus ja riigi sekkumise ulatus (nt küberkindlustuse puhul) vajab täpsemat analüüsi. Edasiste analüüside käigus vajaks vaatlemist küberturvalisuse meetmete koostoime omavahel ja koos teiste valdkondade instrumentidega, mis omavad kaudset mõju küberturbele.

KOKKUVÕTE

Info- ja kommunikatsioonitehnoloogiate lai kasutus eraisikute, erasektori, riigiasutuste jt poolt on tõstnud päevakorda kaitse küberruumis valitsevate ohtude eest ehk küberturvalisuse. Küberturve ei ole eesmärk, vaid seeläbi tagatakse (äri)tegevuse talitluspidevus. Küberruum, areneb väga kiiresti, paigalseisu vältimiseks ja ohtude realiseerumise tõenäosuse vähendamiseks peavad organisatsioonid pidevalt küberturbe valdkonnas tegema investeeringuotsuseid. Küberturbe valdkonda mõjutavad kõik peamised turutõrked: informatsiooni asümmeetria, välismõjud ja avalikud hüvised. Välismõjude ja avalike hüviste mõjul tekib alainvesteerimine, informatsiooni asümmeetria tõttu ei suudeta riske korrektselt hinnata ega investeerita õiges proportsioonis õigetesse turbemeetmetesse.

Avaliku sektori organisatsioonide eesmärgid on laiemad kui kasumi maksimeerimine ning arvesse peab võtma poliitilisi huvisid. Poliitilised eesmärgid võivad valimiste tulemusel perioodiliselt muutuda, millega kaasnevad ka eelarve jaotuse muutused. Avaliku sektori investeeringute puhul ei arvestata ainult majanduslikke mõõdikuid, vaid ka poliitilisi, nagu avalik vastutus või õiglus.

Täielikku turvalisust ei ole võimalik saavutada ning see ei ole kindlasti optimaalne lahendus, oluline on leida tasakaalupunkt riskide aktseptseerimise ja turvalisuse vahel. Küberturbe investeeringud ei too tulu, vaid hoiavad ära võimalikke kahjusid, mis küberriskide realiseerumisel tekkida võivad. Seetõttu ei ole võimalik kasutada klassikalisi kulu-tulu või investeeringu tulususe analüüsi. Alternatiivina on pakutud turbeinvesteeringu tulemuslikkuse mõõdikut (ROSI). ROSI puhul on probleem analüüsiks kasutatavate andmetega: ühest küljest on infoturbes kättesaadavaid andmeid vähe, teisest küljest põhineb osa ROSI arvutamisel kasutatavatest andmetes hinnangutel. See muudab mõõdiku manipuleeritavaks.

Teaduskirjandus poliitinstrumentide kohta on ulatuslik, kuid küberturbe valdkonna võrdlemisi lühikese ajaloo tõttu on meetmete rakendamine ja tulemuslikkus selles kontekstis suuresti analüüsimata. Magistritöös kirjeldati kolme riigi näitel (Soome, Prantsusmaa ja Jaapan) instrumentide rakendamist küberturbe valdkonna turutõrgete vähendamiseks.

Magistritöös kasutati intervjuusid, mis on läbi viidud Majandus- ja Kommunikatsiooniministeeriumi IKT Arenguprogrammi (IKT valdkonna … 2018: 19) raames TalTechi küberkriminalistika ja küberjulgeoleku keskuselt tellitud küberturbe uuringute jaoks avaliku sektori küberturvet tagavate organisatsioonide esindajatega. Kasutati poolstruktureeritud intervjuude meetodit ning magistritöös esitatud tulemused on anonümiseeritud, et tagada aus ja avameelne vestlus ning vältida võimalikku asutusi või töötajaid süüdistavat õhkkonda. Metoodika ja anonüümsus tingivad suurema tulemuste üldistamise taseme.

Intervjuudes kinnitati küberturvalisuse üldiselt head taset ja kõrget rahvusvahelist mainet, kuid mööndi tervikpildi parandamise vajadust. Avaliku sektori asutuste infoturbe enim esile toodud kitsaskoht on ekspertide puudus ning neil asutustel on keeruline heatasemelist palka pakkuvate ettevõtetega konkureerida. Infoturbe töötajate arvu kommenteeriti üheksas intervjuus 15-st, sh ühes asutuses polnud ühtki küberturbe valdkonna töötajat, viies oli töötajaid vahemikus 1-5 ning kolmes jäi töötajate arv vahemikku 6-10. Kolmes asutuses ei ole infoturbe ametipositsioone, kuid ülesanded on jagatud teiste ametikohtade vahel. Keeruliseks osutus küsimus küberturbe-eelarve kohta. Kuna küberturbe-eelarve on osa IT-eelarvest ja on tihti läbipõimunud ja raskelt eristatav, siis enamik (60%) ei soovinud hinnangut eelarve osakaalu kohta anda (või ei saanud seda avalikustada). Vastanutest 33% ei omanud muudel põhjustel ülevaadet küberturbe-eelarve kohta. Küberturbe-eelarve moodustub intervjueeritud asutustes eelmise aasta eelarve põhjal. 12-s intervjuus 15-st mööndi läbivat baasrahastuse probleemi, sh kolmes intervjuus nenditi, et suudetakse tagada vaid baasturve. Intervjuudes kinnitati teadusartiklites kirjeldatut mõõdikute kasutamise ebapopulaarsuse kohta: viies intervjuus öeldi, et kuigi mõõdikuid on kasutud, siis aktiivselt neid ei rakendata. Põhjusena mõõdetavate andmete vähesust, mistõttu palju põhineb sisetundel.

Eestis on mitmeid erialakirjanduses kirjeldatud meetmeid rakendatud. Töös jagati meetmed Eesti kontekstis rakendamise järgi nelja kategooriasse: Eestis olemas, lisasekkumist ei vaja; Eestis olemas, aga vajab jõustamist; Eestis pole rakendatud, aga vajalik ning Eestis pole rakendatud ja inetrvjueeritavad ei hinda jõustatavaks. Samuti märgiti ära instrumendid, mille rakendamise ulatus, võimalikkus või vajalikkus vajab täpsemat analüüsi.

Intervjuude põhjal vajaksid autori hinnangul Eestis olemasolevatest meetmetest jõustamist informatsiooni jagamise soodustamine (sh vabatahtlikud organisatsioonid), lõimturbe lähenemine, T&A rahastamine ning riiklikud regulatsioonid. Täpsemat analüüsi vajaks küberkindlustuse riigipoolne toetamise ja jõustamise vajalikkus ning organisatsioonide rahaline vastutus turberikkumiste eest. Kuigi Eesti riik tegutseb küberturbe turul tellijana, on vajalik analüüsida hankeprotseduuride ümberkujundamise võimalikkust.

Riigipoolsete meetmete mõjude hindamine on keeruline, kuid väärib analüüsimist, et teha läbimõeldud otsuseid. Lisaks eraldiseisvate meetmete mõjudele tuleks vaadata meetmete (sh ka kaudselt küberturbe valdkonda mõjutavate instrumentide) kombinatsioonide mõju. Käesolevas töös identifitseeriti teatava üldistuse tasemega avaliku sektori küberturbe valdkonna kitsaskohad. Autori hinnangul on oluline kirjeldada igapäevaselt valdkonnas tegutsevate intervjueeritute hinnangul esinevaid peamisi takistusi. Küberturbe valdkonna analüüse takistab ühtse definitsiooni puudumine, olemasolevad andmed ei pruugi definitsioonide erinevuse tõttu omavahel võrreldavad olla. Autor leiab, et Eesti-sisese küberturbe maastiku suhtelise väiksuse tõttu oleks huvitav koguda ühtse definitsiooni ja metoodikaga küberturbe valdkonna andmeid, mille põhjal saaks sisulisemalt analüüse läbi viia.

VIIDATUD ALLIKAD

1. Aggarwal, V. K., & Reddie, A. W. (2018a). Comparative industrial policy and cybersecurity: The US case. *Journal of Cyber Policy*, 3(3), 445–466. https://doi.org/10.1080/23738871.2018.1551910
2. Aggarwal, V. K., & Reddie, A. W. (2018b). Comparative industrial policy and cybersecurity: A framework for analysis. *Journal of Cyber Policy*, 3(3), 291–305. https://doi.org/10.1080/23738871.2018.1553989
3. Anderson, R., Moore, T. (2006). The economics of information security. *Science*, 314(5799), 610–613. https://doi.org/10.1126/science.1130992
4. Andress, J. (2014). The basics of information security: Understanding the fundamentals of InfoSec in theory and practice. Steven Winterfeld (Ed.) Oxford, UK: Elsevir Inc. https://www.academia.edu/32643426/Andress_Jason_Basics_of_Information_Security_Second_Edition (15.06.2020)
5. Bartlett, B. (2018). Government as facilitator: How Japan is building its cybersecurity market. *Journal of Cyber Policy*, 3(3), 327–343. https://doi.org/10.1080/23738871.2018.1550522
6. Bauer, J., van Eeten, M. (2011). Introduction to the Economics of Cybersecurity. *Communications & strategies*, no. 81, 1st quarter, 1-9. http://quello.msu.edu/wp-content/uploads/2015/09/Bauer-VanEeten-CS81_Intro_2011.pdf (06.06.2020)
7. Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M. H., Schmidt, J., & Weiss, J. (2012). *Cyber security policy guidebook*. Hoboken, NJ, USA: John Wiley & Sons, Inc. https://doi.org/10.1002/9781118241530
8. Bisogni, F., Cavallini, S., & Di Trocchio, S. (2011). Cybersecurity at European level: The role of information availability. *Communications and Strategies*, No. 81, 105-124, https://ssrn.com/abstract=2021825

9. Bodin, L. D., Gordon, L. A., Loeb, M. P., & Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, 37(6), 527–544. https://doi.org/10.1016/j.jaccpubpol.2018.10.004
10. Bossong, R., & Wagner, B. (2016). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law and Social Change*, 67(3), 265–288. https://doi.org/10.1007/s10611-016-9653-3
11. Campbell, J., McDonald, C., & Sethibe, T. (2010). Public and private sector it governance: Identifying contextual differences. *Australasian Journal of Information Systems*, 16(2). https://doi.org/10.3127/ajis.v16i2.538
12. Chircu, A. M., & Lee, D. H.-D. (2003). Understanding IT Investments in the Public Sector: The Case of E-Government. AMCIS 2003 Proceedings. https://aisel.aisnet.org/amcis2003/99
13. Christou, G. (2016). Introduction. In: Christou, G. (ed.), *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy* (pp 1–10). London: Palgrave Macmillan UK. https://doi.org/10.1057/9781137400529_1
14. Clark, K., Stikvoort, D., Stofbergen, E., & van den Heuvel, E. (2014). A dutch approach to cybersecurity through participation. *IEEE Security & Privacy*, 12(5), 27–34. https://doi.org/10.1109/MSP.2014.83
15. Cordes, J. J. (2011). An Overview of the Economics of Cybersecurity and Cybersecurity Policy. Salvestatud: https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/2011-6_economics_and_cybersecurity_cordes_0.pdf
16. Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835
17. D'Elia, D. (2018). Industrial policy: The holy grail of French cybersecurity strategy? *Journal of Cyber Policy*, 3(3), 385–406. https://doi.org/10.1080/23738871.2018.1553988
18. de Vries, J. (2017). What drives cybersecurity investment? Organizational factors and perspectives from decision-makers. Salvestatud: https://repository.tudelft.nl/islandora/object/uuid%3A119719ff-cb69-44c5-a566-3ee8373509f7

19. Economic analysis of cyber security. (2006) (Final Technical Report) Salvestatud: https://www.researchgate.net/publication/235082256_Economic_Analysis_of_Cyber_Security (22.05.2020)
20. Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (2020) https://www.itl.ee/ (06.08.2020)
21. Eesti infoühiskonna arengukava 2020 https://www.mkm.ee/sites/default/files/elfinder/article_files/eesti_infouhiskonna_arengukava.pdf (01.08.2020)
22. Eesti kaitse- ja julgeolekutööstuse klaster. (2020). https://defence.ee/ (06.08.2020)
23. Eesti Pank. (2020). https://www.eestipank.ee/talitluspidevus (28.07.2020)
24. EISA Estonian information security association. (2020). Salvestatud: https://eisa.ee/ (06.08.2020)
25. ENISA. (2012) *Introduction to return on security investment* (Report). Salvestatud: https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment (10.05.2020)
26. ENISA. (2015) *Definition of Cybersecurity—Gaps and overlaps in standardisation* (Report). Salvestatud: https://www.enisa.europa.eu/publications/definition-of-cybersecurity (15.05.2020)
27. Finantsinspektsioon. (2006) *Nõuded finantsjärelevalve subjekti talitluspidevuse protsessi korraldamisele*. (Juhend). Salvestatud: https://www.fi.ee/failid/talitluspidevuse_juhend1.pdf (28.07.2020)
28. Fraunhofer institute for secure information technology. (2014) *Development of Secure Software with Security By Design.* (Technical report). Salvestatud: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Trendreport_Security_by_Design_EN.pdf?_=1409579733 (30.07.2020)
29. Gordon, L. (2007) *Incentives for improving cybersecurity in the private sector: A cost-benefit perspective* (Congressional Testimony). House Committee on Homeland Security's Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.549.7147&rep=rep1&type=pdf (10.05.2020)

30. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274
31. Gordon, L. A., & Loeb, M. P. (2003). The economics of information security investment. *ACM Transactions on Information and System Security* (TISSEC), 5(4), 438–457. https://doi.org/10.1145/581271.581274
32. Gordon, L. A., & Loeb, M. P. (2006). Economic aspects of information security: An emerging field of research. *Information Systems Frontiers*, 8(5), 335–337. https://doi.org/10.1007/s10796-006-9010-7
33. Griffith, M. K. (2018). *Working paper series a comprehensive cyber security approach: Bolstering cybersecurity capacity through industrial policy.* (Working paper). Salvestatud: https://www.semanticscholar.org/paper/WORKING-PAPER-SERIES-A-COMPREHENSIVE-CYBER-SECURITY-Griffith/d7ab9b909c5e9dbf51420bf72943f000d3005163
34. Harris, R. G., & Carman, J. M. (1984). Public regulation of marketing activity: Part ii: regulatory responses to market failures. *Journal of Macromarketing*, 4(1), 41–52. https://doi.org/10.1177/027614678400400105
35. IKT valdkonna arenguprogramm. (2018) Salvestatud: https://www.mkm.ee/sites/default/files/ikt_arenguprogrammi_uuendamine_29.11.2018.pdf (06.06.2020)
36. Innopolis Konsultatsioonid AS, SEB Pank AS. (2008) *Private public partnership (PPP) projektid: Kohalike omavalitsuste uuring.* Salvestatud http://www.innopolis.ee/UserFiles/Uuringud/SEB_uuring_ppp.pdf (15.07.2020)
37. Jentzsch, N. (2016). *State-of-the-art of the economics of cyber-security and privacy* (SSRN Scholarly Paper Nr ID 2671291). Rochester, NY: Social Science Research Network. Salvestatud: https://papers.ssrn.com/abstract=2671291
38. Juhised infoturbe halduse süsteemi loomiseks. (2017) Salvestatud: https://www.ria.ee/sites/default/files/content-editors/KIIK/juhised_infoturbe_halduse_susteemi_loomiseks.pdf (14.07.2020)
39. Küberintsidentide käsitlemine cert-ee. Riigi Infosüsteemi Amet. (2020) Salvestatud: https://www.ria.ee/et/kuberturvalisus/cert-ee.html (25.07.2020)

40. Küberjulgeoleku strateegia 2008-2013. (2008) Salvestatud: https://www.valitsus.ee/sites/default/files/content-editors/arengukavad/kuberjulgeoleku_strateegia_2008-2013.pdf (05.08.2020)
41. Küberturvalisus. Majandus- ja Kommunikatsiooniministeeriumi. (2020). Salvestatud: https://www.mkm.ee/et/eesmargid-tegevused/kuberturvalisus (05.08.2020)
42. Küberturvalisuse seadus. (2018). Riigi Teataja. Salvestatud: https://www.riigiteataja.ee/akt/K%C3%BCTS (05.08.2020)
43. Küberturvalisuse strateegia 2019-2022 (2019) Salvestatud: https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf (05.05.2020)
44. Ministeeriumi tutvustus. Majandus- ja Kommunikatsiooniministeeriumi (2020). Salvestatud: https://www.mkm.ee/et/ministeerium-kontaktid/ministeeriumi-tutvustus (05.08.2020)
45. Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, 3(3–4), 103–117. https://doi.org/10.1016/j.ijcip.2010.10.002
46. Moore, T., Dynes, S., & Chang, F. (2015). *Identifying how firms manage cybersecurity investment.* Salvestatud: https://cpb-us-w2.wpmucdn.com/blog.smu.edu/dist/e/97/files/2015/10/SMU-IBM.pdf
47. Olukord küberruumis – juuni 2020. (2020) Riigi Infosüsteemi Amet. https://www.ria.ee/sites/default/files/avalik_olukord_kyberrumis_juuni2020.pdf (06.08.2020)
48. Riigi Infosüsteemi Amet (2020) *Riigi Infosüsteemi Ameti aastaraamat 2020*. Salvestatud: https://www.ria.ee/sites/default/files/ria_aastaraamat_2020_48lk_est_veeb.pdf (05.08.2020)
49. Riigikantselei ülesanded ja struktuur. (2020). Salvestatud: https://www.riigikantselei.ee/et/organisatsioon-kontaktid/riigikantselei-ulesanded-ja-struktuur (05.08.2020)

50. Sonnenreich, W., Albanese, J., & Stout, B. (2005). Return on security investment (ROSI): A practical quantitative model. *Journal of Research and Practice in Information Technology,* 38:239-252. https://doi.org/10.5220/0002580202390252
51. Taltech. (2018) ID-kaardi kaasuse õppetunnid. Salvestatud: https://www.ria.ee/sites/default/files/content-editors/EID/id-kaardi_oppetunnid.pdf
52. Taltech. (2019) *Eesti küberturvalisuse võime analüüs*. Asutusesiseseks kasutamiseks.
53. Taltech. (2020a) *Estonia's Industrial Policy Concept for the Cyber Security Market.* (Report). https://www.mkm.ee/sites/default/files/content-editors/failid/E_riik/estonias_industrial_policy_concept_for_the_cyber_security_market.pdf
54. Taltech. (2020b). Estonian cybersecurity R&D concept. (Report) Salvestatud: https://www.mkm.ee/sites/default/files/content-editors/failid/E_riik/estonian_cybersecurity_rd_concept.pdf
55. Understanding difference between cyber security & information security (2016). Salvestatud: https://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information (05.06.2020)
56. Vagle, J. L. (2020). Cybersecurity and Moral Hazard. *Stanford Technology Law Review*, *23*(1), 71–113. https://doi.org/10.2139/ssrn.3055231
57. Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, 57, 101173. https://doi.org/10.1016/j.pacfin.2019.101173
58. Winkler, T.J. (2013). IT Governance Mechanisms and Administration/IT Alignment in the Public Sector: A Conceptual Model and Case Validation. Wirtschaftsinformatik Proceedings. https://aisel.aisnet.org/wi2013/53
59. von Solms, B., & von Solms, R. (2018). Cybersecurity and information security – what goes where? *Information and Computer Security*, 26(1), 2–9. https://doi.org/10.1108/ICS-04-2017-0025
60. von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

LISAD

Lisa 1. Valdkonna mõisted ja definitsioonid

Mõiste	Definitsioon	Kommentaar
Küber-	Eesliide, mis tähistab võrgu- ja infosüsteeme.	Näiteks küberturvalisuse seaduse mõistes on võrgu- ja infosüsteem elektroonilise side võrk, seade või omavahel ühendatud või seotud seadmete rühm, millest vähemalt ühes toimub digitaalsete andmete töötlemine.
Küberturvalisus	Seisund, kus võrgu- ja infosüsteemid on kaitstud ohtude realiseerumise eest.	Inglise keeles defineeritakse antud terminit (cybersecurity) samuti turvalisuse tagamisena. Eesti keeles kasutatakse sellises kontekstis terminit „küberturve“.
Küberturve	Võrgu- ja infosüsteemide turvalisuse tagamine.	Teiste sõnadega on küberturve meetmete rakendamine küberturvalisuse saavutamiseks.
Küberjulgeolek	Seisund, kus riigi julgeolek on kaitstud võrgu- ja infosüsteemide kaudu tekkivate ohtude eest.	Eesti keeles on kasutusel kaks mõistet – turvalisus ja julgeolek. Inglise keeles sellist vahet ei tehta (security). Seetõttu võiks „küberjulgeoleku“ tõlge olla inglise keeles „National Cybersecurity“.
Küberhügieen	Üksikisiku või organisatsiooni elementaarsed toimingud vältimaks võrgu- ja infosüsteemide kaudu tekkivate ohtude realiseerumist.	
Küberintsident	Võrgu- ja infosüsteemis toimuv ootamatu sündmus, mis ohustab või kahjustab süsteemi turvalisust.	Baseerub küberturvalisuse seaduse terminil.
Küberkaitse	Meetmete rakendamine küberrünnakute ennetamiseks ja tõrjumiseks.	Üldjuhul on mõiste kasutusel riigikaitse valdkonnas.
Küberkriis	Küberintsidendist põhjustatud hädaolukord või hädaolukorra oht.	Hädaolukord ja hädaolukorra oht on defineeritud hädaolukorra seaduses.
Küberkuritegu	Kuritegu, mis on toime pandud arvutisüsteemi, või arvutiandmete vastu kasutades IKT vahendeid.	Budapesti konventsioon: *Offences against the CIA of computer data and systems.*
Küberoht	Võrgu- ja infosüsteemi kaudu tekkiv sündmus või asjaolu, mis võib põhjustada kahju.	
Küber-operatsioon	Võrgu- ja infosüsteemide keskkonnas kindlal eesmärgil toimuv küberturvalisust mõjutav tegevus.	Tavaliselt räägitakse operatsioonidest riigi julgeoleku kontekstis.
Küberruum	Võrgu- ja infosüsteemide ühendamisel tekkiv keskkond.	Näiteks on internet globaalne küberruum.
Küberrünnak	Tahtlik tegevus võrgu- ja infosüsteemide kaudu kahju tekitamise eesmärgil.	

Allikas: (Küberturvalisuse strateegia … 2019: 40-42)

Lisa 2. Küberturbe valdkonna stiimulid Soomes, Jaapanis ja Prantsusmaal Carman ja Harris tüpoloogia järgi.

	Turgu loov	**Turgu hõlbustav**	**Turgu muutev**	**Turgu asendav**
	Riiklik poliitika uute turgude loomiseks läbi õiguste, stiimulite	*Edendab või parendab turgude toimimist, tehingukulude vähendamise, stiimulite suurendamise või kulude ja kasude internaliseerimise kaudu*	*Muudab turuosapoolte käitumist või kauplemistingimusi, saavutamaks tingimusi, mida turul muidu ei teki*	*Poliitilised meetmed ressursside eraldamiseks või ressursside teistsuguseks jaotamiseks*
Soome		T&A rahastus	Koostööd soodustavad platvormid	Küberturbe-spetsiifiline haridus
		Riik kui tellija	Klastrid, FISC	Kriitilistele sektoritele riiklik turbeturg
		Küberintsidentide seire, ohuteavitus, nõustamine (NCSC-FI)	Riigikaitsekursused, sh küberturve	Küberajateenistus
		Kübersõja väljaõppekeskus (*Cyber War Room)*		
Jaapan	Küberturvalisuse teadlikkuse tõstmine			Pahavara ja *bot*'ide eemaldamise programm
		Turbekoolituste programmid		Küberturbe haridus
		Poliitika konsultatsioonid		
		T&A-rahastus		
		Regulatiivne võim		
		Maksupoliitika		
				Küberintsidentide seire, ohuteavitus, info jagamine (JPCERT/CC)

Lisa 1. järg

	Turgu loov	**Turgu hõlbustav**	**Turgu muutev**	**Turgu asendav**
Prantsus-maa	Kübertööstuse plaan		Turbestandardid ja juriidilised meetmed kriitilise infrastruktuuri asutustele	
	Küberkaitse klaster			
		Töögrupp standardite väljatöötamiseks, riskide maandamiseks		
		Prantsuse kompetentsikeskus küberkuritegevusega võitlemiseks (PPP)		
		Cyber Defence reservväelaste võrgustik		
		Küberturvalisuse teadlikkuse tõstmine		
		Küberintsidentide seire, ohuteavitus, nõustamine (CERT-FR)		
		Prantsusmaa turbejuhtide võrgustik		
		Riiklikud kriisijuhtimise kursused, sh küberturve		

Allikas: (Harris, R. G., Carman, J. M. 1984: 43; Bartlett, B. 2018, Griffith, M. 2018; D'Elia, D. 2018), autori koostatud.

Lisa 3. Poolstruktureeritud intervjuude küsimustik

- Eesti küberturbe üldise hetkeolukorra kaardistamine
    1) Milline on teie hinnang Eesti riigi küberturvalisuse hetkeolukorrale. Palun põhjendage oma seisukohta.
    2) Kas küberturvalisuse valdkonnas tegutsetakse eraldiseisvalt (igaüks omaette) või koostöös? Palun põhjendage.
    3) Oluline selles kontekstis on interoperabiilsus ehk koostöö võimekus. Kas kõik osapooled on koostöövõimelised ja -tahtelised?
    4) Milline on teie asutuse küberturbe-alane koostöö ettevõtete ja teiste asutustega?
- Asutuse küber-/infoturbe seisund
    5) Kirjeldage oma asutuse rolli küberturvalisuse tagamisel.
    6) Kirjeldage oma asutuse küber-/infoturbe osakonna struktuuri.
        a. Mitu turbele orienteeritud ametikohta on teie asutuses võrreldes teiste IKT ametikohtadega kokku?
    7) Mitu protsenti asutuse IKT eelarvest kulutatakse hinnanguliselt küberturbele?
        a. Kas küberturbe eelarve on piisav võrreldes väljaminekutega?
        b. Mille alusel eelarve moodustub (prognoositavad kulud, eelmiste aastate eelarve vm)?
        c. Kuidas on inforturbe/küberturbe eelarve viimaste aastate jooksul muutunud?
    8) Mis omadus on küberturbe investeeringu puhul teie asutuses kõige tähtsam: kulude vähendamine, vastavusnõuded, riski vähendamine, protsessi parendamine või miski muu?
    9) Kas kasutate turbeinvesteeringute puhul mõõdikuid (kulu-tulu analüüs, ROSI vmt)?
    10) Mille alusel teie asutuses turbeinvesteeringute vajadusi kaardistatakse?
    11) Kas kõrgema juhtkonna toetus küberturbe valdkonnale on teie hinnangul piisav?
        a. Kas toetus on muutunud?
    12) Mis on teie asutuses peamised kitsaskohad küberturbe vaatenurgast?
- Arutelu (võimalike) riiklike meetmete üle

Lisa 3. järg

13) Millised on teie arvates kõige olulisemad riiklikud meetmed, mida Eesti on rakendanud ja peaks oma küberturvalisuse olukorra parendamiseks rakendama?
14) Mis on teie hinnang järgmiste meetmete kasutamisele? Kui need on Eestis juba kasutusel, siis kas see on teie hinnangul edukas? Mis vajaks muutmist?
    a. Informatsiooni jagamise soodustamine
    b. Küberkindlustus
    c. Lõimturve
    d. Maksusoodustused
    e. Organisatsiooni vastutus turbe eest
    f. PPP
    g. Riik kui tellija (sh hangete lihtsustamine)
    h. Riiklikud regulatsioonid
    i. Rünnete teavitused
    j. T&A rahastamine
    k. Teadlikkuse tõstmise kampaaniad
    l. Turbemärgistused
    m. Turbestandardid
    n. Vabatahtlike organisatsioonide loomine

SUMMARY
SUMMARY

PROBLEMS AND POLICY INSTRUMENTS FOR PROMOTING CYBERSECURITY INVESTMENTS BASED ON THE EXAMPLE OF ESTONIAN PUBLIC SECTOR ORGANISATIONS

Martha Jung

ICTsolutions have become the basis of our societies today. People, various organisations and nations use different ITsystems in their everyday lives and it is more difficult than ever to differentiate between the digital and "real world". A lot of attention is given to cybersecurity to tackle the threats from cyberspace. The goal of cybersecurity is to maintain the confidentiality, integrity and availability of the digital information. Cyber security is not a goal in itself, but rather is used to maintain business continuity.

Estonia's society is highly intertwined with ITsolutions. Internationally, Estonia's digital society and e-systems have a very good reputation and the trust in these solutions is also high among its people. Estonia has been a digital society for almost 20 years and the economic impact of using e-solutions is substantial. A developed ecosystem, technological know-how and good reputation will not ensure a good position for the future – cyberspace changes very fast and is difficult to predict. This means that there is an ongoing requirement to contribute into the field and invest in the continuous development of cyberspace.

This Master's thesis researches the main problems of Estonian public sector organisations' cybersecurity investments and presents policy instruments offered in academic literature for cybersecurity investment promotion. The paper investigates organisations that provides cybersecurity either in their governance area or across areas, because their impact on the sector is the biggest.

The following tasks were undertaken to fulfil the research objectives:

- explain the nature and importance of cybersecurity and the market failures affecting cyber security;

- analyse cyber security investment decision-making processes at the organisational level and explain the differences between public and private sector decision-making processes;
- highlight the policy instruments proposed in the academic literature that would help to solve the problems arising from market failures in the field of cyber security, including the quality of investments;
- conduct interviews with representatives of Estonian public sector institutions involved in ensuring cybersecurity in order to gather information on the current state of cybersecurity in Estonia;
- analyse the background of security investments of public sector institutions dealing with cybersecurity on the basis of information gathered from interviews;
- analyse out the measures proposed in the academic literature suitable for the Estonian context.

The theoretical background of the work is formed by academic articles and studies on cyber security economics, organisational security investment decision-making processes and policy measures used to stimulate investments in the field of cyber security. As cybersecurity is part of information security and cybersecurity is a more recent field of research, in addition to the nature of cybersecurity investments, information security investment decision-making processes and governance issues are also examined. Scientific literature describing the differences between the public and private sectors, including IT investments, has also been used. The budget for cybersecurity is part of the IT budget, thus allowing links to be drawn between the two. In the empirical part of this Master's thesis, the author has used interviews conducted in 2019 for research commissioned within the framework of the ICT Development Program with representatives of Estonian public sector organisations providing cybersecurity within or across government areas,. Semi-structured interviews were used and the results presented in the Master's thesis are anonymised in order to ensure honest and open conversation and to avoid apportioning blame. The methodology and anonymity led to a higher level of generalisation of results.

The goals of public sector organisations go beyond profit maximisation and political interests must be taken into account. Political objectives may change periodically as the result of elections, which may be accompanied by changes in the budget distribution. When making investments in public sector organisations, one has to take into account not only economic indicators but also political ones, such as public responsibility or fairness.

Perfect cybersecurity cannot be achieved. For the optimal situation it is important to find a balance between risk acceptance and security. Cybersecurity investments do not generate returns, but prevent potential losses that may arise if cyber risks materialise. Therefore, it is not possible to use classic cost-benefit analysis or return on investment analysis. Alternatively, return on security investment (ROSI) has been proposed. In the case of ROSI, there is a problem with the data used for analysis. Although there is little data available in information security in general, some of it, used to calculate ROSI, is based on estimates. This makes it relatively easy to manipulate.

The scientific literature on policy instruments is extensive, but due to the relatively short history of cybersecurity, the implementation and effectiveness of measures in this context are largely unanalysed. This thesis describes the application of instruments to reduce market failures in the field of cybersecurity using the example of three countries: Finland, France and Japan.

As previously stated, interviews with representatives of Estonia's public sector organisations that provide cybersecurity were used. These confirmed the generally good level of cybersecurity and the country's significant international reputation, but acknowledged the need to improve the overall situational awareness. The most highlighted issue in the information security of public sector institutions is a lack of experts as these institutions find it difficult to compete with private sector companies offering higher salaries. 9 out of 15 interviews commented on the number of cybersecurity employees, including one that had zero employees. Five out of the 9 that answered had 1-5 security employees, three had 6-10 employees and three used other positions to conduct cybersecurity tasks. The question about cybersecurity budgets in the organisations proved difficult. As the cyber security budget is part of the IT budget and is often intertwined and difficult to distinguish, the majority (60%) were reluctant to provide an estimate of the share of the budget or could not make it public. 33% of

respondents did not have an overview of the cybersecurity budget for other reasons. The cybersecurity budget in the interviewed institutions is formed on the basis of the previous year's budget. In 12 of the 15 interviews, the problem of basic funding was acknowledged, including three interviews where it was stated that only basic cybersecurity measures can be implemented. The interviews confirmed what was described in the academic articles about the unpopularity of the use of metrics (like ROSI). Five interviewees said that they have tried using metrics, but they are not actively used. The reason is the lack of measurable data and decisions based on intuition.

In Estonia, several policy measures described in the literature have already been implemented. According to the implementation in the Estonian context, the measures were divided into four categories: already existent in Estonia, no additional intervention is needed; existent in Estonia, but needs enforcement; not existent in Estonia, but should be implemented and not existent in Estonia and the interviewees do not consider it enforceable. Instruments, that needed further analysis in the Estonian context, were also identified.

Based on the interviews, in the author's opinion, the promotion of information sharing (incl. voluntary organisations), the security-by-design, R&D funding and state regulations would need enhancing. A more detailed analysis is needed on cyber insurance and if the state should support and enforce it. Also a deeper look into procurement procedures used in the public sector is needed, as this was one of the issues that was identified that does not allow easy collaboration between the private and public sector.

Assessing the effects of policy measures is complex, but it is worth analysing to make informed decisions. In addition to the effects of individual measures, the effects of combined instruments, including instruments that indirectly affect cybersecurity, should be considered. This paper identified a number of issues in the field of public sector cybersecurity in Estonia and a certain level of generalisation. It is the author's opinion, it is important to identify the main problems that real-life experts working in cybersecurity have. Analysis in the field of cyber security are hindered by the lack of a common definition of cybersecurity, which means existing data may not be comparable due to differences in definitions. In the author's opinion that it would be interesting to collect data in the field of cybersecurity in Estonia due to the relatively small size of the

cybersecurity ecosystem within the country, with a common definition and methodology. Further and more substantive analyses could be performed on that data.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Martha Jung,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose Küberturbe investeeringute probleemid ja meetmed turbeinvesteeringute soodustamiseks Eesti avaliku sektori organisatsioonide põhjal,

   mille juhendaja on prof. Kadri Ukrainski, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Martha Jung
/digitaalselt allkirjastatud/
11.08.2020