TARTU ÜLIKOOL

Majandusteaduskond

Kristjan Põldre

ORGANISATSIOONI ÜLENE KÜBERRISKIDE MAANDAMINE EESTI HAIGLATE NÄITEL

Magistritöö ärijuhtimise magistrikraadi taotlemiseks
strateegilise juhtimise erialal

Juhendaja: dotsent Eneli Kindsiko, PhD

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

2017. aasta algas päris tumedates toonides, kui pahavara nimega Wannacry, mis krüpteeris[1] Microsoft Windows operatsioonisüsteemiga arvutite kõvaketta ja nõudis dekrüpteerimise[2] eest lunaraha, tekitas kokku maailmas organisatsioonidele üle 8 miljardi dollari kahju (Parenty & Domet, 2019, lk 104). Sellele järgnes koheselt sarnane uus lunavara rünnakulaine Petya/NotPetya, mis levis kokku 65 riiki ja tekitas kahjusid üle 1,2 miljardi dollari. Puutumata ei jäänud ka Eesti ettevõtted nagu Saint-Gobain Eesti, Kantar Emor ja Ehituse ABC (Riigi Infosüsteemi Amet, 2018, lk 24). Neist viimane, Ehituse ABC, suutis tagantjärgi hinnata tekkinud kahjuks 2 miljonit eurot, sest poed olid kinni ligi 2 nädalat. Kokku registreeris Riigi Infosüsteemi Amet (edaspidi ka RIA) 2019. aastal 24 369 juhtumit, kuid tegemist on ainult murdosaga juhtumitest Eestis, sest paljudest intsidentidest ei antagi teada (Riigi Infosüsteemi Amet, 2020, lk 2).

2020. aasta alguses seisis maailm silmitsi uue olukorra ja kriisiga, COVID-19 pandeemia. Kui suurem osa ettevõtetest, näiteks muuhulgas turismi- ja meelelahutussektor, tõmbasid äritegevust koomale, siis küberkuritegelik tegevus muutus kordades aktiivsemaks. Tsehhi Vabariigis jäi 2020. aasta märtsis Brno Ülikooli Kliinikum pahavara rünnaku alla ja oli sunnitud kõik infosüsteemid välja lülitama ning seda olukorras, kus levis koroonaviirus ja antud kliinikum oli piirkonna üks testimise ning ravikeskuseid (Porter, 2020).

Infotehnoloogia- ja kommunikatsioonilahendused osa meie igapäevast, nii tööl kui kodus, ja lisaks saab nende abil luua murranguid erinevates valdkondades, näiteks haridus ja tervishoid (Ki-moon, 2013). Paljud organisatsioonid ei mõista riske uute tehnoloogiate kasutusele võtmisel ehk kuidas iga lisanduva tehnoloogiaga kaasnevad ka küberohud. Isegi kogenud infotehnoloogia eksperdid Põhja-Ameerikast ja Lääne-Euroopast tunnevad muret pidevalt kasvava keerukusega tehnoloogias ja küberohtudes, samuti on alarmeeriv

[1] Krüpteerimise eesmärgiks on muuta failis asuvad andmed võõrastele loetamatuteks ehk info salastada.
[2] Vastupidine tegevus krüpteerimisele, et oleks võimalik andmeid lugeda.

andmemahtude kasv ja karmimad regulatsioonid andmekaitses (Lundell, 2020, lk 31). Üle maailma kulutatakse küberturvalisusele miljardeid, kuid sama jõudsalt kasvavad ka kahjud – selle üheks põhjuseks on, et antud teema jäetakse lahendada ainult infotehnoloogia (IT) osakondadele ning juhtkond distantseerub, kuna teema jääb liiga keeruliseks (Parenty & Domet, 2019, lk 104).

ÜRO peasekretär Ban Ki-moon väljendas juba 2013. aasta pöördumises, et küberrünnakutel on potensiaal tekitada globaalse mõjuga ebastabiilsust, seega peab küberturvalisus olema kõigi mure (Ki-moon, 2013). Esmalt on oluline on saavutada baasteadmised küberohudest juhtkonna tasemel ning selgitada välja kõik organisatsiooni toimimiseks olulised komponendid. Seejärel analüüsida, kuidas ja kelle eest peab end kaitstma – tunne oma vaenlast – ning küberriskide maandamise vastutus peab liikuma osaliselt IT osakonnalt organisatsiooni juhtkonnale (Parenty & Domet, 2019, lk 104).

Erinevate infotehnoloogiliste süsteemide arendamiseks ning ülevalhoidmiseks kulub palju ressursse ja on vaja kõrgelt kvalifitseeritud tööjõudu. Üldiselt jääb vastuseta küsimus, kuidas luua ja käidelda süsteeme võimalikult madalate kuludega – säilitades sealjuures tasakaal kasutuse kvaliteedis, mugavuses ja turvalisuses. Paraku on tihti nii, et kokkuhoid saavutatakse just küberturvalisuse pealt, kuna tegemist on esmalt hoomamatu riski ja suure kuluga. Organisatsioonid ei näe terviklikku pilti, et kui küberrünnaku tulemusel varastatakse andmeid, siis millised kahjud ja mõjud võivad sellega kaasneda.

Küberohud on kasvanud viimastel aastatel kordades, muutudes pidevalt nii vormilt kui ka sisult. Ühe uuringu kohaselt, kuni 85% organisatsioonidest puutuvad kokku pahavaraga igapäevaselt (Lundell, 2020, lk 34). Eelnevalt mainitud lunavarade vastu on leitud küll kaitsemehhanisme, kuid kahjuks on ka uute küberohtude areng pidev. Uute rünnakute väljatöötamisel on kurjategija ikka ühe sammu eespool. Lisaks on vähem teada asjaolu, et küberrünnaku tellimine on odavam tegevus kui võiks eeldada. Näiteks ligipääs häkitud arvutisse võib maksta kõigest 35 dollarit (Arvutimaailm, 2020).

Analüüsides Eesti haiglate näitel võimalikke küberohte ja nende tajumist on magistritöö eesmärk teha ettepanekuid küberriskide maandamiseks organisatsiooni üleselt. Eesmärgi täitmiseks on autor seadnud järgmised uurimisülesanded:

1) anda ülevaade küberohtude olemustest, eesmärkidest ja trendidest;
2) anda ülevaade küberohtudest tervishoiusektoris ja meetmetest küberriskide maandamiseks;
3) dokumendianalüüsi ja poolstruktureeritud intervjuude toel analüüsida Eesti haiglate struktuuri, arengukavasid, hankeid ja tulemiaruandeid, et selgitada välja küberriskide maandamise võimalused organisatsiooni üleselt – baseerudes teoreetilistel ja empiirilistel uuringutel;
4) ettepanekute tegemine küberriskide maandamiseks organisatsiooni üleselt Eesti haiglatele.

Uurimisülesannete täitmiseks analüüsib autor erialast teaduskirjandust, kuid ka rahvusvaheliste ekspertide ja organisatsioonide raporteid ning hinnanguid. Tallinna Tehnikaülikoolis on varasemalt kaitstud sarnaseid magistritöid. Näiteks Erik Tamsalu magistritöö 2019. aastal teemal „Elektrivõrgu digitaliseerimisest tulenevate küberriskide ja nende võimalike mõjude analüüs“ ning Michael Anywar magistritöö 2018. aastal teemal „Eesti haiglate küberohu võimalikkus: Haiglates kasutusel olevate küberjulgeoleku standardite hindamine, tõkestamaks küberohte“. Eelpool mainitud tööd keskendusid pigem küberturvalisuse tehnilise poolele, hinnates haiglate võimekust ja valmisolekut erinevate tehnoloogiate ja regulatsioonide vaatest. Käesoleva magistritöö eesmärgiks on keskenduda küberriskide maandamisele organisatsiooni üleselt.

Magistritöö jaguneb kaheks osaks – teoreetiliseks ja empiiriliseks. Esimeses, teoreetilises osas, käsitleb autor erinevaid küberriske, selgitamaks välja peamiste küberohtude olemuse, trendid ja küberrünnakute eesmärgid. Teoreetilise osa teises alapunktis keskendub autor tervishoiusektoriga seotud küberriskidele ning nende arengule, kuid toob ka välja meetmed ja lahendused, keskendudes organisatsiooni ülestele küberriskide maandamisele. Töö teises, empiirilises, osas kajastab autor dokumendianalüüsi ja poolstruktrureeritud intervjuude tulemusi, et selgitada välja Eesti haiglate võimekus organisatsiooni üleselt küberriske maandada ning teeb ettepanekuid selle parandamiseks.

Märksõnad: küberturve, organisatsioonid, riskid.

Teaduseriala kood CERCS: S190 Ettevõtte juhtimine.

1. KÜBEROHTUDE MÕJUD JA KÜBERRISKIDE MAANDAMINE TERVISHOIUSEKTORIS

1.1. Küberohtude olemus

Sõjakunsti raamatus on Sun Tzu (6.-5. saj. e.Kr.) öelnud, et tunne oma vaenlast ja tunne iseennast, et pidada vastu kasvõi 100 võitlust. Analoogselt saame käsitleda ka organisatsioonide vastaseid küberrünnakuid, kus ühelt poolt on oluline teada, millised on erinevad häkkerite liigid ja küberohud ning võimalikud mõjud. Teiselt poolt aga on oluline organisatsiooni varade tundmine, mida on vaja kaitsta. Eelpool mainitud aspektid on käesoleva alampunkti eesmärgiks ning lisaks käsitleb autor ka küberohtude arenguid ning trende.

Eesliidest *küber-* kasutatakse üldiselt erinevate infotehnoloogiliste süsteemide kirjeldamiseks ning küberoht on eelnevalt mainitud süsteemide kaudu tekkiv sündmus või asjaolu, mis võib põhjustada erinevat tüüpi kahju (Gordijn et al., 2020, lk 11–12). Küberohu termin on tulnud kasutusele aastakümneid tagasi, 1980ndatest, kui hakkasid laialdasemalt levima personaalarvutid. Küberohtude ja organisatsiooni küberkaitse olemust, mida käsitleb autor käesoleva magistritöö raames, kirjeldab joonis 1.

Joonis 1. Küberohtude ja organisatsiooni küberkaitse olemus (autori koostatud).

Küberohtu põhjustab üldiselt häkker ehk arvutialaste pahatahtlike soovidega inimene (Franklin et al., 2019, lk 16; Seebruck, 2015, lk 38). Kuigi esialgselt võeti see termin kasutusele Massachusettsi Tehnoloogiainstituudi personali kohta, kes kasutasid sealseid arvuteid liigselt ning mitte sihipäraselt, kuid mitte siiski kriminaalselt (Moore, 2010, lk 18). Hilisemalt levis häkkeri kui küberkriminaali mõiste enim läbi filmide ja televisiooni

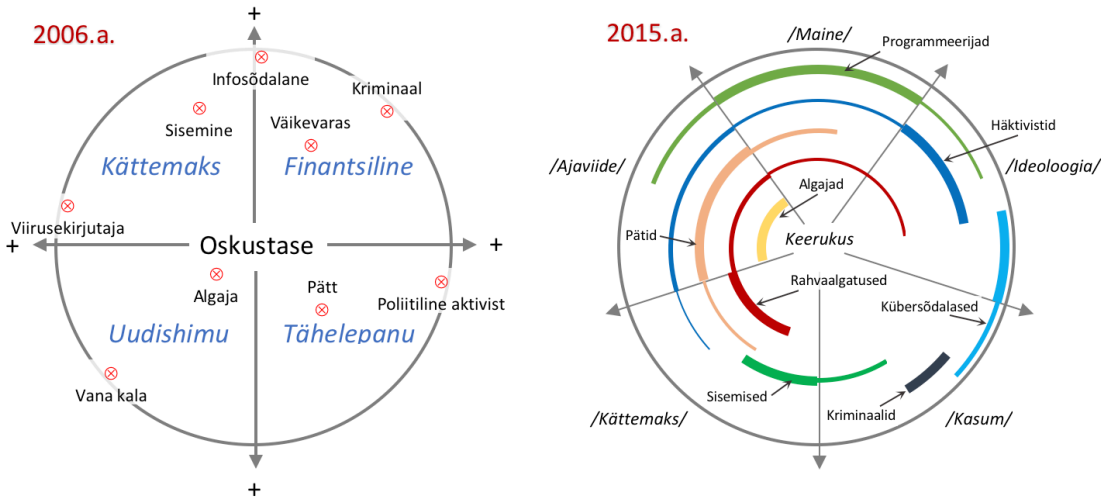
(näiteks 1982. aastal „Tron“, 1992. aastal „Sneakers“, 1995. aastal „The Net“, 2007. aastal „Die Hard“ jne), mis pigem tekitab inimestes eelarvamusi, kuid ei anna õiget ettekujutust nende olemustest, ideoloogiast ega eesmärkidest (Franklin et al., 2019, lk 2–16; Morgan, 2020).

Häkkerite määratlemisega, mis on küll ajas muutuv, tegi algust Bill Landreth 1985. aastal ning jagas tol hetkel häkkerid viieks kategooriaks, sõltuvalt nende oskustest ja motivatsioonist – koerus, väljakutse, põnevus, ego ja kasum (Seebruck, 2015, lk 38). Aja jooksul on need teatud määral muutunud ja näiteks on lisandunud häkkerid, kelle peamiseks motivatsiooniks on sotsiaalsed, poliitilised, usulised või patriootlikud põhimõtted, keda nimetatakse ka häktivistidest (inglise keeles *hacktivist*) (Seebruck, 2015, lk 39; Thomas, 2001, lk 1). Analüüsides edasi Moore ja Rogers poolt tehtud häkkerite liigitamist, saab nad jagada rollide põhiselt koos vastavate oskustasemete ja motivatsioonidega (vt lisa 1) (Moore, 2010, lk 24–26; Rogers, 2006, lk 98–99). Autori hinnangul näitab häkkerite klasifitseerimine, et häkkerite oskustasemed ja motivatsioonid on erinevad ning sellest tulenevalt ka nende poolne ohtude ulatus on väga lai ja otseselt ei ole küberohust puutumata mitte keegi (Rogers, 2006, lk 101). Autor toob alloleval joonisel välja kolm häkkeri tüüpi koos oskustaseme ja motivatsiooniga, mis kujutavad endast erinevat küberohtu organisatsioonile (vt joonis 2).

Joonis 2. Kolme häkkeri tüpoloogia - oskused ja motivatsioon (Moore, 2010, lk 24–26; Rogers, 2006, lk 98–99), autori koostatud.

Häkkereid klasifitseerinud Roger (2006) ja Seebruck (2015) koostasid lisaks ringikujulised skeemid, et visualiseerida häkkerite potentsiaalset haaret. Selles on

kajastatud erinevad häkkeri tüübid, oskustasemed, keerukused ning motivatsioonid. Võrreldes neid graafikuid kõrvuti, avaldub selgelt 10 aasta jooksul toimunud valdkonna areng (vt joonis 3). Erinevate häkkerite ja motivatsioonide tundmine annab olulise sisendi organisatsiooni küberturvalisuse ülesehitamisele ning hoidmisele. Näiteks, kui koduleht satub rünnaku alla ja häkker jätab sinna uhkustavalt avalikud jäljed oma saavutusest, siis on arvatavasti selle taga küberpätt ning samuti on aimatav tema motivatsioon ja see aitab osaliselt lahendada tekkinud probleemi (Seebruck, 2015, lk 43).



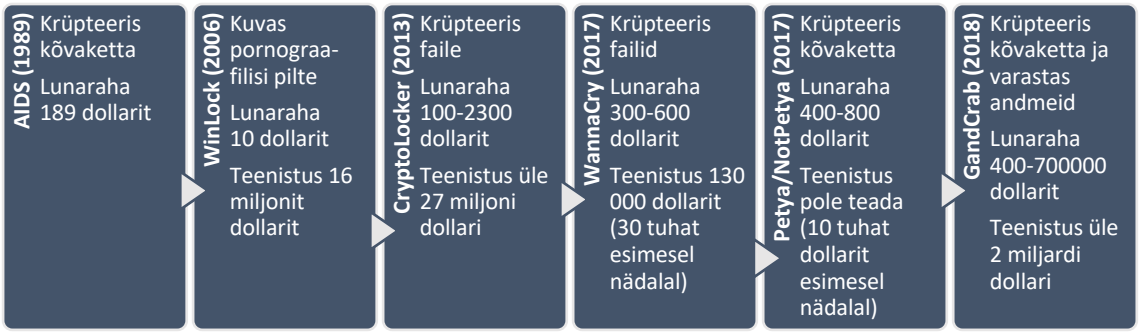
Joonis 3. Häkkerite tüpoloogia muutus ajas (Rogers, 2006, lk 100; Seebruck, 2015, lk 45), autori kohandused.

Häkkerite esialgsest fookusest, kui eesmärk oli pigem organisatsioonide tegevust häirida, on tekkinud olukord, kus enam ei saa väita, et küberohud organisatsiooni ei mõjuta, sest isegi kui neid otseselt ei rünnata, siis võib sattuda rünnaku alla kaudselt läbi mõne teise organistatsiooni (Grispos, 2019, lk 5). Kuigi eelnevalt on arvatud, et suur osa häkkereid tegutsevad pigem üksi, siis keerulisem on kindlasti olukord, kus mitmed häkkerid tegutsevad omavahel koos. Tänapäeval ongi juba täiesti tavapärane, et tehakse koostööd suuremate rünnakute puhul, kus sellest tulenevalt võib ka tulemus skaleeruda vastvalt suuremaks ja seda põhjusel, et häkkerite motivatsioonid võivad olla erinevad (Grispos, 2019, lk 3). Viimased uuringud on samuti tõestanud, et häkkerid suudavad teostada keerulisemaid ja tulusamaid rünnakuid, kui nad moodustatavad selleks gruppe, jagavad omavahel informatsiooni ning ressuresse (ENISA, 2019). Oluline on meelde jätta, et küberrünnakud on erinevad, sest häkkerite tüpoloogia on erinev - nende oskused, motiivid ja maailmavaated (Franklin et al., 2019, lk 2; Seebruck, 2015, lk 3).

Kui on teada, et kes võib organisatsiooni rünnata, siis samuti on oluline mõista millised on võimalikud meetodid ja mida vaja kaitsta (Ben-Asher & Gonzalez, 2015, lk 59–60). Küberrünnak, mis oma iseloomult on tahtlikult kahju tekitava eesmärgiga tegevus võrgu- ja infosüsteemide vastu, teostatakse peamiselt just häkkerite otseste või kaudsete tegevuste kaudu (Gordijn et al., 2020, lk 11–12; Seebruck, 2015). Iga rünnaku teostamiseks, sõltuvalt häkkeri tüübist, kasutatakse erinevaid vahendeid ning üldiselt jaotuvad need sihitud ja mittesihitud rünnakuteks. Sihitud rünnakud on konkreetsete isikute või organisatsioonide vastu, kuid mittesihitud küberohud levivad laialdaselt erinevate kodulehtede ja e-posti vahendusel ning enamasti on selleks pahavarad.

Üks kõige enam levinud küberrünnaku liike ongi tänapäeval pahavara. Pahavara, mis levib lisaks e-postile ka veebilehtedel, mälupulkadel ja (mobiili)rakendustes, on kuritegelikul eesmärgil loodud tarkvara, et kasutada nakatunud seadet info varguseks, krüpteerimiseks või rünnakuteks robotvõrgustikus ja krüptoraha kaevandamisel (Gordijn et al., 2020, lk 26–28). Pahavara, mille tulemusel krüpteeritakse kasutaja failid ning dekrüpteerimise eest nõutakse häkkeri poolt lunaraha, nimetatakse lunavaraks ning tihti levivad paremini just suuremates organisatsioonides (Gordijn et al., 2020, lk 121).

Teadaolevalt esimene pahavara, mis kandis koodnime AIDS (tuntud ka kui *Aids Info Disk* või *PC Cyborg Trojan*), tuvastati juba 1989. aastal. Õnneks tol ajal oli levik vägagi piiratud, kuna lauaarvutid polnud nii palju kasutuses ega internet kättesaadav ja seega pidi antud viiruse levitamiseks kasutama flopi-ketast, mida tegigi antud viiruse autor ise Maailma Terviseorganisatsiooni AIDS-teemalisel konverentsil (Srinivasan, 2017, lk 7). Alljärgneval ajateljel (vt joonis 4) on märgitud viimase 30. aasta olulisemad pahavarad.



Joonis 4. Märkimisväärsemate pahavarade ajajoon aastatel 1989-2018 (KnowBe4, s.a.), autori koostatud.

Rahaline motivatsioon on üldiselt pahavara loomise taga, kuigi tulemused varieeruvad suurelt (vt joonis 4) ja võib juhtuda, et organisatsioonidele tehtav kahju on kordades suurem, kui häkkeri saadav rahaline kasum (Gordijn et al., 2020, lk 127–129). Teine organisatsiooni toimimist kahjustav laiemalt levinud rünnaku tüüp on (hajutatud) teenusetõkestusründed (inglise keeles *(Distributed) Denial of Service*), mille eesmärgiks on takistada tavakasutajate, klientide või töötajate juurdepääs infosüsteemi(de)le. Teenustõkestusrünnaku puhul kasutatakse spetsiaalseid süsteeme võrguliikluse mahu märkimisväärseks suurendamiseks ning hajutatud teenustõkestusrünnakute puhul kasutatakse ka teostuseks eelnevalt pahavaraga nakatatud süsteeme globaalselt (Gordijn et al., 2020, lk 38). Erinevaid küberohtusid on palju ning parema ülevaate saamiseks koostas autor koondtabeli (vt lisa 2), kus on toodud välja peamised küberohu liigid koos nende lühikirjelduste ja võimalike mõjude osas. Autori hinnangul on järgnevalt oluline siduda omavahel erinevate motivatsioonidega häkkerid ja küberohud ning seejärel vaadata trende küberohtudes täpsemalt.

Tabel 1. Häkkeri (gruppide) eelistused küberohtude osas.

Küberoht	**Häkkeri (gruppide) tüüp**					
	küber-kriminaal	siseohustaja	rahvuslik	korpora-tiivne	häkitivst	küber-terrorist
Pahavara	✓	✓	✓	✓	✓	✓
Rakenduse rünnak	✓		✓	✓	✓	✓
Kalastamine	✓	✓	✓	✓	✓	
Teenustõkestusrünnak	✓				✓	✓
Andmevargus	✓	✓	✓	✓	✓	✓
Siseohud	✓	✓		✓		✓
Füüsiline manipulatsioon	✓	✓	✓	✓	✓	✓
Küberspionaaž		✓	✓	✓		

Märkused: ✓ - häkkeri esimene valik; ✓ - häkkeri teine valik

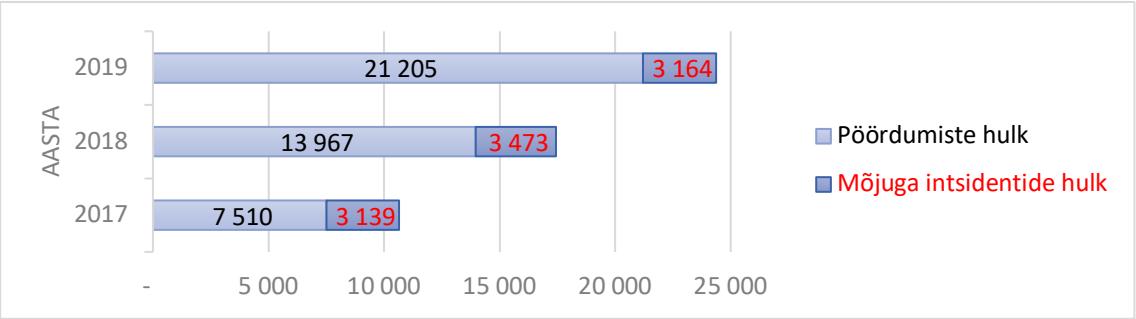
Allikas: (Sfakianakis et al., 2018, lk 124), autori kohandused.

Motivatsioonidest ja oskusest tulenevalt kasutavad häkkerid erinevaid meetodeid oma eesmärkide saavutamiseks. Häkkerite motivatsioon ja küberohud on ajas muutuvad, seega ei saa üheselt piiritleda ega paika panna kindlaid reegleid, kuid siiski teatud eelistused joonistuvad välja, nagu näha ülal toodud jaotusest (vt tabel 1). Tuleb silmas pidada, et ei ole ühtegi häkkeri või rühmituse tüüpi, kes kasutaks ainult ühte ja konkreetset

küberohtu. Väikeste erisustega kasutatakse kõiksuguseid vahendeid ning eriti just rahvuslike ja korporatiivsete rühmituste poolt (Sfakianakis et al., 2018, lk 118–123). Samuti on näha, et võrreldes Moore (2010) poolt tehtud uuringuga on muutunud peamised häkkerite tüübid ning saanud suuremat rõhku grupeeringud.

Küberkuritegevus, mille peamiseks motivatsiooniks on raha, on aastate jooksul moodustanud suurema osa rünnakutest ja moodustas 2019. aastal 84% kõikidest raporteeritud rünnakutest (Passeri, 2020). Raporteeritud rünnakutest räägitakse selle pärast, et tegelikult pole teada kõik toimunud küberrünnakud. Hinnanguliselt raporteeritakse kõigest 15% küberrünnakutest, kuna ei soovita kaasnevat halba mainet ja kulu, kuid see on viimastel aastatel paranenud seoses sellega, et organisatsioonid on teadlikumad kehtivatest regulatsioonidest (Sukhai, 2004, lk 131).

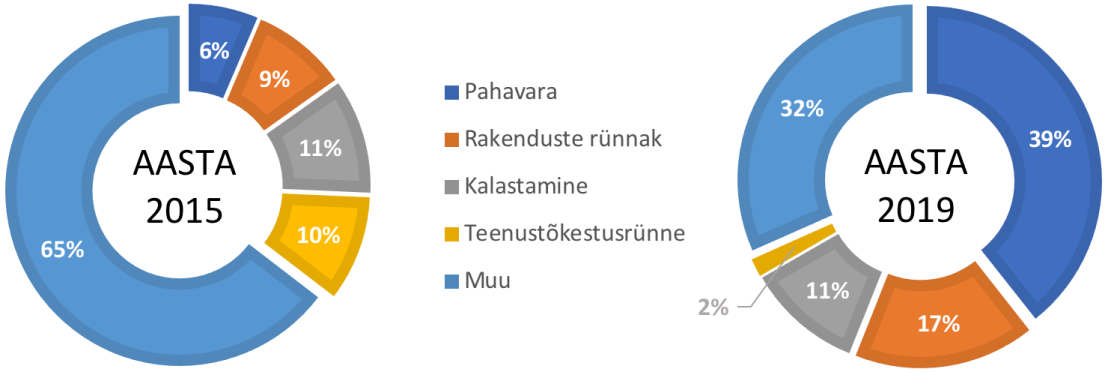
Eesti on riigiasutustel ja juriidilistel isikutel on kohustus teavitada küberrünnakutest Riigi Infosüsteemi Ametit (RIA) ning isikuandmete kaitsmise rikkumisest Andmekaitse Inspektsiooni (AKI) ja seda hiljemalt 72 tunni möödudes intsidendi teada saamisest. Küberrünnakud näitavad kasvutrende üle maailma ja Eestis, kus vastavad numbrid kerkivad iga aastaga, kuid õnneks mõjuga[3] intsidentide arvus pole suuremat kasvu märgata (vt joonis 5). 2018. aastal jõudustunud Euroopa andmekaitse üldmäärus (*General Data Protecion Regulation* ehk GDPR) on kindlasti ka Eestis osaliselt pöördumiste statistiliste numbrite tõusu taga, kuna sellega seati teavitamise kohustus andmekaitseametnikule (Euroopa Komisjon, 2019, lk 12; Gordijn et al., 2020, lk 120).



Joonis 5. RIA poole pöördumiste ja mõjuga intsidentide hulk aastatel 2017-2019 (Riigi Infosüsteemi Amet, 2018, 2019, 2020), autori koostatud.

[3] Mõjuga intsidentideks loetakse sündmusi, mille tulemusel on häiritud teabe või süsteemi konfidentsiaalsus, terviklikkus või kättesaadavus (Riigi Infosüsteemi Amet, 2020, lk 2).

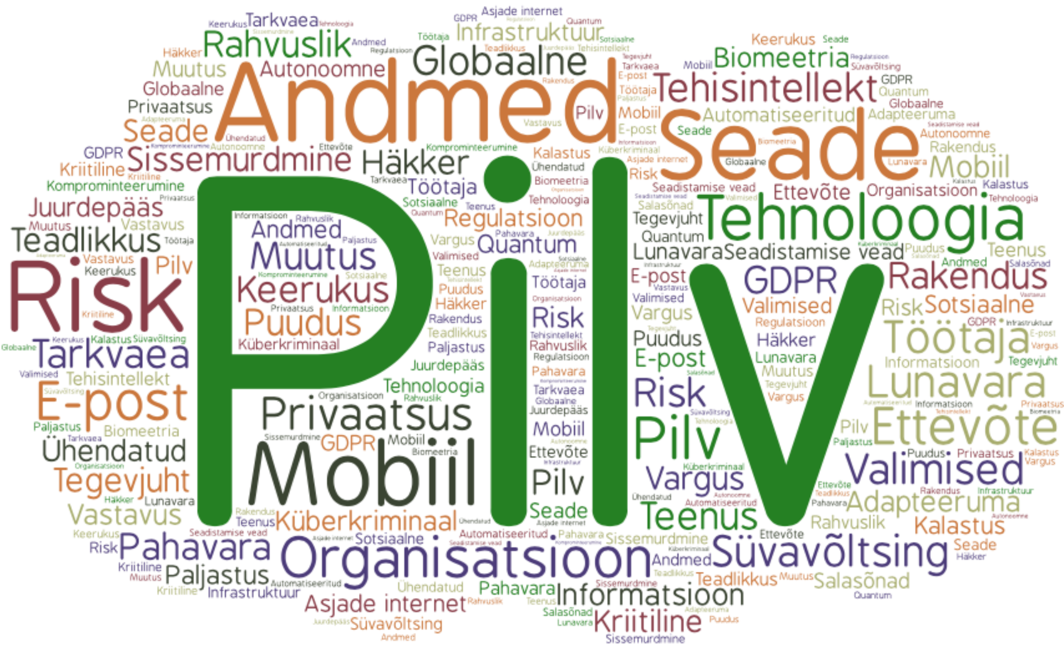
Kui vaadata 2015.-2019. aastate küberohtude trende, siis kõige suurem osa raporteeritud rünnakutest on seotud erinevate pahavaradega, pahavara osakaal kõigist küberohtudest on suurim nii Eestis kui teistes riikides (vt joonis 6). Joonis 6 põhiselt on näha, et kõige enam ongi viimase viie aastaga kasvanud pahavara osakaal. Samas esineb väiksema osakaaluga, kuid potensiaalselt suurema mõjuga küberohtusid – näiteks ka Eestis, kus rahvusvahelisel tasandil toob Välisluureamet välja oma viimases raportis Venemaa poliitilised huvid (Välisluureamet, 2020, lk 15).



Joonis 6. Raporteeritud küberrünnakute jagunemine 2015. ja 2019. aastal (Passeri, 2020), autori koostatud.

Kiire küberohtude kasvu põhjused tulenevad meie digitaalsest sõltvusest – inimeste ja organisatsioonide harjumustest ning vajadustest tehnoogia ja teenuste osas, olgu selleks siis lihtsalt võimalus kõikjalt kiire ligipääs internetipõhistele teenustele või keerukamad masinõppe ja tehisintellekti tehnoloogiad, mis aitavad veelgi tõhusamalt töötada (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 2–3). Põhja-Ameerikas ja Lääne-Euroopas läbiviidud uuringu põhiselt, kõigest 5% organisatsioonidest ei planeeri kasutusele võtta uuenduslikke digitaalseid platvorme, kuid teised pingutavad, et saavutada parem efektiivsus, kasutajakogemus või arendada uusi ärimudeleid (Lundell, 2020, lk 22–23). Eesti on samuti digitaalselt hästi arenenud – arvutid on kasutusel 99,8% organisatsioonides ja 98,9% omavad ka internetiühendust ning sealjuures koguni 79,2% organisatsioonidest pakuvad lisaks ka mobiilse internetiühenduse võimalust töötajatele (Statistikaamet, s.a.). See näitab ka, et globaalne ja eestlaste digitaalne sõltuvus on väga suur, mis omakorda annab aluse laiemale küberohtude hulgale (Fish, 2017; Majandus- ja Kommunikatsiooniministeerium, 2019, lk 3).

Tuleviku trendide vaatest koostas autor sõnapilve potsentsiaalsetest arengutest tehnoloogias ja küberohtudes, mida peaks organisatsiooni küberturvalisuse loomisel juba 2020. aastal arvesse võtma (Kushwaha, 2019; Lohrmann, 2019).



Joonis 7. Küberohtude trendid 2020. aastal (Lohrmann, 2019), autori koostatud.

Eelnevalt toodud joonis 7 põhiselt toob autor välja mõned olulisem küberohud, mis on seotud andmete ja tehnoloogiaga. Peamiselt kerkib esile pilve tehnoloogia (inglise keeles *Cloud Technology*) kasutusele võtmisega seotud küberohud, kus tihti unustatakse ära rakendada vajalikku küberturvalisust. Samuti asjade-interneti (inglise keeles *Internet of Things* (IoT)) laialdasem kasutusele võtmine, nii kodudes kui organisatsioonides, laiendab küberohu võimalusi. Jätkuvad erinevad pahavara ja lunavara rünnakud, kus fookus liigub ohvrile ja nutiseadmetele kohandatud versioonidele, kuid jäävad ka laialdaselt kõigile suunatud küberohud. Kokkuvõtvalt näitavad trendid keerulisemaid, põhjalikumaid ning automatiseeritud ründeid seoses masinõppe ja tehisintellekti tehnoloogiate arenguga, millega võimalik kasutavatest küberkaitsest mööda pääseda.

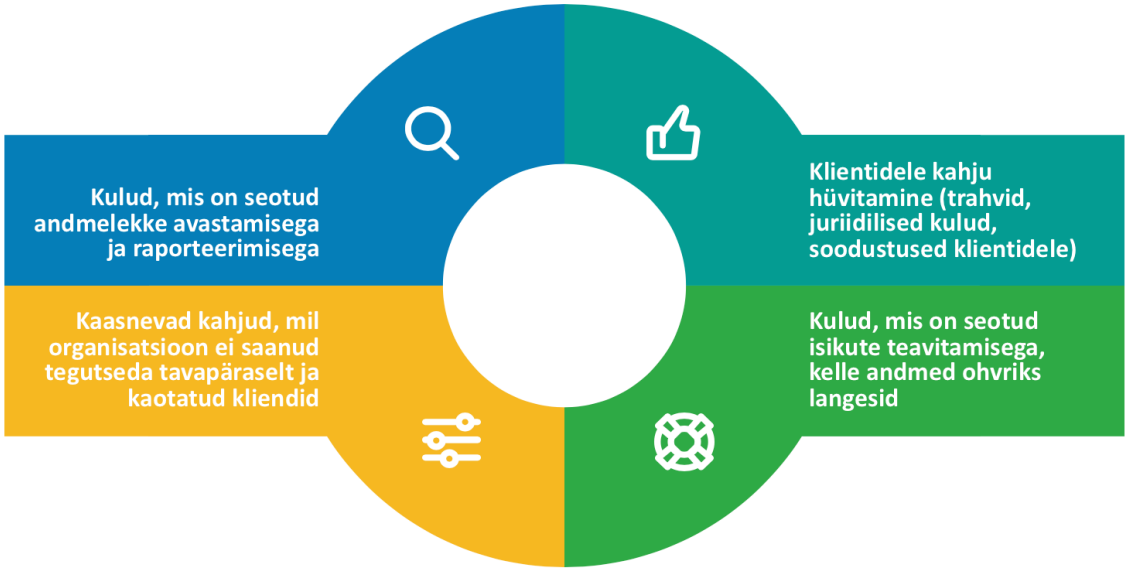
Uueks suunaks on ka küberrünnakute tellimine teenusena (inglise keeles mõiste *as-a-Service*), mille tulemusel laieneb potentsiaalsete küberkurjategijate arv märgatavalt, kuna ei eelda häkkerilt oskusi küberrünnaku läbiviimiseks enda poolt. Mittetehnoloogilise trendina jätkub puudujääk spetsialistidest küberturvalisuses, mida korvab paralleelselt

ohtudega kasvav küberturvalisusega seotud teenuste ja lahenduste turg. Hinnanguliselt areneb pakkumiste valik aastaga suurusjärgus 10%, mis annab organisatsioonidele rohkem võimalusi ja valikuid oma küberturvalisuse tõstmiseks. Sarnaselt küberohtude arengutrendidele on ka küberturvalisuse organisatsioonid keskendunud digitaalsele arengule, asjade interneti laiemale levikule ning veelgi keerulisemate rünnakute kaitsele (AustCyber, 2019, lk 17, 19).

Üks olulisi puudujääke nüüd ja tulevikus on küberkaitse oskustega töötajad, mille põhjuseks on peamiselt kaks asjaolu – tööandjad ja haridus. Tööandja poolseks puuduseks on tihti liialt kõrged ootused töötajale ning teiseks ei koolitata piisavalt olemasolevaid spetsialiste. Teiselt poolt on olnud puudulik rakendus- või kõrgharidus (riiklikult) (De Zan & Di Franco, 2019, lk 10–11). Uuringu kohaselt oli Euroopa Liidus 2018. aastal küberturvalisuse ekspertide puudus hinnanguliselt 142 000 inimest, kuid aasta hilisemas uuringus oli see number tõusnud juba üle kahe korra suuremaks (suurusjärgus 291 000), lisaks on suuremaid probleeme töötajate palkamisega, kuna pole piisavalt usaldust ning juriidilised protsessid venivad tihti 6-12 kuu pikkuseks (De Zan & Di Franco, 2019, lk 9). Sarnaselt ülejäänud Euroopale on ka Eesti tegemas samme küberturvalisusega seotud teadus- ja arendustegevuse toetamiseks ning on seadnud selle üheks küberturvalisuse strateegiliseks eesmärgiks (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 28–29). Autori hinnangul on vähene töötajate arv tugevalt seotud ka asjaoluga, et keskmiselt kulub andmevarguse avastamiseks 206 päeva ning sellele lisandub veel keskmiselt 73 päeva tekkinud olukorra kontrolli alla saamiseks (Ponemon Institute, 2019, lk 6). Tööjõu puuduse leevendamiseks kiireid meetmeid ei ole ning sellepärast peaksid organisatsioonid leidma võimalused teenuse sisseostmiseks.

Küberohtude mõjusid ja riske on võimalik mõista, kui on teada potensiaalsed häkkerid, küberohud ning nende arengud. Arvestama peab, et küberriski realiseerumisel on kahjud nii materiaalsed kui ka mittemateriaalsed. Suurte organisatsioonide, kus on 25 000 ja enam töötajat, võivad küberrünnakute kahjud olla küll suured ning jäävad selgelt silma (keskmiselt 5,1 miljonit dollarit juhtumi kohta), aga tegelikult kannatavad palju suuremate kahjude all ettevõtted, kus on kuni tuhat töötajat ning töötaja kohta kahju on 17 korda suurem (Ponemon Institute, 2019, lk 6).

Küberriskide hindamine on keeruline, kuna nad on dünaamilised ning puuduvad selged reeglid, sealjuures iga organisatsioon, varad ning keskkonnad on erinevad. Seega pigem võiks hinnata küberriske samaväärselt teiste organisatsiooni riskidega (Eling & Wirfs, 2019, lk 1109–1118). Küberrünnakute, mille tulemusel toimub ka andmevargus, mõju organisatsioonile võib kokku jaguneda 2-3 aasta peale. Mõjud, millest on välja jäetud küberturvalisusesse ja tehnoloogiasse tehtavad investeeringud, jagunevad erinevateks kategooriateks (Ponemon Institute, 2019, lk 5, 12, 34) (vt joonis 8).



Joonis 8. Andmevargusega seotud mõjude jagunemine (Ponemon Institute, 2019, lk 5, 12, 34), autori koostatud.

Kui üks finantsiline mõju tuleneb otseselt küberrünnaku kahjude likvideerimisest, siis teiseks pooleks on erinevad seadused ning regulatsioonid. Vaadates valdkondasid, kus on karmimad regulatsioonid (näiteks tervishoiusektoris) võib küberrünnaku poolne mõju kesta kuni kolm aastat ning sellega kahjud jagunevad keskmiselt 53% esimesele aastale ning järgnevatele aastatele vastavalt 32% ja 16% (Ponemon Institute, 2019, lk 5). Regulatsioonidest üks peamisi Euroopa andmekaitse üldmäärus (GDPR) on kehtinud peagi 2 aastat ning 2020. aasta märtsi seisuga on erinevate rikkumiste eest väljastatud vähemalt Euroopas 231 trahvi (numbrid võivad olla suuremad kuna kõiki rikkumisi ja trahve ei avalikustata), millest 62 on ebapiisavate informatsiooni turvalisuse tehniliste ja organisatsiooni meetmete rakendamise eest ning antud trahvide kogusumma ulatub üle 332 miljoni euro (CMS Legal, s.a.). Digitaalsete andmete igakülgne kaitsmine nende

eluea jooksul, nende käitlemine loomisest ja jagamisest kuni arhiveerimiseni välja, ongi küberturvalisuse tagamine ning küberohud kaasnevad selle protsessi igas faasis, olenemata kas andmed asuvad mõnes seadmes või on kättesaadavad e-teenuse kaudu (Rikk, 2018).

Küberturvalisuse tagamine ei ole ainult IT osakonna või mõne üksiku inimese tegevus. Sellesse peab olema kaasatud terve organisatsioon ning juhtkonnal on oluline roll küberturvalisuse tagamisel, kuna nende käes on võim ja võimalused teha vajalikke otsuseid ning muudatusi – sh organisatsioonikultuuris. Selleks peavad nad aru saama millised on peamised varad, andmed ja infosüsteemid, nende kriitilisus, riskid ning võimalikud ohustajad (Parenty & Domet, 2019, lk 106). Lisaks peab toimima pidev ja regulaarne küberriskide ja -kaitse hindamine, mille eest vastutab samuti juhtkond (KPMG, 2017, lk 2). 2019. aastal Marsh ja Microsoft poolt läbiviidud uuringus, kus osales üle 1500 organisatsiooni üle maailma, peeti jätkuvalt infotehnoloogia osakonda küberriskide haldajaks (88% vastanutest oli see üks valikutest) ning juhtkonna liikmetest kõigest 17% pühendusid küberriskidele rohkem kui mõne päeva aastas, kuid samas, 64% organisatsioonidest hakkavad tegelema küberriskide hindamisega alles peale küberrünnakut (Marsh, 2019, lk 7).

Antud alapunkti kokkuvõtteks, küberohtude olemus ja häkkerite motivatsioonid on väga erinevad ning otseselt kaitstuna ei saa tunda ennast keegi. Kuigi osaliselt on küberohtude trend spetsiifiliselt organisatsiooni suunas, siis ei kao kuskile ka laialdaselt levivad pahavarad, mille ohvriks võivad langeda kõik. Peamiselt peab kaitsma andmeid, ükskõik kus nad ka ei asuks, kuigi ka ründed teenuste halvamiseks on jätkuvalt aktuaalsed. Oluline on organisatsioonide juhtkondade kaasamine küberohtudega tegelemisesse ning juhtkonna tugi vastavate meetmete rakendamisele või vähemalt teadlikult riskide võtmine.

Kui käesolevas alapunktis tõi autor esile küberohtude ja häkkerite liigid üldisemalt, siis järgmises alapunktis keskendub konkreetselt tervishoiusektori küberohtudele ning mõjudele.

1.2. Küberohud tervishoiusektoris ja meetmed maandamiseks

Käesolevas alapunktis käsitleb autor küberohtusid tervishoiusektoris ning selgitab välja, miks on antud valdkond fookuses häkkerite vaatest ja millised võivad olla kaasnevad mõjud organisatsioonile. Alapunkti teises pooles toob autor välja meetmed ja soovitused küberohtudega seotud riskide maandamiseks organisatsioonides, keskendudes just eelkõige organisatsioonilistele meetmetele ja mitte tehnilistele.

Suurbritannia riiklik tervishoiuteenus (UK National Health Service ehk NHS) sai 2017. aasta mais väga tõsiselt kannatada WannaCry pahavaraga, mil ühelt poolt nõuti 300 kuni 600 dollarit suurust lunaraha iga nakatatud arvuti kohta, et taastada ligipääs pahavaraga krüpteeritud andmetele, kuid teiselt poolt oli nädalaks halvatud juurdepääs arstiabile ning operatsioonidele (Srinivasan, 2017, lk 7). Hinnanguliselt kujunes kahju küberrünnaku ajal üle 19 miljoni naela ning tagajärgede likvideerimisele kulus lisaks veel 72 miljonit naela (kokku 92 miljonit naela), millele lisaks eraldati küberturvalisuse tõstmiseks üle 250 miljoni naela järgnevaks neljaks aastaks (Cyber Security Policy, 2018, lk 7–14).

Ameerika Ühendriikides paiknev Erie maakonna tervisekeskus (Erie County Medical Center) hindas oma küberrünnakust saadud kahju ligi 10 miljoni dollari peale, kuigi lunarahaga nõuti kõigest suurusjärgus 30 000 dollarit (24 krüptoraha *Bitcoin*). Lunaraha ei makstud, kuna ekspertide hinnangul kõigest 47% maksjatest saavad failid tagasi, ning otsustati tegeleda probleemiga teisiti (Davis, 2017). Samuti läks NotPetya pahavararünnak Ameerika päritolu rahvusvahelisele farmaatsiatootjale Merck hinnanguliselt otseste ja kaudsete kuludena maksma 870 miljonit dollarit, kuid olulisemaks võiks pidada asjaolu, et see mõjutas ka ühe vähiravimi tootmist, mille puudumisel on otsene mõju inimeludele (Parenty & Domet, 2019, lk 107).

Kõigist teostavatest kriminaalsetest pettustest organisatsioonide suhtes on küberkuritegevus teisel kohal, moodustades 34% kõikidest raporteeritud tegevustest (esikohal kliendipettused 35%ga), kuid tervishoiusektoris on juba praegu küber-kuritegevus esikohal 16% osakaaluga (PricewaterhouseCoopers, 2020, lk 4). 2019. aastal tervishoiu sektorile suunatud rünnakute osakaal on kõikidest küberrünnakutest maailmas tõusnud 9,5% peale, mida on pea kolm korda enam kui 2015. aastal (2,6%) (Passeri, 2020). Üks põhjustest on selles, et tervishoiuandmete eest makstakse tumedas võrgus

(inglise keeles *Dark Web*) kõige suuremat hinda. Tumedaks võrguks nimetatakse virtuaalset keskkonda, kus häkkerid vahetavad omavahel teavet ja kaupa. Näiteks võivad ühe inimese andmed maksta tumedas võrgus keskmiselt 150 dollarit, kuid tervishoiuteenusega seotud info üle kahe korra rohkem (Nahai, 2019, lk 2; Ponemon Institute, 2019, lk 3).

Kui mõne rünnaku mõju on koheselt tajutav, siis andete vargusega seotud tegevused jäävad pikalt varjatuks. Andmelekke avastamine on keeruline protsess, kuid võrreldes teiste sektoritega kulub tervishoiusektori organisatsioonidel kõige rohkem aega nende avastamiseks (keskmiselt 236 päeva), samuti ka olukorra kontrolli alla saamine (keskmiselt 93 päeva), mis viib keskmise küberrünnaku lahendamise kulu 6,45 miljoni dollari peale (Ponemon Institute, 2019, lk 54). Lisaks on tuvastatud, et peale andmevargusega seotud küberintsidenti on tervishoiusektori kliendid kõige altimad vahetama oma teenusepakkujat, koguni 7% klientidest, mis kindlasti mõjutab organisatsiooni finantse pikemaajalisemalt (Ponemon Institute, 2019, lk 42–45).

Küberrünnakuid Eesti tervishoiusektorile on esinenud samuti, näiteks 2019. aasta raportis kajastatakse lekkinud terviseandmeid ja lunavaraga krüpteerimisi näiteks perearstidel, statistika kohaselt on neid esinenud ligi 10% tervishoiu ja sotsiaalhoolekande organisatsioonidel (Riigi Infosüsteemi Amet, 2019, lk 14; Statistikaamet, s.a.). Eesti on digitaalselt hästi arenenud, näiteks on igapäevane mobiilse internetiühenduse kasutamine, ja ka 88,9% tervishoiu ja sotsiaalhoolekande organisatsioonidest võimaldab kaugtööd oma töötajatele. See aga tähendab, et enamus organisatsioonidest lubavad ühel või teisel viisil töötajatel juurdepääsu tööga seotud andmetele väljaspool organisatsiooni sisevõrku. Samas on hinnanguliselt 70% edukatest rünnakutest saanud alguse just (nõrgalt kaitstud) lõppseadmetest ja kasutajatest väljaspool organisatsiooni sisevõrku (Fortinet, 2020; Statistikaamet, s.a.).

Eelmises alapunktis oli toodud välja jätkuva trendina teenuste ja lahenduste digitaliseerimine, mis on samas ka üks küberohu riskide suurenemise põhjuseid. Tervishoiusektori digitaalseks muutmine on toimunud juba kümneid aastaid, luuakse erinevaid infosüsteeme, soetatakse uusi tehnoloogilisi lahendusi ning ühendatakse omavahel erinevaid komponente parema tervishoiuteenuse tagamiseks (Le Bris & Asri, 2017, lk 3). Eesti riigiasutused ja organisatsioonid on üldiselt tervishoiusektori

digitaalsete lahenduste väljatöötamisel ning rakendamisel olnud pigem eeskujuks teistele, näiteks: Patsiendiportaal, Digiretsept, Pildipank, e-kiirabi ning e-konsultatsioon jm.

Haiglate infrastruktuurist väga suure osa moodustavad erinevad spetsiifilised meditsiiniseadmed ning ajalooliselt ei ole maailmas nende küberturvalisuse tagamine olnud väga teemaks, kuid see trend on kindlasti muutunud (Gordijn et al., 2020, lk 146–148). Mayo haigla (Mayo Clinic) Ameerika Ühendriigis lasi testimise eesmärgil küberrünnakuid teostada oma erinevatele meditsiiniseadmetele (näiteks ultraheli- ja röntgenseadmed, ventilaatorid jmt), mille tulemusel langes iga päev mõni eelpool mainitud seade rivist välja (Andre, 2017). Seda muidugi kontrollitud tingimustes ning inimelusid ohtu ei seatud, mida ei saa aga väita soovimatu küberrünnaku puhul.

Üheks peamiseks puuduseks tervishoiusektori küberturvalisuse ülesehitamisel on olnud see, et organisatsioonid ei ole teadlikud, kes ja kuidas neid võiksid rünnata ning kaitstakse peamiselt ainult patsiendi andmeid. Kui näiteks võtta fookusesse kaks teemat - patsiendi tervis ja patsiendi terviseandmed ning vaadelda neid koos peamiste küberohu liikidega, siis on küberturvalisuse vajadus juba hoopis teine (vt tabel 2). Tervishoiusektori ja haiglate omapärad ongi peamiselt nende erinevates infosüsteemides ja meditsiiniseadmetes, mis on ristkasutuses paljude erinevate osapooltega ja ühendatud selleks võrku, et nende kasutus ja haldus oleks lihtsam ning efektiivsem.

Tabel 2. Erinevate häkkerite huvid patsiendi tervisele ja andmetele

	Patsiendi tervis		**Patsiendi andmed**	
Küberoht	Sihitud rünnak	Valimatu rünnak	Sihitud rünnak	Valimatu rünnak
Üks või mitu häkkerit				☑
Häktivist (sh poliitiline)			☑	
Organiseeritud küberkuritegevus	☑		☑	☑
Küberterrorism	☑	☑		
Rahvuslikud organisatsioonid	☑	☑	☑	☑

Märkused: ☑ - rünnaku motivatsioonid patsiendi tervisele ja andmetele;

☑ - peamiselt keskendunud kaitse

Allikas: (Independent Security Evaluators, 2016, lk 3), autori kohandused.

Autori hinnangul on motivatsioonidest (vt tabel 2) selgelt näha, et tegelik eksponeeritus küberohtudele on palju laiem, kui küberkaitse peamine fookus. Lisaks peab juurde arvestama ka isikliku motivatsiooniga küberohud sisemiselt. Küberohtude fookus ei ole ainult patsiendi andmetel, ligi pooled on suunatud ka patsiendi tervisele. Muidugi ei saa seda üldistada, kuna tervishoiusektoris on organisatsioonid erinevate suuruste ja spetsialiseerumistega, mis määratleb ka teiste osapoolte rünnakute huvi (Independent Security Evaluators, 2016, lk 19–24). Näiteks võivad rahvuslikud küberrünnakud olla suunatud tervishoiuasutustele, mille patsiendid on riikliku või rahvusvahelise tähtsusega. Sellegi poolest on tervishoiusektor keerulises seisus, sest küberkaitset peaks looma iga ohu vastu, kui siduda erinevad motivatsioonid ja küberrünnakud.

Lisaks kahjudele, mis tekivad küberrünnaku tulemusel, on veel erinevad seadused ja regulatsioonid, mille rikkumisel võivad järgneda organisatsioonile sanktsioonid. Euroopas on andmekaitse üldmäärus, mille alusel on trahvitud 2020. aasta märtsi seisuga vähemalt 8 Euroopa haiglat kokku summas üle 1 miljoni euro (peamiselt paragrahvide 5 ja 32 rikkumised). Lisaks on veel 16 erinevat organisatsiooni Euroopas terviseandmete käsitlemise rikkumiste eest trahvitud summas üle 17 miljoni euro ning Ameerika Ühendriikides 2019. aastal terviseandmete kaitse seaduse (inglise keeles Health Insurance Portability and Accountability Act ehk HIPAA) alusel on kokku väljastatud trahve üle 15 miljoni dollari (CMS Legal, s.a.; Compliancy Group, s.a.).

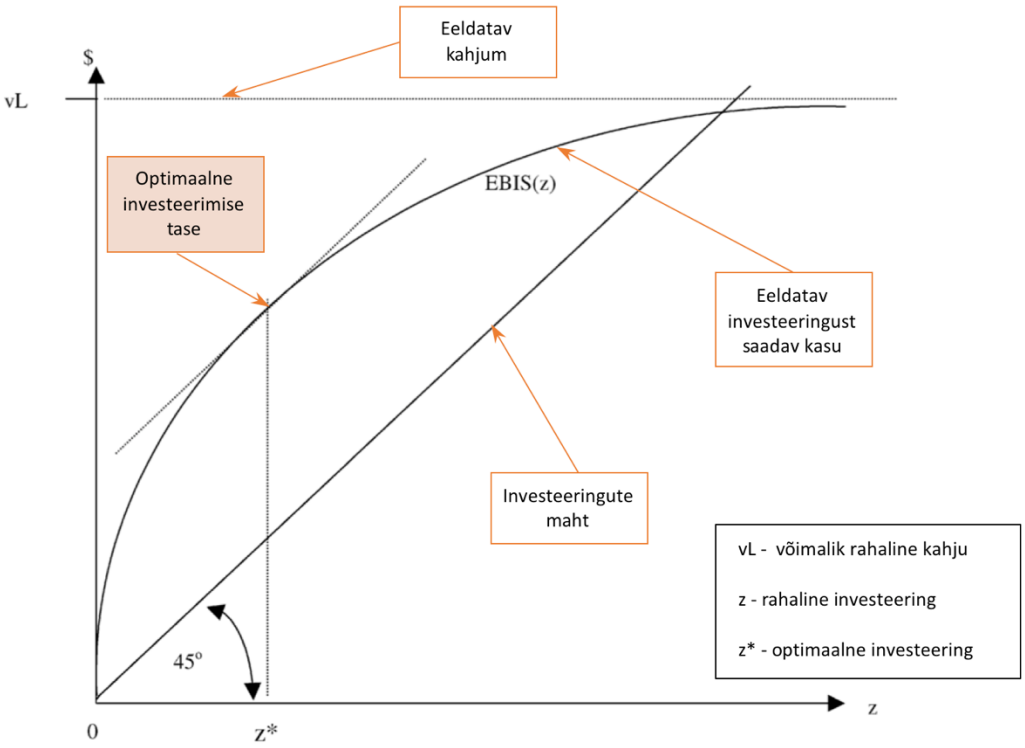
Eestis kehtib haiglatele veel lisaks teiste seaduste hulgas ka küberturvalisuse seadus (lühend - KüTS), millega seatakse samuti konkreetsed reeglid isikuandmete töötlemisele ja kohustus tagada andmete konfidentsiaalsus, terviklikkus ja käideldavus. Haigla peab kasutama vajalikke küberturvalisuse meetmeid ja lahendusi, et keegi ilma pädeva õiguseta ei pääseks ligi ega töötleks andmeid, mis on nende kasutuses. Samuti peavad haiglad suutma vajadusel tuvastada (logide pealt) rikkumisi tagantjärgi eelpool mainitud kohustuste osas ehk suutma tuvastada: kas, millal ja millistele andmetele on ligi pääsetud (Andmekaitse Inspektsioon, 2019, lk 38).

Eesti info- ja kommunikatsioonitehnoloogia (IKT) turvalisuse uuringu kohaselt rakendatakse erinevaid küberturvalisuse meetodeid tervishoiusektoris üle keskmise (94,4%) (vt lisa 3). Siiski, teatud tehnoloogiate, näiteks virtuaalse privaatvõrgu (inglise keeles *Virtual Private Network* ehk VPN) ja turvaintsidentide logifailide käsitlemise

tehnoloogiaid ei ole veel Eestis tervishoiu ja sotsiaalhoolekande organisatsioonides valdavalt kasutust leidnud. Kehvem on olukord organisatsioonisiseste ressursside ja protsessidega, kus on näiteks näha, et kõigest 8,9% tervishoiusektori orgnisatsioonidest omavad küberturvalisusega tegelevaid inimesi ja protseduure (Statistikaamet, s.a.).

Riskide maandamiseks on organisatsioonidel üldiselt kaks meedet – finantsilised ja mittefinantsilised. Hoolimata asjaolust, et tervishoiusektorile suunatud küberohud kasvavad kõige kiiremini, on kahjuks küberturvalisusele eraldatav eelarve keskmiselt kõigest 6% kogu infotehnoloogia eelarvest (Andre, 2017), võrreldes finantssektoriga, kus küberturvalisusele panustatav osa on IT eelarvest keskmiselt 10% ning moodustab käibest keskmiselt 0,3% (Friedman & Gokhale, 2019, lk 4–5). Autori hinnangul on siin kindlasti seos asjaoluga, et kuivõrd küberohu teadlik on vastav organisatsioon ning selle juhtkond. Teiseks puuduseks on tihti küberturvalisusele tehtavate kulutuste põhjendamise oskuse puudumine organisatsiooni siseselt, sest kui tõsisemaid intsidente pole juhtunud, millega kaasnevad ettenägematud kulud, siis nähakse seda tihti ainult kuluna (Crawley, 2019; Leszczyna, 2019, lk 127).

Piisavate finantsvahendite eraldamine oleks kindlasti paljudele organisatsioonidele küsimus, millele pole lihtne vastust leida – kui palju on vaja investeerida küberturvalisusse, et see oleks piisav. Ühest vastust siin ei olegi, kuna organisatsioonid ning võimalused ja vajadused on erinevad. Ühelt poolt ei soovi ju keegi kulutada rohkem kui vaja ning teadvustades, et 100% küberturvalisust ei ole võimalik saavutada. Teiselt poolt kaasnevad liiga suured riskid, kui see valdkond on alafinantseeritud. Erinevaid riskide ja küberriskide hindamise teooriaid on selleks olemas ning valemid ja meetodid, näiteks Gordon ja Loeb (2002) poolt koostatud Gordon-Loeb mudel (vt joonis 9). Gordon-Loeb mudeli puhul on kolm peamist komponenti, mida organisatsioon peab arvestama (Gordon et al., 2016, lk 4–5). Esiteks tuvastama ja hindama omatavat informatsiooni ning andmeid, teiseks hindama oma küberturvalisuse haavatavust ja potentsiaalset andmekadu eduka küberrünnaku puhul. Viimaseks, veel kõige keerulisem, analüüsida ja hinnata küberturvalisusesse tehtava investeeringu tasuvust.



Joonis 9. Investeeringud küberturvalisusesse (Gordon & Loeb, 2002, lk 445), autori kohandused.

Joonis 9 põhiselt on näha, et kui on olemas kõik vajalikud andmed, siis on võimalik arvutada välja optimaalne küberturvalisusse tehtav investeering. Organisatsioonide jaoks on kindlasti oluline leida üles enda jaoks sobilik optimaalne investeerimise tase, kuid samas peab arvestama, et see on ajas muutuv - näiteks, kui lisandub mõni regulatsioon või muu kohustus, mille rikkumisega võib kaasneda kahju.

Esimese peamise sammuna on vaja tuvastada organisatsiooni infovarad, mida näeb ette Eestis kasutusel olev infosüsteemide kolmeastmeline etalonturbe süsteem (ISKE), mis on avaliku teabe seaduse määruse alusel rakendatav kõigil riigi ja kohalikel asutustel. Iga organisatsioon peab suutma välja selgitada, millised digitaalsed andmed (infovarad) neil organisatsioonis on kasutusel, nende andmete kõik asukohad ja kellel või millel peab olema õigus neid töödelda. Seejärel hindama andmete väärtust organisatsiooni jaoks, arvestades juurde ka võimalikke trahve või muid kohustusi, mis võivad kaasneda andmelekke puhul. Eelnimetatu põhiselt on võimalik hakata hindama riske, mis on otseselt seotud küberturvalisuse ja andmekaitsega, ja valida vastav lähenemine (NIST, 2020, lk 4–5) (vt joonis 10).

Joonis 10. Küberriskidega tegelemine (NIST, 2020, lk 4–5), autori koostatud.

Järgmise sammuna ei ole organisatsiooni küberturvalisuse tagamiseks vajalik ainult finantsilist ressurssi - sama oluline on ka struktuur, rollid, protseduurid, reeglid, koolitused, jms, mis toetaksid organisatsiooni küberturvalisust (Le Bris & Asri, 2017, lk 10). Soovitused küberohuga seotud riskide maandamiseks tervishoiusektorile ja haiglatele ei erine suuresti teiste organisatsioonide lähenemistest (vt tabel 3).

Tabel 3. Küberturvalisuse soovitused tervishoiusektorile tervikuna, kuid ka haiglatele.

Soovitused tervishoiusektorile üldisemalt	Laiapõhjalisem küberohtudest tulenevate riskide maandamine st riskid patsiendi tervisele, mitte ainult tema andmetele.
	Regulatsioonide ja standardite järgi ei tohiks seada kõiki prioriteete, need on küll väga olulised ja nendele peab vastama, kuid fookus peaks olema tervikliku küberturvalisuse tagamine.
	Patsiendile rohkem otsustusjõudu ja parem teavitamine, et kuidas ja mille jaoks nende andmeid kasutatakse ning kes omab juurdepääsu või õigusi.
	Rohkem mõjuvõimu ja usaldust infotehnoloogia ja - turvalisuse juhtidele ning nende kaasamist erinevate tehnoloogiate soetamisel (st mitte ainult IT lahenduste).
	Küberturvalisuse tagamiseks ei piisa ainult kulukate lahenduste soetamisest, vajalik on ka koolitada ja harida töötajaid.
Soovitused haiglatele	Küberturvalisuse raamistiku loomiseks kasutada eelnevalt väljatöötatud juhendeid, soovitusi, standardeid. Kohandada vastavalt vajadustele.
	Pikaajalise plaani koostamine ning organisatsiooni juhtkonna tugi ja pühendumine selle elluviimisel. Oluline on ka plaani regulaarne ülevaatus ning uuendamine vastavalt olukorra muutustele.
	Eraldada piisavat eelarvet, mis oleks ka seotud pikaajalise plaaniga, toetamaks lahenduste, inimeste, koolituste ja konsultatsioonidega seotud kulusid.
	Küberohtudega seotud koolitused, mitte ainult infotehnoloogia töötajatele, vaid ka juhtkonnale ning kõikidele teistele töötajatele.
	Eraldada infoturvalisuse osakond infotehnoloogiast, kuna üldiselt üks osakond ei saa vastutada tehnoloogilise arengu ja küberturvalisuse eest samaaegselt - tekib huvide konflikt ja ressursi puudus.

Allikas: (Independent Security Evaluators, 2016, lk 53–55), autori koostatud.

Üks tabelis 3 toodud soovitus on arendada organisatsiooni küberturvalisust, luues selleks pikaajalised plaanid. Plaanidega on võimalik siduda tegevused ning selleks vajalikud ressursid, eelarved ning muud vahendid (Gordijn et al., 2020, lk 339). Plaani loomise esimeseks sammuks peaks olema organisatsiooni küberturvalisuse taseme hindamine ning soovitud tasemele eesmärgi seadmine. Organisatsiooni küpsuse taseme hindamiseks, küberturvalisuse vaatest, on võimalik jagada organisatsioonid neljaks tasemeks (vt tabel 4). Kõige rohkem arenenud organisatsioone iseloomustab adaptiivsus, kus juhtkond on kaasatud ning igapäevases ja strateegilises juhtimises arvestatakse küberturvalisusega. Samuti räägitakse nendest teemadest kõigile (mitte ainult infotehnoloogia osakonnale) ning küberturvalisuse teema seotakse ka organisatsiooni üldiste ja strateegiliste eesmärkidega (Friedman & Gokhale, 2019, lk 4–13; NIST, 2020, lk 38–39).

Tabel 4. Organisatsiooni küberturvalisuse tasemed.

Osaline ja vajaduse põhine (1. tase)		
	Küberturvalisusega seotud riskide juhtimist ei teostata, tegeletakse vajadusel tagantjärgi. Puuduvad vastavad protsessid ja strateegia arengu osas. Küberturvalisusse ei investeerita ja on puudulik, puudub teadlikkus andmetest. Töötajaid ei informeerita ega koolitata korrapäraselt.	
Riskiteadlik, kuid passivne (2. tase)		
	Küberturvalisusega seotud riskid on teadvustatud ning riskide juhtimine on juhtkonnal teada, kuid ei ole korralikult juurutatud. Juhtkonda on keeruline veenda küberturvalisusse investeerima. Riskide hindamist tehakse, kuid ebaregulaarselt. Töötajad teavad osaliselt oma vastutust ning koolitusi tehakse harva.	
Riskiteadlik ja aktiivne (3. tase)		
	Küberturvalisusega seotud riskide juhtimine on juhtkonna poolt vastu võetud ning organisatsioonis juurutatud, seotud teiste protsesside ja eesmärkidega. Uuendatakse ja hinnatakse riske regulaarselt. Riske maandatakse ka lepinguliselt kolmandate osapooltega ning töötajaid koolitatakse regulaarselt. Samuti on olemas valdkonnaga tegelev spetsialiseeritud personal.	
Adaptiivne ja ennatlik (4. tase)		
	Organisatsioon kohandab oma küberturvalisusega seotud riskide juhtimist vastavalt kogemustele ning keskendub ennetavale tegevusele. Küberturvalisuse strateegia on osa organisatsiooni strateegiast. Küberturvalisus on saanud osaks organisatsiooni kultuurist. Lepingutega seotud kaitse riske maandatakse ennetavalt. Regulaarselt tehakse värskeima olukorra põhiselt koolitusi ja on paigas erinevate vastutustega rollid organisatsioonis.	

Allikas: (Friedman & Gokhale, 2019, lk 2; NIST, 2020, lk 37–39), autori koostatud.

Küberturvalisuse evolutsioon organisatsioonis on oluline, kuid autori hinnangul ei ole vaja käsitleda olukorda, kus organisatsioon on oma arengult esimesel tasemel, kuna sinna

ei areneta, vaid ollakse, st kui ei tehta mitte midagi. Teise taseme saavutamiseks peaks organisatsioon järgima soovitusi küberohtudega tegelemiseks, näiteks peab (Le Bris & Asri, 2017, lk 10–11; Sfakianakis et al., 2018, lk 137):

- juhtkond olema rohkem kaasatud ja teadlik;
- olema võimeline hindama vara (andmeid);
- saavutama piisava täpsusega teadlikkuse küberriskidest;
- teostama minimaalsel määral koolitusi;
- juurutama küberohu teadlikkusega seotud protsessid;
- olema teadlik oma koostööpartnerite küberturvalisuse kvaliteedis.

Loetletud punktidest viimane on kindlasti üks keerukamaid, kuna teiste organisatsioonide tegutsemist ja toimimist reguleerida on keeruline, võimalik on ainult omapoolseid lepingutingimusi suunata vastavalt (Gaidosch et al., 2019, lk 20). Sarnane on olukord Eesti (digi)riigis üldisemalt, kuna pole detailselt kokkulepitud ja juurutatud üheseid turvareegleid või -standardeid, mis aitaks usaldada ühtset süsteemi (Majandus- ja Kommunikatsiooniministeerium, 2019, lk 12).

Järgnevalt toob magistritöö autor välja meetmed ja soovitused, mida kasutusele võtta, et jõuda järgmistele tasemetele, kus organisatsioon teadlikult ja aktiivselt tegeleb küberturvalisusega, et maandada küberohtudega seotud mõjusid veelgi enam (Carlton et al., 2019, lk 103–107; Ponemon Institute, 2019, lk 38–39, 58–62).

- Juhtkond on põhjalikumalt kaasatud ja mõistab küberturvalisuse vajadust. Samuti on tegeleb aktiivselt küberohtudega seotud info jagamises, kaasab tervet organisatsiooni ja seob strateegiliste eesmärkidega.
- Organisatsiooni siseselt tehakse pidevat koostööd – juhtimise, teavituse, arenduse, turvalisuse ja halduse vaatest.
- Küberriskide maandamiseks eraldatakse piisavalt ressursse.
- Struktuuris on eraldi küberturvalisuse ekspert ja andmekaitsespetsialist.
- Koolitatakse töötajaid küberturvalisuse osas, informeeritakse pidevalt.
- Infosüsteeme testitakse teatud regulaarsusega küberrünnakute vastu, selle jaoks on loodud vastavad protseduurid ja protsessid.
- Küberturvalisuse teenuse ja kindlustuse kasutamine teatud riskide maandamiseks.

- Liigutakse kaasa küberohtude trendidega ning seotakse need küberturvalisuse pikaajaliste plaanidega.
- Juurutatud lahendused küberturvalisusega tegelemiseks ja olukorra analüüsimiseks.
- Võetakse kasutusele põhjalikumad küberkaitse lahendused, näiteks andmevargust kaitsevad süsteemid ja/või identiteedivarguskaitse lahendused.

Kokkuvõttes ei ole oluline niivõrd taseme määramine, vaid pigem organisatsioonis küberohtudega seotud riskide teadvustamine, aksepteerimine (või jagamine ja/või mitteaksepteerimine) ning teatud arenguplaani olemasolu (National Cyber Security Centre, 2018; Sallos et al., 2019, lk 587–589).

Kui vaadelda tervishoiusektorit, siis peab keskenduma küberturvalisuse loomisel ja hoidmisel tähelepanu alljärgnevatele valdkondadele (vt tabel 5).

Tabel 5. Tervishoiusektori küberohu valdkonnad.

Valdkond	**Põhjendus**
Patsiendi tervis	Andmete või seadmete rike võib olla inimese tervisele ohtlik
Patsiendi terviseandmed	Sisaldavad privaatset ja konfidentsiaalset informatsiooni
Tervishoiuteenuse kättesaadavus	Kriitilised teenused ja ka administratiivsed
Intellektuaalse omandi kaitsmine	Erinevad uuringud, retseptid, teadustöö, jm
Hea maine kaitsmine	Patsiendi ja tervishoiu töötaja ning organisatsiooni vahel peab olema usalduslik suhe

Allikas: (Le Bris & Asri, 2017, lk 1–2), autori koostatud.

Kindlasti ei ole tervishoiusektori asutuses küberkaitse loomine lihtne tegevus, arvestades selle komplektsust ja mitmekesisust ning asjaolu, et nad kuuluvad ka kriitilise infastruktuuri alla. Ühe ennetava meetmena, küberohtudega seotud riskide maandamiseks, on soovitatav uute seadmete ja lahenduste hankeprotsessi kaasata infotehnoloogia ja -turvalisusega seotud töötajaid. Euroopa Liidu Küberturvalisuse Amet (ENISA) on välja töötanud 30 erinevat soovitust, mida on tervishoiusektoril ja haiglatel võimalik rakendada hankeprotsessi erinevates faasides, sisaldades nii organisatoorseid kui ka tehnilisi juhiseid, ning see toetab 2018. mais kehtima hakanud meetmeid Euroopa Parlamendi ja Nõukogu direktiivi (EL) 2016/1148, mille eesmärgiks on tagada võrgu- ja

infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus[4] (Drougkas et al., 2020, lk 7–12; Gordijn et al., 2020, lk 104).

Käesoleva peatüki kokkuvõtteks koostas autor tabeli (vt tabel 6) olulisemate teemade osas ning moodustas nendest viis teemaplokki, mille juurde lisas teoreetilise osa põhitulemused.

Tabel 6. Teoreetilise osa kokkuvõte teemaplokkideks organisatsiooni vaates.

Teemaplokk	**Teoreerilise osa põhitulemused**
1. teema: Teadlikkus küberohtudest	Häkkerid ja küberrünnakud on pidevas muutuses. Küberturvalisuse tagamisel on abiks, kui organisatsioonid suudavad ära määrata, et millised on peamised võimalikud häkkerid ja motivatsioonid ning millised on nende poolt peamised küberohud. Ära ei tohiks unustada ka sisemisi ohte.
2. teema: Küberohtude tunnetatud mõju	Küberrünnaku tulemusel võib organisatsioon kannatada miljonitesse ulatuvaid kahjusid, perioodil 2-3 aastat peale küberrünnaku avastamist, kuigi kõik rünnakuga kahjud ei pruugi olla materjaalsed. Lisaks võivad kaasneda regulatsioonide rikkumisega trahvid ja mainekahju, millega kaasneb klientide ja partnerite usalduse kaotus.
3. teema: Küberriskide maandamine	Kuigi 100% küberturvalisust pole võimalik saavutada, siis organisatsiooni jaoks on oluline alustada riskide hindamisest. Selgitada välja, mida saab maandada, jagada, vältida või aksepteerida. Kuigi eelarve eraldamisel on suur roll küberturvalisuse tagamisel, siis mitte kõik meetmed ei vaja suuri investeeringuid. Juhtkonna kaasamine, struktuuri ja rollide jagamine, inimeste koolitamine, lepingute korrigeerimine, protsesside loomine ning täiustamine – on näited, mida tihti saab ka teha ilma suurema eelarveta.
4. teema: Küberturvalisuse tase	Kasulik on hinnata organisatsiooni küpsust küberohtudega tegelemisel ning seada eesmärke paremale tasemele jõudmiseks. Tasemele, kus küberohtude maandamisega seotud pikaajalised plaanid, strateegiad ja protsessid on lõimitud organisatsiooni üleste strateegiliste plaanide ja eesmärkidega. Oskus tellida küberturvalisust (osaliselt) teenusena.
5. teema: Trendid	Tervishoiusektor, mis on ka osa kriitilisest infrastruktuurist, peab tagama teenuse kättesaadavuse ning küberohtude eest kaitsma tervise andmeid, ärisaladusi ning oma mainet, kuid ennekõike patsiendi tervist. Digitaliseerimine ja areng tervishoiu sektoris on möödapääsmatu ja vajalik, kuid samuti ka arenevad küberohud ning suurenevad riskid.

Allikas: (Ben-Asher & Gonzalez, 2015; CMS Legal, s.a.; Eling & Wirfs, 2019, lk 1109–1118; Friedman & Gokhale, 2019, lk 2; Gordijn et al., 2020, lk 127–129; Independent Security Evaluators, 2016, lk 53–55; Le Bris & Asri, 2017, lk 1-3,10; Moore, 2010, lk 24–26; NIST, 2020, lk 4-5,37-39; Ponemon Institute, 2019, lk 5, 42–45; Rogers, 2006, lk 98–99; Sfakianakis et al., 2018, lk 26–115, 124), autori koostatud.

[4] https://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:32016L1148&from=EN

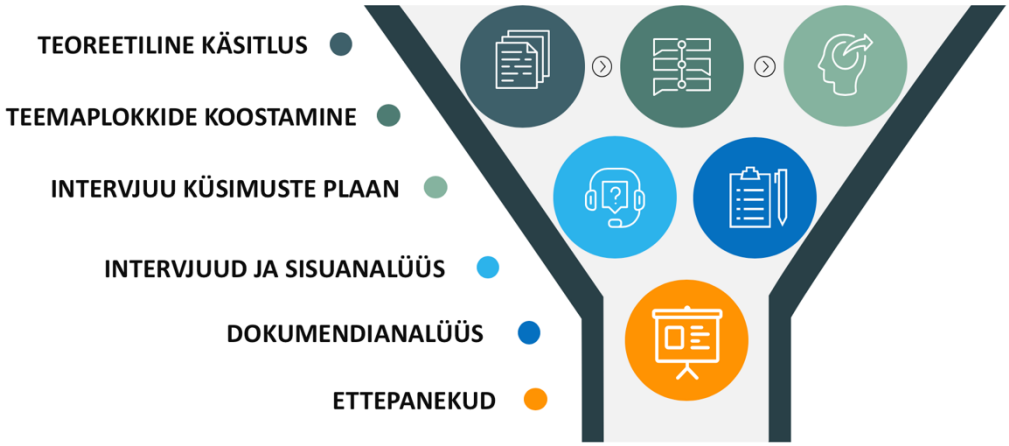
Käesoleva alapunkti, kus sai käsitletud erinevaid küberohtusid ja nende trende tervishoiusektorile, kokkuvõtteks saab öelda, et on erinevaid meetmeid organisatsiooni küberriskide maandamiseks, kuid nende rakendamisel on oluline leida tasakaal. Kindlasti on oluline nii juhtkonna kui ka terve organisatsiooni kaasamine, kuni hankeprotseduurideni välja. Abiks on organisatsiooni taseme hindamine küberturvalisuse osas ning pikajaliste plaanide tegemine ja nende sidumine organisatsiooni strateegiliste eesmärkidega. Olulist rolli mängivad organisatsiooni enda võime hinnata oma vara ja väärtust ning riskide maandamiseks vajalikke investeeringute mahtu, jagades tegevusi plaanidele ja võimekusele.

Magistritöö järgmine, empiirline peatükk kasutab ülaltootud tabelit (vt tabel 6). Autor uurib erinevate teemaplokkide kaupa haiglate näitel organisatsiooni küberturvalisuse taset ja teeb teemaplokkide kaupa ettepanekuid organisatsiooni üleselt küberriskide maandamiseks.

2. ORGANISATSIOONIS KÜBERRISKIDE MAANDAMINE EESTI HAIGLATE NÄITEL

2.1. Uurimisprotsessi ja valimi tutvustus

Käesoleva peatüki eesmärgiks on selgitada välja Eesti haiglate organisatsiooni ülene tase küberriskide maandamiseks ning teha ettepanekuid selle parandamiseks. Selles alapunktis kirjeldadab autor eesmärgi täitmiseks vajalikke uurimisprotsesse ja rakendatud meetodeid. Magistritöö autori poolt koostatud plaani kohaselt on, peale teoreetilise käsitluse ja teemaplokkide koostamise, järgnevaks ees intervjuu küsimuste plaani koostamine (vt joonis 11).



Joonis 11. Magistritöö teoreetilise ja empiirilise käsitluse plaan (autori koostatud).

Magistritöö eesmärgi täitmiseks rakendab autor andmete kogumise meetodina poolstruktureeritud intervjuusid andmekaitse, infoturbe ja infosüsteemi valdkonna spetsialistide ja juhtidega ning samuti dokumendianalüüsi avalikult kättesaadavate dokumentide üle. Analüüsimeetodiks valis autor kvalitatiivse sisuanalüüsi lähenemise, kuna see annab parema võimaluse:

- anda hinnang antud valdkonna küpsustaseme kohta, tuginedes ekspertide intervjuudele ilma, et paneks ohtu mõne organisatsiooni küberturvalisuse;

- analüüsida organisatsiooni struktuuri, arengukava, strateegilisi plaane ja eesmärke, korraldatud ja korraldatavaid hankeid ning avalikke küberturvalisusega seotud regulatsioone;
- poolstruktureeritud intervjuuks, kuna võimaldab püsida etteplaneeritud küsimuste raamides, kuid samas on piisavalt paindlik, et vajadusel mõne teema osas ka süvitsi minna.

Dokumendianalüüs ja intervjuud viidi läbi 2020. aasta mai alguses. Intervjuude kestvus oli keskmiselt 54 minutit, jäädes 40 ja 73 minuti vahele, ning viidi läbi Microsoft (MS) Teams keskkonnas. Kokku 271 minutit helifaile ja 88 lehekülge transkriptsioone (Times New Roman teksti suurusega 12 ja 1,5 reavahe), täpsem informatsioon intervjuude kohta toodud töö lisas 4. Intervjuud olid esialgselt plaanis läbi viia silmast-silma kohtumiste käigus ning intervjueeritavate nõusolekul salvestada intervjuusid helivormingus, kuid seoses 12. märtsil 2020 Eestis kehtestatud COVID-19 eriolukorraga langesid ära planeeritud vormis intervjuud. Autor asendas need veebipõhiste intervjuudega, mis eriolukorrast tingitud ajanappuse tõttu viidi läbi mai alguses. Intervjuude transkriptsioonid, konfidentsiaalsuse hoidmise vajaduse tõttu, ei kuulu magistritöö lisade hulka, küll aga kasutab autor intervjuudest lubatud tsitaate. Autor ei anna hinnanguid valimi organisatsioonidele eraldi vaid Eesti tervishoiusektori suurematele haiglatele tervikuna ning keskendudes pigem andmetest tekkinud mustritele: võrdleb erinevaid seisukohti teemaplokkide kaupa, olles neid eelnevalt kodeerinud ja kategooriatesse jaganud.

Haiglate valimisse kuuluvad Eesti piirkondlikud ja keskhaiglad. Kolm piirkondlikku haiglat: SA Põhja-Eesti Regionaalhaigla, SA Tartu Ülikooli Kliinikum ja SA Tallinna Lastehaigla. Lisaks neli keskhaiglat: AS Ida-Tallinna Keskhaigla, AS Lääne-Tallinna Keskhaigla, SA Ida-Viru Keskhaigla ja SA Pärnu Haigla (Sotsiaalministeerium, s.a.).

Intervjueeritavate valim koosneb viie organisatsiooni juhtidest, ekspertidest ja spetsialistidest, kes kõik omavad vähemalt 10-aastast kogemust infotehnoloogia, küber- või infoturbe valdkonnas (vt tabel 7).

Tabel 7. Intervjueeritavate valim ja intervjuu toimumise info.

Organisatsioon ja kirjeldus **Intervjueeritava nimi, ametikoht**	**Kuupäev, kanal, kestvus**
Fortinet – rahvusvaheline küberturvalisusega seotud lahenduste tootja Ahto Tomingas, küberturvalisuse spetsialist	05.05.2020 MS Teams 54 min
Eesti Haigekassa – riikliku ravikindlustuse korraldamine ja tervishoiuteenuste kättesaadavuse võimaldamine Karl-Henrik Peterson, juhatuse liige	07.05.2020 MS Teams 43 min
Siseministeeriumi infotehnoloogia- ja arenduskeskus – siseturvalisuseks ja elude päästmiseks vajalike infosüsteemide arendamine Uko Valtenberg, infoturbeosakonna juhataja	07.05.2020 MS Teams 73 min
Cybexer Technologies – küberturvalisusega seotud koolitused ja õppused Aare Reintam, küberturvalisuse ekspert ja koolitaja	11.05.2020 MS Teams 61 min
Tervise ja Heaolu Infosüsteemide Keskus – ITK kompetentsikeskus tervishoiusektorile Tõnis Komp, infoturbeosakonna juhataja	12.05.2020 MS Teams 40 min

Allikas: autori koostatud.

Riskide, mis on seotud organisatsiooni küberturvalisuse detailide avaldamisega, maandamiseks ei toimunud intervjuusid haiglate esindajatega ning dokumendianalüüsiks kasutati ka ainult avalikku infot kodulehekülgedelt ja riiklikest registritest. Dokumendianalüüsi jaoks kogus autor kokku valimi haiglate kodulehekülgedel oleva avaliku informatsiooni arengukavade, strateegiate, struktuuri, teenistuste ja hankeplaani osas. Dokumendianalüüsi eesmärgid ja allikad on toodud töö lisas 5 ja dokumentide kogumise kava toodud lisa 5 järg tabelis. Haiglate poolt 2015.-2019. aastatel teostatud riigihangete andmete osas kasutas autor Rahandusministeeriumi riigihangete registri andmebaasi päringuid. 2019. aasta tulemiaruanded hankis autor saldoandmike infosüsteemist. Seadusandlus ja regulatsioonid kehtivad haiglatele üheselt, seega nende käsitlemiseks kasutas autor Riigi Infosüsteemi Ameti ning haiglate kodulehekülgedel olevat informatsiooni.

Uurimisprotsessi, poolstruktureeritud intervjuu küsimuste plaani ettevalmistamisel lähtus autor teoreetilise osa lõpus moodustatud teemaplokkidest (vt tabel 6) ning koostas nende põhiselt küsimused (vt lisa 4). Intervjuu küsimuste plaanis, milles sisalduvad ka üldised küsimused alguses ning lõpus, on 23 põhiküsimust, kuid vajadusel kasutab autor ka

toetavaid küsimusi, et hankida lisainformatsiooni või täpsustada detaile. Sissejuhatavate üldiste küsimuste eesmärk on tutvustav ning kokkuvõtvate küsimustega katta üldisemaid teemasid. Teemaplokkides koostatud küsimuste põhjal selgitas autor välja intervjueeritavate arvamused üldisemalt ja haiglatele suunatud küberohtudest, võimalikest mõjudest, riskide maandamisest, küberturvalisuse tasemest ja valdkonna trendidest. Intervjuu küsimused on jaotatud sissejuhatavaks, 5-ks teemaplokiks ja kokkuvõtteks.

Dokumendianalüüs ja intervjuud kokku annavad laiapõhjalisema ülevaate küberriskide maandamise olukorrast ja võimalustest. Alljärgnevas tabelis on autor toonud kokku teemaplokkide kattuvuse dokumendianalüüsi ja intervjuude osas (vt tabel 8).

Tabel 8. Dokumendianalüüsi ja intervjuude kattuvus teemaplokkide osas.

	1. teema: Küberohtude teadlikkus	**2. teema:** Küberohtude mõjud	**3. teema:** Küber-riskide maandamine	**4. teema:** Küber-turvalisuse tase	**5. teema:** Trendid
Arengukava				✕	✕
Struktuur	✕		✕		
Tulemiaruanne					
Hankeplaan			✕	✕	
Hanked 2015-19			✕	✕	
Regulatsioonid		✕			
Intervjuud	✕	✕	✕	✕	✕

Märkused: ✕ - sisend sisuanalüüsi

Allikas: autori koostatud.

Autor kasutas dokumendianalüüsiks Microsoft Excel liigendtabeli vahendeid. Järgnevas magistritöö alapeatükis toob autor välja uuringute tulemused dokumendianalüüsi ja intervjuude teemaplokkide osas, koos järelduste ja soovitustega iga teema kohta.

2.2. Küberturvalisusega seotud intervjuude ja dokumentide analüüsi tulemused

Käesolevas alapeatükis esitab autor tulemused vastavalt dokumendianalüüsi ja intervjuu küsimuste plaanile aluseks olnud teemaplokkidele: teadlikkus küberohtudest, küberohtude tunnetatud mõju, küberriskide maandamine, küberturvalisuse tase ja trendid. Iga teema juures kirjeldab autor põhjalikumalt intervjuudest tekkinud koode ja loodud

kategooriaid ning samuti kasutab toetavaid tsitaate intervjuudest. Autor analüüsib iga loodud kategooriat eraldi, sidudes omavahel teooria, intervjuu ja dokumendianalüüsi tulemused ning lisab juurde omapoolsed ettepanekud teemade kokkuvõtteks. Esimeseks teemaks on **teadlikkus küberohtudest**, mis jagati tulemuste koodide põhiselt viieks kategooriaks.

Tabel 9. Esimeses teemaplokis loodud koodid ja kategooriad

Teema	Intervjuu tulemuste koodid	Loodud kategooriad
1. teema: Teadlikkus küberohtudest	* Lunavara ja krüptovara * Pettused e-posti vahendusel * Teenuste katkestus * Andmevargus * Sisemised ohud	Küberohud
	* Patsiendi (tervise) info * Oht inimese elule * Teenuste takistus, eriti eriolukorras * Võrku ühendatud meditsiiniseadmed * Teadusuuringud ja arendus	Spetsiifilised küberohud
	* Raha * Tehnoloogia spionaaž * Pahatahtlik inimene * Sisemised ohud * Kättemaks (isiklik või ebavõrdsus) * (Geo)poliitilise pinged	Küberrünnakute motivatsioon
	* Patsiendi andmed * Seadmed, võrk ja tarkvara * Varade tuvastamine ja riskide kaardistus (audit) * Erinevate süsteemidega liidestused * Tööjõu puudus	Küberkaitse loomine
	* Kelle ja mille eest vaja kaitsta * Kaasnevad riksid * Tegevusvaldkond väga lai * Tasakaalu leidmine	Küberohtude teadlikkus

Allikas: autori koostatud.

Esimeseks kategooriaks on **küberohud**, kus peamiselt tuuakse välja erinevad pahavarad, mille tulemusel krüpteeritakse seade ning nõutakse lunavara. Samuti tuuakse välja e-posti teel levivad petukirjad, mis 2020. aasta COVID-19 eriolukorras on nii Eestis kui ka ülejäänud maailmas väga levinud. Suurt osa küberohtudest peetakse siiski mitte-sihilikeks ning laialdaselt levitavateks. Vähem esineb sihilikke rünnakuid tervishoiuteenustele, millega võivad tekkida katkestused haiglate töös, ja patsientide terviseandmetele. Üks intervjueeritav tõi lisaks välja ka võimalikud sisemised ohud ning

valesti seadistatud lahendused. Intervjuust tulnud küberohtude kategooria koodid ja tulemused kattuvad suuremas osas töö teoreetilises osas toodud küberohu liikidega (Sfakianakis et al., 2018, lk 26–115), mis näitab küberohud ei piirne ainult laialdaselt leviva pahavaraga.

Antud teema teiseks kategooriaks on **spetsiifilised küberohud** haiglatele, mis intervjueeritavate hinnangul suuresti ei erine eelmises kategoorias toodud küberohtudest. Küll aga toodi mitmel korral välja sihitud rünnakutena patsiendi ja tervise andmete vargused. Üks intervjueeritav tõi välja kasvanud küberohud eriolukorras teadusuuringutele, mille eesmärgiks on saada informatsiooni ravi, vaktsiinide, ravimite ja analüüside osas. Sarnaselt ka teenustõkestusründed eriolukorras, kus ravi ja info saamine võib olla veelgi kriitilisema tähtsusega. Kaks intervjueeritavat tõid välja suuremaid riske inimese tervisele ning seda peamiselt läbi meditsiiniseadmete – ühelt poolt asjaolu, et meditsiiniseadmed on tihti kallid ning kasutusiga pikk, kuid nende infotehnoloogiline tase on nõrk. Teine meditsiiniseadmete küberoht on seotud ka uuemate seadmetega, näiteks südamestimulaatoriga, mille tööd on võimalik mõjutada kolmandal isikul kuna nad ühendatud võrku. Sarnaselt teoreetilises osas käsitletud haiglale suunatud küberohtudele (vt tabel 2) on ka intervjueeritavate arvamus sama – küberohtusid on nii sihitud kui ka mitte-sihitud:

„Spetsiifilisi rünnakuid Eesti haiglate vastu on olnud vähe, sest lihtsalt pole olnud põhjust rünnata Eesti haiglaid. Aga mis puudutab viimaseid tendentse, siis COVID-ga seoses jällegi, on haiglaid hakatud ründama seoses sellega, et mis researchi tehakse ja mis valdkonnas"(A. Reintam, 11.mai 2020)

Kolmandaks kategooriaks sai **küberrünnakute motivatsioon**, kus peamiselt toodi välja rahalised ja omakasupüüdlikud eesmärgid. Sama oluliseks saab pidada ka andmete vargust, mille juures toodi välja patsiendi andmed ja ärisaladused. Sihitud rünnakutega varastatud patsiendi andmeid avalikustatakse ja kasutatakse ära kindlal ajal ja eesmärgil, kus tihti jääb teadmata kes, kus kohast ja millal andmeid varastas. Viimati mainitud näide üldiselt avalikkuseni ei jõua ja on seotud (geo)poliitiliste pingete tekitamiseks ja infosõjaks, millega kaasneb ka riikliku julgeoleku mõõde. Ärisaladustega, näiteks mis andmeid kogutakse ja kuidas neid analüüsitakse teadustööks, seotud informatsiooni hankimise taga on peamiselt riikide vaheline konkurents, kus peetakse oluliseks olla

esimene näiteks uue ravimi või vaktsiini väljatöötamises. Eraldi motivatsioonidena toodi veel välja sisemised ohud ja isiklikest või ebavõrdsusest tingitud kättemaksud. Intervjueeritavate arvamus langeb kokku töö teoreetilises osas käsitletud peamiste motivatsioonidega (Moore, 2010, lk 24–26; Rogers, 2006, lk 98–99), mis annab võimaluse hinnata võimalike häkkerite tüüpe ja nende poolt teostatavaid küberohte.

„Peaasjalik motivatsioon on ikkagi raha. Haiglad liigutavad palju raha ja haiglatel on palju raha, seda avalikkuses ei räägita väga palju. /.../ Teine võibki olla seotud isikliku kaotuse või halva kogemusega meditsiinivaldkonnas. Hüpoteetilisest vaatest keegi ei tahaks sünnitusmaja ründama minna“ (U.Valtenberg, 7. mai 2020)

Neljandaks kategooriaks antud teema koodide põhiselt on **küberkaitse loomine**. Küberkaitse loomisel toodi enim välja patsiendi andmete kaitse vajadust, kuid ka masina- ja seadmepargi ning tarkvara turvalisust. Kõige aluseks toodi varade kaardistust ja prioriteetide seadmist, kus vajadusel kasutada ka välise eksperdi või auditeerimise abi, mis annab eelduse küberkaitse loomisele. Eestis kasutusel olev kolmeastmeline etalonturbe süsteem (ISKE) on heaks töövahendiks ja abiks küberkaitse loomisel ning hoidmisel. Lisaks oma süsteemidele tuleb küberturvalisust arvestada ka kolmandate osapoolte ja süsteemidega liidestamisel, sest rünnatakse tihti just kõige nõrgemat lüli. Töö teoreetilises osas on samuti välja toodud, et esimese sammuna küberkaitse loomisel on vajalik selgitada välja, mis on organisatsiooni andmed (infovara) ning kus ja kuidas neid töödeldakse (Gordon et al., 2016, lk 4–5). Lisaks rõhutatakse nii intervjuudes kui ka teoreerilises osas kvalifitseeritud tööjõu puudusele, mis ajas on pigem kasvav (De Zan & Di Franco, 2019, lk 9).

Küberohtude teadlikkus on viimaseks loodud kategooriaks antud teemas, kus kõik intervjueeritavad tõdevad, et erinevate küberrünnakute ja motivatsioonide tundmine on küberturvalisuse ülesehitamisel väga oluline.

„Kui küberohtude teadlikkus jõuab sinna tasemele, et sa vähemalt tead, millised on võimalikud tagajärjed ja miks sa pead oma asjade eest hoolt kandma, siis see on juba märkimisväärne, kvalitatiivne tõus küberturbe maailmas.“ (A.Reintam, 11.mai 2020)

Kui pole teada kelle või mille eest peab kaitset looma, siis kaasnevad sellega suure tõenäosusega antud valdkonna ala- või ülefinantseerimine. Suuremate haiglate puhul lisab keerukust kindlasti asjaolu, et organisatsioonid on väga suured ning laia haardega. Lisaks, haiglate poolt pakutavale igapäevasele tervishoiuteenusele, on nad seotud ka teadustööga ja teiste organisatsioonidega nagu näiteks ülikoolid ja perearstikeskused. Küberohtude teadlikkus on ka töö teoreetilises osas toodud üheks peamiseks küberturvalisuse loomise aluseks (Parenty & Domet, 2019, lk 106).

„Vaieldamatult, et kui sa ei tea, mille eest sa oma andmeid pead kaitsma, milliste rünnakute ja võimaluste eest, siis sa ei oska neid ka kaitsta. Vaieldamatult on see A ja O, millest tuleb lähtuda oma süsteemide ja meetmete rakendamisel.“ (T.Komp, 12. mai 2020)

Antud teema juurde teostas autor dokumendianalüüsi valimi haiglate struktuuri ja koosseisu osas, millest lähtuvalt oleks võimalik hinnata organisatsiooni teadlikkust erinevast küberohtudest. Kõikide haiglate struktuuris on olemas infotehnoloogia valdkonnaga tegelev osakond või teenistus. Eraldi on ühe haigla struktuuris välja toodud ka infoturbejuht ning teisel on ühendkantselei koosseisus andmekaitse ja infoturbe roll. Võimalik, et infoturbe rolli täitev isik on mõne muu teenistuse või osakonna koosseisus, sest kõike detaile koduleheküljel ei avalikustata. Autori hinnangul annab eraldi infoturbega tegelev ressurss parema sisendi organisatsioonile küberohtude teadlikkuse osas, mis omakorda aitab küberturvalisust üles ehitada.

Esimese teema kokkuvõtteks, põhinedes teoreetilisele osale, intervjuude sisuanalüüsi ja dokumendianalüüsile, on autori poolseks ettepanekuks omada organisatsioonis inimest, kes on teadlik valdkonnapõhistest küberohtudest ja saab anda vajalikku sisendit. Otseselt ei oma tähtsust, kus ta struktuuris asub, pigem on prioriteet antud rolli olemasolu, vastutus ja väärtuse loomine organisatsioonile – kaardistades varad ja tuues välja nendega seotud küberriskid ning võimalikud ohustajad, mille põhjal on võimalik küberturvalisust luua ja hoida.

Järgmise teemaplokina käsitleb autor **küberohtude tunnetatud mõju** organisatsioonis, kus intervjuude tulemuste koodide põhjal on loodud neli kategooriat. Antud teemaploki

juures kasutas autor lisaks dokumendianalüüsi regulatsioonide ja seadusandluse osas, et selgitada nende mõju küberohu tunnetamisele.

Tabel 10. Teises teemaplokis loodud koodid ja kategooriad

Teema	Intervjuu tulemuste koodid	Loodud kategooriad
2. teema: Küberohtude tunnetatud mõju	* Rahalised mõjud * Ravimata juhtumid rikutud seadmest või teenusest * Sanktsioonid * Toimimismõju * Mõju inimeludele	Mõjud küberintsidendist
	* Maine * Usaldus * Poliitiline või ühiskonnakorralduslik mõju * Ravi peatub * Inimese tervis	Mittefinantsiline tunnetatud mõju
	* Pahavaraga ründed lühema mõjuga * Seadme rikkumisel pikemad mõjud * Süsteemide taastamiseni	Mõjude kestvus
	* Vajalik baasturvalisuseks * Standardiseerimine * Ülereguleerimise oht	Reguleerimine

Allikas: autori koostatud.

Teise teemaploki esimeseks kategooriaks on **mõjud küberintsidentidest**. Peamiselt on siiski kõige lihtsamalt mõõdetavad mõjud on rahalised, kas siis otseselt lunavaraks või kuidagi teisiti küberrünnakust tekkinud kulude katteks või siis regulatsioonidest tulenevad sanktsioonid. Lisaks toodi välja mainekahju ja usalduse kaotus, millele on rõhutatud samuti töö teoreetilises osas, et kuni 7% klientidest on altid vahetama teenusepakkujat tervishoiusektoris (Ponemon Institute, 2019, lk 42–45). Mitmel korral toonitati toimimismõju – ravi kättesaadavust, meditsiiniseadmete rikkeid, esmaabi osutamise keerukust ja lisaks ka mõju inimeludele. Enamus haigla teenuseid on seotud infotehnoloogiaga ning kui sellega on probleeme, siis on probleeme ka tervishoiule teenuse osutamisega.

Teine kategooria antud teemaplokis on sarnane esimesele, kuid koondab täpsemalt **mittefinantsilisi tunnetatud mõjusid**. Sarnaselt eelmisele punktile tuuakse peamiselt välja mainekahju ja usalduse kaotus, aga samuti ravi peatumine ning ohu inimese tervisele. Lisaks aga ka andmed, kus hoolimata nende kaardistamisest ja riskihindamisest,

millele ei suuda otseselt finantsilist numbrit külge panna. Ühe uuema valdkonnana tuuakse sisse poliitiline ja ühiskonnakorralduslik mõju, millele samuti ei ole võimalik üheselt fintantsmõõtmeid külge panna. Haiglatel on andmete kogumine ja analüüsimine vajalik arenguks, kus näiteks geenivaramu andmed omavad suurt potentsiaali:

„Võtame näiteks geenivaramu ja kui keegi selle info kätte saab, et kui kõik on teada millised geenid ja asjad seal on, siis võib igasuguseid asju välja tulla sealt" (A.Tomingas, 5.mai 2020)

Järgmiseks kategooriaks on toimunud küberrünnakutest tekkinud **mõjude kestvus**. Üldiselt leitakse, et eelkõige pahavaradega tekkinud mõjude kestvus ei ole pikk, pigem tundide, päevade või nädalate küsimus. Mainekahju ja usalduse kaotusega seotud mõju hinnatakse pigem pikemaajalisemaks. Samuti ka mõjud rünnakutega, mille tulemusel rikutakse olemasolevad tehnoloogilised lahendused või meditsiiniseadmed, on pikemaajalised, kuna taastamine võib teatud juhtudel olla võimatu ning meditsiiniseadmete hankimine võtab aega. Töö teoreetilises osas on organisatsioonile mõju kestvuseks toodud 2-3 aastat (Ponemon Institute, 2019, lk 5), mis antud sisuanalüüsist välja ei tule. Autori hinnangul võib olla põhjuseks asjaolu, et Eestis ei ole suuremaid küberintsidente haiglatega toimunud.

Viimaseks kategooriaks antud teemaplokis on **reguleerimine**, mille juures autor teostas ka dokumendianalüüsi. Regulatsioonid on kindlasti üks peamisi põhjuseid, miks küberturvalisusega organisatsioonides tegeletakse ja pigem ennetavalt. Nende puudumisel ilmselt väheneksid ka investeeringud küberturvalisusse, lõigatakse nurkasid, mille tulemused võivad olla haigla mõistes karmid. Standardiseerimine on samuti väga suureks abiks, kasvõi juba sellepärast, et erinevad organisatsioonid ja inimesed mõistaksid asju üheselt. Üleliigne reguleerimine võib viia olukorra vastupidiseks ning omada tööd pärssivat tulemust ja kalduda liiga juriidika poole. Standardite ja regulatsioonide olemasolu ei vabasta kohustusest omada organisatsioonis kompetentsi ja tegutseda ratsionaalselt.

Dokumendianalüüsi tulemusel toob autor välja olulisemad küberturvalisuse regulatsioonid haiglatele, mis kuuluvad ka kriitilise infrastruktuuri alla, kus intsidentsist

tulenev mõju võib olla üleriigiline: küberturvalisuse seaduse, Euroopa andmekaitse üldmääruse ja ISKE standardi aluse:

- „Käesolev seadus sätestab ühiskonna toimimise seisukohast oluliste ning riigi ja kohaliku omavalitsuse üksuse võrgu- ja infosüsteemide pidamise nõuded, vastutuse ja järelevalve ning küberintsidentide ennetamise ja lahendamise alused.“ (Küberturvalisuse seadus (KüTS), § 1 lõige 1);
- „Isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kaotamise, hävitamise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid („usaldusväärsus ja konfidentsiaalsus“)“ (Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, artikkel 5, punkt 1 lõige f);
- „Turvameetmete süsteemi rakendamine seisneb infoturbe eesmärkidele vastavate turvaklasside määramises ja nendele vastavate turvameetmete valimises vastavalt infosüsteemide kolmeastmelise etalonturbe süsteemi (edaspidi ISKE) rakendamisjuhendile ja nende rakendamises ning rakendamise auditeerimises.“ (Infosüsteemide turvameetmete süsteem, § 2).

Autori ettepanekud antud teemaploki osas, tulenevalt sisuanalüüsist ja teooriast, on jaotatud kaheks. Mõjude seisukohast lähtuvalt soovitab autor ennetavalt hinnata oma varad ja riskid, millest lähtuvalt on võimalik mõjude ulatusi ja kestvusi organisatsioonil hinnata. Esialgselt on mõistlik seada suuremate mõjudega küberohtudele prioriteet, kuna kõigega korraga pole võimalik tegeleda, ning aktsepteerida riske ohtude osas, mida pole võimalik esmajärjekorras maandada. Teiseks ettepanekuks on jälgida regulatsioone ning eelnevalt loodud standardeid küberturvalisuse osas, kuid läheneda ratsionaalselt ja vastavalt oma võimetele. Näiteks ei ole mõtet seada eesmärke, mille täitmiseks puuduvad organisatsioonil vajalikud ressursid.

Kolmanda teemaplokina käsitles autor **meetmeid küberriskide maandamiseks** ning koostas intervjuude tulemuste koodide põhjal neli kategooriat (vt tabel 11). Dokumendianalüüsi raames uuris magistritöö autor haiglate struktuuri ja koosseisu ning selgus, et kahel haiglal on eraldi struktuuris välja toodud infoturbejuhi positsioon ning lisaks on ühel haiglal ka juhatuses esindatud infotehnoloogiajuht. Lisaks analüüsis autor haiglate 2019. aasta tulemiaruandeid ning teostatud riigihankeid.

Tabel 11. Kolmandas teemaplokis loodud koodid ja kategooriad

Teema	Intervjuu tulemuste koodid	Loodud kategooriad
3. teema: Küberriskide maandamine	* Laiapõhjaline arusaam * Küberriskidest teadlikkus * Prioriteetide seadmine * Delegeerima rolle ja korraldama tegevusi * Järelkontroll * Vastutus * Jääkriski otsus * Protsesside loomine ja parendamine"	Juhtkond
	* Funktsioonide täitmine * Koostöö * Juhtkonnas infotehnoloogia (-turve) * Mittehierarhiline vaid lame * Vastutused paigas ja jagatud	Struktuur
	* Koolitused baasteadmiste osas * Protsessid, protseduurid ja reeglid * Pidev informeerimine, teavitamine ja meeldetuletus * Juhtumitest rääkimine * Koostöö ja suhtlus	Mitte-finantsilised maandamised
	* 100% turvalisust pole võimalik tagada * Hinnanguliselt 10-12% IT eelarvest minimaalselt * Iga-aastane püsikulu * Oleneb organisatsioonist * Jääkriski aksepteerimine	Finantsilised maandamised

Allikas: autori koostatud.

Esimeseks loodud kategooriaks on organisatsiooni **juhtkond**. Kõik intervjueeritavad märkisid organisatsiooni juhtkonna olulisust küberriskide maandamise juures. Eelkõige toodi välja laiapõhjaline teemade valdamise oskus, kus tänapäeval juht ei saa ignoreerida infotehnoloogilist sõltuvust ega sellega kaasnevaid küberriske. Juhtkond ei pea koosnema küberturvalisuse ekspertidest, kuid omama pädevust küsida õigeid küsimusi ning langetada otsuseid, ning selle juurde kaasama oskuslikke inimesi, kellele ülesandeid delegeerida. Juhtkond vastutab organisatsiooni üleselt ning kehtestab vajalikke protsesse ja protseduure, kuid samuti peab teostama järelkontrolli ja võtma vastu otsuseid aksepteeritud riskide osas. Töö teoreetilises osas on toodud välja asjaolu, et juhtkond pigem distantseerub antud valdkonnast, kuna ei tunne ennast pädevalt ega mõista sisu (Parenty & Domet, 2019, lk 104), kuid kategooria sisuanalüüs näitab juhtkonna kaasatuse olulisust.

„Et täpselt sama moodi, et tunne oma vaenlast, pead sa tundma oma protsesse ja seda ümbritsevat keskkonda sama moodi. /.../ Juhtkonna arusaamine, eestvedamine, tagant tõukamine kõikides tööprotsessides turbe tagamisel on ikkagi väga oluline.“ (T.Komp, 12.mai 2020)

Järgnev kategooria, organisatsiooni **struktuur**, täiendab eelnevat lõiku. Küberriskide maandamist toetaks pigem lame organisatsiooni struktuur, mitte niivõrd hierarhiline ülesehitus, mis toimib käsuvormis. Meeskonnatöö, kus on jagatud selged funktsioonid, rollid, vastutused ja ootused ning toimib koostöö, saavutab alati püstitatud eesmärgid kõige paremini. Intervjueeritavad jäid eriarvamusele, kas juhtkonnas peaks olema infotehnoloogia või -turbe eest vastutav isik, kuid oluliseks peeti nende valdkondade teema esindatust juhtimistasandil. Infoturbega tegeleva isiku olemasolu on kindlasti oluline, kuid pole oluline otseselt eraldi struktuurüksusena. Töö teoreetiline osa kattub antud sisuanalüüsiga, kus on märgitud olulise osana organisatsiooni küberriskide maandamisel struktuuri, rolle ja protseduure (Le Bris & Asri, 2017, lk 10).

Kolmas loodud kategooria antud teemaplokis on **mittefinantsilised meetmed** küberriskide maandamiseks organisatsioonis. Esiteks tõid interjueeritavad esile, et on oluline kõikide töötajate informeerimine, harimine ja koolitamine baasteadmiste osas (Friedman & Gokhale, 2019, lk 2). Teiseks, eriti oluline on eelneva juures järjepidevus ja juhtumitest avatult rääkimine – ühekordsed intentsiivsed koolitused omavad pigem hetkelist mõju. Lisaks on relevantsed organisatsiooni protsessid ja protseduurid, mille juures on võimalik minimaalsete kuludega märgatavalt maandada organisatsiooni küberriske (Le Bris & Asri, 2017, lk 10). Kolmanda asjaoluna toodi välja olemasolevate infotehnoloogiliste lahenduste seadistamine, mis aitaks küberriske maandada. Tihti käivad viimased kaks maandamise meedet ka koostöös erinevate osapoolte vahel, näiteks salasõnade loomise ja kasutamise protseduurid juhtkonna poolt ja nende rakendamine süsteemides IT osakonna poolt.

Viimaseks kategooriaks küberriskide maandamise teemaplokis on **finantsilised meetmed**. Kindlasti ei ole antud teemal ühest vastust võimalik anda, kuna paljud asjaolud sõltuvad organisatsiooni suurusest ning täpsemast tegevusvaldkonnast. Samuti asjaolust, kas eelarve on stabiilne või esineb mõnel aastal alarahastamist. Kahtlemata on suur vahe, kas tegemist on tervishoiu- või infotehnoloogiasektori organisatsiooniga, kuid igal juhul

saadakse eelarve esmane sisend varade ja riskide hindamisest. Intervjueeritavate arvamusel peab küberturvalisuse eelarve olema ligi 10% organisatsiooni ITK eelarvest ja kõige madalamaks piiriks toodi 5%, mida hinnati antud valdkonna puhul minimaalseks. Varasemate uuringute najal on näiteks tervishoiusektori keskmiseks 6% IT eelarvest (Andre, 2017), mille suurusjärk langeb kokku intervjueeritavate arvamusega.

Riigihangete registrist, kus haiglad teostasid 2019. aastal kokku 751 hanget, tuvastas autor analüüsi tulemusel 65 ITK valdkonna hanget. Hankeid, mis sisaldasid arvutivõrgu ja küberturbe lahendusi oli kõigest 9, mida autori hinnangul on vähe. Teiseks analüüsis magistritöö autor haiglate 2019. aasta tulemiaruandeid. Selgus, et ITK kulu haiglate tegevuskuludest moodustas 0,55-1,88%, mida haiglate eripärast sõltuvalt ei ole märkimisväärselt vähe ning rohkem kui 3-kordne erinevus tuleneb ilmselt haiglate IKT küpsustasemest ja pakutavatest teenustest (Friedman & Gokhale, 2019, lk 4–5).

Esimese ettepanekuna toob autor välja eelnevas lõigus käsitletud IKT kulude ja eelarve stabiilse planeerimise vajalikkuse, sest see toob rohkem läbipaistvust ning arusaama juhtkonna tasemele. Ühekordsete ja suuremate kulude tegemine üle mitme aasta tekitab probleeme eelarve tasakaalus. Autori soovitus on peale varade ja riskide hindamist planeerida minimaalselt 5% IKT eelarvest küberriskide maandamisele. Samuti soovitab autor esimeses järjekorras alustada tegevustest, mis ei nõua märkimisväärseid finantsilisi vahendeid – protseduurid, reeglid, informeerimine ja suhtlus. Kindlasti on vajalik infotehnoloogilisi ja küberriskidega seotud teadmisi organisatsiooni ning juhtkonna tasandil, mis on autori hinnangul ka esimene samm antud ettepanekute tegevustest.

Neljanda teemaploki, **küberriskide taseme hindamine,** intervjuu tulemuste koodide põhiselt moodustas autor neli kategooriat – valmisolek, strateegia, pikaajaline plaan ning teenus. Intervjuudele lisaks tegi autor dokumendianalüüsi haiglate arengukavadele (strateegiale), 2020. aasta hankeplaanile, 2015.-2019. aastal toestatud riigihangetele ja mõju omavatele regulatsioonidele (standarditele).

Tabel 12. Neljanda teemaploki tulemuste koodid ja kategooriad

Teema	Intervjuu tulemuste koodid	Loodud kategooriad
4. teema: Küberturvalisuse tase	* Laiahaardelised organisatsioonid * Suuremaid intsidente pole toimunud * Väiksemate intsidentidega saavad hakkama * Süsteemide küberturbe testimine ja parandamine * Auditeerida kolmanda osapoole poolt * Jälgimine ja analüüs	Valmisolek
	* Juure tasandil * Seotud suuremate strateegiliste eesmärkidega * IT ja küberturvalisus mõlemad * Tööprotsessi lahutamatu osa * Küberturvalisuse strateegia on detailsem	Strateegia
	* Suure pildi omamine * Tulevikuga arvestamine * Pidevalt muutuv olukord * Peab suutma mõõta, et tuvastada kitsaskohti * Plaani mitte omamine tekitab hiljem paanikat	Pikaajaline plaan
	* Tööjõu puudus * Baasteadmised organisatsioonis * Lepingulised kohustused tasakaalus * Jagada vastutust * Kvaliteedisertifikaadid * Valdkonnapõhised teadmised	Teenus

Allikas: autori koostatud.

Käesoleva teemaploki esimene loodud kategooria on **valmisolek**. Intervjueeritavad tõid välja, et suuremaid küberintsidente pole toimunud, kuid lisasid juurde keerukuse küberturvalisuse tagamise haiglate puhul:

„Valdkond on nii suur, lisaks ülikoolid, nad tegelevad nii miljoni asjaga ja fookus on nii lai, et tegelikult ründeskaala on sama lai kui tegevusaladki. /.../ Ründed tulevad sisse sealt, kus on nõrgim lüli“ (A.Reintam, 11.mai 2020)

Haiglatel on kohustus tagada töövõime ööpäevaringiselt, hoolimata riigipühadest või muudest asjaoludest, seega on kindlasti tehtud head tööd ja õnnestunud hoiduda suurematest intsidentidest. Kindlasti aitab kaasa pidev jälgimine ja analüüs, kuid ka auditeerimised ja küberturbe testimised, mida toetavad ka teoorias käsitletud meetmed küberriskide maandamiseks (Ponemon Institute, 2019, lk 38–39, 58–62).

Teiseks kategooriaks on organisatsiooni **strateegia**. Intervjueeritavate üldine seisukoht oli, et küberturve ja ITK tervikuna peab olema seotud organisatsiooni strateegiaga

suuremas pildis, küll mitte detailsuses. Seda põhjusel, et tõenäoliselt on enamus strateegilisi eesmärke seotud ühel või teisel viisil IT lahenduste kasutamisega. Kasulik oleks omada küberturvalisuse strateegiat eraldi, nagu see on loodud riigi tasemel. Strateegiline planeerimine on tööprotsessi lahutamatu osa ning ilma selleta organisatsioon ei toimi. Küberturvalisuse strateegia sidumine organisatsiooni strateegia ja eesmärkidega ning selle juures tasakaalu leidmine on üheks soovituseks küberriskide maandamiseks (Ponemon Institute, 2019, lk 38–39), isegi kui on strateegiast inimestel erinev arusaam:

„Inimesed saavad strateegiatest erineval moel aru. /.../ Strateegia on tegelikult see kavalus või loogika läbi mille, nende piirangute keskkonnas kus me oleme, kus meil kõige jaoks ressurssi ei jätku ja kõiki asju ei suuda teha. Et kuidas me oma väljakutsed või probleemid suudame ära lahendada. /.../ Et kuidas saada 80% tulemit 20% kuluga." (K.H. Peterson, 7.mai 2020)

Pikaajaline plaan on kolmandaks kategooriaks küberturvalisuse taseme teemaplokis. Intervjueeritavad pidasid kõik väga oluliseks pikaajalise plaani omamist küberturvalisuse suurema pildi nägemise jaoks, kuigi see valdkond on ajas pigem kiiresti ja palju muutuv, kuna muutuvad nii tehnoloogiad kui küberohud. Plaani on oluline regulaarselt üle vaadata ning vajadusel teha korrektuure, et oleks võimalik anda vajalikke sisendeid organisatsiooni eelarve ja ressursi kavandamiseks. Ühe näitena toodi Euroopa andmekaitse üldmäärus (GDPR), mille rakendamine oli teada rohkem kui aasta ette, ent ikka oli organisatsioone, kes ei lisanud seda oma plaanidesse. Nendel organisatsioonidel tekkis paanika üldmääruse kehtima hakkamisel 2018. aastal, kuna puudusid vajalikud ressursid – kuigi tegelikkuses oli aega kaks aastat neid planeerida. Pikaajalise plaani koostamine, regulaarne ülevaatus ning uuendamine on ka üks soovitustest haiglatele (Independent Security Evaluators, 2016, lk 53–55).

Viimaseks kategooriaks on küberturvalisuse **teenus** ja selle sisseostmise võimalikkus. Haiglate peamine eesmärk on tagada patsientidele kvaliteetset tervishoiuteenust. Infotehnoloogia ja küberturve on pigem toetavad teenused, mis on küll igapäevaselt vajalikud, kuid mida on võimalik teenusena ka sisse osta. Ülemaailmselt on küberturvalisuse ekspertidest puudus. Näiteks tõi üks intervjueeritav välja 30% puudujäägi, mille skaala kattub teoreetilises peatükis välja tooduga (De Zan & Di Franco,

2019, lk 9). Teenuse sisseostmist peavad võimalikuks ja vajalikuks kõik intervjueeritavad, kuid samas toovad nad välja ka erinevad kitsaskohad. Usalduse ja vastutuse jagamise teema on kriitiline, kuid samuti kvaliteedi tagamine, mille puhul võiks riiklikult seada standardid või kvaliteedisertifikaadid, nagu on kasutusel näiteks Soomes.

„Omal peab majas olema siiski nö pädev ja kompententne kontaktisik. Mõistlik valik ning turule on tulnud ka vastavaid teenuseid. Paljud pelgavad erakätesse andmist, ei kontrolli enam olukorda, kuid palju tegelikult sõltub lepingust ning tingimustest.“ (U.Valtenberg, 8.mai 2020)

Dokumendianalüüsi kohaselt saab öelda, et kuuel haiglal seitsmest on erinevas vormis ja detailsuses arengukavad olemas, millest mõni sisaldas ka strateegilisi eesmärke. Ühel juhul on ainult visiooni ja missiooni kirjeldatud ning teisel juhul on lisaks detailsele arengukava tabelile strateegia välja toodud ka eraldi dokumendina. Muidugi on kõikide haiglate eesmärgiks tagada patsientidele kvaliteetset tervishoiuteenust, kuid autori eesmärk oli leida dokumentidest, kas ja kui palju on IT või küberturvalisuse teemat kaasatud.

Kõigis arengukavades oli ära märgitud meditsiinitehnoloogia arendamine ja ITK arendamise vajadused. Neljal haiglal olid välja toodud eesmärkidena arendada erinevaid e-lahendusi, näiteks e-konsultatsioon ja e-saatekiri, ning samuti oli esile toodud infotehnoloogia olulisus nii haigla arengu kui ka juhtimise seisukohalt. Kolmel juhul oli välja toodud andmete või infosüsteemi turvalisuse tagamise vajadus. Autor soovib rõhutada, et kahes arengukavas on eraldi välja toodud tehnoloogia ja e-haigla strateegiad. Pideva ja süsteemse koolitamise vajadus infosüsteemide ja andmekaitse osas oli samuti märgitud ära kahes arengukavas. Antud dokumendianalüüsi kokkuvõtteks leiab autor, et haiglad arvestavad oma arengukavades tehnoloogiaga, samuti e-lahenduste ja turvalisusega, mis näitab, et see valdkond on prioriteediks organisatsiooni üleselt. Lisaks näitab see organisatsiooni küberturvalisuse küpsustaset, kus teemaga tegeletakse adaptiivselt ja ennatlikult (Friedman & Gokhale, 2019, lk 2; NIST, 2020, lk 37–39).

Töö autor analüüsis ka haiglate poolt teostatud riigihankeid aastatel 2015-2019, et anda hinnang nende valmisolekule küberturvalisuse valdkonnas. Kuigi riigihangete registris ei kajastu kõik hanked, näiteks väiksemad soetused või suuremate raamhangete alt tehtud

ostud, siis on selline kogum siiski piisav hinnangute andmiseks. Riigihangete registri andmete põhiselt teostasid haiglad antud perioodil kokku 3 520 hanget, millest keskmiselt 4,6% moodustasid erinevad infotehnoloogiaga seotud hanked, mis varieerusid haiglatel 1,8-9,3% vahel. Võrgu- ja küberturbelahenduste osakaal sellest oli omakorda 6,2% ning ainult küberturbele kõigest 2% ITK hangetest. Võttes arvesse, et registri andmed ei näita tõenäoliselt kõiki kulutusi, on siiski autori hinnangul need mahud liiga väiksed piisava küberturvalisuse tagamiseks haiglatele tervikuna, mida toetab ka teoreetiline käsitlus (Andre, 2017; Friedman & Gokhale, 2019, lk 4–5).

Viimaseks analüüsis autor haiglate hankeplaane 2020. aastaks küberturvalisuse seisukohast. Kõikide haiglate hankeplaanid olid koduleheküIgedel saadaval, kuid oma ülesehituselt ja detailsuselt erinevad ning sisaldavad üldiselt uusi planeeritavaid hankelepinguid. Kolmel haiglal ei tuvastanud autor ühtegi küberturvalisusega seotud hanget esitatud plaanides. Teistel on hankeplaanis vähemalt üks hange 2020. aastal ning ühe puhul on märgitud eesmärgiks hankida küberturvalisust teenusena. Ühel haiglal on hankeplaanis kaks küberturvalisusega seotud hanget ning veel lisaks kaks IT teenuse hanget. Võttes aluseks 2015.-2019. aastatel teostatud ja 2020. aastal planeeritavad hanked, siis saab autori hinnangul ainult ühe haigla puhul pidada küberturvalisuse arengut stabiilseks. Teiste haiglate dokumendianalüüs on vastuolus intervjueeritavate arvamuse ning teoreetilises osas käsitletud soovitustega haiglate pikaajaliste plaanide ja eelarvete osas (Independent Security Evaluators, 2016, lk 53–55).

Autori soovitused küberturvalisuse taseme teemaplokile baseeruvad intervjuudel ja teoreetilises osas käsitletud soovitustest haiglatele küberturvalisuse osas (Independent Security Evaluators, 2016, lk 53–55). Eelkõige on oluline siduda organisatsiooni arengukavadesse ja strateegiatesse infotehnoloogia ja küberturvalisusega seotud eesmärgid ning koostada pikaajaline plaan küberturvalisuse osas. Pikaajalise plaani abil on võimalik planeerida vajalikke resursse tegevuste ellu viimiseks ja jaotada võimalusel tegevused aastate peale, et ei tekiks kohustuste kuhjumisi ühte perioodi. Teise soovitusena tasuks kaaluda küberturvalisusega seotud teenuste sisseostmist, kuna kvalifitseeritud küberturvalisuse ekspertide puudus tööjõuturul on pigem kasvav trend (De Zan & Di Franco, 2019, lk 9).

Viimase teemaplokina on **trendid**, kus autori poolt on loodud kolm kategooriat tervishoiusektori, tehnoloogia ja meditsiiniseadmete hankimise osas. Antud teemaploki raames teostas autor dokumendianalüüsi haiglate aregukavadele.

Tabel 13. Viiendas teemaplokis loodud koodid ja kategooriad

Teema	Intervjuu tulemuste koodid	Loodud kategooriad
5. teema: Trendid	* Kõik seadmed on ühendatud võrku * Lahenduste omavaheline sidumine * Pilve kasutamine * Andmete avamine, ühiskasutus (*OpenHealthcare*) * Massandmed ja analüüs * Privaatsus ja konfidentsiaalsus	Tervishoiusektori trendid
	* Pilve kasutamine ja turvalisus * Iga seade on sisaldab arvutit ja asjade internet * Massandmed, analüüs ja personaliseerimine * Standardiseerimine * 5G võrk seadmete vahel * Automaatsed ründed	Tehnoloogia trendid
	* Meditsiiniseadmetes on palju IT'd * Võrku ühendamine * Spetsiifilised ja keerulised lahendused * Tagantjärgi keeruline * Koostöö meeskondade vahel	Meditsiiniseadmete hankimine

Allikas: autori koostatud.

Kõikides avaldatud arengukavades on tehnoloogia areng ning erinevate digitaalsete arenduste vajadused esile toodud, seda nii infotehnoloogiliste kui ka meditsiiniliste lahenduste osas. Üks haigla toob välja eraldi pilvetehnoloogia kasutusele võtmise ja selle juures andmekaitse tagamise („Uuendada eHL tehnilist alusplatvormi (rakendusserverid, andmebaasiserverid, andmemassiiv), et tagada võrgustunud haiglate kaugtöö ja andmete turvaline majutamine.“ TÜK arengukava tegevuseesmärgid 3.2.4), kuid küberturvalisuse olulisust on esile toonud kokku neli haiglat. Mainides ära olulisena patsiendi andmete kaitse ja privaatsuse tagamise olulisuse. Autori hinnangul on haiglate arengukavades tehnoloogia arengut kaetud piisaval määral, kuid otseselt puudub suurem innovatsioon ja vaade kaugemale tulevikku. Ühe positiivse näitena saab tuua arengukava, kus on sees ka andmeanalüüsi prioriteet ning *start-up* ettevõtete kaasamine innovatsiooni loomiseks.

„Teeme koostööd start-up ettevõtetega innovaatiliste e-lahenduste väljatöötamiseks.“ SA Põhja-Eesti Regionaalhaigla arengukava aastateks 2019–2021.

Esimeseks loodud kategooriaks trendide teemaplokis on **tervishoiusektori trendid**. Intervjueeritavate hinnangul ei saa küll tuua üheselt välja kindlaid küberriske, mis kaasnevad mõne uue tehnoloogia kasutusele võtmisega, ning pigem peab arvestama kõikide olemasolevate küberohtudega ja võimalustega, et neid lisandub juurde. Lahenduste sidumised, kiirused ja kättesaadavused muutuvad, mida on näha ka erinevate haiglate e-teenuste areguplaanidest. Pilvetehnoloogia kasutusele võtmisel võivad tekkida küsimused andmete hoidmise osas ning andmetega seotud konfidentsiaalsuse ja privaatsuse teemad. Teiselt poolt (mass)andmete kogumine, kasutamine ja analüüsimine on kindlasti trend, kus võiks tulevikus olla teemaks isegi erinevate riikide haiglate vaheline andmevahetus ja analüüs kvaliteetsema tervishoiuteenuse tagamiseks. Kokkuvõtvalt on peamiseks trendiks tervishoiusektoris digitaliseerimine, mis samuti ka töö teoreetilises osas esile toodud (Le Bris & Asri, 2017, lk 3).

Järgmise kategooriana on küberohtude ja **tehnoloogia trendid** üldisemalt. Suuremalt osalt kattuvad tervishoiusektoriga seotud arengud üldiste suundadega, kuid teatud määral tuuakse antud sektori omapärana välja meditsiiniseadmete pikaajalist kasutust, mille tulemusel võivad mõned tehnoloogilised trendid jõuda haiglateni viitega, mis ei ole alati halb. Iga uue tehnoloogia kasutusele võtmisega kaasnevad riskid ning tasub kasutada võimalust õppida teiste vigadest ja kogemustest. Ühe arengusuunana toodi välja loodav uus 5G tehnoloogia, millega kaasnevad uued võimalused andmete kogumiseks, analüüsiks ning seadmete omavaheliseks suhtluseks. Asjade interneti ja andmete kasutamisel on küll võimalik väga personaalseid teenuseid ja pakkumisi teha, kuid samal ajal viia läbi ka automatiseeritud rünnakuid, mis kattuvad teoreetilises osas kajastatuga (Lohrmann, 2019). Lisaks toodi välja asjaolu, et kõik tänapäeva seadmed sisaldavad arvutusvõimsust, mis veel mõned aastad tagasi polnud kasutatav isegi tavapärases personaalarvutis – kõike seda on võimalik ära kasutada erinevatel eesmärkidel, ka pahavara poolt. Eraldi toodi intervjuudes veel välja ressursi puudusest tulenev trend standardiseerimise ja teenuste sisseostmise suunas, mille põhjuseks võib tuua ka globaalse elanikkonna vananemise.

„Ära tee kõike ise - muudatus mõtlemises on eelduseks uutele lahendustele. Standardiseerida nõuete poolt, muidu tehakse kõike 2-20 kordselt - kuna nõuded on

erinevad. Nõudeid peab ühtlustama, siis saab lahendusi integreerida ning sellest tekib võimalus teatud ressurssi kasutada innovatsiooniks.“ (K.H. Peterson, 7.mai 2020)

Viimaseks kategooriaks on **meditsiiniseadmete hankimine**. Kõige olulisemana mainiti siin koostöö vajalikkust ja infovahetust erinevate osakondade vahel. Üldiselt ühendatakse meditsiiniseadmed haiglate võrkudega, et oleks võimalik nende seadmete ja uuringute tulemusi kasutada teistes infosüsteemides või arhiveerida hilisemaks analüüsiks. Intervjueeritavad nõustuvad, et antud valdkonna seadmete hankimisse tuleks kaasata ka infotehnoloogia ja küberturvalisusega seotud inimesi, et ennetavalt maandada võimalikke riske (Drougkas et al., 2020).

„Kindlasti on väga olulime teada, et mida sa hangid. Tagantjärgi võib-olla liiga hilja - raha läinud, andmed läinud või midagi muud hullemat.“ (T.Komp, 12.mai 2020)

Antud teemaploki kokkuvõtteks on autori ettepanek jälgida valdkonnapõhiseid trende nii tehnoloogia kui küberohtude osas, et ennetavalt siduda olulisemad arengud organisatsiooni arengukavade ja strateegiatega. Kõikide käesoleva teemaploki kategooriate osas saab tuua esile vajaduse teha koostööd erinevate inimeste ja osakondade vahel, et tagada parem infovahetus ning ressursikasutus.

Intervjuude kokkuvõtvates küsimustes uuris autor veel arvamusi, kuidas oleks võimalik riiklikult tagada parem tugi antud valdkonnaga tegelemiseks, kuna haiglad on osa riigi kriitilisest infrastruktuurist. Suuremas pildis võib tuua välja geopoliitilise olukorra, kus riik peaks laiemalt mõtlema võimalikele stsenaariumitele, kuid praktilisema lähenemise poolest jätkama teavitustööga, mida on ka juba tehtud. Eelkõige on vajalik asjakohaste juhendite olemasolu, koolituste korraldamine – võimalikult väheste vahenditega katta maksimaalselt palju. Suure tõenäosusega ei ole riigil võimalik haiglatele spetsiifilist küberturvalisuse teenust pakkuda.

„Riigil oleks mõistlik üle vaadata see kvaliteet, see IKT teenuse kvaliteet tervishoius ja kuidas seda paremini saaks tagada, et üks võti ongi vaadata põhjanaabrite poole, et kuidas neil see korraldatud on. Et ikkagi tervise teenuse osutamiseks mõeldavate tarkvara lahenduste osas peaks olema selline kvaliteedisertifikaat ikkagi kõigil võtta, mis

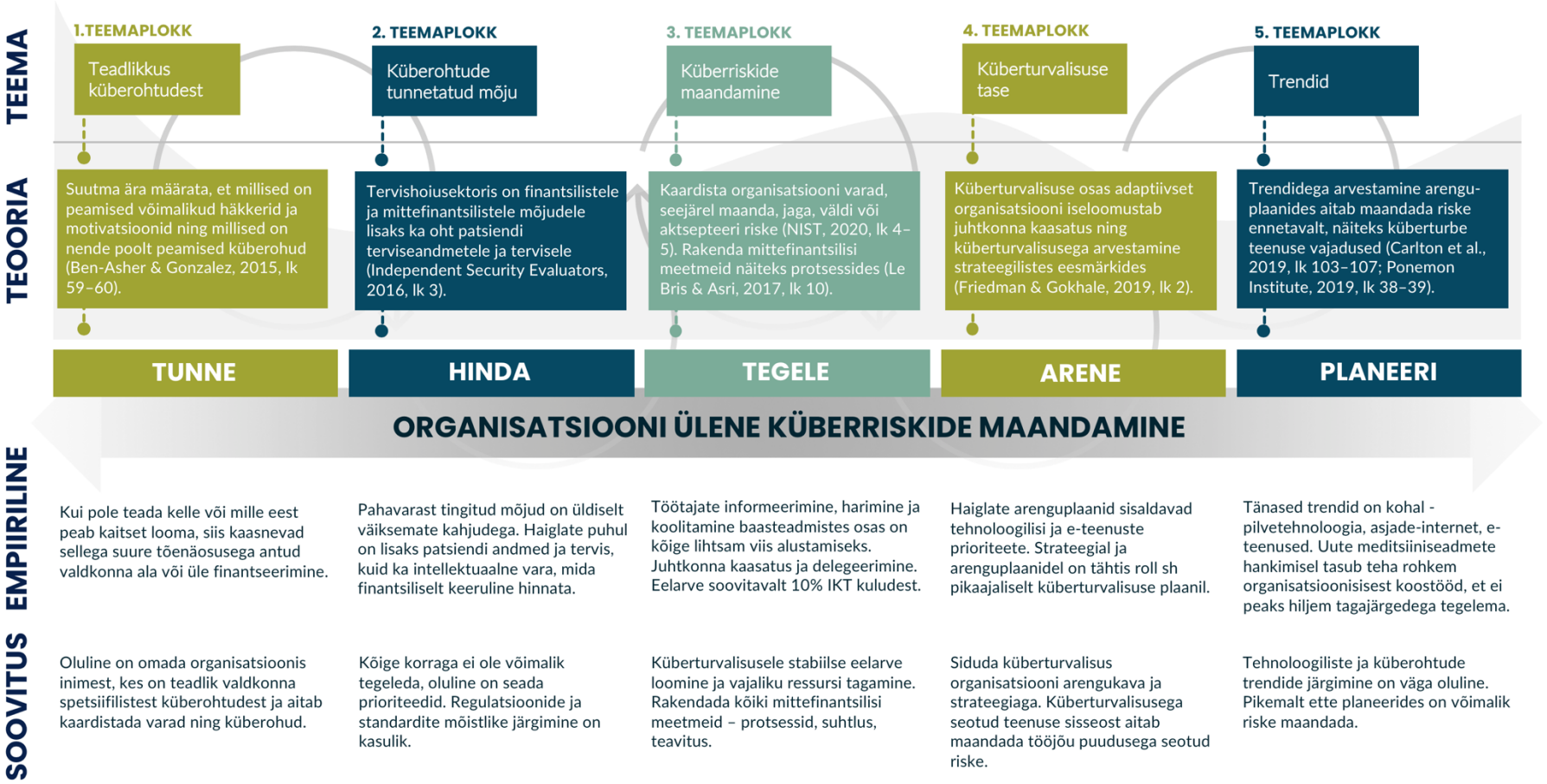
kindlustaks, et tegemist on ausa ja hea asjaga, et hiljem ei tekiks sellist tagantjärgi tarkust, et see ei olnud see, mida me tahtsime“ (T.Komp, 12.mai 2020)

Intervjuu lõpus küsis autor kokkuvõtvalt veel küberturvalisuse vaatenurgast kõige kriitilisemat asjaolu tervishoiusektoris, kus enim märgiti oluliseks koostööd nii organisatsiooni siseselt kui ka erasektoriga, samuti andmete privaatsuse ja konfidentsiaalsuse ning kesksüsteemide kaitset, et turvateadlikkus käiks strateegiliste ja taktikaliste suundadega kaasas.

„Punkt üks on koostöö. /.../ Number kaks on, et peab aru saama, mis on need konkreetsed väljakutsed selles asutuses on /.../ demograafia muutused, kõik mured, mis on vaja lahendada ühel või teisel moel, muidu tervishoiusüsteem lõpetab toimimise, sest raha saab lihtsalt 2026. aastal otsa. /.../ Lahendus ei ole see, et korrutame oma inimeste arvu 1,2ga – selleks ei ole raha ega inimesi. Kui on teada põhjus, miks me peame muutma, kui see on selge, siis saab tegelikult kõik infoturbelahendused sinna külge panna, vajalikud innovatsioonid ära reastada, et jõuda järgmisele tasemele.“ (K.H. Peterson, 7.mai 2020)

Autor ei käsitlenud oma töös otseselt demograafiga seotud probleeme, kuid on nõus intervjueeritava väljaütlemisega, et terve organisatsiooni kaasamine ja suurema pildi omamine on väga oluline küberturvalisuse vaatest.

Käesolevas empiirilises peatükis teostas magistritöö autor teemaplokkide kaupa sisuanalüüsi, võrreldes tulemusi teooriaga ning tegi ettepanekuid küberriskide maandamiseks organisatsiooni üleselt. Magistritöö tulemused võtab kokku alljärgnev joonis 12.



Joonis 12. Organisatsiooni ülene küberriskide maandamine – teooria ja empiiriline käsitlus (autori koostatud).

Kokkuvõtteks saab öelda, et intervjueeritavate arvamused kattusid suuresti magistritöö teoreetilise osaga. Dokumendianalüüsist järeldab autor, et Eesti haiglate küberriskide maandamise tase on erinev, kuid küberturvalisuse ja tehnoloogiliste strateegiate sidumine organisatsiooni arengukavadega on märkimisväärselt oluline samm. Sarnaselt, on oluline teada, milliste küberohtude eest on vaja oma organisatsiooni varasid kaitsta ning tõsta teadlikkust küberohtudest organisatsiooni siseselt. Küberriskide maandamiseks organisatsiooni üleselt on vajalik eraldada ressursse – oluline on stabiilne eelarve, kuid on võimalik ka mittefinantsiliste meetmete rakendamine.

KOKKUVÕTE

Küberohtudega tegelemine on organisatsioonide jaoks saanud igapäevaseks viimase paarikümne aasta jooksul, kuid eriti just viimase dekaadi jooksul, sest erinevate küberrünnakute mahud on märgatavalt kasvanud. Küberriskide maandamine on algselt olnud üksikute isikute või osakondade ülesandeks, seda peamiselt asjaolust, et valdkonda on väga spetsiifiline ja keeruline mõista. Üldine tehnoloogia kasutus, kättesaadavus ning digitaliseerimine on viinud olukorrani, kus küberturvalisuse tagamiseks on vaja kaasata terve organisatsioon. Käesoleva magistritöö eesmärgiks oli teha ettepanekuid Eesti haiglatele küberriskide maandamiseks, analüüsides võimalikke küberohte ning nende tajumist. Eesmärgi täitmiseks oli autoril neli uurimisülesannet, mis sisaldas nii küberohtude olemuse kui ka küberriskide maandamise meetmete kirjeldamist, kuid ka kvalitatiivne sisuanalüüs. Teema tundlikkusest lähtuvalt kasutas autor dokumendianalüüsiks üksnes avalikult kättesaadavaid dokumente ja registreid ning viis läbi intervjuud oma ala eksperidega, mitte haiglate personaliga.

Magistritöö teoreetilises osas tõi autor välja häkkerite tüpoloogia, mis on küll ajas muutuv, kuid sõltuvalt nende kogemustest, oskustest ja motivatsioonidest on võimalik seostada erinevate küberohtudega ning sellest tulenevalt saada sisendit küberturvalisuse ülesehitamisele. Samuti kajastas autor küberohtusid ning nendega kaasnevaid võimalikke mõjusid organisatsioonidele, mis peamiselt on küll välised (nt küberkurjategija ja pahavara), kuid peab arvestama ka sisemiste ohtudega (nt vallandatud töötaja kättemaks). Küberrünnaku mõjud ei ole ainult finantsilised, kaasnevad ka mainekahju ja usalduse kaotus, mille kestus võib olla 2-3 aastat valdkondades, mis on tugevamalt reguleeritud (näiteks haiglad). Küberohtudega seotud riske pole täielikult võimalik maandada ning selle pärast peab jääkrisk olema teadlikult aksepteeritud juhtkonna poolt.

Esimeseks sammuks on igal organisatsioonil oma varade kaardistamine ja hindamine, sellele järgnevalt on võimalik planeerida tegevusi küberriskide maandamiseks. Piisava

eelarve tagamine on küll üks olulisemaid meetodeid, kuid samas on võimalik organisatsiooni küberriske maandada ka väga minimaalsete finantsiliste meetmetega. Protsesside, protseduuride ja reeglite väljatöötamine ja juurutamine ei tekita suuremaid kulutusi, nagu ka töötajate pidev informeerimine ja koolitamine küberturvalisuse osas. Oluline on kindlasti, et juhtkond oleks kaasatud ja paigas vastutused ning rollid organisatsiooni üleselt. Lisaks on oluline, et küberturvalisusega tegeletakse pidevalt ja jätkusuutlikult, koostades nii lühi- kui pikaajalisi plaane ning sidudes küberturvalisust organisatsiooni strateegiliste eesmärkidega. Töö teoreetilises osas tõi autor välja trendid, mida peaks samuti võimalusel pikaajaliste plaanide tegemisel arvestama. Digitaalne areng on paratamatu valik igale organisatsioonile, kuid peab arvestama, et sellega kaasnevad ka riskid.

Magistritöö empiirilises osas viis autor läbi kvalitatiivse uuringu, kasutades informatsiooni saamiseks dokumendianalüüsi ja poolstruktrueeritud intervjuusid küberturvalisuse valdkonna juhtide ja spetsialistidega. Sisuanalüüsist selgus, et küberturvalisuse loomise ja hoidmise juures on väga oluline teada, milliste motivatsioonidega küberohud on organisatsioonile kõige tõenäolisemad. Selle jaoks on kõige mõistlikum omada struktuuris vastava kvalifikatsiooniga töötajat, kes suudaks need ohud ära kaardistada, kuid ei ole kõige olulisem tema kuulumine juhatusse ning pigem on oluline hea koostöö erinevate struktuurüksuste vahel. Haiglatele suunatud küberohud ei erine küll suurel määral mõnest muust organisatsioonist, kuid küberrünnaku mõju võib põhjustada teenuse katkemist või seada ohtu patsientide elu. Seepärast ongi oluline ära kaardistada organisatsiooni varad ja andmed ning ära hinnata, et oleks võimalik nendega kaasnevaid küberriske maandama hakata. Arvestama peab küberriske haiglate meditsiiniseadmetele või patsiendi andmetele, mille mõju võib olla ka inimeste tervisele. Kindlasti on oluline ja samas ka kasulik järgida kehtivaid regulatsioone ning standardeid.

Loodud standardeid tasub kasutusele võtta ja juurutada küberriskide maandamiseks, mitte kalduda üleliia detailsusesse ja juriidikasse, millega võib kaasneda vastupidine efekt. Organisatsiooni juhtkonnale jääb vastutus küberriskide osas, kuid samuti delegeerimise ja järelvalve kohustus. Samuti on juhtkonna pädevuses juurutada protsessid ja protseduurid, mille rakendamine aitab maandada küberriske, kuid ei vaja märkimisväärseid finantsilisi meetmeid. Pidev informeerimine, koolitamine ja

intsidentidest avalikult rääkimine aitab kõige paremini tõsta organisatsiooni teadlikkust küberohtudest ning seeläbi on võimalik ka maandada riske. Finantsmeetmete osas on kõige mõistlikum see, et eelarve oleks tagatud iga-aastaselt ning ei oleks koondunud liigselt ühte perioodi. Kuigi kõiki riske pole võimalik maandada, siis hinnanguliselt 10% organisatsiooni infotehnoloogia eelarvest võiks olla küberturvalisuse tagamiseks, et tagada selle valdkonna jätkusuutlikus.

Infotehnoloogia ja küberturvalisusega seotud teemad peaksid olema seotud organisatsiooni strateegiliste eesmärkide ja arengukavadega. Omades pikaaajalisi ja strateegiaga seotud plaane on võimalik tegutseda teadlikult ja küberriskide taset madalana hoida uute lahenduste väljatöötamise algusest peale. Küberturvalisuse valdkonna tööjõupuudus on probleemiks, kus kõikidel organisatsioonidel pole võimalik piisaval määral personali palgata – selle üheks lahenduseks on antud teenuse sisseostmine. Oluline on omada organisatsioonis küberturvalisuse temaatika baasteadmisi, kuid samas lepingulised kohustused ja vastutused jagada, et oleks usalduslik ja kvaliteetne teenus. Digitaalseid, tehnoloogilisi ja küberohtude trende on väga oluline jälgida ning siduda ka valdkonna jaoks olulisi teemasid pikemaajaliste plaanidega. Lahenduste standardiseerimine ja koostöö erinevate meeskondade vahel saab samuti olema tulevikus veelgi suurema tähtsusega, seda ainuüksi juba ressursipuudusest tingituna.

Käesolev magistritöö on suunatud konkreetsemalt Eesti haiglatele, kuid küberturvalisuse ülesehitamise vaatest on kasutatav ka kõikide teiste valdkondade organisatsioonide poolt. Sarnaselt antud tööle on võimalik igal organisatsioonil hinnata oma varad, mõelda kaasnevatele küberohtudele ja meetmetele, mida oleks võimalik küberriskide maandamiseks rakendada – kas siis mittefinantsilisi või finantsilisi. Magistritöö teoreetilise ja empiirilise osa kokkuvõtteks saab öelda, et küberriskide maandamine on organisatsiooni ülene tegevus. Autori hinnangul vajaks edaspidist lahendamist probleem, kuidas oleks võimalik küberturvalisuse maandamine juurutada organisatsioonikultuuri nii, et küberturvalisuse temaatikaga tegelemine muutuks organisatsiooni loomulikuks osaks.

VIIDATUD ALLIKAD

1. Andmekaitse Inspektsioon. (2019). Avaliku teabe seaduse täitmisest ja isikuandmete kaitse tagamisest aastal 2018.
2. Andre, T. (2017). Cybersecurity an enterprise risk issue. Healthcare Financial Management, 71(2).
3. Arvutimaailm. (2020). Sinu isikukood maksab mustal turul sama palju, kui tass kohvi. Arvutimaailm (am.ee). https://www.am.ee/node/7444
4. AustCyber. (2019). Australia's Cyber Security Sector Competitiveness Plan. 2019(May).
5. Ben-Asher, N., & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48, 51–61. https://doi.org/10.1016/j.chb.2015.01.039
6. Carlton, M., Levy, Y., & Ramim, M. (2019). Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. Information and Computer Security, 27(1), 101–121. https://doi.org/10.1108/ICS-11-2016-0088
7. CMS Legal. (s.a.). GDPR Enforcement Tracker. Salvestatud 14. aprill 2020, https://www.enforcementtracker.com
8. Compliancy Group. (s.a.). HIPAA Fines. Salvestatud 14. aprill 2020, https://compliancy-group.com/hipaa-fines-directory-year/
9. Crawley, K. (2019). How to justify your cybersecurity budget in 2019. AT&T. https://cybersecurity.att.com/blogs/security-essentials/how-to-justify-your-cybersecurity-budget
10. Cyber Security Policy. (2018). Securing cyber resilience in health and care. October.
11. Davis, H. L. (2017). ECMC spent nearly $10 million recovering from massive cyberattack. The Buffalo News. https://buffalonews.com/2017/07/26/cost-ecmc-ransomware-incident-near-10-million/

12. De Zan, T., & Di Franco, F. (2019). Cybersecurity Skills Development in the EU (Number December). European Union Agency for Cybersecurity (ENISA), 2019. https://doi.org/10.2824/525144
13. Drougkas, A., Liveri, D., Zisi, A., & Kyranoudi, P. (2020). ENISA Procurement Guidelines for CyberSecurity in Hospitals (Number February). European Union Agency for Cybersecurity (ENISA), 2020. https://doi.org/10.2824/943961
14. Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? European Journal of Operational Research, 272(3), 1109–1119. https://doi.org/10.1016/j.ejor.2018.07.021
15. ENISA. (2019). Cybercriminals are increasing efficiency with coordinated attacks. https://www.enisa.europa.eu/publications/info-notes/cybercriminals-are-increasing-efficiency-with-coordinated-attacks
16. Euroopa Komisjon. (2019). GDPR – uued võimalused ja kohustused. https://doi.org/10.2838/64230
17. Fish, I. (2017). The Future of Cyber Security. Itnow, 59(4), 43–43. https://doi.org/10.1093/itnow/bwx130
18. Fortinet. (2020). Every Second Counts in Endpoint Protection: Why Real Time Matters. https://www.fortinet.com/blog/business-and-technology/every-second-counts-in-endpoint-protection-why-real-time-matters.html
19. Franklin, M., Adams, R. E., & Henry, C. C. (2019). What the hack is a hacker ?
20. Friedman, S., & Gokhale, N. (2019). Pursuing cybersecurity maturity at financial institutions: Survey spotlights key traits among more advanced risk managers. Deloitte Insights.
21. Gaidosch, T., Adelmann, F., Morozova, A., & Wilson, C. (2019). Cybersecurity Risk Supervision. Departmental Papers / Policy Papers (Kd 19, Number 15). https://doi.org/10.5089/9781513507545.087
22. Gordijn, B., Christen, M., & Loi, M. (2020). The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology. http://www.springer.com/series/7761
23. Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. ACM Transactions on Information and System Security, 5(4), 438–457. https://doi.org/10.1145/581271.581274

24. Gordon, L. A., Loeb, M. P., & Zhou, L. (2016). Investing in Cybersecurity: Insights from the Gordon-Loeb Model. Journal of Information Security, 07(02), 49–59. https://doi.org/10.4236/jis.2016.72004
25. Grispos, G. (2019). Criminals: Cybercriminals. Encyclopedia of Security and Emergency Management, March, 1–7. https://doi.org/10.1007/978-3-319-69891-5
26. Independent Security Evaluators. (2016). Securing Hospitals - A research study and blueprint. https://securityevaluators.com/hospitalhack/
27. Ki-moon, B. (2013). Secretary-General's Video-Message for Model UN Security Council Conference on Cyber Security. https://www.un.org/sg/en/content/sg/statement/2013-10-21/secretary-generals-video-message-model-un-security-council
28. KnowBe4. (s.a.). KnowBe4 - Ransomware. Salvestatud 18. aprill 2020, https://www.knowbe4.com/ransomware
29. KPMG. (2017). Juhised infoturbe halduse süsteemi loomiseks. https://www.ria.ee/sites/default/files/content-editors/KIIK/juhised_infoturbe_halduse_susteemi_loomiseks.pdf
30. Kushwaha, A. S. (2019). Emerging Trends in Cyber Security on Business and its impact. Journal of the Gujarat Research Society, 21(6), 456–460.
31. Le Bris, A., & Asri, W. El. (2017). State of CyberSecurity & Cyber Threats in Healthcare Organizations. ESSEC Business School.
32. Leszczyna, R. (2019). Cost of Cybersecurity Management. Cybersecurity in the Electricity Sector: Managing Critical Infrastructure (lk 127–147). Springer International Publishing. https://doi.org/10.1007/978-3-030-19538-0_5
33. Lohrmann, D. (2019). The Top 20 Security Predictions for 2020. Government Technology. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-20-security-predictions-for-2020.html
34. Lundell, B. (2020). ESG Research Report, 2020 Technology Spending Intentions Survey (Number February).
35. Majandus- ja Kommunikatsiooniministeerium. (2019). Küberturvalisuse Strateegia 2019-2022.
36. Marsh. (2019). 2019 Global Cyber Risk Perception Survey. Microsoft Insights, September. https://www.microsoft.com/security/blog/wp-

content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf

37. Moore, R. (2010). Cybercrime: Investigating High-Technology Computer Crime. Elsevier Science.
38. Morgan, S. (2020). The Complete List Of Hacker And Cybersecurity Movies, Version 2.0. Cybercrime Magazine. https://cybersecurityventures.com/movies-about-cybersecurity-and-hacking/
39. Nahai, F. (2019). General Data Protection Regulation (GDPR) and Data Breaches: What You Should Know. Aesthetic Surgery Journal, 39(2), 238–240. https://doi.org/10.1093/asj/sjy296
40. National Cyber Security Centre. (2018). 10 steps to cyber security. https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/introduction-to-cyber-security/executive-summary
41. NIST. (2020). Nist Privacy Framework: a Tool for Improving Privacy Through Enterprise Risk Management. https://www.nist.gov/system/files/documents/2020/01/16/NIST Privacy Framework_V1.0.pdf
42. Parenty, T. J., & Domet, J. J. (2019). Sizing Up Your Cyberrisks Focus first on the threats to your key activities — not on the technology itself . December, 102–110.
43. Passeri, P. (2020). Cyber Attacks Statistics. Hackmageddon. https://www.hackmageddon.com/
44. Ponemon Institute. (2019). Cost of a data breach report. IBM Security.
45. Porter, S. (2020). Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak. Healthcare IT News. https://www.healthcareitnews.com/news/europe/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak
46. PricewaterhouseCoopers. (2020). PwC's global economic crime and fraud survey 2020 fighting fraud: a never-ending battle.
47. Riigi Infosüsteemi Amet. (2018). Küberturvalisus 2018.
48. Riigi Infosüsteemi Amet. (2019). Küberturvalisus 2019.
49. Riigi Infosüsteemi Amet. (2020). Trendid ja tähelepanekud küberruumis – I kvartal 2020.

50. Rikk, R. (2018). Teadlane teab: Mis on küberturvalisus? TLU. https://www.tlu.ee/dt/uudised/teadlane-teab-mis-kuberturvalisus-raul-rikk
51. Rogers, M. K. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. Digital Investigation, 3(2), 97–102. https://doi.org/10.1016/j.diin.2006.03.001
52. Sallos, M. P., Garcia-Perez, A., Bedford, D., & Orlando, B. (2019). Strategy and organisational cybersecurity: a knowledge-problem perspective. Journal of Intellectual Capital, 20(4), 581–597. https://doi.org/10.1108/JIC-03-2019-0041
53. Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. Digital Investigation, 14, 26–45.
54. Sfakianakis, A., Douligeris, C., Marinos, L., Lourenço, M., & Raghimi, O. (2018). ENISA Threat Landscape Report 2018 (Number January). https://doi.org/10.2824/622757
55. Sotsiaalministeerium. (s.a.). Haiglavõrk. Salvestatud 3. mai 2020, https://www.sm.ee/et/haiglavork
56. Srinivasan, C. R. (2017). Hobby hackers to billion-dollar industry: the evolution of ransomware. Computer Fraud and Security, 2017(11), 7–9. https://doi.org/10.1016/S1361-3723(17)30081-7
57. Statistikaamet. (s.a.). Statistikaamet.
58. Sukhai, N. B. (2004). Hacking and cybercrime. 2004 Information Security Curriculum Development Conference, InfoSecCD 2004, 128–132. https://doi.org/10.1145/1059524.1059553
59. Thomas, J. L. C. (2001). Ethics of Hacktivism. SANS Institute.
60. Välisluureamet. (2020). Eesti rahvusvahelises julgeolekukeskkonnas 2020.

Lisa 1. Häkkerite jagunemine vastavalt oskustasemele ja motivatsioonile

Nimetus	Oskustase	Motivatsioon
Professionaalsed kurjategijad, küberkriminalid ja küberterroristid	Kõrgelt arenenud nii tehnoloogiliselt kui ka psühholoogiliselt.	Puhtalt rahalised eesmärgid, väldivad täielikult avalikkust ja vahele jäämist. Teevad tihti tööd mõnele kriminaalsele rühmitusele. Küberterroristide eesmärk on tekitada hirmu ning paanikat või kaost.
Infosõdalased	Väga kogenud ja tehnoloogiselt pädevad, tihti nö esimese põlvkonna häkkerid, kes oskavad ka ise vajadusel pahavara luua.	Patriotism on peamiseks motivatsiooniks, et kaitsta või hankida informatsiooni ja andmeid oma riigi jaoks.
Küberpätid	Omavad baasteadmisi ja -oskusi, et ise programmeerida lihtsamaid pahavarasid ning tunnevad süsteeme, mida soovivad rünnata. Sihilikult rikuvad kodulehti ning saavad rämpsposti, vähesel määral tegelevad ka pettuste ja vargustega (krediitkaardi).	Teatud määral on finantshuvi, kuid peamiseks ajendiks on kuulsus läbi meediakajastuste ja seetõttu rünnatakse tihti just ettevõtteid, kes oma probleemiga meediasse jõuavad. Tekitavad tööd oma ringkonnale.
Algajad, pisivargad ja viirusekirjutajad	Algajad on alles alustanud selle valdkonnaga ning kasutavad peamiselt eelnevalt väljatöötatud tarkvarasid ning tööriistasid. Pisivargad õpivad vastavalt vajadusele ja omandavad sedasi vajalikke oskusi, mis on küllaltki pädevad. Viirusekirjutajad õpivad vastavalt vajadusele ja omandavad sedasi vajalikke oskusi, mis on küllaltki pädevad.	Enesetõestamise vajadus, tihti ego tõstmiseks ja närvikõdi saamiseks. Samuti tõestamine, et saavutada nö kõrgem tase. Pisivargad pigem väldivad avalikku huvi ja on hakanud sellega tegelema, kuna nende sihtgrupp on liikunud tehnoloogia- ja internetipõhiseks. Peamiselt motiveerib rahaline kasu, kuid vahest ka kättemaks. Viirusekirjutate jaoks on tähtis enesetäiendus ja -areng.
Rahvaalgatused ja häktivistid (inglise keeles *hacktivist)*	Rahvaalgatuslikud häkkerid on pigem keskpärased ja häktivistid ülekeskmiste oskustega.	Rahvaalgatustel on üldiselt sotsiaalsed eesmärgid, kättemaks, mida üheskoos täita (näiteks avalikustada korrumpeerunud riigiametnikud). Häktivistid on peamiselt motiveeritud oma ideoloogiast (sh ka poliitilisest).
Siseohustajad	Peamiselt endised töötajad, kelle oskuste tase on erinev sõltuvalt nende tööst ja kogemustest, kuid üldiselt IT spetsialisti või administraatori tase.	Kättemaks on põhiline ajend, ja kuigi finantsiline kasu on vähe levinud, siis just kõige suuremad kahjud kaasnevad just nende poolt, kuid tihti ei jõua avalikkuseni.

Allikas: (Moore, 2010, lk 24–26; Rogers, 2006, lk 98–99) autori koostatud.

Lisa 2. Küberohu liigid, kirjeldused, võimalikud mõjud ja 2018. aasta trendid.

Küberohu liik	Lühikirjeldus	Võimalik mõju
Pahavara sh lunavara, krüptovara, robotvõrk Trend: stabiilne	Enimlevinud küberohu liik (sh alamliigid näiteks lunavara ja krüptovara), seni enam levitatav failidega kasutades eposti või kodulehti, kuid kasvava trendina mobiilirakendustes ning ka failita nakatumine.	Andmeleke Krüpteeritud või kahjustatud andmed Ressursi väärkasutus Turvaaugu loomine
Koduleheküljе ja rakenduste rünnakud Trend: kasvab	Laialdaselt levinud rünnakud, mille aluseks on koduleheküljed ja nendega seotud teenused sh lehitsejate ja nende lisade haavatavused, kus kasutatakse ära vigasid ja turvaauke, et pääseda ligi süsteemidele ja levitada pahavara.	Pahavara levitamine ja nakatumine. Erinevate andmete (kasutajanimed, paroolid, isikuandmed jne) vargused
Kalastamine Trend: kasvab	Erinevaid petuskeeme kasutades ja maskeerudes kellekski, et saada teada kasutajate isiklikke andmeid – eelkõige kasutajanimesid ja paroole. Samuti levivad ka mobiilsetel seadmetel (kõned ja sms'id). Sihitud ründed on mõne organisatsiooni või isikuga seotud.	Pahavara levitamine ja nakatumine Kasutajanime/parooli vargus Raha ülekanded
Teenustõkestus-ründed Trend: kasvab	Rünnakute eesmärgiks on takistada juurdepääs näiteks kodulehele, teenusele, rakendusele või seadmele	Teenuse käideldavuse probleem Seadmete rikked
Andmevargused ja infolekked Trend: kasvab	Infolekked, sarnaselt andmevargustega, on seotud isikute või organisatsioonide andmetega, mida on kogutud erinevatel eesmärkidel (näiteks kasutajanimed ja paroolid). Infolekked on peamiselt põhjustatud pahatahtmatult.	Mainekahju Trahvid ja sanktsioonid
Siseohud Trend: väheneb	Oht igas organisatsioonis, kui endine või olemasolev töötaja, koostööpartner või muu usaldutud isik kasutab teadmata või teadlikult talle antud juurdepääse või õigusi.	Andme- ja infolekked Ärisaladuste vargus
Füüsiline manipulatsioon Trend: stabiilne	Tagajärjeks võib olla seadmete rike, millel konfidentsiaalsed andmed või juurdepääsud organisatsiooni siseressurssidele (näiteks sülearvuti, nutitelefon, mälupulk jmt).	Andme- ja infolekked Ärisaladuste vargus Pahavara levitamine Rahaline kahju
Identiteedi vargus Trend: kasvab	Rünnakud, kus kasutatakse eelevalt varastatud ning ohvri andmeid. Ei ole kõige lihtsam teostada, kuna vajab pikemaajalist informatsiooni ja ligipääsude hankimist.	Erinevad sõltuvalt rünnaku eesmärgist
Küberspionaaž Trend: väheneb	Rahvusvaheliselt toetatud küberrünnakud teiste riikide organisatsioonide vastu.	Andme- ja infolekked Ärisaladuste vargus Pahavara nakatumine

Allikas: (Sfakianakis et al., 2018, lk 26–115) autori koostatud.

Lisa 3. IKT turvalisus Eesti organisatsioonides 2019. aastal

IKT turvalisus	**Eesti keskmine (%-des)**	**Tervishoiusektori keskmine (%-des)**
Kasutatakse IKT turvalisuse meetodeid	86,1	94,4
Tugev paroolide autentimine	61,1	80,8
Värskeimate tarkvara versioonide kasutamine	70,7	77,7
Andmete, dokumentide, e-kirjade krüpteerimine	30,2	70,0
Andmete varundamine eraldi keskkonda	64,6	75,6
Võrgujuurdepääsu kontroll	60,0	74,7
VPNi kasutamine	39,9	40,5
Turvaintsidendi logifailide kopeerimine ja säilitamine analüüsiks	35,8	53,7
IKT turvalisuse tegevuste teostajad on ettevõtte enda töötajad	42,2	44,0
IKT turvalisuse tegevusi teostab väline teenusepakkuja	55,9	68,1
Dokumendid IKT turvalisuse hindamise, praktikate, protseduuride kohta	28,0	39,6
Ettevõttes IKT spetsialistid ja dokumendid IKT turvalisuse hindamise, praktikate ja protseduuride kohta	8,9	14,1
Turvapoliitikat muudeti viimati viimase 12 kuu jooksul	18,1	23,7
Turvapoliitikat muudeti viimati 12 kuni 24 kuud tagasi	4,9	13,6
IKT riskianalüüside teostamine	24,9	43,9
IKT turvatestid	28,8	34,2
Kindlustus IKT turvaintsidentide vastu	6,8	7,4
Töötajaid teavitatakse IKT turvalisusest eri viisidel	57,7	87,8
Kohustuslikud koolitused, kohustusliku materjali lugemine	44,8	72,9
IKT turvalisusega seonduv on fikseeritud lepingus	36,6	63,5
Eelmisel aastal kokkupuude IKT turvaintsidendiga, IKT teenused polnud kättesaadavad	6,1	9,4
Eelmisel aastal kokkupuude IKT turvaintsidendiga, andmete hävitamine või rikkumine	4,0	10,4
Eelmisel aastal kokkupuude IKT turvaintsidendiga, konfidentsiaalsete andmete leke	3,3	10,8

Allikas: Autori koostatud Eesti Statistikaameti andmebaasi alusel. Uuringus osalenud kõikide Eesti organisatsioonide keskmine protsent võrreldes kõikide Eesti tervishoiu ja sotsiaalhoolekande organisatsioonidega (Statistikaamet, s.a.)

Lisa 4. Intervjuu küsimuste plaan

Teema	Küsimus
Üldised küsimused	1. Palun kirjeldage oma organisatsiooni ja ametipositsiooni peamiseid tööülesandeid ja vastutuse valdkonda.
1. teema: Teadlikkus küberohtudest	2. Millised on teie arvates peamised haiglatele suunatud küberrünnakud?
	3. Mille poolest erinevad küberohud (rünnakud) haiglatele, võrreldes teiste organisatsioonidega?
	4. Millised on haiglale suunatud võimalikud küberrünnakute motivatsioonid?
	5. Mille kaitsmisele peaksid haiglad kõige enam tähelepanu pöörama?
	6. Milline tähtsus on erinevate küberrünnakute ja motivatsioonide tundmisel küberturvalisuse ülesehitamisel?
2. teema: Küberohtude tunnetatud mõju	7. Milliseid on võimalikud tunnetatud mõjud haiglale seoses toimunud küberintsidendiga?
	8. Millised on võimalikud kaasnevad mittefinantsilised mõjud küberintsidendist?
	9. Kui kaua, teie hinnangul, võivad küberintsidendist erinevad mõjud avalduda haiglale?
	10. Millist mõju omavad regulatsioonid küberturvalisuse tagamisel?
3. teema: Küberriskide maandamine	11. Milline roll on küberriskide maandamisel haigla juhtkonnal?
	12. Milline haigla struktuur (osakonnad/ koosseis) toetab küberriskide maandamist?
	13. Milliseid tegevusi on võimalik teostada küberriskide maandamiseks, mis ei tekita kulu (märkimisväärselt)?
	14. Millised on piisavad finantsmeetmed küberturvalisusele? Milline protsents (IT) eelarvest küberturvalisusele?
4. teema: Küberturvalisuse tase	15. Kuidas hindate haiglate valmisolekut küberintsidendiks ja kuidas oleks võimalik seda parandada?
	16. Kuidas peaks olema seotud küberturvalisuse tagamine haigla üldiste strateegiliste plaanide ja eesmärkidega?
	17. Kuivõrd oluline on haiglal omada pikaajalist plaani küberturvalisuse tagamiseks?
	18. Kas ja kuidas oleks võimalik haiglatel küberturvet tellida teenusena?
5. teema: Trendid	19. Millised võimalilkud küberohud kaasnevad tervishoiusektori digitaliseerimise ja uute tehnoloogiate kasutusele võtmisega?
	20. Millised on peamised tehnoloogia ja nendega kaasnevate küberohtude arengu trendid, millele peaks eriliselt tähelepanu pöörama?
	21. Kui oluliseks peate kaasata küberturvalisuseksperte ja -tingimusi meditsiiniseadmete hankeprotsessi?
Kokkuvõtvad küsimused	22. Millist tuge oleks võimalik riiklikul tasemel pakkuda haiglatele, et antud valdkonnaga paremini tegeleda?
	23. Kokkuvõtteks, mis on teie arvates küberturvalisuse teema puhul tervishoiusektoris kõige kriitilisema tähtsusega?

Allikas: autori koostatud.

Lisa 5. Dokumendianalüüsis kasutatud dokumentide nimekiri

	Dokumendi tüüp	Allikas	Kasutamise aeg	Eesmärk
1	Arengukavad, strateegiad, plaanid, eesmärgid	Haiglate koduleheküljed	04.05.2020	Uurida välja, kuidas organisatsioonid arvestavad küberturvalisusega oma tuleviku eesmärkide seadmisel. Samuti aitab hinnata küberturvalisuse taset ja arengu suundasid (trende). Teemad 4 ja 5.
2	Struktuur, koosseis, teenistused	Haiglate koduleheküljed	04.05.2020	Struktuuri, koosseisu ja/või teenistuste uuring aitab analüüsida organisatsiooni teadlikkust küberohtudest, lisaks ka hinnata küberriskide maandamisese ja küpsustaset. Teemad 1 ja 3.
3	Hankeplaan	Haiglate koduleheküljed	04.05.2020	Hankeplaanide uurimise eesmärgiks on analüüsida organisatsiooni küberriskide maandamist ja küpsustaset. Teema 4.
4	Tulemiaruanne, 2019	Saldoandmike infosüsteem	08.05.2020	2019. aasta tulemiaruande põhjal hinnata IT osakaalu organisatsiooni eelarvest ja analüüsida selle põhiselt organisatsiooni küberriskide maandamist ja küpsustaset. Teema 3.
5	Riigihanked perioodil 2015-2019	Riigihangete register	06.05.2020	Riigihangete analüüsimise eesmärk on selgitada välja 2015-2019 teostatud hangete põhjal organisatsiooni küberriskide maandamise osakaal ning hinnata küpsustaset. Teemad 3 ja 4.
6	Regulatsioonid	Haiglate koduleheküljed, RIA koduleht	04.05.2020 -12.05.2020	Analüüsida peamiste kehtivate regulatsioonide mõju ning seotust küberriskide maandamisega ja samuti kasu küpsustaseme hindamisel. Teema 2.

Allikas: autori koostatud.

Lisa 5 järg. Dokumendianalüüsiks vajalike dokumentide kogumine.

Haigla	Edaspidine viide	Arengukava (A) / strateegia (S)	Struktuur (S)/ teenistused (T)	Hankeplaan (H)/ tulemiaruanne (T)	Hanked 2015-2019	Regulatsioonid
SA Põhja-Eesti Regionaalhaigla	PERH	A	T	H / T	eRH	§
SA Tartu Ülikooli Kliinikum	TÜK	A / S	T	H / T	eRH	§
SA Tallinna Lastehaigla	TLH	A	S	H / T	eRH	§
AS Ida-Tallinna Keskhaigla	ITKH	A	S	H / T	eRH	§
AS Lääne-Tallinna Keskhaigla	LTKH	A	S	H / T	eRH	§
SA Ida-Viru Keskhaigla	IVKH	A	S	H / T	eRH	§
SA Pärnu Haigla	PH	A	S	H / T	eRH	§

Allikas: autori koostatud.

SUMMARY

ORGANIZATION WIDE CYBER RISK MANAGEMENT
ON THE EXAMPLE OF ESTONIAN HOSPITALS

Kristjan Põldre

Organizations are going through digital transformation, because the need to use resources more efficiently and make offered services accessible to wider range of customers and partners. Most of the newly adopted services will also bring new unwanted threats to handle. Cyber threats are growing constantly by numbers and also with complexity, therefore dealing with cyber risks are no longer just responsibility of single induvial – it has to be handled organization wide. Although data has the most value in today's world, hospitals need also to ensure security to patients' health and not only clinically, but also technologically - targeted cyber-attack on medical devices could have severe results.

Main objective for this thesis was to make suggestions for Estonian hospitals to manage their cyber risks by analyzing different cyber threats and their perception. Thesis is divided to theoretical and empirical part and author divided the research to four subtasks, which included following:

- Give overview of different cyber threats with their past and future trends, using science literature and also global expert and organization reports. Also, to cover possible hackers and their motivations, and what kind of attacks might occur with possible results.
- Give insights to healthcare related cyber threats and cover methods to manage cyber risks, using science literature and also global expert and organization reports.
- Find out measures to better manage cyber risks by conducting document analyze on Estonian hospital structures, development plans, procurements and financial results. Also, interview IT and cyber security experts and managers, and make analysis one the transcripts.
- Make suggestions to Estonian hospitals how to handle cyber risk organization wide.

In the theoretical part of the thesis, author brought out the typology of hacker. Typology is dynamically changing over time, but by knowing hacker's skillset and motivation it is possible to estimate possible attack methods and to use that knowledge to build up cyber security. Various cyber threats have different impact on organization from which financial is the main one, but there are other implications like trust and reputation. Non-financial perceptions last always longer and can have also financial impact by losing customers.

It is not possible to have bulletproof cyber security and eliminate all risks, therefor it is important for organization to accept some level of risks. The first step to risk management is to have relevant awareness about assets and their value for organization - in cyber space we mostly have data and technology (including medical devices which are connected to other systems). While financial instruments are definitely important part, then there are several non-financial steps that organizations can make to lower cyber related risks. Low cost related are processes and rules that can be applied within organizations and also with 3rd party contracts. Also, informing all employees and training them for base knowledge about cyber threats, constantly and with relevant information. Long term plans for cyber security and connection with organization strategic goals, plays also important part.

In the empirical part of thesis author made research, as described above, and made suggestions for Estonian hospitals to handle cyber risks organization wide. It is very important know what kind of cyber defense you have to build – what are the motivations of the hackers and what tools they might use. This kind of knowledge is usually covered by cyber information security officer, second distinctive knowledge is healthcare specific and for those reasons it is important for hospitals to have this resource within the organization. Every hospital has to know what data and assets they own, who and where has access and what could be possible cyber risks – what implication might bring cyber incident if (patient) data have been compromised or unauthorized access to medical devices has occurred. Regulations and standards play also important part for hospital cyber risk management – from one side sanctions might follow when regulations are not met, but standards give possibility to build cyber security based on common ground which will be also advantage when hospital would like to outsource part of cyber security

or IT services. Cyber security outsourcing is definitely one of the key topics in near future, as there are not enough qualified specialist available, therefor available resources have to be shared. There are concerns with outsourcing – legal aspects, having trust and sharing responsibility. One help could come, from national perspective, if common standards and certification would exist – then it would be possible to match expected and delivered service quality.

The most important role in organization wide cyber risk management is played by management. In today's world it is important to understand and acknowledge the need for IT and cyber security, the basics and competence to ask the right questions and delegate specific functions to qualified personnel. Processes and rules, as mentioned before, implementation is hospital management responsibility, but also the acceptance of risks that will not be handled by other cyber security mechanism. Also, to have cyber long-term cyber security plan and connecting it with hospital strategic goals to deal forehand with cyber risk management. Future involves more advanced digitalization, especially within healthcare sector, with new cyber threats evolving, it is important to deal with cyber risk management organization wide and not to leave this just to few selected persons.

Although current thesis was focused on Estonian hospitals, it is possible to use the same principles to build up any other organization cyber security and risk management. Start by assessing the needed assets for organization to exist, think of the value for the organization, evaluate possible cyber threats and how it would be possible to lower cyber risks – organization wide.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Kristjan Põldre,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „Organisatsiooni ülene küberriskide maandamine Eesti haiglate näitel“, mille juhendaja on dotsent Eneli Kindsiko, 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.

Kristjan Põldre
25.05.2020