POLIITIKAUURINGUTE KESKUS

PRAXIS

Küberturbe valdkonna tööjõuvajaduse ja hariduse uuring

Uuringu aruanne, 29.03.2019

Euroopa Liit
Euroopa Sotsiaalfond

Eesti tuleviku heaks

2019

CENTER FOR POLICY STUDIES

Uuringu tellis Majandus- ja Kommunikatsiooniministeerium. Uuringut rahastatakse Euroopa Liidu Sotsiaalfondist majandus- ja taristuministri käskkirjaga „Toetuse andmise tingimused digitaalse kirjaoskuse arendamise toetamiseks" kinnitatud toetusskeemi eelarvest.

Autorid

Kirsti Melesk

Eve Mägi

Kaupo Koppel

Aleksandr Michelson

Töö valmimisse on andnud olulise panuse ka

Sandra Haugas (kõrghariduse õppekavade ja Põltsamaa Ühisgümnaasiumi dokumendianalüüs)

Andi Kiissel (Äriregistri andmete analüüs)

Lee Maripuu ja **Liisa Past** (Mõttehommiku korraldamine)

Lembe Kullamaa (kvalitatiivsete andmete kogumine)

Margaret Pulk (kõrghariduse õppekavade ülevaade)

Anto Veldre (konsulteerimine)

Põltsamaa Ühisgümnaasium ning kõik intervjuudel ja Mõttehommikul osalenud ettevõtjad, valdkonna spetsialistid, õpilased ja üliõpilased.

Poliitikauuringute Keskus Praxis on Eesti esimene sõltumatu, mittetulunduslik mõttekeskus, mille eesmärk on toetada analüüsile, uuringutele ja osalusdemokraatia põhimõtetele rajatud poliitika kujundamise protsessi.

praxis
mõttekoda

Poliitikauuringute Keskus Praxis
Tartu maantee 50, V korrus
10115 Tallinn
tel 640 8000
www.praxis.ee
praxis@praxis.ee

Sisukord

Põhisõnumid

Aastaks 2023 vajab Eesti küberturbe valdkond juurde 270-870 küberturbe kompetentsidega spetsialisti. Võrreldes 2017. aasta tasemega tähendab see tööjõu kasvu vahemikus 32-86%.

Kõige konservatiivsema stsenaariumi kohaselt on aastaks 2023 vaja küberturbe sektoris tänasega võrreldes juurde 270 inimest. See stsenaarium realiseerub, kui valdkonnas ei toimu suuri arenguhüppeid ning ettevõtete kasvutempo on madal. Küberturvalisuse ettevõtted ja asutused ise hindavad tööjõu kasvuks umbes 10% aastas, mis tähendaks viie aasta möödudes täiendavalt ligi 800 küberturbe oskustega spetsialisti vajadust. Sealjuures on küberturbe kompetentside vajadus laiem ning ulatub ka teistesse sektoritesse, mida siinne uuring ei kata. Seetõttu on oluline küsimus, kuidas tagada Eestis piisava küberturbe oskuste ja teadmistega tööjõu olemasolu.

Küberturbe tööjõuvajaduse katmiseks on vajalik erinevate ja mitmekülgete küberturbe karjääriteede tõhustamine. **Talentide pealekasvu soodustab püramiidikujuline skeem, kus aluseks on võimalikult laia spetsialistide baasi ehitamine, mis lihtsustab karjääriteed küberturbe spetsialistiks ning ühtlasi soodustab küberturbe kompetentside levikut teistes valdkondades**. Laiale baaskompetentsile omandatakse juurde spetsiifilisemad küberturbe oskused, mis võimaldab sügavama kompetentsi kujunemist valitud valdkondades. Uuringu põhjal eristub neli võtmevaldkonda küberturbe kompetentside arendamiseks ja tööjõuvajadusele vastamiseks:

1. IKT hariduseta inimeste kaasamine küberturbe valdkonda

- IKT-spetsialistidest on suur puudus, kes on senini peamiseks küberturbe kasvulavaks. Seega on otsustamise koht, kuivõrd suunata tööjõuvajadusele vastamise koormus vaid IKT sektorile või mil määral laiendada küberturbe sektori tööjõu haaret ja seega ka potentsiaalse tööjõu hulka.
- Uuringu kohaselt on nii avalikus kui erasektoris ligikaudu kuuendik küberturbe valdkonna spetsialistides infotehnoloogia välise taustaga inimesed, näiteks õigusteaduse, finantsjuhtimise, ajaloo või rahvusvaheliste suhete eriala lõpetanud töötajad. Seejuures on eelneva tehnilise hariduseta inimesed esindatud nii analüütikutena kui küberturvalisuse valdkonna juhtimises.
- Mitmed ettevõtted viitavad, et värbamisel ei ole määrav vaid kindlalt suunitletud küberturbe alaste teadmiste ja hariduse olemasolu, vaid laiemad infotehnoloogiaalased põhiteadmised ning pidev valmidus täiendõppeks.
- Sellise laiapõhjalise koolitamise oluliseks takistuseks on küberturvalisuse eriala ainete keerulisus ja tehnilisus. Seetõttu on ka olulised piirangud, milliseid oskusi on võimalik eelneva tugeva tehnilise baasita inimestele anda ja milliseid ametikohti nad saavad täita.
- Ka teised riigid on jõudnud sarnaste lähenemiste juurde küberturbe valdkonna arendamisel. Singapur on võtnud eesmärgiks kasvatada küberturbe spetsialistide arvu arendades ümberõppe ja küberturbe oskuste täiendamise võimalusi teiste seotud valdkondade spetsialistidele.

2. Noorte küberturbe kompetentside arengu toetamine haridustasemeid läbivalt

- Praegu toimub küberturbe kompetentside omandamine pigem formaalhariduse väliselt huvihariduse või iseseisva õppimise läbi. Esmased oskused ja hoiakud - mis on olulised nii küberturbe karjääri huvi kasvatamiseks kui ka küberturbe mõtteviisi juurutamiseks laiemalt - kujunevad välja just üldhariduse omandamise perioodil nooremas ja keskmises koolieas. Küberteadlikkuse tõstmiseks noorte seas on vajalik praegusest oluliselt süstematiseeritum huvi suunamine ja kanaliseerimine formaalhariduses toetamaks sügavamat huvi küberturbe vastu ja mitmekülgsemaid karjäärivalikuid.

- Küberturbe kompetentsi arendamise soodustamiseks on olemas nt küberkaitse valikained gümnaasiumis, mõnes üksikus koolis küberkaitse õppesuund, küberturvalisuse võistlused ja harjutused kooliõpilastele. Samas toimivad need tegevused eraldatult ja ligipääs on pigem juhuslik.
- Küberturbe kompetentsi arendamine peab toimuma mitte eraldiseisvalt, vaid lõimitult IT-, õpetajakoolituse, meditsiini- ja õigusteadusega valdkondadega.
- Praegu omandavad üldhariduses küberturbe kompetentse väike hulk õppureid (nt Põltsamaa Ühisgümnaasiumi küberkaitse suuna õpilased) ja baastaseme teadmiste edastamisega peavad tegelema ülikoolid. Kuniks küberturbe kompetentside baastaset ei omandata üldhariduses, peab seda kompenseerima kas kõrghariduses või täienduskoolituse kaudu ettevõttes. Nii avaliku sektori, kõrgkoolide kui ettevõtete esindajad näevad sobivama lahendusena küberturbe kompetentside baastaseme omandamist üldhariduses, mis annab võimaluse kõrgkoolis ehitada olemasolevatele kompetentsidele spetsiifilisemaid küberturbe oskusi erinevatel erialadel.

3. IKT erialadele küberturbe kompetentside tihedam integreerimine

- Uuringu järgi on IKT haridus kõige tavapärasem karjääritee küberturbesse. Kõige levinumad küberturbe töötajate erialad on seotud IKT taustaga, sh informaatika ja IT süsteemide administreerimine.
- Küberturbe alased spetsiifilised teadmised ja oskused tulevad iseseisvalt juurde õppides või ettevõtetes koolitusega. IKT kõrghariduse õppekavadel on küberturbe õppeaineid, kuid nende ulatus ja teemad on erinevad ning sageli on tegemist valikainetega.
- Küberturbe oskuste ja teadmiste suurem lõimimine IKT erialadesse omab kahte potentsiaalset mõju: (A) soodustada olemasoleva küberturbe teadlikkusega IT spetsialistide pealekasvu ning (B) äratada IKT erialade õpilaste sügavamat huvi küberturbe karjäärivalikute vastu.
- Küberturbe perspektiivis on vajadus eelkõige süsteemiadministraatorite, IT-arhitektide, informaatika ja ka arendajate-programmeerijate järele – kompetentsid, kus küberturbe sektor konkureerib kogu IT sektoriga laiemalt.
- Samal ajal rõhutavad ettevõtjad, et väga spetsiifiliste oskuste asemel on pigem vaja laiapõhjaliste teadmiste ja oskustega inimesi, kes suudavad näha seoseid erinevate alavaldkondade vahel. Mõttehommikul osalenud eksperdite arvamusel eristusid teistest kompetentsidest selgelt kolm kompetentsi, mille järgi on vajadus suurem – ettevõtete küberturbe valdkonna juhtimine; küberturbe õppekavade ja -ainete arendus ning küberjulgeoleku riskide analüüs ja juhtimine.

4. Konkurentsieeliste leidmine võistlusel küberturbe talentide pärast globaalsel tööjõuturul

- Küberturbe tööjõuturg on globaalne – ettevõtete talendiotsing ulatub üle riigipiiride. See võimaldab ka väga spetsiifiliste kompetentsidega inimeste otsingu laiendamist, keda Eesti tööjõu turul ei leia või on vähe. Ettevõtted leiavad, et välisspetsialistide kaasamine võimaldab toetada ka ekspordi tegevusi.
- Eesti ettevõtetes on vähe välisspetsialiste, välismaise taustaga inimesi kaasatakse pigem projektipõhiselt ja suurettevõtetes. Rahvusvahelistes ettevõtetes toimib edukalt spetsialistide liikumine ettevõtte üksuste vahel erinevates riikides, kus välisspetsialisti ei ole Eestis otseselt palgatud, kuid nende kompetentsi pagasit on võimalik ettevõttel siiski kasutada.
- Küberturbe valdkonnas kehtivad olulised piirangud välisspetsialistide värbamisele, seda eriti seoses küberkaitse teemadega ning vastavale infole ligipääsu piiramisega välismaalastele. Uuringu järgi takistab välismaalaste värbamist ka Eesti turu spetsiifika - Eestis teenust pakkudes on vaja aru saada enamasti eestikeelsest keskkonnast, nõuetest jne. Lisaks kehtivad tavapärased välistööjõu värbamise probleemid (kohanemise toetamine aja- ja ressursimahukas, raskused asjaajamisel, keelebarjäär).

Uuringu eesmärk

Info- ja kommunikatsioonitehnoloogiate kiire areng on kaasa toonud üha suurema sõltuvuse küberruumist nii üksikisiku igapäevaelu, kui ka majanduse ja riigi toimimise tasandil. Küberruumist olenevad üha enam pakutavad avalikud teenused, sh elutähtsad teenused nagu pääste, elektri- ja veevarustus, telefoni ja andmeside, raharinglus ja makseteenused või isiku identiteedi haldamine. Küberruumi liigub ka üha enam isikutega seotud andmeid, mis tekivad erinevate era- ja avalike teenuste kasutamisel, aga ka erinevates andmesidevõrkudesse ühendatud seadmetest. Sellega seoses on muutunud komplitseeritumaks ka küberruumi ohukeskkond ning suureneb küberruumi kuritarvitamise oht, mille realiseerumine avaldab üha suuremat mõju nii riigi julgeolekule kui ka igapäevase elukorralduse toimimisele. Küberruum on kujunenud üha enam poliitilise võitluse, sõjapidamise ja kuritegevuse osaks.

Nende arengutega kasvab vajadus küberturbe alaste teadmiste ja oskuste järele, et küberruumis valitsevaid ohte ennetada ning realiseerunud ohtudele reageerida. Mitmed varasemad uuringud on toonud esile IKT valdkonna spetsialistide suure tööjõupuuduse (Mets & Leoma, 2016). Ühtlasi on esile tõstetud just infoturbe alaste teadmiste ja oskuste puudust (Psience OÜ, 2017). Siiski on küberturbe valdkonda ja küberturbe tööjõudu Eestis varasemates uuringutes vaid pealiskaudselt puudutatud. **Siinse uuringu eesmärk on ennekõike kaardistada küberturbega tegelevate spetsialistide vajaduse lähitulevikus nii era- kui avalikus sektoris**. Selleks on uuringus esmakordselt kaardistatud põhjalikult küberturbe valdkonnaga seotud ettevõtted ja asutused ning küberturbe põhikompetentsid. Analüüsitud on tööjõu hetkeolukorda ning vajadust viie aasta perspektiivis (kuni 2023) ja küberturbe valdkonna spetsialistide ettevalmistust läbi koolituse ja haridussüsteemi. Selleks on analüüsitud küberturbe ettevõtete Äriregistri andmeid, kogutud on täiendavaid andmeid veebi- ja telefoniküsitluse teel ning läbi on viidud 29 intervjuud ettevõtete, valdkonna spetsialistide, haridussüsteemi esindajate ning õpilaste ja tudengitega (metoodikast vt lähemalt Lisas 2). Kogutud andmete põhjal on koostatud soovitused ja ettepanekud kvalifitseeritud tööjõu tagamiseks küberturbe valdkonnas (vt ptk 5). Uuringus esile kerkivad olulisemad märksõnad on toodud järgneval joonisel.

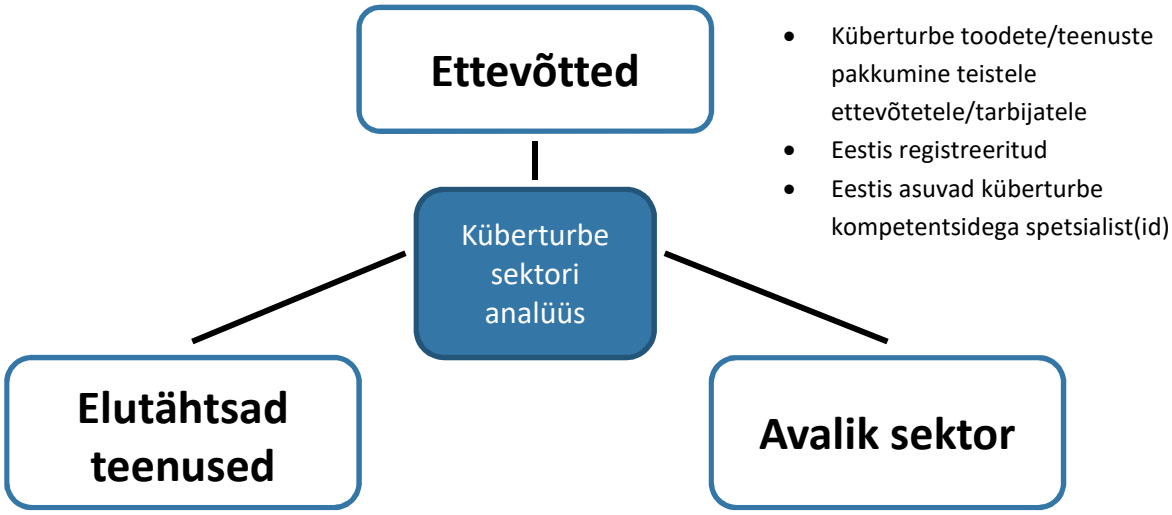
1. Mis on küberturvalisus ja kes on küberturbe spetsialist?

1.1. Sektori määratlus

Küberturbe sektorit on raske piiritleda. Seoses suureneva andmehulgaga ja internetti ühendatud süsteemidega on küberturve muutunud horisontaalseks. Selle järgi on vajadus kõigis tegevusvaldkondades alates põllumajandusest lõpetades tervishoiuga. Seega, et oleks võimalik analüüsida küberturbe valdkonna tööjõu struktuuri ja tööjõuvajadust, on oluline seada fookus – milliseid ettevõtteid analüüsis küberturbe valdkonnana arvestada?

Tihti lähtuvad sektori-põhised tööjõuvajaduse uuringud selgelt piiritletud tegevusvaldkondadest – majandustegevuse määratluse (EMTAK kood) alusel on võimalik piiritleda sektori tegevusala ning koguda statistilisi andmeid valdkonnas tegutsevate ettevõtete kohta. Küberturbe valdkond on väga spetsiifiline osa IKT sektorist, mida ei ole võimalik eristada muust IKT sektorist äriregistri andmetes ega muudes ettevõtete statistilistes andmekogudes. Seega on siinse uuringu aluseks eraldi küberturbe valdkonna kaardistus. Fookus on seatud kolmele võtmevaldkonnale: küberturbe tooteid ja teenuseid pakkuvad ettevõtted, avalik sektor ja elutähtsaid teenuseid pakkuvad ettevõtted (Joonis 1).

JOONIS 1. KÜBERTURBE ANALÜÜSI FOOKUS.



1.1.1. Küberturbe ettevõtted

Küberturbe ettevõtetena on uuringus defineeritud need, kes pakuvad tooteid ja/või teenuseid, mille eesmärk on tagada teistele ettevõtetele/tarbijatele küberturvalisus. Seega ei arvestata küberturbe sektorina siinkohal neid ettevõtteid, kelle tegevuses on küberturve küll oluline osa, kuid kelle küberturbe alane tegevus on suunatud sissepoole (enda toodete, teenuste, andmete turvalisuse tagamine).

Kaardistatud on Eestis tegutsevad ja Eesti äriregistris registreeritud ettevõtted, kellel on Eestis töötavaid küberturbe kompetentsiga spetsialiste. Seega on uuringust välja jäetud Eestis tegutsevad rahvusvahelised ettevõtted, kelle küberturvalisuse kompetents asub mõne teise riigi üksuses.

Küberturbe tooteid ja/või teenuseid pakkuvate ettevõtete kaardistamise aluseks on:

- Startup Estonia poolt kaardistatud küberturbe ettevõtted, start-upid[1];
- Eesti Kaitsetööstuse Liidu liikmed[2], kelle tegevusalade seas on loetletud küberkaitse;
- Äripäeva IT ettevõtete TOP100 sirvimine[3], selekteerides ettevõtted, kelle tegevused on seotud küberturbe/ andmekaitsega;
- ettevõtete otsing erinevate küberturbega seotud märksõnadega;
- valdkonna eksperdid.

Tuginedes ettevõtete endi esitatud kirjeldustele küberturbe tegevusalade kohta, ettevõtetega tehtud intervjuudele ja ettevõtete kodulehtedel pakutavate toodete ja/või teenuste kirjeldusele, on grupeeritud ettevõtete põhilised küberturbe alased tegevusvaldkonnad 9 alavaldkonna vahel. Alavaldkonnad on järgnevalt kirjeldatud suuruse järjekorras ja illustreeritud koos ettevõtete nimedega järgneval joonisel. Ettevõtted on kaardistatud 2018. aasta mai kuu seisuga. Kuivõrd küberturbe ettevõtetest puudub täielik loetelu, võivad pildilt täiendavalt puududa mõned ettevõtted, kes siiski tegutsevad küberturbe valdkonnas. Ettevõtete kaardistust haldab peale uuringu lõppemist Majandus- ja Kommunikatsiooniministeerium.

- **Auditeerimine, nõustamine (*compliance, data protection policies*)**: riskianalüüsid, andmeturbe poliitikate ja tegevuskavade koostamine (sh seadmete, võrgu, paroolihalduse kasutamise korrad ja juhendid, infoturbe sise-eeskirjad jne), andmekaitse ja infoturbe nõuete rakendamine ja selle alane nõustamine (sh ISKE, RIHA, GDPR, eIDAS [4], ka välisriikide vastavad seadusandlused, ISO sertifikaatidele vastavus), turvaauditite läbiviimine/ riskianalüüsid (turvariskide välja selgitamine, ohtude realiseerumise hindamine ja kaasnevate kahjude analüüs), klientide konsulteerimine

[1] https://www.startupestonia.ee/

[2] Allikas: https://defence.ee/members/

[3] 2016. aasta majandustulemuste põhjal koostatud Äripäeva TOP (27.10.2017): https://www.aripaev.ee/standardne-top/2017/10/27/top-parimad-it--ja-arvutifirmad

[4] ISKE=Infosüsteemide kolmeastmeline etalonturbe süsteem. Allikas: Vabariigi Valitsuse määrus „Infosüsteemide turvameetmete süsteem“, jõustunud 1.1.2008. https://www.riigiteataja.ee/akt/13125331?leiaKehtiv

RIHA=Riigi infosüsteemi haldussüsteem, https://www.riha.ee/Avaleht

GDPR=Euroopa Parlamendi ja nõukogu Isikuandmete kaitse üldmäärus (EL) 2016/679, 27.4.2016, https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32016R0679

eIDAS=Euroopa Liidu Nõukogu ja Euroopa Parlamendi määrus e-identimise ja e-tehingute jaoks vajalike usaldusteenuste määramine (EL) 910/2014, 23.7.2014, https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32014R0910

turvaküsimustes. Nõustamise valdkonda kuulub ka IT riskijuhi/ turvajuhi teenuse ja konsultatsiooni müük. Tegemist on Eesti ettevõtete arvu poolest kõige suurema küberturbe alavaldkonnaga. Tihti eelnevad IT auditid ja riskide analüüs erinevartele küberturbe teenuste pakkumisele, et hinnata konkreetse ettevõtte riski taset ja vajadusi.

- **Tuvastamine ja ennetamine (*detection and prevention*)**: teenuste ja toodete pakkumine, mille eesmärk on hälvete, anomaaliate tuvastamine andmeliikluses, et ennetada ja avastada ohte ja ründeid; monitooringuteenuste pakkumine, võrguliikluse seire ja analüüs, logianalüüsid ja -haldus (sh lahendused võrgu pidevaks monitoorimiseks kui ka pisteline kontroll), intsidentidest teavitus.
- **Võrguturve (*network security*)**: infovarade kaitse välisvõrguohtude eest, sh tulemüürilahenduste juurutamine, turvalise kaugjuurdepääsu lahenduste juurutamine, viiruse- ja ründetõrje. Siia alla kuulub ka turvalise võrgulahenduse väljatöötamine, paigaldamine ja juurutamine, mis võimaldab kasutajate ja juurdepääsu kontrolli, kuritahtliku võrgu kasutamise tuvastamise ning rakendab meetmeid sisevõrgu kaitseks väliste ohtude eest.
- **Identiteet, autentimine (*identity management, authentication*)**: sh ligipääsuhaldus, identiteedihaldus (ka kasutajaõiguste haldamine), autentimissüsteemide ja digitaalse indentiteedi süsteemide arendus, haldus, loomine (nt digiallkirjastamine, ajatemplid, elektrooniline ID, andmete krüpteerimine, jm isikutuvastussüsteemid).
- **Koolitused, õppused, teadmuse kasvatamine (*training and awareness*)**: küberturbe alased koolitused ja seminarid spetsialistidele/tehnikutele, küberõppused (*redteaming*), teavitus ja küberhügieeni alased koolitused laiemale sihtrühmale
- **Lõppseadmete turve (*endpoint security*)**: statsionaarsete ja mobiilsete seadmete individuaalne turve, sh viirusetõrje ja lõppseadmetele suunatud turbelahenduste loomine, seadistamine, hooldus. Eesti kontekstis on tegemist enamasti lõppseadmete turbele suunatud lahenduste edasimüügiga, klientide nõustamise ja lahenduste paigaldamise ning hooldamisega. Arvesse on võetud ettevõtted, mis loovad lõppseadmete turbele suunatud lahendusi (hetkel kaardistatud üks ettevõte) või pakuvad lõppseadmete turbe haldamise teenust (sh vajaliku riist- ja tarkvara paigaldamine, haldamine, hooldus). Välja on jäetud ettevõtted, kes üksnes müüvad edasi viirustõrje tarkvara.
- **Intsidendile reageerimine ja turvakriminalistika (*incident response and forensics*)**: teenuste ja/või toodete pakkumine, mis võimaldavad intsidentide tuvastamist, jäädvustamist ja analüüsimist erinevatest digitaalsetest seadmetest; intsidendi allikate väljaselgitamine ning vajadusel tõendite kogumine; intsidentidele reageerimise teenus (intsidentide lahenduskäikude soovitamine, lahenduste rakendamine).
- **Veebiturve (*web security*)**: veebiserverite turve, krüpteeritud virtuaalserverid, veebilehtede ja -rakenduste turvalisuse tagamine
- **Haavatavuse hindamine (*cyber posture*)**: turvalisuse taseme hindamine, sh ründesimulatsioonid, turvatestimine (läbistustestimine)

EESTI KÜBERTURBE ETTEVÕTTED 2018

AUDITEERIMINE, NÕUSTAMINE

Andmevara
Baltic Computer Systems
Price Waterhouse Coopers
Stallion
CGI Eesti
BHC Laboratory
Bytelife Solutions
Leego Hansson
Datafox
Ernst ja Young Baltic
FocusIT
GV Audit
I&T Advisor
ITmees Eesti
Levikom Eesti
Max123
Nortal
Secteam
Security Software
Consultit
Buraeu Veritas Eesti
KPMG Baltics

TUVASTAMINE JA ENNETAMINE

Stallion
Telegrupp
BrowserID
Bytelife Solutions
Datafox
GuardTime
Iptron.net
Koodur
Max123
Santa Monica Networks
Security Software
SpectX
Zone Media
TitanGrid
Malwarebytes

VÕRGUTURVE

Stallion
Telegrupp
Atea
CGI Eesti
Bytelife Solutions
Datafox
Iptron.net
Iteraction
Max123
Levikom
Security Software
Spark Systems
Võrguvara
Baltic Computer Systems

IDENTITEET, AUTENTIMINE

Stallion
Telegrupp
Cybernetica
GuardTime
Koodur
Modirum
Nortal
SK ID Solutions
Twilio Estonia
Veriff
Messente Communications

KOOLITUSED

Stallion
BCS Koolitus
BHC Laboratory
Bytelife Solutions
Clarified Security
Vequrity
ASA Quality Services
Secteam
Security Software
Consultit
Cybexer Technologies

LÕPPSEADMETE TURVE

Andmevara
Baltic Computer Systems
Malwarebytes Estonia
Telegrupp
Digiflak
ITmees
Max123
Spark Systems
Stallion
Iteraction

INTSIDENTIDELE REAGEERIMINE, TURVAKRIMINALISTIKA

Reaalsüsteemid
FocusIT
GuardTime
Passware
SpectX
Malwarebytes Estonia
Security Software

VEEBITURVE

Andmevara
Spark Systems
Zone Media
nodeSWAT

HAAVATAVUSE HINDAMINE

BHC Laboratory
Clarified Security
FocusIT
ASA Quality Services

Euroopa Liit
Euroopa struktuuri- ja investeerimisfondid
Eesti tuleviku heaks
praxis sõttekoda

1.1.2. Küberturve avalikus sektoris

Avalikus sektoris on kaardistatud eelkõige neid asutusi, kes tegelevad otseselt küberturbe valdkonna kujundamisega ning tagavad küberturvalisuse avaliku sektori asutuste infosüsteemides. Siia alla on arvestatud ka küberturbe alane haridus ja teadustegevus (kõik asutused selles alavaldkonnas ei ole vaid avaliku sektori asutused). Oluline osa avalikust sektorist on ka siseturvalisuse tagamine (küberkuritegude ennetemine ja nende uurimine) ning julgeolek (riigikaitse ja küberkaitse valdkond). Kuivõrd küberkaitse tööjõu arvu ja haridustausta kohta käivad andmed on piiratud ligipääsuga, ei olnud seda alavaldkonda uuringu läbiviimisel võimalik arvesse võtta (st tööjõu hetkeseisu kaardistus avalikus sektoris ei sisalda andmeid küberkaitse valdkonna kohta). Siiski on siinse uuringu järeldused olulised ka küberkaitse valdkonna tööjõu vajaduse katmisel.

1.1.3. Elutähtsad teenused

Lisaks on uuringusse kaasatud elutähtsaid teenuseid osutavad ettevõtted. Elutähtsad teenused on need teenused, millel on ülekaalukas mõju ühiskonna toimimisele ja mille katkemine ohustab vahetult inimeste elu või tervist või teiste teenuste toimimist. Küberturbe seisukohalt on oluline tagada nende teenuste järjepidevus ja toimimine võimalike küberintsidentide korral.

Elutähtsate teenuste valdkond on Eestis reguleeritud hädaolukorra seaduse alusel[5]. Elutähtsaid teenuseid on hädaolukorra seaduses loetletud 14. Siinse uuringu tarbeks on analüüs keskendunud neljale alavaldkonnale, mis katab seaduses loetletust seitset elutähtsat teenust:

1. **Vältimatu arstiabi**: riiklikkusse haiglavõrku kuuluvad haiglad[6] ning riikliku kiirabiteenuse pakkujad. Analüüsist on välja jäetud erahaiglad ja -kiirabi teenuse pakkujad, samuti avalikud õendushaiglad ja erihaiglad.
2. **Makseteenused ja sularaharinglus**: analüüsi on kaasatud Eesti Panga Presidendi määruse[7] alusel loetletud elutähtsat teenust osutavad krediidiasutused ja välisriikide krediidiasutuste filiaalid (3), teised Finantsinspektsiooni tegevusloa alusel Eestis tegutsevad krediidiasutused (5) ning Eesti Pank.
3. **Elektriga varustamine**: analüüsi on kaasatud Elektrituru seaduse[8] mõistes elutähtsa teenuse osutajad (6 ettevõtet): (1) tootja, kelle elektrijaama netovõimsus on suurem kui 200 MW; (2) liinivaldaja, kelle riigipiiri ületava elektriliini ülekandevõimsus on suurem kui 100 MW; (3) põhivõrguettevõtja; (4) võrguettevõtja, kelle jaotusvõrguga on ühendatud üle 10 000 tarbija.
4. **Telefoni, mobiiltelefoni ja andmesideteenus**: analüüsi on kaasatud Elektroonilise side seaduses[9] nimetatud elutähtsa teenuse pakkujad (5 ettevõtet), so telefoni, mobiili- või andmesideettevõtted, millel on vähemalt 10 000 lõppkasutajat ning Eesti Interneti Sihtasutus.

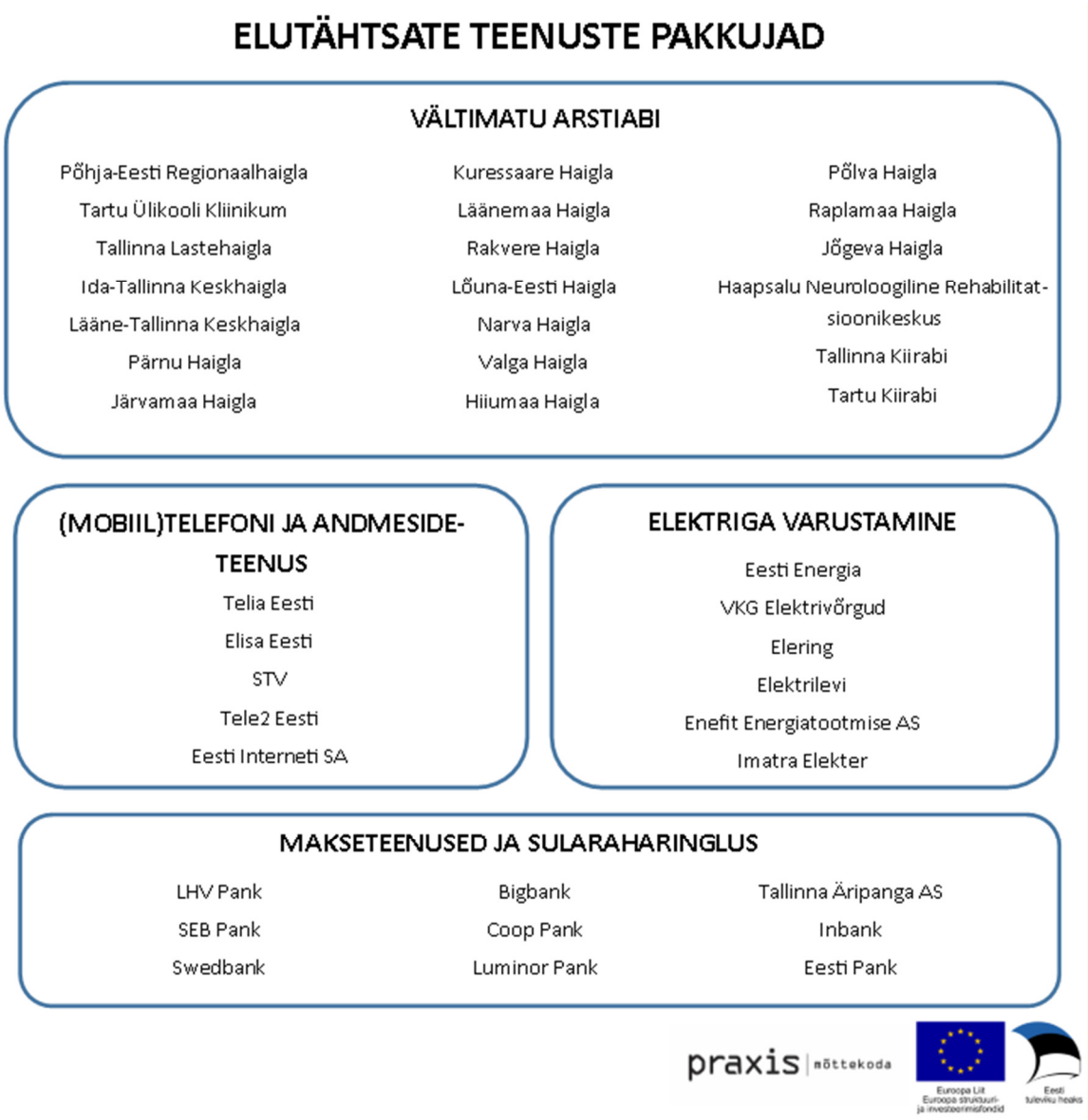
[5] Hädaolukorra seadus, jõustunud 1.7.2017. https://www.riigiteataja.ee/akt/122052018005?leiaKehtiv

[6] Vabariigi Valitsuse määrus „Haiglavõrgu arengukava“, jõustunud 14.04.2003. https://www.riigiteataja.ee/akt/111072015003?leiaKehtiv

[7] Elutähtsat teenust osutavate krediidiasutuste ja välisriigi krediidiasutuste filiaalide loetelu, jõustunud 6.03.2017. https://www.riigiteataja.ee/akt/112122017044

[8] Elektrituruseadus, jõustunud 1.07.2013 https://www.riigiteataja.ee/akt/130062017028?leiaKehtiv

[9] Elektroonilise side seadus, jõustunud 1.01.2005. https://www.riigiteataja.ee/akt/101072017002?leiaKehtiv



1.2. Küberturvalisuse kompetentsid

Küberturbe spetsialisti ei ole võimalik määratleda läbi ametinimetuste või traditsioonilise ametirühmade jaotuse mitmel põhjusel. Kuivõrd küberturbe valdkond on piisavalt spetsiifiline, ei kajastu see tavapärastes statistilistes jaotustes. Teiseks täidab sageli üks spetsialist mitut rolli (nii küberturbe valdkonnas kui ka selle väliselt) ning ametinimetused ei peegelda täidetavaid rolle küberturbe perspektiivis. Seega on vaja küberturbe spetsialisti määratlusele läheneda läbi kompetentside, mida küberturbe spetsialistilt oodatakse ning ülesannete, mida nad oma töökohal täidavad. Tuginedes dokumendianalüüsile (peamiselt USA põhisele kompetentside kaardistusele NICE[10]) koostati esmane küberturbe kompetentside profiil. Seda täiendati ning kohandati Eesti oludele uuringus tehtud intervjuude põhjal küberturbe ettevõtete ja asutustega. Selle

[10] NICE Cybersecurity Workforce Framework (National Institute of Standards and Technology, U.S. Department of Commerce) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

tulemusel on järgnevalt määratletud küberturbe spetsialisti **põhikompetentsid**. Oluline on silmas pidada, et sageli täidavad küberturbe spetsialistid mitut rolli, omades erinevaid küberturbe valdkonna kompetentse. Samuti on sageli tegemist IKT üldiste kompetentsidega, kuid küberturbe valdkonnas on neil juures just turvalisuse aspekti rõhutamine ning sellega arvestamine.

DISAIN JA ARENDUS

Tarkvaraarendus: uue tarkvara arendamine, programmeerimine või olemasoleva modifitseerimine, pidades silmas turvalisuse ja andmekaitse nõudeid. Küberturbe perspektiivis on see kompetents ühest küljest seotud otseselt küberturbe tagamiseks suunatud tarkvara arendusega, teiselt poolt peetakse üha olulisemaks ka laiemalt teadlikku turvalist tarkvaraarendust, nö *security and privacy by design*. Siin on oluline tarkvaraarendaja kogemus ja kompetents ning teadlikkus turvalisest tarkvara disainist.

Süsteemide arhitektuur (*systems arhcitecture, security engineering*): turvaliste infosüsteemide planeerimine, loomine või olemasolevate parandamine, vastavalt kliendi vajadustele (sh äri vajadustele, funktsionaalsus) ning turvalisuse vajadustele (sh nii väljastpoolt kui seesmiselt seatud standarditele ja andmekaitse nõuetele). Sarnaselt tarkvaraarendusega on ka süsteemiarhitektide töö laiem kui vaid küberturbe toodete/teenuste pakkumine, oluline on ka laiemalt turvaliste infosüsteemide ülesehitus erinevates valdkondades, nö *security by design*. Süsteemiarhitektid seisavad selle eest, et turvalisuse eest seisvad komponendid oleks infosüsteemide loomisel arvesse võetud.

Teadus ja arendus: uute tehnoloogiate analüüs, arendus, hindamine, küberturbe integreerimine nendesse süsteemidesse; prototüüpide koostamine; küberturbe tehnoloogia arendamine, küberruumi ja haavatavuse analüüs.

Turvatestimine ja -hindamine: turvatestide planeerimine, ettevalmistamine ja läbiviimine, eesmärgiga hinnata rakenduste või IT-süsteemide haavatavust ja riske, nende vastavust seatud (kvaliteedi) nõuetele ja spetsifikatsioonidele. Siia kuulub ka läbistustestimine (penetration testing) kui sissetungirünnete imiteerimine turvameetmete toimivuse kontrollimiseks. See on spetsiifiline oskus, mida üldjuhul koolitatakse välja ettevõtetes. Oluline on baasteadmine veebirakenduste tehnoloogiatest, soodus on arendaja taust, mis annab vajaliku oskuste ja kogemuste pagasi.

Oluline spetsiifiline kompetents, mida sageli eraldi rõhutatakse on **krüptograafia**, so andmete turvaomaduste tagamine matemaatika kaudu ning võimaldades turvalise identifitseerimise. Krüptograafial on oluline osa usaldusväärsuse ülesehitamisel (sh nt ID-kaardi süsteemi usaldusväärsus, autentimine jne).

TEENUSED JA SÜSTEEMIDE KÄITLEMINE

Andmehaldus: andmebaaside ülesehitamine, administreerimine, analüüs, andmekaitse; andmesüsteemide haldus (turvaline andmete säilitamine, päringute tegemine, andmekaitse).

Klienditeenindus ja tehniline tugi: klientide päringutele/ soovidele vastamine, süsteemide hooldus, probleemide adresseerimine. Küberintsidentide puhul annab tüüpiliselt edasi esmase informatsiooni küberintsidendiga tegelemiseks.

Võrguteenused/ võrkude turvalisus (network security): võrkude ja nende tulemüüride haldamine, testimine, opereerimine, tagamaks infosüsteemide ja andmete turvalisus.

Süsteemide analüüs ja administreerimine: infosüsteemide üles seadmine ja haldamine, kasutajakontode ja süsteemile ligipääsu haldamine; võrgu liikluse monitooring, analüüs; turvariskide identifitseerimine. Oluliseks peetakse süsteemiadministraatorite võimekust identifitseerida ja analüüsida turvariske ning selle olemasolu nende väljaõppes. Oluline on IT baasharidus ning süsteemihalduse kogemus.

JUHTIMINE, JÄRELEVALVE

Strateegiline planeerimine, poliitikakujundamine: küberturbe valdkonna poliitikakujundamine, valdkonna arendamine ja selle esindamine nii riigisiseselt kui rahvusvaheliselt. Näiteks kuulub siia alla ka rahvusvaheliste suhete arendamine ja küberdiplomaatia ning Eesti küberturbe esindamine, arendamine rahvusvaheliste partnerite suunal.

Küberturbe ettevõtete juhtimine: küberturbe tooteid või teenuseid pakkuvate ettevõtete/asutuste töö ja meeskondade juhtimine. Eesti turul on puhtalt küberturbe ettevõtteid vähe ja sageli on need väikesed ettevõtted. Seetõttu on küberturbe ettevõtete juhiks pigem inimesed, kes valdavad ise tehniliselt valdkonda hästi. Seega on eelduseks pigem tehniline valdkonna tundmine, millele lisaks on vajalik juhtimiskompetents.

Küberturbe valdkonna juhtimine: ettevõtte/asutuse küberturbe valdkonna juhtimine, sh infoturbe haldamine; strateegiline juhtimine, meeskonna komplekteerimine ja juhtimine, ettevõtte küberturbe poliitikate arendamine ja rakendamine, juhtkonna/teiste valdkondade teavitamine turbevajadustest jne. Oluline ettevõtte küberturbe ja infoturbe mõistmine formaalsel ja protsesside juhtimise tasandil, küberturbe toimivuse tagamine. Samuti on oluline riskide juhtimise kompetents: küberriskide juhtimise põhimõtete koostamine, riskide kaardistamine, dokumentatsiooni koostamine, korrastamine, riskide hindamine organisatsiooni siseselt. Sageli on seda kompetentsi täitvad rollinimetused: Chief Information Security Officer (CISO)/ Certified Chief Information Security Officer (CCISO), turvajuht, infoturbejuht. See on ka ainus küberturbe spetsiifiline roll, mida on kirjeldatud Eesti kutsesüsteemi raamistikus.

Järelevalve, nõustamine: küberturbe standarditele vastavuse jälgimine, analüüs ja nõustamine, sh andmekaitsenõuetele vastamine, küberturbe auditite läbiviimine (compliance). Nõuded/standardid võib määratleda ettevõte/asutus ise või tulenevad need seadusandlusest, standarditest vms. See nõuab erinevate infoturbe sertifikaatide ja nende nõuete tundmist, seadusandluse tundmist (nii Eestis kui rahvusvaheliselt) ning oskust neid nõuded ettevõtte protseduuridele kohandada. Ettevõtted on intervjuudes viidanud, et selle rolli täitmisel ei ole tehniline teadmine primaarne. Inimesi on nii IT-, juristi, audiitori (nt siseaudiitor, IT-audiitor) jms taustaga. Kosultatsiooniteenuste pakkumise puhul on viidatud, et oluline on interdistsiplinaarsus: nt oskus viia kokku äriteadmist IT teadmistega (sh spetsiifilisemalt küberturbega).

Euroopa Isikuandmete kaitse üldmäärus on loonud ka uue rolli andmekaitse perspektiivis: data protection officer (DPO). DPO ülesanne on hallata ettevõtte andmekaitse strateegiat ja rakendamist ning tagada ettevõtte andmehalduse süsteemide vastavuse GDPR nõuetele. Sageli täidavad formaalselt DPO nõudeid ettevõtte administratiivtöötajad kuivõrd sellist kompetentsi, mida DPO puhul eeldatakse, veel turul ei pakuta ning kui seda on, on tasu kallis. Ettevõtted on intervjuudes viidanud, et selle tulemusel ei vasta DPO võimekus alati sellele, mida sellelt rollilt eeldatakse.

Küberturbe projektide juhtimine: ajaliselt ja eelarveliselt piiritletud küberturbe toodete/teenustega seotud projektide juhtimine. Suuresti kombineerib küberturbe projektide juhtimine eelnevalt loetletud kompetentse, sh oskus komplekteerida ülesande sooritamisele orienteeritud meeskonna, meeskondade ja protsesside juhtimine, projektile seatud nõuetele vastavuse tagamine ning projekti spetsiifikaga seotud tehniline teadmine.

HARIDUS, KOOLITUS

Küberturbe alane haridus: küberturbe valdkonna õpetamine erinevatel haridustasemetel ning erinevatel õppekavadel; küberturbe õppekavade loomine, arendamine. Siinjuures on oluline lisaks valdkonna teadmistele pedagoogilised oskused ja õpetamismetoodikate valdamine – oskus oma küberturbe alaseid eriala teadmisi õpilastele edasi anda.

Küberturbe alane koolitus: nii spetsialistidele suunatud koolitus kui ka laiema sihtrühma koolitamine/ teadlikkuse tõstmine küberturbe vajadusest; küberturbe spetsiifiliste koolituskavade loomine, arendamine.

Küberõppused: eraldi küberturbe spetsiifilise kompetentsina on mitmes intervjuus rõhutatud küberõppusi, nende planeerimist ja läbiviimist, seda nii rahvusvaheliselt (nt NATO küberkaitsekeskuse korraldatud Locked Shields, EL kaitseministritele suunatud küberõppus EU CYBRID 2017 jne), Eesti siseselt (sh õpilastele suunatud KüberNaaskel ning Küberpähkel) kui ka organisatsioonide tasandil.

KÜBERTURVE: ENNETAMINE JA INTSIDENTIDE HALDAMINE

Ennetustegevus, küberruumi seire: küberkaitse jaoks vajaliku informatsiooni kogumine (sh võrguliikluse jälgimine, süsteemi hoiatuste analüüs, logide analüüs) ja analüüs, et tuvastada võimalikke ohuallikaid ning tekkida võivad turvaintsidente. Sageli annab just seire esimese hoiatuse võimalikust turvaintsidendist või ohuallikast.

Küberjulgeoleku riskide analüüs ja juhtimine: seotud eelneva kompetentsiga – kogutud info põhjal riskide analüüs ja haavatavuse hindamine, süsteemi hälvete analüüs, riskitaseme hindamine, sobivate vastumeetmete väljatöötamine ja/või soovitamine operatiivsel või mitteoperatiivsel tasandil. Riskide analüüs toimib nii proaktiivselt (olemasoleva info põhjal intsidentide ära hoidmine, riskiallikate ennetamine) kui ka juba toimunud turvaintsidentide analüüs. Siia kuulub ka olemasoleva pahavara hindamine ja analüüs, mille põhjal on võimalik hinnata ohutaset ja edastada vajalik info vastumeetmete väljatöötamiseks ning intsidentide ennetamiseks.

Küberkaitse infrastruktuuri haldamine: küberkaitse süsteemide riistvara ja tarkvara haldamine, nende testimine, hooldamine, rakendamine. Riigikaitse valdkonnas lisanduvad siia väga spetsiifilised kompetentsid, seoses relvasüsteemide jms juhtimise ja haldamisega.

Operatiivtegevus: turvaintsidentide haldamine, käsitlemine, lahendamine; otsestele ja võimalikele küberohtudele reageerimine tagamaks toiminud intsidentide puhul maksimaalselt väikesed kahjud (vara ja elude säilimine, info kaitse). Riigikaitse valdkonnas spetsiifilisemalt ka küberoperatsioonide planeerimine ja läbiviimine (sh küberrünnete korraldamise võimekus).

KÜBERKURITEGEVUSE TÕKESTAMINE, UURIMINE

Küberkriminalistika: tõendite identifitseerimine, kogumine, uurimine; tõendite kogumise dokumenteerimine nii kriminaaluurimise raames kui ka küberjulgeoleku tagamiseks. Ka **digitaalne kriminalistika**, mis on kitsamalt arvutitega seonduvate tõendite kogumine, käitlemine, analüüs.

1.3. Küberturbe ametikohtadel vajalikud oskused ja teadmised

Küberturbe spetsialistide oskused ja teadmised tuginevad suures osas IT valdkonnas omandatud baasharidusele ja valdkonnas töötades omandatud kogemustele, millele on iseseisvalt või läbi täiendõppe

omandatud juurde küberturbe spetsiifilised oskused ja teadmised. Üha enam on muutumas aktuaalseks ka teistest valdkondadest tulenevad teadmised ning tehnilisi oskusi täiendavad üldoskused.

1. **Küberturbe tehnilise baasi tagab tugev IT-alane haridus ja IT valdkonnas omandatud kogemus**

Suure osa küberturbe (tehniliste) funktsioonide täitmiseks vajalikke oskusi võib vaadelda püramiidina, kus küberturbe alased oskused ja teadmised tuginevad tugevale IT-baasharidusele ja IT valdkonnas omandatud kogemusele. Küberturbe spetsiifilisemad oskused ja teadmised on enamasti omandatud juurde kas iseseisvalt või läbi täienduskoolituste.

Intervjuudes ettevõtetega on välja toodud, et küberturbe valdkonnas on IT erialadelt vajadus eelkõige süsteemi administraatorite, IT-arhitektide, informaatika ja ka arendajate-programmeerijate järele, kellest kasvavad välja küberturbe personal. Nende oskuste ja teadmistega inimestele konkureerib küberturbe valdkond kogu IT sektoriga laiemalt ja kohati ka teiste valdkondadega, kus nende oskuste ja teadmistega inimesi aina enam värvatakse. Varem on leitud, et aastal 2013-2020 peab IKT tööjõud kasvama 1.5 korda, et vastata turu nõudlusele (Mets & Leoma, 2016). Oluliselt nähti just IKT-süsteemide arendajate ja haldajate kasvu, IKT-süsteemide ja tarkvara analüütikute ja -arhitektide kasvu ning tarkvaraarendajate kasvu, mis on kõik ka küberturbe valdkonnas nõutud oskused.

Mitmes intervjuus on rõhutatud, et Eesti küberturbe spetsialistide eelis on nende teadmiste ja oskuste laiapõhjalisus vaid ühe valdkonna süvitsi tundmise ees. Seega peetakse oluliseks nn T-kujulist oskuste profiili, kus laiapõhjalisi teadmisi erinevatest IT alavaldkondadest täiendavad süvitsi minevad oskused mõnes spetsiifilisemas (küberturbe) valdkonnas. See tagab tõhusama valdkondade vahelise koostöö – programmeerija saab paremini aru, mida on vaja võrkude turvalisuse tagamiseks jne. Seeläbi sünnivad ka paremad lahendused, mis arvestavad erinevate süsteemi osapoolte vajadustega. Selle tagamiseks on oluline, et kõikidel IKT erialadel on võimalik omandada küberturbe baasteadmised, mis annab vajalikud küberturbe oskused tulevastele IT spetsialistidele kui loob ka eeldusi uute küberturbe spetsialistide pealekasvuks.

> *Soomes […] sa saadki terve karjääri spetsialiseeruda mingisugusele konkreetsele skillsetile, siis kui sa võtad Eesti IT-inimese, siis nad on tegelikult proovinud Windowsi, Linuxi tulemüüri, võrgundust, põhimõtteliselt nende ampluaa on ikkagi lai […]. Ei tasu ka rõhuda nende vajaduste täitmisel sellele, et on vaja konkreetseid spetsialiste. Seda laiapõhjalisust ja seda, et oleks igal tasemel see teema sees, on olulisem. (Küberturbe ettevõte)*

2. **Üha rohkem kaasatakse küberuturbe valdkonda ka IKT-väliste valdkondade teadmiste ja oskustega inimesi.**

Juba praegu on küberturbe spetsialiste nii õigusteaduse, finantsjuhtimise, ajaloo või rahvusvaheliste suhete eriala lõpetanute seast. Sealjuures töötatakse nii analüütikute kui küberturbe juhi ametikohtadel. Ka intervjuudes on viidatud, et IT alane haridus ei ole värbamisel alati primaarne. Mitmed tänaseks heaks spetsialistiks kujunenud inimesed on ise õppinud ja vajalikud kogemused omandanud IT valdkonnas töötamisega.

Eraldi tuuakse välja, et juhtimise ja järelevalve (vastavuse tagamise ehk compliance) kompetentside puhul ei ole alati oluline sügav tehniline teadmine. Olulisemaks muutuvad nõuetest ja seadusandlusest arusaamine, protsesside juhtimise, organisatoorsed ja tegevusplaanide koostamise oskused. Siin muutub oluliseks oskus vaadata küberturbe valdkonda laiemalt, nt seostada seda laiemalt ärijuhtimise, õiguse või teiste valdkondadega.

> *Aga üks profiil on seotud selle küberturve standarditega, seotud auditite ga ja organisatoorse poole korraldamisega. See tehniline teadmine seal juures on oluline, aga see ei ole nii primaarne, et see ei pea olema süsteemi arhitekt või administraator selleks, et seda teha. (Riigiasutus)*

Ka teistes riikides on võetud suund IKT väliste spetsialistide kaasamiseks küberturbe valdkonda. Näiteks Singapur on võtnud eesmärgiks kasvatada küberturbe spetsialistide arvu arendades ümberõppe ja oskuste täiendamise võimalusi teiste seotud valdkondade spetsialistidele küberturbe valdkonnas.

3. **Küberturbe spetsiifilised oskused ja teadmised õpitakse juurde läbi täienduskoolituse ning kogemuse.**

IT- või muu valdkonna baasharidusele õpitakse juurde küberturbe spetsiifilisi oskusi täienduskoolitustel nii Eesti siseselt kui rahvusvaheliselt, sh suurte rahvusvaheliste ettevõtete täienduskoolitused (uued ohud, turvanõrkused, pahavara). Seega võtab küpseks ja heal tasemel infoturbe spetsialistiks kasvamine aega – paljud teadmised omandatakse iseseisvalt juurde ning paljud oskused on tööga õpitavad ja tuginevad kogemusele. Sealjuures ei oodatagi, et koolist tuleks valmis küberturbe teadmiste ja oskustega spetsialiste, vaid need on oskused, mida saab ise juurde õppida või läbi kogemuse omandada.

Omandatud küberturbe alaseid oskusi või teadmisi näitavad vastavad sertifikaadid. On oluline, et kui on tööandjaid, kellele see on märk teadmistest ja oskustest, siis on ka mitmeid tööandjaid, kes ei pea sertifikaate heaks oskuste ja teadmiste peegelduseks - olulisemaks peetakse eelkõige varasemat kogemust.

Küberturbe spetsialisti oskuste ja teadmiste baas tuleb suuresti kogemusest ning seetõttu otsitakse nendele ametikohtadele pigem juba eelneva kogemusega inimesi. Oluline on siinjuures kokkupuude erinevate turvaprobleemidega ja nende lahendamisega, mis annab vajaliku praktika.

> *Sa ei saa logisid analüüsida, kui sa pole näinud, kuidas pahad logid välja näevad või kuidas ründed välja näevad. Et seda ei saa lihtsalt hakata niimoodi tegema. (Küberturbe ettevõte)*

Intervjuudes rõhutatakse ka läbi harjutuste praktiseerimise olulisust ja vajalikkust (st simulatsioonide abil ja küberõppustel küberturbe intsidentide kogemist), mis annab teatava praktika ja võimaluse proovida simuleeritud keskkonnas erinevaid võimalikke lahendusi. See on üks võimalik keskkond, mille kaudu küberturbe probleemide lahendamist kogeda ja praktiseerida.

> *Tähendab on vaja toota inimesi, kellel juba kusagilt tulles oleks mingisugune praktiline [kogemus]. Et see ei pea olema ilmtingimata see, et ta on kusagil juba töötanud, aga et nad on vähemasti mänginud. Blueteamingud, capture tagid, neid on hetkel maailmas tegelikult meeletult olemas. Et lihtsalt lastagi inimesi läbi sellest, et need samad arendajad peavad olema mänginud läbi selle, et kuidas nad ründavat rakendust 60 erineval viisil. (Küberturbe ettevõte)*

4. **Tehniliste küberturbe oskuste kõrval muutuvad üha olulisemaks ka nn üldoskused**

Küberturbe tehniliste oskuste kõrval rõhutatakse ka nö üldiseid oskusi, mis on vajalikud valdkonnas töötamiseks ja erinevate osapooltega info vahetuseks, koostööks. Rõhutatakse, et küberturve ei baseeru

suuremas osas vaid tehnilisele oskusteabele, vaid vaja on ka väga erinevate osapooltega koos töötada, mõtestada lahti nii sisulisi kui tehnilisi küsimusi, selgitada kliendi vajadusi jne. Muuhulgas rõhutatakse järgmisi oskusi: rahvusvaheline suhtlus (sh keelteoskus), kliendisuhtlus, koostööoskused (meeskonnatöö oskused), koostöövõrgustike loomine ja hoidmine, analüüsi oskused.

5. **Järgmise viie aasta perspektiivis toovad tehnoloogilised arengud kaasa uusi funktsioone küberturbe spetsialistidele, millega on vaja kaasas käia ning vastavalt sellele oma oskusi ja teadmisi kohandada.**

Tulevikku vaadates on oluline silmas pidada, kuidas tehnoloogilised muutused mõjutavad küberturbe tagamiseks vajalikke oskusi ja teadmisi. Seoses üha laialdasema pilveteenuste kasutamise mahuga ning andmehalduse teenuste sisseostmisega, muutub vajalikuks **oskus nende teenuste kvaliteeti hinnata**. Sealjuures ei ole oluline sügav tehniline teadmine vaid arusaamine teenuse olemusest, suutlikkus jälgida kes ja kuidas ettevõtte andmeid kolmanda osapoolena kasutab ning oskus hinnata, kas teenusepakkuja rakendatavad turvameetmed on ettevõtte vajadustele piisavad.

Seoses kasvava turvaintsidentide hulgaga muutub olulisemaks ka **turvaintsidentide analüüs ja diagnostika**. Kuigi see ei ole uus kompetents, arvatakse, et see vajadus ajas kasvab, seoses uute ja suuremate turvaintsidentide hulgaga. Mitmel juhul viidatakse, et seni ei ole suuremaid turvaintsidente olnud, kuid suuremate ja keerukamate olukordadega toime tulekuks ei ole piisavalt teadmisi ja seetõttu oleks sel juhul vaja täiendavat abi väljastpoolt.

Uute tehnoloogiliste suundadena, mis mõjutavad oluliselt küberturbe valdkonda, tuuakse välja:

- **Tehisintellekti ja asjade interneti levik** – rakenduste loomisel eeldab turvakomponendi kaasamist algsest programmeerimisest ja arhitektuuri disainist (sh ligipääs tehnoloogiatele, kuidas tehisintellekt klientide andmeid haldab ja jagab jne). Oluliseks muutub see, milliseid andmeid kogutakse, kuidas neid kasutatakse ning kuidas tagatakse nende andmete turvalisus. Vajalikuks muutub väga erinevate seadmete kaitse küberruumis (sh televiisorid, kodumasinad jne). Teiselt muutub oluliseks, et klientidel on oskus hinnata, kas loodud tehisintellekti lahendused on piisavalt turvalised (sh nii tavatarbijate teadlikkus kui ka tehisintellekte kasutavate äriklientide teadlikkus).
- **Biomeetria** – hoogu koguvad identiteedi tuvastamise lahendused näotuvastuse, iirisetuvastuse jms tehnoloogiate abil. Ka selliste tehnoloogiate loomine ja kasutamine eeldab uut tüüpi oskuste ja teadmiste omandamist.
- **Kvantarvutite tekkimine** – viie aasta kontekstis tuleks mõelda kuidas valmistuda kvantarvutite tekkimiseks, kuidas kaitsta süsteeme kvantarvutite vastu. See on tehnoloogiline areng, milleks tuleks valmistuda ja oskusi arendada juba praegu.
- **Krüptograafia arenemine** – olulise kohana tuuakse välja krüptograafia võimekuse arendamist Eestis. See ei ole küll täiesti uus kujunev valdkond vaid eelkõige pidevalt muunduv ja arenev. Oluline on oskus proaktiivselt hinnata kas tänased krüptolahendused on adekvaatsed ka viie aasta perspektiivis ja millised on vajalikud kohandused, et tagada nende süsteemide turvalisus.

2. Küberturvalisuse sektor 2018

2.1. Eesti küberturbe ettevõtete ülevaade

Küberturbe sektori ülevaade tugineb veebi ja telefoni küsitluse raames kogutud andmetel ning nende ettevõtete kohta kogutud Äriregistri andmetel.

1. 2017. aasta seisuga on Eesti küberturvalisuse sektoris 52 ettevõtet, kellest 47 on mikro- või väikettevõtted (ettevõtete jagunemist alavaldkondade vahel vt ptk 1.1.1 eespool). Üle viimaste aastate on ettevõtete arv püsinud selle piiri lähedal, ent peamiselt ühese EMTAK määratluse puudumise tõttu ja ka mikroettevõtete kiire loomise ning kadumisega jäävad täpsed varasemad arvud ebamäärasemaks.
2. 26 ettevõttes ehk pooltes firmadest moodustab küberturvalisusega seotud käive või töötajate arv üle 50% ettevõtte kogukäibest või kõikidest töötajates. Seejuures on madalama küberturbe osakaaluga pigem suurettevõtted.
3. 2017. aastal tegeles ekspordiga 28 ettevõtet (vt Tabel 2). Keskmine aastane küberturvalisusega seotud ekspordimaht oli 566 000€, miljonit ületav maht oli viiel ettevõttel. Küberturvalisuse ettevõtete ekspordi kogumaht 2017. aastal oli 16 miljonit eurot, mis on vähem kui aasta varem (18,8 mln), ent üle aastate tõusev. Perioodi 2016-2017 langust ei tohiks pidada oluliseks muutuseks, kuivõrd 2017. aastal ei ole üksikud ettevõtted oma ekspordi tulusid Äriregistrisse esitanud. Pigem võib eeldada, et küberturbe ekspordi mahud on püsinud stabiilsena.

TABEL 1. IKT JA KÜBERTURVALISUSE SEKTOR

	2012	2013	2014	2015	2016	2017
IKT sektor						
…ettevõtteid	2 917	3 364	3 527	3 896	4 141	*
kasv (%)		15,3%	4,8%	10,4%	6,2%	
…töötajaid	18 776	19 552	20 429	20 938	21 379	
kasv (%)		4,1%	4,4%	2,5%	2,1%	
…müügitulu (tuh €)	3 487	3 638	3 749	3 546	3 712	
kasv (%)		4,3%	3,1%	-5,5%	4,7%	
Küberturvalisuse ettevõtted						
…ettevõtteid	*	*	*	*	*	52
kasv (%)						
…töötajaid	*	*	272	264	367	510
kasv (%)				-3,0%	39,0%	38,9%
…müügitulu (mln €)	*	*	39,6	44,8	55,4	67,1
kasv (%)			3,4%	13,2%	23,7%	21,1%

IKT teave statistikaameti andmetest

**2017. aasta Äriregistri andmeid on korrigeeritud ettevõtjate öeldud küberturbe spetsialistide osakaalu ja näitajatega. 2012-2013 on andmelünkade osakaal küberturvalisusega tegelevates ettevõtetes liiga suur usaldusväärse töötajate arvu hinnangu esitamiseks*

TABEL 2. KÜBERTURBE SEKTORI ETTEVÕTETE EKSPORDI MÜÜGITULU, EURODES

	2012	2013	2014	2015	2016	2017
Eksportinud ettevõtete koguarv	15	19	23	24	30	28
Ekspordi kogumaht (mln €)	6,19	9,45	9,74	12,57	18,89	15,86

Allikas: Äriregistri andmete põhjal uuringu autorite arvutused

4. Kõikide küberturbe sektori ettevõtete vaid küberturvalisusega seotud müügitulu on hinnanguliselt 67 miljonit eurot ja on viimastel aastatel suurenenud 13% - 20% aastas. Keskmine küberturvalisusega seotud müügitulu oli 1,1 mln eurot, olles stabiilselt suurenenud (2013. a 911 000€). Miljonit ületava müügituluga oli 11 ettevõttet. Kõikide ettevõtete mediaantulu on 200 000 eurot.
5. Küberturvalisusega seotud ametikohtade arv on suurenenud ligikaudu samal määral müügituluga. Elutähtsaid teenuseid osutavates ettevõtetes, teistes eraettevõtetes ja avalikus sektoris on 2017. aastal kokku 500 töötajat, kelle igapäevatöö on otseselt seotud küberturvalisusega seotud toodete või teenuste pakkumisega ja haldamisega. Toodud number ei arvesta kaitsetööstusega, mille andmeid uuringu läbiviijatele ei jagatud.

TÖÖTAJATE TAUST JA HARIDUS

Siinne kirjeldus põhineb kokku ligikaudu 150 töötajal, kelle kohta täideti personaliankeet. Teisisõnu tuleb osakaalude tõlgendamisel arvestada, et kui küberturbe sektoris on kokku ligikaudu 1000 töötajat, siis võivad küllaltki madala esindatuse tõttu sektori tegelikud osakaalud alltoodust mõneti erineda.

1. **Tööjõud avalikus ja erasektoris ei erine soo, vanuse ega ametikohtade struktuurilt.**

Nii elutähtsaid teenuseid osutavates ettevõtetes, avalikus sektoris kui eraettevõtetes moodustavad mehed ligikaudu 80% sektori tööjõust. Töötajate demograafia ei erine ka vanuse põhjal – nii meeste kui naiste keskmine vanus on 35 – 37 eluaastat sõltumata töötamisest era- või riigisektoris. Nooremate inimeste seas on levinumad ametinimetused „seirespetsialist“, „konsultant“, „testija“ või „kasutajatugi“. Vanuse tõustes on ametinimetuste varieeruvus suurem, ent teistest mõneti sagedamalt esinevad „audiitor“, „süsteemiadministraator“ ning „tegev- või tootejuht“.

2. **Erinevused elutähtsaid teenuseid osutavate ettevõtete ja muude erasektori ettevõtete töötajate vahel ilmnevad haridustaustas.**

Küsitlusele vastanud erasektori ettevõtetest omasid kõrgharidust 60% töötajatest, kellest omakorda üle poole olid bakalaureusekraadiga. Magistritaseme ja rakendusliku kõrgharidusega osakaal kõikidest erasektori töötajatest on kokku 25%. Samal ajal omasid elutähtsaid teenuseid osutavate ettevõtete personalist kõrgharidust 85% töötajatest, kusjuures nii bakalaureuse- kui magistrikraadiga töötajate osakaal on ligikaudu 35%.

3. **Personali hariduses ei ole ükski konkreetne eriala teistest oluliselt sagedamini esindatud, ühine on vaid IKT tausta suurem sagedus.**

Kõige levinuim haridusasutus küberturbe valdkonna spetsialistide seas on TalTech (va IT kolledž), kust on pärit 25% töötajatest. Teistest sagedasemini tulevad töötajad ka Tartu Ülikoolist (18%) või IT-kolledžist (9%), mõne välismaa ülikooli lõpetanuid on personali seas 3%.

Kui TalTechist omandatud erialad on eranditult IKT seosega (nt tööstuselektroonika, sidetehnoloogia, informaatika, küberkaitse, arvuti- ja süsteemitehnika, telekommunikatsioon), siis näiteks Tartu Ülikoolist on

pärit mitmed õigusteaduse, finantsjuhtimise ajaloo või rahvusvaheliste suhete eriala lõpetanud töötajad. Seejuures ei ole sotsiaal- või humanitaar-haridusega töötajad vaid üldpositsioonidel, vaid ka nende seas on juhtivanalüütikuid, küberturvalisuse valdkonna juht ja infoturbe analüütik.

Kõige levinuimad omandatud erialad informaatika ja IT süsteemide administreerimine, millest viimane seostub eelkõige IT kolledži taustaga. Taltechi küberturbe magistreid on kõikidest töötajates 2%.

4. Töötajate struktuur erineb eelkõige suur- ja mikroettevõtetes.

Väiksemaid ettevõtteid iseloomustab eelkõige üldkompetentsidega töötajate hoidmine. Püsivaid küberturvalisuse tippspetsialiste ja neile suunatud ametikohta saavad lubada vaid kõige suuremad või väga kõrge eriala spetsiifilisuse tasemega ettevõtted.

> *Ja kui sa vaatad laia perspektiivi, et sa pead tekitama tiimid, kus on erinevad kompetentsid hästi esindatud, siis on see ettevõttele kõige kasulikum. See, et sa oled jube kõva infoturbe ekspert, see on tore, aga sellises Eesti väikesel turul on seda päris raske utiliseerida suurettevõtte kontekstis (Küberturbe ettevõte)*

> *Ka sealhulgas arvestades meie meeskonna väiksust, siis peame hästi palju erinevaid teemasid valdama ja kui nüüd on tõesti kuskil vaja hästi sügavuti minna, näiteks biomeetriliste andmetega, siis me kasutamegi tegelikult lihtsalt oma võrgustikku (Küberturbe ettevõte)*

5. Välisspetsialistide toomist Eestisse raskendab tugev konkurents IKT ja küberturbe spetsialistidele kõigis riikides. Barjääre on nii tööandjatele välisspetsialiste värbamiseks kui ka välisspetsialistidele Eestisse kolimiseks.

Täidetud personaliankeetide põhjal on 95% kübervaldkonna püsiva ametikohaga töötajates eesti rahvusest, välismaise taustaga inimesi kaasatakse pigem projektipõhiselt ja suurettevõtetes. Samas on ettevõtjad valmis vajadusel välistööjõu kaasamist kaaluma, seda nähakse kui ühte võimalust suure tööjõuvajaduse leevendamiseks. Selleks on vajalik praktiliste takistuste ületamine, mis on ühised kõigi valdkondade välismaalaste kolimisel Eestisse: keelebarjäär, dokumentide ajamine, perearsti saamine jne. Ettevõtete jaoks on sellise tugisüsteemi loomine välisspetsialistile suhteliselt ressursimahukas ning seetõttu on välisspetsialisti värbamine suurema kuluga võrreldes kohalike spetsialistide värbamisega.

Välismaalastel on Eesti küberturbe valdkonnas raske olla konkurentsivõimeline: Eestis teenuste pakkumisel ning Eesti nõuetest ja seadustest arusaamiseks on vajalik eestikeele oskus. Samas on see iseloomulik ka paljude teiste riikide turgudele ning kohaliku konteksti ja seadusandluse valdamine on vajalik ka teistes riikides teenuseid pakkudes.

> *mis on hästi, hästi praktiline ja mis töötaks selle mõtte poolt, oleks sellest eesti keele oskuse nõudest kuidagi lahtisaamine. Eestis e-teenuseid pakkudes on praktiliselt võimatu palgata inimesi, kes ei räägi eesti keelt. Mitte selle pärast, et meie ei taha siin rääkida, vaid selle pärast, et see, millega ta peab kursis olema on eestikeelne. Seda, mida ta peab ütlema, on eestikeelne. Kogu kliendibaas on eestikeelne. Isegi Eesti kodanikku, kes väga hästi ei räägi eesti keelt, on väga raske palgata (Küberturbe ettevõte)*

Samuti seab Eesti väiksus oma piirangud tegevusmahtudele – väga spetsiifiliste oskustega spetsialistidel ei oleks vaid Eestis tegutsedes võimalik oma oskusi täies mahus realiseerida. Seetõttu on välisspetsialistide kaasamise valmisolek suurem eelkõige eksportivates ettevõtetes, kus on inglisekeelne töökeskkond ja kus välisspetsialistid saavad toetada välisturgudele suunatud tegevusi.

Eraldi piiranguid seab välisspetsialistide päritoluriik. Küberturbe valdkonnas on oluline usaldus ja seetõttu muutub just EL välistest riikidest pärit spetsialistide puhul oluliseks päritoluriik ning küsimus, kas ollakse valmis vastava riigi spetsialistile andma ligipääsu Eesti küberturbe teadmiste baasile. Usalduse ehitamiseks vajavad ettevõtted tuge täiendava taustakontrolli tegemiseks riigi poolt, mis eeldab vastava seadusandliku raamistiku välja töötamist ja rakenduasutuse määramist (vt ka ptk 5 Soovitused).

Välisspetsialistide kaasamine Eesti ettevõtetes ei sõltu vaid tööandjate valmisolekust välisspetsialiste värvata. Vähemalt sama oluline on küsimus, kuivõrd on välisspetsialistid valmis Eestisse tulema. Siin muutuvad jällegi kaalukaks praktilised küsimused (võimalus tuua ka oma pere Eestisse, leida lastele lasteaed ja kool, kasutada inglise keelt kõneleva perearsti teenuseid jne). Samuti on oluline ettevõtte töökultuur ja kui mugavalt välismaalased end selles tunnevad (võimalus olla inglisekeelses töökeskkonnas, töövälised tegevused, võrgustiku loomine jne). Mitmed ettevõtjad on viidanud varasemale kogemusele tuginedes, et välisspetsialistid lahkuvad Eestis pigem kiiresti kui neil ei ole tekkinud siin tugevat sotsiaalvõrgustikku.

Eraldi on püstitatud küsimus, milline on küberturbe valdkonna välistudengite potentsiaal Eesti tööturul. Siinjuures on oluline kuivõrd välistudengite profiil vastab sellele, mida küberturbe ettevõtted vajavad ning milliseid ootusi tööjõu oskustele seavad. Ettevõtted otsivad enamjaolt teatud kogemusega spetsialiste. Välisspetsialistide värbamise puhul muutub sageli oluliseks ka teatud väga spetsiifilise oskuse ja teabe olemasolu, mida Eesti tööjõuturult ei leia. Eestis õppivad küberturbe magistriõppekava välistudengid on aga tihti küllaltki vähese erialase töökogemusega. Üks intervjueeritud välistudeng viitab, et Eestis on välistudengitel pigem keeruline erialast tööd leida. Samuti vaadatakse küberturbe tööjõuturgu globaalsemana ning seetõttu ei piirata tööotsinguid vaid Eestiga.

Välistudengite valmisolekut Eestisse tulla mõjutab ka õppimise hind – Eesti küberturbe õppekava konkureerib teiste küberturbe programmidega Euroopas ja laiemaltki. Välistudengite valikuid mõjutab oluliselt see, kui palju õppimine tema jaoks maksab. Kui õppemaks on võrreldavas suurusjärgus suuremate riikide tasudega, valitakse pigem suuremad riigid, kus vastavalt suurem töö leidmise potentsiaal. Tasuta õppimise võimalust pakub lähiriikidest ka Soome. Seetõttu muutub tudengitele oluliseks stipendiumi saamise võimalus, kuivõrd tasuliste programmidega on rakse konkureerida teiste, suuremate ülikoolide ja riikidega.

2.2. Küberturvalisuse trendid maailmas

Uuringus on kaardistatud küberturbe alased uuringud, mis on ülevaatlikult esitatud Lisas 1 koos viitega uuringu avaldamise ajale ning geograafilisele ulatusele.

Lühidalt uuringu põhijäreldusi kokku võttes võib esile tuua, et küberturbe sektor kasvab üle maailma kiiresti. Prongoositud on küberkuritegevuse kulude kahekordistumist maailmas 2015-2021. aastani kuue triljoni USA dollarini aastas (Cybersecurity Ventures, 2017, lk 3). Samuti kasvavad kogukulutused küberturbe toodetele ja teenustele üle maailma (Morgan, 2017). Küberturbe sektori maht kasvab maailmas ühe hinnangu alusel 8 kordseks aastaks 2023 (P&S Market Research, 2017; Report Buyer, 2017).

Küberturbe sektori käibe suurenemisega kaasneb suurem nõudlus küberturbe spetsialistide järele. Hinnangud tööjõuvajadusele varieeruvad uuringute ja analüüside lõikes kindla ja läbipaistva metoodika

puudumise tõttu. 2015. aastal tehtud prognoosi järgi on selle valdkonna spetsialistide tööjõupuudus 1,8 miljonit aastaks 2022. See on 20% tööjõu kasv võrreldes 2015. aastaga (Frost & Sullivan, 2017, lk 3). 2016. aastal kaheksas riigis üle maailma läbi viidud uuring näitas, et ettevõtete hinnangul jääb neil aastaks 2020 küberturbe spetsialistide töökohtadest 15% täitmata (Center for Strategic and International Studies, 2016, lk 6). 2017. aastal prognoositi aastaks 2022 küberturbe spetsialistide tööjõupuudust Euroopas 350 tuhande inimeseni (Frost & Sullivan, 2017, lk 8). Tööjõupuudus on püsiv ka USAs vaatamata kõrgetele töötasudele võrreldes teiste IKT sektori ametikohtadega (Bedding & de Jongh, 2017, lk 9).

Küberturbe sektori kasvu oluliseks faktoriks nimetatakse:

- tehnoloogia areng ja seadmete suurem ühilduvus, sh murranguline tehnoloogia (nt asjade internet, pilvandmetöötlus) areng (Australian Cyber Security Growth Network, 2017, lk 2; Mets & Leoma, 2016, lk 44; PricewaterhouseCoopers, 2016, lk 9);
- internetipõhise majandusetegevuse ning omavahel ühendatud seadmete ja süsteemide arvu kiire kasv (Australian Cyber Security Growth Network, 2017, lk 7; Libicki, Senty, & Pollak, 2014, lk 5);
- eelkõige andmeid koguvate ja neid jagavate seadmete plahvatuslik kasv (Collins McNicholas, 2016, lk 7)
- küberohtude kasvav sagedus, keerukus (Australian Cyber Security Growth Network, 2017, lk 6–7; Mets & Leoma, 2016, lk 44; PricewaterhouseCoopers, 2016, lk 9; University of Phoenix, 2014, lk 3) ja suurem mõju[11] (Cabaj, Domingos, Kotulski, & Respício, 2018, lk 24).

Andmete mahu suurenemine on üks peamisi faktoreid (Cabaj et al., 2018, lk 24): kui 2013. aastal on andmete maht üle 4,4 zettabaiti[12], siis 2014. aastal prognoositi, et see arv kasvab 2020. aastaks üle 44 zettabaiti, ehk üle 44 triljoni gigabaiti (International Data Corporation, 2014), mis suurendab nõudlust turvalahenduste järele.

Küberkuritegevuse intensiivistumise juures märgitakse küberturbesektori kasvu faktoriks ka kasutaja riskiteadlikkuse kasvu pahatahtlikust kuritegevusest ja vajadusest kaitsa oma andmeid ja IKT süsteeme (Australian Cyber Security Growth Network, 2017, lk 7; Libicki et al., 2014, lk 6; van Lakerveld et al., 2014, lk 112). Küberturvalisuse valdkonna reguleerimine peamiselt strateegiliste dokumentide ning mh andmekaitset puudutavate uute seaduste ja olemasolevate seaduste muudatusettepanekute vastuvõtmisega veelgi kiirendavad küberturbesektori kasvu (Australian Cyber Security Growth Network, 2017, lk 7; PricewaterhouseCoopers, 2016, lk 9; van Lakerveld et al., 2014, lk 112).

Riigid kavandavad ja rakendavad meetmeid, mis aitaksid lahendada tööjõupuudust. Paljud riigid on juba välja töötanud ja avaldanud küberturvalisuse strateegiaid. Euroopa Liidus toimub sellise strateegia väljatöötamine liikmesriikide tasemel, kusjuures kõik need strateegiad on küberturvalisuse hariduse ja koolitamisega seotud meetmete poolest üldiselt sarnased, kuid siiski erinevad detailides ning koostatud tegevusplaanides (Parrish et al., 2018). Praeguse hetkega puudub tööjõuvajadusele ja sellega seotud poliitikameetmetele keskendunud ülevaatlik uuring Euroopa kohta. Tegevused maailma eri riikide strateegiates puudutavad mh õppekavade täiendamist ja atraktiivsuse tõstmist potentsiaalsetele tudengitele, õppimise motivatsiooni tõstmist, seotud valdkondade spetsialiste ümberõppimist ja olemasolevate spetsialiste oskuste täiendamist. Kuid rakendatud

[11] Otsene või kaudne mõju; kaudne mõju on nt organisatsiooni maine kahjustus (van Lakerveld et al., 2014, lk 112).

[12] Zetta on 10^{21}.

meetme mõju ei ole võimalik hinnata, osaliselt selle tõttu, et neid hakati rakendama alles kahe-kolme viimase aasta jooksul, osaliselt vastava info puudumise tõttu inglise keeles.

Tööjõupuudus küberturvalisuse sektoris on üks kolmest peamisest turutõrgetest Ühendkuningriigis, kes on rakendanud erinevaid meetmeid alates riikliku küberturvalisuse strateegia rakendamisest 2011. aastal (Carr & Tanczer, 2018). Ühendkuningriik on püüdnud parandada inimeste oskusi hariduse kaudu kahel viisil: küberturvalisuse teadmiste ja oskuste arendamine alg- ja keskkoolides (õpilased Ühendkuningriigis hakkavad spetsialiseeruma keskkooli lõpus ainult kolmele teemale; tegevuste hulka kuuluvad õpetajatele mõeldud juhendi väljatöötamine, et toetada õpetajaid küberturvalisuse teadmiste ja oskuste kasutamist oma igapäevastes toimingutes, ning tasuta veebipõhistest õppematerjalidest parooli turvalisusest kuni õelvara ja muude küberturvalisuse ohtudeni koosnev akrediteerimisprogramm alg- ja keskhariduse õpetajatele, kes soovivad saada rohkem teadmisi küberturvalisuse ja oskuste levitamise kohta õpilastele) ning suuremaid investeeringuid nõudnud doktoriprogrammide ja teadusuuringute rahastamine, mille toel loodi spetsiaalsed uurimiskeskused ja instituudid, mis töötavad koostöös ettevõtete ja valitsusega (Carr & Tanczer, 2018). 2018. aasta seisuga ei olnud teada, kuivõrd need eespool toodud initsiatiivid koos Ühendkuningriigi digiteerimisstrateegia meetmetega aitavad vähendada tööjõupuudust (Carr & Tanczer, 2018). Eraldi teemadena käsitletakse Ühendkuningriikides jätku- ja kõrghariduse ning soolise tasakaalu rolli küberturvalisuse oskuste arendamises (Department for Digital, Culture, Media and Sport, 2018). Hiljuti on ka Ühendkuningriikides küberturvalisuse sektorit kaardistatud (Pedley, McHenry, Motha, & Shah, 2018).

Soomes on oskuste puudus ja küberturvalisuse spetsialistide järele nõudluse plahvatuslik kasv toonud kaasa arutelud konkreetsete turvaülesannete automatiseerimise kohta masinõppe ja tehisintellekti kaudu (Griffith, 2018). Ühe meetmena on Soome alates 2015. aastast hakkanud pakkuma kõigile ajateenijatele küberturvalisuse koolitust, kes seejärel kasutasid saadud teadmisi ja oskusi oma tööl, kuid osa ajateenijatele pakutakse spetsiaalseid koolitusi, mille tulemusena asuvad need tööle küberturvalisuse sektoris; tänu sellele meetmele tugevdab kaitseväge oma küberturvalisuse pädevust ning parandab küberturvalisuse kompetentsust laiemas tsiviiltöös (Griffith, 2018). Sarnast lähenemist küberturbe kompetentside kasvatamiseks kaitsevaldkonnas kasutab ka Eesti.

Singapur võttis vastu riikliku küberturvalisuse strateegia 2016. aastal[13], mis sätestab riigi visiooni, eesmärke ja prioriteete küberturvalisuse valdkonnas (Ter, 2018). Üheks suunaks on töötada välja küberturvalisuse valdkonna kvalifitseeritud tööjõuga elujõulise ökosüsteemi arendamine, millele eraldatakse oluline osa riigi valitsuse infotehnoloogia eelarvest[14] (Ter, 2018). Vastavalt strateegiale töötatakse välja meetmeid, mis julgustavad olemasolevaid spetsialiste edasi töötama küberturvalisuse valdkonnas ja toetavad nende professionaalset arengut, kehtestatakse selged karjäärivõimalused (sh töötakse välja küberturvalisuse spetsialistide oskuste raamistik), tõstetakse VKEde teadlikkust küberturvalisuse spetsialisti tööst ja nende võimalikust panusest ettevõtete toimimisse, edendatakse sertifitseerimist ja tugevaid praktikakogukondi (ingl *communities of practice*), tehakse koostööd tööstuse ja kõrgkoolidega, et meelitada ligi uusi tudengeid (nt kõrgkoolid ajakohastavad oma õppekavad tööstusharu vajadustele vastavaks ning õppekavade raames omandavad tudengid praktilisi oskusi) ja muuta teiste seotud valdkondade spetsialiste küberturbespetsialistideks, pakutakse küberturvalisuse stipendiume ja sponsorlust paljutõotavate

[13] Cyber Security Agency of Singapore. (2016). Singapore's Cybersecurity Strategy. https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf

[14] 8%, kuid ajaline periood ei ole täpsustatud.

üliõpilaste ligimeetitamiseks ning ümberõppe ja oskuste täiendamise võimalusi täies tööeas olevatele seotud valdkondade spetsialistidele paremate tööalaste väljavaadete paranemiseks küberturvalisuses (Cyber Security Agency of Singapore, 2016). 2018. aastal jõustus strateegia üldplaan[15], kus 2014. aastal käivitatud riiklik küberturvalisuse uurimis- ja arendustööde programm on käsitletud mh küberturvalisuse ekspertteadmiste ja -oskuste arendamise meetmena (Cyber Security Agency of Singapore, 2016; *Singapore's National Cybersecurity Masterplan 2018*, 2018). Singapuri küberturvalisuse valdkonna meetmete mõju analüüs puudub.

Austraalia küberturvalisuse strateegia alusel on loodud küberturvalisuse akadeemilised kvaliteedikeskused (ingl *Academic Centres of Cyber Security Excellence*) kahe ülikooli juures[16], mis hõlbustavad strateegia eesmärkide rakendamist õppeasutuses, valmistades ette töövalmis spetsialiste tööjõu pakkumise suurendamiseks, tehes maailmas liidripositsioonil uurimistööd ning pakkudes rakenduskoolitusprogramme ettevõtetele ja avalikule sektorile (Australian Government, 2017). Vastavalt Austraalia strateegiale on kõrgharidus jätkuvalt oluline küberturvalisuse sektori arenguks, kuid planeeritakse pöörata rohkem tähelepanu algatustele keskkoolides ja n-ö kutsekoolides (ingl *Technical and further education*, ehk TAFE) (Australian Government, 2017). Lisaks eespool mainitud kvaliteedikeskuste asutamisele kuuluvad planeeritud tegevuste hulka mh kehtestada koolitusporgrammid töötavatele inimestele küberturvalisuse teadmiste ja oskuste parandamiseks erinevatel ametikohtade tasanditel, alustades juhtivatest ametikohtadest, ning jätkata keskkoolides teadlikkuse tõstmist küberturvalisuse põhioskuste kohta (Australian Government, 2017).

On välja pakutud, et üheks võimaluseks vähendada tööjõupuudust küberturbe valdkonnas on küberturbeoskuste arendamine elanike seas, julgustades neid alustada õppimist küberturvalisuse erialal, kuid selle oluliseks takistuseks on küberturvalisuse eriala ainete keerulisus ja tehnilisus (Kam, Menard, Ormond, & Katerattanakul, 2018). Naiste ja vähemuste osakaalu suurenemise toetamine on veel üks võimalik vahend spetsialiste puuduse vähendamiseks (Carr & Tanczer, 2018; Nobles & Burrell, 2018), mida teadvustatakse ka Inglismaal (Department for Digital, Culture, Media and Sport, 2018). On leitud, et just naiste varase teadlikkuse tõstmine küberturvalisuse valdkonnast eeskujude, mentori ja pere toel on võtmetegur nende toetamisel karjäärivaliku tegemisel küberturvalisuse valkonna kasuks (Lingelbach, 2018). Üks planeeritud tegevustest Autraalia küberturvalisuse strateegias on mõista, miks on vähe naisi, kes valivad küberturbespetsialisti karjääri, ning tegeleda tuvastatud põhjustega (Australian Government, 2017).

Nagu eespool toodud näited teistest riikides näitab, püütakse lisaks spetsialistide koolitamisele kõrghariduse kaudu tõsta ka inimeste teadlikkust küberturvalisusest, arendada teadmisi ja oskusi juba koolisüsteemis nii õpilaste kui õpetajate seas, et võimalikult vara mõjutada inimeste karjäärivalikuid. Püütakse samuti arendada neid teadmisi ja oskusi horisontaalselt täiskasvanute seas, et tõsta üldist küberturvalisuse kompetsentsi. Teiste riikide praktikate analüüsimisel ilmneb, et meetmeid planeeritakse rakendada erinevate huvirühmade (eelkõige valitsus, õppeasustused, teadusringkonnad, ettevõtted) koostöös. Leitakse, et suurendada küberturvalisuse spetsialistide pakkumust tööturul on võimalik osaliselt ka naiste osakaalu kasvuga. Just need on meetmete raamistik, mille kaudu teiste riikide meetmete mõju analüüsi puudumisel tuleb Eestis otsida lahendusi küberturvalisuse tööjõu puudusele sidusrühmade tihedas koostöös.

[15] Singapore's National Cybersecurity Masterplan 2018. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/NationalCyberSecurityMasterplan%202018.pdf

[16] Academic Centres of Cyber Security Excellence (ACCSE). https://www.education.gov.au/academic-centres-cyber-security-excellence-accse

3. Küberturvalisuse karjääriteed

Uuringus läbi viidud intervjuude põhjal joonistuvad välja karjääriteed küberturbe valdkonnas – need on olulised tegurid, mis mõjutavad küberturbe spetsialistiks saamist. Siin mängivad olulist rolli nii küberturbe alane spetsiifiline haridus, kui ka üldisem IKT haridus ja täiendus- ning ümberõpe. Küberturbe valdkonnas ei ole ühte kindlat viisi valdkonna spetsialistiks saamisel, seetõttu on oluline analüüsida küberturbe karjääriteid kogu selle mitmekesisuses.

Eesti haridusasutustes on küberteemadele keskenduvaid õppekavasid kolm, sealhulgas keskhariduses üks, „Küberkaitse“ Põltsamaa Ühisgümnaasiumis (PÜG), ja kõrghariduses kaks, „Küberturbe tehnoloogiad“ (BA) TalTechis ning „Küberkaitse“ (MA) TalTechi ja Tartu Ülikooli (TÜ) ühisõppekavana. Haridustasemetele omaselt, kui PÜG-i õppekava keskendub ennekõike sellele, et kujundada teadlikke kodanikke ning tekitada huvi edasisteks kõrgharidustaseme õpinguteks, siis ülikoolide õppekavad on sihistatud kübervaldkonnas töötavate ekspertide ettevalmistamisele.

PÜG-i õppekava on suunatud nii teoreetilistele kui praktilistele tulemustele – nii sellele, et õppijad omandaksid baastaseme teadmised sellistel teemadel nagu küberkaitse olemus ja põhimõtted, Eesti küberkaitse korraldus ja IKT regulatsioonid, kui ka sellele, et õppijatel kujuneks suutlikkus tulla toime nii drooni ehitamise kui modelleerimise, nii vastutustundliku interneti kasutamise kui enda ja oma lähedaste kaitsmisega enamlevinud küberrünnakute eest.

Ülikoolide õppekavad on orienteeritud laiapõhjaliste küberteemaliste teadmiste ja oskuste õpetamisele, kusjuures magistritaseme õppekava (küberkaitse) puhul on tudengil võimalik õpingute spetsiifiline fookus ise paika panna. Küberturbe tehnoloogiate (BA) õppekava eesmärk on õpetada välja kübervaldkonna eksperte, kes on võimelised iseseisvalt disainima, rakendama ja haldama turvanõudeid järgivaid IT-süsteeme. Küberkaitse õppekava eesmärk on aga kujundada kübervaldkonna eksperte, kellel on laialdased teadmised ja oskused (sõltuvalt üliõpilase valikust) kas küberkaitse, digitaalse ekspertiisi või krüptograafia valdkonnas.

3.1. Küberturvalisus üldhariduses

KÜBERKAITSE SÜVENDATUD ÕPPIMINE KESKHARIDUSES PÕLTSAMAA ÜHISGÜMNAASIUMI NÄITEL

Kuigi mitmes Eesti üldhariduskoolis leidub küberkaitse valikainena, siis terviklik õppesuund on 2018. aastal valitav vaid Põltsamaa Ühisgümnaasiumis (PÜG), kus igal aastal võetakse kübersuunada vastu paarkümmend õpilast.

1. **Küberkaitse õppesuund valitakse koduläheduse, huvi ja enda konkurentsivõime tõstmise eesmärgil**

Õpilased põhjendavad PÜGi küberkaitse suuna valikut suuresti koduläheduse ga ja vaid üksikud õpilased on pärit kaugematest piirkondadest. Samas tugineb õppesuuna valik ka huvile IT ja küberturvalisuse vastu ning neid oskusi kõrgelt hindavale tööturule. Valikut on õpilaste sõnutsi suunanud ka kübersuunal eelnevalt õppinud sõbrad või vilistlased, kes on kiitnud õppe sisu või innustanud läbi oma karjäärivalikute.

> *IT ja küberkaitse on päris tulevik ja neid töökohti on nii palju, kus saaks tööle ja palk on sellel ka väga hea ning annabki motivatsiooni õppida. (PÜG küberkaitse õppesuuna õpilane)*

Oma eelnevat haridusteed küberturvalisuse vaatenurgast hinnates leiavad gümnasistid, et põhikooli lõpetades olid nende teadmised algelised ja pigem ise omandatud kui koolis käsitletud.

2. Karjäärivalikud küberturbe õppesuunal on laiemad kui vaid kitsalt küberturbe või IT alane haridus.

Eesti Hariduse Infosüsteemi (EHIS) andmetel on PÜGi küberkaitse õppesuuna esimese lennu lõpetanud õpilased jätkanud haridusteed enamasti IKT välistel erialadel: nt ehituserialad, põllumajandus, keeleõpe, muusika ja elektrienergia. 2018. aastal lõpetanutest jätkas vahetult järgneval õppeaastal küberkaitse sarnases õppekavarühmas üks õpilane, kes asus õppima andmebaaside ja võrgu disaini kutsehariduse tasemel. Samas on praeguseni lõpetanud on vaid üks lend. Pooled sellel aastal PÜGi kübersuuna lõpetanutest järgmisel aastal ülikooli või kutsekooli õppima ei läinud, mistõttu ei ole võimalik jälgida ka kõigi kübersuuna lõpetanute edasisi haridusvalikuid. Üheks suuremaks põhjuseks, miks paljud edasise õppimise andmed puuduvad, on kaitseväeteenistusse asumine. Seega võib üks võimalik suund küberkaitse õppesuunalt olla astumine küberajateenistusse, ent seda ei ole võimalik EHISe andmete põhiselt kontrollida.

Gümnaasiumijärgse karjäärivalikuna ei ole mitmete PÜGi abiturientide mõtetes küberturvalisus, vaid pigem tajuvad õpilased küberturvalisust kui kompetentsieelist valdkonnavälise karjäärivaliku puhul. Näiteks nimetatakse võimalike erialavalikutena ärijuhtimist, filmindust, aga ka IT-valdkonda ja/või küberturvalisust spetsiifiliselt. Juhtkonna vaates on niisugune trend küberkaitse õppesuuna eesmärkidega kooskõlas, kuna eesmärgina nähakse küberturvalisuse valdkonnaga lähemalt tutvumist informeerituma karjäärivaliku tegemiseks ja isikliku küberturbe kompetentsi arendamiseks.

> *Meie eesmärk ei ole kasvatada tulevasi küberkaitsjaid, vaid teadlikku kodanikku, kes käitub eetiliselt, teab, et küberhügieen on oluline ja teab üht-teist ka võrgundusest. Muidugi loodame, et ta läheb [edasi õppima], aga samal ajal on tal seda teadmist ükskõik kus vaja. (PÜG esindaja)*

PÜGi küberkaitse õppekava eesmärkide ja lõpetanute tulevikuväljavaadete osas leiavad nii õpilased, õpetajad kui juhtkond, et õppesuuna põhiline tugevus on hea stardiplatvorm küberturvalisuse kompetentsi omandamiseks, mille kasu nii tööturul (olemenata eriala valikust) kui isiklikul tasandil on raske alahinnata. Näiteks nimetatakse kasuteguritena võimalust olla teadlikum netikäituja ja nõustada pereliikmeid.

> *Pole sellist õppesuunda väga mujal, et need, kes lähevad õppima, neil on kindlasti võimalusi. See õppimine tasub end siin ära, kuna oskad ise ka ennast kaitsta ja see areneb kogu aeg ja saab juurde õppida. (PÜGi küberkaitse õppesuuna õpilane)*

Kuigi küberturvalisuse õppesuuna õpilased on üldjoontes rahul, ootavad nad senisest suuremat praktilist rõhuasetust. Näiteks praegusest rohkem võimalusi praktiseerida erialast inglise keelt, rohkem õppekülastusi ja väljasõite ning samuti küberkaitse spetsiifikaga õppeaine õpetamist praegusest suuremas mahus.

3. Üldise õppesuunaga rahulolu taustal on vajadus süsteemse koostöövõrgustiku ja materiaalse toe järgi

Vestlusest õpetajate ja juhtkonnaga jäävad küberkaitse õppekava arendamise ja õpingute läbiviimise peamiste väljakutsetena kõlama **materiaalsete ressursside puudus**, **IT-õpetajate nappus** ning **koostöövõrgustiku loomisega seotud keerukused.** Kogemusele põhinedes selgitavad töötajad, et

küberkaitse õpetamine on kallim kui paljude teiste õppekavas olevate teemade käsitlemine, nõudes nii järjepidevaid investeeringuid tehnoloogiasse kui õppevahendite olemasolu. Samas nimetatud eripäradega koolide rahastamisel ei arvestata, mis muudab keeruliseks õppekavale seatud ootuste täitmise. Samal ajal on kõrgkoolidele küberkaitse jaoks teatavat lisarahastust võimaldatud.

Küberkaitse õppesuuna teostamiseks vajalikke ressursse on PÜGi juhtkond seni kogunud erinevatest allikatest – peamiselt (RIA vahendatud) projektitoetustest, vähemal määral koostööst kohalike ettevõtjatega ning osalemisest rahvusvahelistel valdkondlikel võistlustel. Juhtkond toob esile üksiklahendustel põhineva rahastuse riske ja rõhutab vajadust süsteemse rahastussüsteemi järgi.

Küberturbe õppesuuna tegevuste ja toimimise vastu on kooli esindajate sõnul suur huvi nii rahvusvahelisel tasandil kui kodumaal. PÜGi juhtkond rõõmustab et kõikide institutsioonide esindajad, kellega õppesuuna loomisprotsessis ühendust võeti, on olnud koostööaltid ning üheks peamiseks õnnestumiseks loevad nad tugeva võrgustiku loomist. Võrgustiku koostöö partneritena nimetatakse näiteks RIA, TalTech, Tartu Kutsehariduskeskus, Kaitseliidu küberkaitse üksus, NATO küberkaitsekeskus, HITSA, Eesti Teadusagentuur, Ettevõtluse Arendamise Sihtasutus (e-Estonia Showroom), erinevad koolid ja eraettevõtteid. Ühiselt on õpilastele organiseeritud õppereise ning hangitud õppematerjale (nt droone, lennukeid, ruutereid).

Koostööd valdkonnas olulisemate osapooltega nii riigi- kui erasektoris ning erineva taseme haridusasutustega peavad PÜGi esindajad küberkaitse õppesuuna säilitamise ja arendamise üheks alustalaks. Selle teeb keeruliseks esiteks isikupõhisus: kui kooliga koostööd teinud isik oma ametikohalt või asutusest lahkub, siis on uue kontaktisiku leidmine ja kaasamine osutunud ajamahukaks ülesandeks. Niisugune protsess murendab omakorda võrgustiku toimimist ja lahustab koostöövalmidust erinevate asutuste vahel. Teiseks muudab koostöö keerukaks valdkonnaga tegelevate asutuste paljusus (küberturvalisus jaguneb mitme ministeeriumi haldusala vahel) koos erinevate asutuste nägemuste või tegevusplaanidega. Seetõttu on oluline osapoolte koordineeritud tegutsemine ja ühtsete eesmärkide seadmine.

Riigiasutustes jagatakse PÜGi küberkaitse õppesuuna kohta kiitvaid sõnu. Samuti nähakse küberkaitse õppesuuna kui hea praktika levitamisel potentsiaali ja ühte võimalust kasvava küberturbe kompetentside nõudluse leevendamiseks ja talentide kasvu toetamiseks.

> *Me oleme seal (PÜGis) koostööd teinud. See on väga hea, et ta on väga praktiline ka. Seal ehitavad droone, panevad neid liikuma, üritavad neid krüpteerida, lahti krüpteerida. Seda kõike on väga lai pagas. See ei ole, et tegeleme küberhügieeniga. See on juba oluliselt süvitsi minek. On vaja õpetajaid ja metoodikat.. Aga see on hea näide. Võiks jõuda sinna, et meil on selliseid koole rohkem. Ilmselt igas teises ei saa, aga mõned valitud võiksid seda teha. (Riigiasutus)*

Ka ülikoolid hindavad gümnaasiumitasemel küberturbe oskuste õpetamist, kuid tunnistavad ressursside piiratust vajaliku toe pakkumises gümnaasiumitele nagu PÜG, kus küberkaitse õpetamisega süvenenumalt tegeletakse. Lühikest ja pigem juhuslikku koostööd on aeg-ajalt ette tulnud, aga ülikooli esindaja nendib, et küberturbe kompetentsidega lisaressurss tööjõu näol läheb kohe kasutusse.

> *Gümnaasiumitega meil on natuke keeruline, kuna seal on see koht, kus ei jätku jõudu. Me oleme ise paari gümnaasiumi alt vedanud, kus tullakse [ülikooli] juurde, et teil on inimesed, rääkige midagi ja hoolimata sellest, et nimekiri on pikk, ei saa sellel*

> *konkreetselt päeval või kellaajal keegi minna, punkt. /…/ Siin on jälle, et kust võtta need inimesed. Selle ühe sutsaka me ilmselt leiaks, aga kui me tahame võtta sellist pikaajalist kohustust, siis me peaks terve terve see poolaasta või aasta iga nädal seal käima ja midagi tegema. See läheb juba üldkasulikust tööst välja./…/ Peamine probleem nende sutsakatega on, et inimeste aeg on kallis ja nende aega on väga keeruline ette planeerida niimoodi. (Ülikool)*

4. IT-alase õpetamiskompetentsi leidmine on keeruline

2018/19. õppeaastal on küberkaitse õppesuunal PÜGis vaid üks õpetaja, kellele langeb põhiosa õppekava läbiviimise koormusest ning kes vastutab koolis ka üldisemalt infotehnoloogia valdkonna eest. Ehkki õpetamisse küberkaitse õppesuunal annavad oma panuse ka teised õpetajad, vilistlased ja eksperdid väljastpoolt (põhiliselt läbi õppekäikude ja külalisloengute), on täiendav tööjõud õpetamiskomptenetsi näol PÜGi juhtkonna ja õpetajate sõnul terav puudujääk õppesuuna toetamisel ja arendamisel, kuid täiendavat inimressurssi ei saa kool erinevatel põhjustel endale lubada. Peamiste kitsaskohtadena tuuakse siinkohal välja IT-õpetajate madalat palka (eelkõige väikepiirkondades) ja kvalifitseeritud õpetajate üldist põuda.

> *Kogu aeg peab kursis olema ja spetsialist - kui nüüd tahakski siia eraldi mingi... see ei ole võimalik. Sest kui mitte ainult küber, vaid IT, siis mina küll ei näe, et riik või ministeerium toetaks. Jah, nad töötavad välja digipädevuste mudeli, mida peab teadma. Nüüd saab HITSAst taotleda vahendeid, aga sellest on vähe. IT õpetajale peaks olema ka mingi toetus, et saaksime õpetaja, kes on pädevad. (PÜG esindaja)*

Arvestades IT-sektori kõrget tööjõunõudlust ja üldist palgasurvet, on kohalik omavalitsus ja kool IT-pädevustega õpetajate värbamisel keerulises olukorras. Sobiva inimressursi nappus õppesuuna rakendamisel tähendab lisaks ühele õpetajale langevale liigsuurele koormusele ka riski, et õppekava ei jõuta läbida kavandatud tempos ning õppurid ei saa õpetajalt piisavas mahus individuaalset tähelepanu.

Lahendustena IT-kompetentsiga tööjõu puuduse leevendamiseks peetakse riigi poolset senisest aktiivsemat osalust nii digipädevuse kujundamisel kui IT-õpetaja töötasu katmisel. Seda lähtudes eeldusest, et digipädevus üldhariduses on riiklik prioriteet (vt Gümnaasiumi riiklik õppekava[17]).

5. Õppe kvaliteedi edendamiseks on vajalik nii digi- kui küberturbe kompetentsi tõus õpetajate ja õpilaste hulgas

Küberturbe kompetentside kui digioskuse osa edendamine õpetajate hulgas on väljakutseks. Hoolimata õpetajate positiivsetest hoiakutest digivahendite kasutamisele, hindavad kolmandik neist just oma puudulikke oskusi takistusena digioskuste õpetamisel (Leppik, Haaristo, & Mägi, 2017). Kui internetis suhtlemist nõudvaid oskusi hindavad õpetajad suurepäraseks, siis vajakajäämised ilmnevad probleemilahendusega seotud digioskuste rakendamises ning millegi loomisega (nt veebileht, mäng, rakendus) seotud oskustes. Kuna küberturbe kompetentsid eeldavad heal tasemel digioskusi, siis viimase puudumisel on keerulisem küberturbe oskusi omandada.

[17] Gümnaasiumi riiklik õppekava: https://www.riigiteataja.ee/akt/129082014021?leiaKehtiv

PÜGi õppekava ja õppekorraldus eeldavad, et küberturbe kompetentse kasutatakse ka küberturvalisuse suunaga seotud õppeainetest väljaspool ja **õppekavade üleselt.** Õpetajate hinnangul on komistuskiviks saanud osaliselt see, et õppekava üldosa, kus digikompetentsid kirjas on, ei rakendu süsteemselt. Läbivate teemade ja riikliku õppekava üldosas toodud eesmärkide tulemuslikku ja süsteemsemat rakendamist on käsitletud laiema probleemina (OECD, 2016 ja TALIS[18]). Ka ülikoolide ja riigiasutuste esindajad näevad ettevalmistusel riski küberturvalisusele liialt killustatud lähenemises nii sisuliselt kui kooliastmeti.

> *Minu arust need läbivad teemad ei toimi ikkagi. Meil on ikkagi praegu vanem generatsioon, kes on puhtalt aineõpetajad. Ehk siis me õpetame oma ainet. Aga kui läbiv teema on IKT digipädevusega seotud, siis me oleme väga ainekesksed ikkagi. IKT-oskuste koha pealt niivõrd-kuivõrd üks või teine oskab, siis oskab, aga sellist suurt läbivat teemat, et kõik õpetajad õpetavad, tegelikult tuleb välja, et lõpuks ei õpeta mitte keegi. (PÜG esindaja)*

PÜGi õpetajad toovad välja positiivseid näiteid õpetajate ja õpilaste koostööst küberhügieeni teemal, kus eksperdi rollis on olnud eelkõige õpilased. Õpilase ja õpetaja roll partnerite ja vastutuse jagajatena õppeprotsessis on üldiselt tugevamalt esindatud positiivse hoiaku kui reaalse kaasamistegevuse kaudu õppeprotsessis, mis tähendab, et õpilaste kaasamise potentsiaali digioskustega seotud õppetöö planeerimisel ja korraldamisel ei ole kasutatud (Leppik et al., 2017). Kooli siseselt korraldatakse õpetajatele PÜGis täienduskoolitusi ja igapäevast nõustamist, mille sisuks on erinevate keskkondade kasutamine, mitmeastmeline autentimine, paroolide tugevus jms. Haridusvaldkonna tööandja hinnangul on küberturvalisuse valdkonnas tingitud kiiretest arengutest vaja teadmisi iga-aastaselt uuendada, kuid riiklikult rahastatud küberturvalisuse teemal täienduskoolitusi õpetajatele keeruline leida: HITSA ja TÜ pakutud arvukatest täienduskoolituste nimekirjast ei leidnud ta ühtegi sobivat varianti.

Vaatamata väljakutsetele ja õpilaste arvu langusele PÜGis, on õpetajad ja juhtkond küberkaitse õppesuuna tulevikuväljavaate osas positiivselt meelestatud. Õppekava arendamisel ja tulevikuplaanide realiseerimisel on PÜGi ootus süsteemsele riigipoolsele toele ja koostöövõrgustike senisemast regulaarsemale koostööle. PÜGi juhtkonna sõnul tõestab sagedane huvi küberkaitse õppesuuna tegemiste vastu, et nende tegevuses nähakse potentsiaali ja õppesuuna arendamine aitab kaasa mitte ainult Eesti kui e-riigi kuvandile väliselt, vaid ka sisuliselt.

Mitmed erialased kombinatsioonid võivad olla ka küberturbe valdkonna arengu perspektiivis olulisteks valikuteks (nt elektrienergia, haridus- või tervishoiutehnoloogia, ärijuhtimine või õigusteadus kombineerituna küberturbega võivad anda neid olulisi kompetentse, mida küberturbe valdkond täna vajab). Seetõttu on oluline analüüsida haridusvalikuid ka rohkem süvitsi, vaadates kaugemale ka kitsalt IKT ja küberturbe erialadest.

OOTUSED KÜBERTURVALISUSE KOMPETENTSIDE ARENDAMISEKS ÜLDHARIDUSES

1. **Küberturbe kompetentside arendamine nii individuaalsete küberturbe oskuste kui ühiskonna teadlikkuse tagamiseks peab algama varases eas: lasteaiast ja üldhariduses**

[18] TALIS (OECD Teaching and Learning International Survey) uuringust lähemalt: http://www.oecd.org/education/talis/

Kuna vajadus küberturbe teadlikkuse järele kasvab, siis peavad nii riigiasutuse esindajad, ettevõtjad kui ka valdkonna eksperdid arenguhüppe saavutamiseks ja kasvulava tekitamiseks vajalikuks küberturbe kompetentsi lõimimist üldharidusse ja teadlikkuse tõstmist juba lasteaiast alates. Proaktiivse lähenemisega on seeläbi juba varakult võimalik tegeleda harjumuste kujundamisega. Tähtsaks peetakse nii elementaarsete küberhügieeni-alaste teadmiste omandamist kui ka "küberprillide" laiendamist ehk horisonaalse lähenemise kaudu küberhuvi tekitamist ning säilitamist, unustamata seejuures loomingulist külge.

> *Kõigil on täna vaja elementaarset küberkaitsealast haridust ja arusaamu, siin tulekski algkoolist alustada ja minna vastavalt edasi põhikooli, gümnaasiumisse. /…/ Küberkaitse elementaarsed teadmised, küberhügieen, on valdkond nagu liiklus, nagu liikluses liiklemisoskus või seksuaalharidus, millega tuleks algust teha koolis. /…/ Seitsmeaastastel on nutitelefon peos ja ühes sellega peaks kohe kaasnema elementaarne oskus orienteeruda selles maailmas, mis ongi küberhügieen. (Küberturbe ettevõte)*

> *Päeva lõpuks su suurim risk on see kasutaja, kes on täpselt nii teadlik, kui teadlikuks on ta suudetud ühiskonna ja haridussüsteemi poolt luua. (Küberturbe ettevõte)*

Küberturbe baaskompetentsi omandamist üha varasemas eas on ettevõtjate hinnangul tõenäoline prognoosida ja juba ka märgata. Põhjustena esitatakse nii karjäärivalikute mitmekesistumist, kasvavat vajadust küberturbe kompetentsi järgi igapäevaelus kui ka tarbijate ja tellijatena digilahenduste kasutamist ning turvalisust.

Küberturbe tööjõuturule sisenemine eeldab teatud määral üldhariduse perioodil kujunenud huvi suunamist praktikasse töökogemuse ja/või IT-alase erialavaliku kaudu. Küberturbe alast karjäärivalikut küll tingimata põhikoolis ega gümnaasiumis ei tehta, kuna enamasti ei nähta nii spetsiifilist valikut haridustee jooksul ühelgi hetkel lõppsihina. Noored ei pea vajalikuks küberturvalisuse spetsiifilist haridust, vaid pigem eelistatakse juba varakult laiemaid IT-erialasid, kus küberturvalisus on üks osa paljudest (Koppel, Tammsaar, Solnik, & Jaanits, 2018). Küberturvalisuse eriomaste töökohtade ja karjäärivalikute juurde jõutakse hiljem ja enamasti mitte-erialaste õppekavade kaudu. Samas on just vanus 10 kuni 14 selline, kus kasvab välja sügavam huvi kübermaailma vastu, tekib küberentusiasm, kasvab huvi arvutite, programmeerimise ja häkkimise vastu (Koppel et al., 2018). Seega kujunevad esmased oskused ja hoiakud just üldhariduse omandamise perioodil, mis on olulised nii küberturbe kui karjäärihuvi kasvatamisel. Küberturbe teadlikkuse laiemaks juurutamiseks noorte huvi suunamise kaudu on võtmetähtsusega just noorem ja keskmine kooliiga.

2. **„Küberprillide" teravdamisel ehk küberturbe kompetentside edendamisel on keskne koht lõimitusel ja võrdväärse ligipääsu võimaldamisel**

Küberturvalisuse käsitlemist lõimituna IKT ja teiste valdkondadega peavad eksperdid „küberprillide" teravdamisel ja stereotüüpse kuvandi murdmisel peamiseks eduteguriks.

> *See on nagu edevas autos turvameetmed. Et sa ei räägi ainult oma turvapadjast ja turvavööst, vaid räägid autost tervikuna. Täpselt samuti IT-s, küberkaitse on osa sellest suurest pildist (Küberturbe ettevõte)*

Praktiktilise näitena riiklikult prioriteetse teema kompetentside juurutamisel toovad ettevõtjad riigikaitse valdkonna osana ühiskonnaõpetuse, mille juurutamisega on süstemaatiliselt tegelenud Kaitseministeerium. Protsessi toetamiseks on loodud riigikaitseõpetajate süsteemne koolitus. Kübeturvalisuse eksperdid peavad oluliseks ka küberturvalisuse kompetentsi edendamisel samalaadset praktikat rakendada.

Arvestades, et küberturvalisus on osa laiapõhjalisest riigikaitsest, on üks võimalus kirjeldatud parima praktika põhjal küberturbe oskuste lõimimist piloteerida. **Protsessi alustalaks peavad eksperdid nii era- kui riigisektorist küberturbe kompetentside sisseviimist õpetajahariduse programmi ja õpetamist toetavate kvaliteetsete õppematerjalide (sh digiõppevara) loomist ning arendamist.**

> *Alustada tuleb õpetajatest. Et pakkuda kõigepealt neile koolitust, sest kõik algab koolidest. Lapsed tulevad siis robinal järele (Küberturbe ettevõte)*

Kuna õpetajate ettevalmistust lastele küberturbe oskuste arendamiseks juba varasest east alates peetakse üheks võtmeteguriks, siis peavad eraettevõtete esindajad siin oluliseks ühiskondlikku vastutust ja avaldavad valmisolekut selleteemaliseks koostööks ministeeriumitega (nt HTM ja MKM). Täpsemalt näevad eraettevõtjad oma rolli kogemuste süsteemsel jagamisel ja pikemaajalises partnerluses, püüdes vältida projektipõhist ning lühiajalist lünklikku koostööd. Just pikaajaline perspektiiv ja riigi tasandi valmisolek küberturvalisusega süsteemselt tegeleda on ettevõtete hinnangul nende jaoks peamiseks motivatsiooniks koostööd teha, olles valmis ka märkimisväärseks kulude katmiseks. Mitmed ettevõtted hindavad senist kogemust era- ja riigisektori koostööst pigem demotiveerivaks eelkõige juhusliku iseloomu ja lühiajalisuse tõttu.

Küberturbe kompetentside omandamiseks peavad haridueksperdid oluliseks kübersisuga veebikoolitusi, mis on täna erasektoris levinud täienduskoolituse vorm. Iseõppimist võimaldav atraktiivne digiõppevara võiks hõlmata ka arvutimänge ja videomaterjali. Veebikoolitused ja digiõppevara on aitaks kaasa küberturbe alasele õpp ligipääsuprobleemile. Ligipääs huviharidusele on regionaalselt erinev ja koondunud Tallinna ja Tartu piirkonda, andes seal elavatele noortele eelistatud positsiooni tehnoloogiaalases huvihariduses (Koppel et al., 2018).

> *Kui on võimalik teha online-koolituse raames, siis ütleks, et see võiks eskaleeruda kogu Eesti haridusmaastikule ja laiemalt. Seda kahtlemata tasuks. See koht on minu arvates veel lahti, et kus kohas noorena haridusteel ta peaks selle kätte saama. (Ülikool)*

3. **Valdkondadeülese küberturvalisuse teema eestvedamiseks on vaja eestkõnelejat, kes protsessi juhiks, eesmärke seaks, tegevuskava looks ja koostööd tugevdaks**

Ühe keskse probleemina valdkonna arengus toovad ettevõtjad, eksperdid ja haridusasutuste esindajad kübervaldkonna eestvedamise nõrkust ja eestkõneleja puudumist. Kriitikat kõlab erinevate institutsioonide, sh MKMi, HTMi ja Riigikantselei suunas. Eksperdid tajuvad, et ministeeriumite praegune osa on Eesti digivõimaluste investeerimisse promomine, aga kui valdkonnal puudub süsteemne eestvedamine ja tervikpildi tajumine, siis ei ole edu loota. Küberturvalisuse strateegia loomine ei kompenseeri ametkondliku juhtimise ja eestkõneleja puudumist täidesaatva võimu volitustega, kes strateegiat ellu viiks valdkonda visioneeriks. Koostööd tajutakse pigem individuaalsel kui institutsionaalsel tasandil.

> *Ettevõtete tasemel on koostöö väiksem, küll aga on ekspertide vahel väga suur koostöö. See on community, inimesed tunnevad üksteist, suhtlevad üksteisega, info liigub kiiresti. See on tegelikult üks Eesti arengueeliseid, et see network on nii väike ja inimesed teavad, mis toimub. (Küberturbe ettevõte)*

3.2. Küberturvalisus kõrghariduses

KÜBERTURBE INTEGREERITUS KÕRGHARIDUSE ÕPPEKAVADES

Saamaks ülevaate, millisel määral on küberturvalisus esindatud kõrghariduse õpetamisel laiemalt, viidi töös läbi andmekaeve kõikide Tartu Ülikooli ja TalTechi bakalaureuse- ning magistritaseme õppekavades ning -ainetes. Lõplikusse valikusse jäänud 27 märksõna valiti välja koos projekti kaasatud eksperdiga. Tulemustes eristati esinemist õppekava eesmärkides, õpiväljundites; õppemooduli eesmärkides ja väljundites ning kohustuslikes ainetes ja valikainetes.

1. **Mida spetsiifilisem märksõna, seda vähem ta esineb**

27 märksõnast pooled ei esinenud üheski vormis (mh „autentimine“, „logi“, „lunavara“, „isikusertifikaat“, „teenustõkestus“) ning eelkõige oli tegemist kõrgema spetsiifilisusega tehnilisemate märksõnadega. Kõikide tasemete ja õppekavade peale levinumad märksõnad olid üldisema iseloomuga („digi-“, „infosüsteem“, „e-riik“, ent ka „küber-“).

Teaduskondadest esinevad märksõnad nii bakalaureuse kui magistritasemel ootuspäraselt enim TalTechi infotehnoloogiateaduskonnas - 83 juhtu bakalaureuseõppekavadel ja 189 magistrantuuris. Võrdluseks TÜ loodus- ja täppisteadustes samad arvud 26 ja 14 ning TalTechi inseneriteaduskonnas 95 ja 10. Mitte ühtegi märksõna ei esine TÜ meditsiiniteadustes, kõikides teises kahe ülikooli teaduskondades on vähemalt viis etteantud sõnade esinemisjuhtu.

2. **IKT õppekavadel esineb erinevaid küberturbe sisuga õppeaineid nii kohustuslike kui valikainete seas. Paljude õppeainete puhul ei ole võimalik nimetuse järgi hinnata, kas ja kui palju seal on küberturbe komponenti.**

Näiteks on Tartu Ülikooli IKT õppekavadel järgmised õppeained: andmeturve, andmeturve ja krüptoloogia, infoturve. Kõige rohkem on küberturbega seotud õppeaineid infotehnoloogiliste süsteemide arenduse õppekaval. TalTechi bakalaureuse õppeainete seas on näiteks: küberturbe alused, andmeturve ja krüptoloogia, logimine ja süsteemiseire, arvutivõrkude turvalisus. Küberturbe ained on tugevalt sees IT süsteemide administreerimise õppekaval.

Magistritasemel on IKT õppekavades rohkem küberturbega seotud õppeaineid ning need on magistritaseme õppele omaselt suurema spetsiifilisuse astmega. Näiteks on Tartu Ülikooli IKT õppekavadel: kvantarvuti ja kvantkrüptograafia alused, kvantkrüptograafia, krüptograafia uurimisseminar, krüptoloogia, infoturve, turvalise tarkvaradisaini põhimõtted ja turvalise programmerimise alused. Õppekavadest pakuvad krüptograafia suunalist spetsialiseerumist nt arvutitehnika ja robootika ning informaatika inglisekeelsed õppekavad. TalTechis on õppeainetena nt: küberturbe põhialused ja juhtimine, krüptograafia, krüptograafia eriteemad, küberturbe arhitektuur, turvalise programmeerimise meetodid, turvalise tarkvaradisaini põhimõtted. Paljud küberturbe ained IKT õppekavadel on valikained, mis tähendab, et nende läbimine eeldab ka tudengi poolt motivatsiooni ja nende teemade tähtsustamist enda eriala kontekstis.

Seega on IKT erialadel Tartu Ülikooli ja TalTechi õppekavade näitel erineva spetsiifilisuse astmega küberturbe aineid. Samas ei leidu kõigil õppekavadel läbivalt küberturbe aluspõhimõtetele viitavat ainet, et luua ühtne lähtekoht turvalisuse perspektiivis kõigil õppekavadel. Siinses uuringus ei ole hinnatud , kas ja kuivõrd on sellised üldpõhimõtted integreeritud teistesse õppeainetesse, mis ei ole küberturbe spetsiifilised.

3. Ootus IKT õppekavadele on sihistatud ettevõtete küberturbe valdkonna juhtide koolitamine

Praxise Mõttehommikul osalejad valisid kolme enim vajamineva kompetentsi sekka ettevõtetes küberturvalisuse **valdkonna juhtimise kompetentsid**. Seejuures peegeldus ootus, et juhil on nii sisuline võimekus küberteemades kui ka suutlikkus vahendada suhtlust ettevõte juhi ja otseste andmetöötlejate vahel. Kogutud peronaliankeetide põhjal on valdkonna juhid valdavalt IKT-alase kõrgharidusega. Eeldades sama tausta ligilähedast osakaalu ka tulevikus, on vajalik adresseerida küberturbe juhtide kompetentside tõstmist senisest rohkem IKT kõrghariduse õppekavades. Üks viis selleks on riskijuhtimise ja turvalise programmeerimise õppeainete lisamine kohustuslikena IKT õppekavadesse, millele lisaks tuleb sõnastada vastavasisuline õppekava või -mooduli eesmärk.

Paralleelselt vaid küberturbega tegelevate ettevõtete küberturvalisuse valdkonna juhtide koolitamisele aitab sihistatud teguviis kaasa ka IT juhtide üldisele küberturbe kompetentside tõusule. Näiteks küberturbe tagamine vältimatu abi valdkonnas - väiksemates haiglates ei ole ressurssi, mis võimaldaks turvajuhi ametikoha täitmist ning vastutus küberturvalisuse eest on eelkõige just haigla IT juhil ja meeskonnal. IT juhi jaoks on seega eluline oskus hinnata küberturbe vajadusi enda valdkonnas ning kaasata õigeid koostööpartnereid. Teisisõnu oskus sisuliselt mõista küberturbe probleemi ja selle ulatust, vahendada seda asutuse juhile ning vajadusel kaasata tippspetsialistide tugi.

> *Enda kogemuses, mis ma olen siin viimaste aastatega omandanud, näen, et lihtsam on heale spetsialistidele piisavalt ITd juurde õpetada, kuivõrd IT-inimesest teha head juhti (Riigiasutus)*

> *Järgmine oluline komponent on kindlasti tavaliste IT-laste n-ö harituse osa. Olgu ta süsadmin, kes haldab serverit, olgu ta rakenduste admin, kes haldab rakendusi, haldab serveri peal töötavat veebilehte või andmebaasi või olgu ta programmeerija. Nendel kõikidel õppekavadel peaks olema teatud osa, mis puudutab küberkaitset ja üldse IT-turvet (Küberturbe ettevõte)*

4. Kui praegu esinevad IKT välistel õppekavadel vaid üldisema sisuga küberturvalisuse märksõnad, siis pikaajaliselt tuleb tagada küberturbe baasoskuste andmine ka IKT välistes õppekavades

Suur nõudus IKT oskustega inimeste järele ja IKT spetsialistide üleüldine puudus on Eesti tööjõuturul jätkuv ning mõjutab selgelt küberturbe sektorit. Samas ei saa küberturbe tööjõuvajaduse katmise koormust kõrghariduses asetada ainult juba niigi koormatud IKT valdkonna õppekavadele. Sellega võib süveneda küberturbe kompetentside jätkuv seostamine vaid infotehnoloogia-valdkonnaga, mis stigmatiseerib küberturbe oskuseid kui vaid kindla ringkonna inimestele vajalikuna ning eraldab ja piirab edasist spetsialistide kasvulava.

Praegu esinevad kõrgkoolides loodus- ja täppisteaduse kõrval märksõnad teistest rohkem TÜ sotsiaal- ja TalTechi majandusteaduskonnas, ent seos küberturvalisusega on kaudsem – peaaegu kõik esinemisjuhud on

märksõnadest „digi-“, „infosüsteem“, „andmekaitse“ või „e-riik“. Näited märksõnade esinemisest täppisteaduste välistel õppekavadel:

- TÜ sotsiaalteaduskonna rahvusvahelise õiguse ja inimõiguste ingliskeelse õppekava valikaine: „**Küberruum**, tehnoloogia ja rahvusvaheline õigus“
- TÜ õigusteaduse õpimoodulite väljundites: „omab süsteemset ülevaadet IT-õiguse valdkondadest (sh. elektrooniline side, intellektuaalne omand, privaatsusõigus, andmekaitse, e-kaubandus, **küberkaitse**, **küberkuritegevus** jne.“
- TalTechi majandusteaduskonna avaliku sektori innovatsiooni ja e-valitsemise õppekava õpimooduli eesmärkides: „ajastatakse **infosüsteemide**, andmebaaside ja IT-põhiste innovatsioonide juhtimist avalikus sektoris ja nende osas aset leidnud arenguid“
- TÜ sotsiaalteaduskonna ingliskeelse infotehnoloogiaõiguse õppemooduli väljundites: „omab peamisi tehnilisi teadmisi IT-õiguse valdkonnas kerkivate probleemide lahendamiseks, sobivate meetodite valikuks ning valikute tagajärgede hindamiseks (sh. arusaama informatsiooni infrastruktuurist ja arhitektuurist, programmeerimisest, **infoturbest**, **krüptograafiast**“

Üldistatuna on küberturvalisus IKT-väliselt osaliselt sidustatud sotsiaalvaldkonna ainekursustesse, seda pigem õppekava ühe alaeesmärgina teiste seas („omab ülevaadet küberkuritegevusest“) või üldisemal tasemel ilma tegeliku küberturvalisuse sisuta („arhiividokumentide digitaliseerimine“). Küberturvalisust ei ole õppekava eesmärkide, õpiväljundite või õppeainete nimetuste tasemel integreeritud humanitaar-, loodus- ega meditsiinivaldkonna õppekavadesse ja õppeainetesse. Ehkki märksõnade esinemine ei viita küberturvalisuse või -hügieeni täielikule puudumisele – näiteks patsiendi andmekaitse arstiteaduskonnas – on nende puudumine õpiväljunditest märk teema kui prioriteedi puudumisest.

Mõttehommikul osalenud ettevõtjad tõstavad loodus- ja täppisteaduste välistest õppekavadest esile õigusteadust kui küberturvalisuse lõimingut nõudvat valdkonda, seonduvalt eelkõige küberõiguse valdkonna arendamise ja spetsialistide koolitusega. Intervjuudes kerkis samal ajal küberturbe suurem integreerimine eelkõige arstiteaduskonna õppekavasse. Siiski viitab näiteks meditsiinivaldkonna õppejõud, et nii õppetöö planeerimisel kui ka ainetevahelises lõimingus küberkaitse fookusega ei arvestata. Ka arstiteaduskonna praeguse tudengi sõnul on arusaaam küberturvalisusest meditsiiniõppes kui pigem füüsiline käsitlus andmekaitsest.

> *Arstid on ilmselgelt äärmiselt oluline valdkond, kogu inimeste terviseandmed on äärmiselt sensitiivne informatsioon (Ettevõte)*

> *Ma ütleks, et see pigem kuulub elementaarsusekategooria alla ja kas me nüüd eraldi oleme sellest tudengitele mõne loengu pidanud või residentidele - seda mitte (Meditsiini eriala õppejõud)*

> *Olen nüüd üle kolme ja poole aasta arstiteadust, mul ei tule ette, et meile oleks midagi õpetatud küberturvalisusega seoses. Küll aga on meil seoses erinevate õppeainetega just meditsiinieetika, patsiendikeskne suhtlemine, et kuidas tagada privaatsust, et need andmed, mis ma arvutisse kirjutan, ei läheks kolmandatele isikutele või kolmandad isikud ei näeks seda /…/ et kui patsiendi nimekiri jääb mulle arvutisse ja ise lahkun*

ruumist, siis tegelikult ju andmed jäävad näha ja kes on huvitatud asjast läheb ja klikib sinna nime peale (Meditsiini eriala tudeng)

Otsustuskoht riiklikul tasandil on see, kuivõrd jätkata püramiidi laiendamist selle tipust ning suunata küberturvalisuse tööjõuvajadusele vastamise koormus veelgi enam IKT haridusse. Lisaks vajab kaalumist, millisel määral ja kuidas panustada püramiidi aluste laiendamisele, tagades küberhuvi arendamise varasest east ja laiema spetsialistide baasi, et toetada nii järelkasvu kui talentide ja tippspetsialistide kasvamist. Uueneva tööturu ja rahvastiku muutuste taustal eeldab viimane valik senisest suuremat paindlikkust nii inimestelt kui riigilt. Potentsiaalset lahendust nähakse erinevate valdkondade lõimimsel küberturvalisusega.

> *Kui me räägime tulevikust, siis on vaja ka näiteks juriste, kes räägiksid IKT keelt, humanitaare, kes räägiksid IKT keelt, antropolooge, sotsiolooge, kes suudaks ühiskonnas vaadata …. me natukene reklaamime liiga palju, et see valdkond eeldab, et tuleb ainult kõva reaalteadusi minna õppima (Küberturbe ettevõte)*

KÜBERTURVALISUSE ÕPPEKAVAD TALTECHIS JA TARTU ÜLIKOOLIS

1. **TalTechi küberturbe tehnoloogiate bakalaureuseõppe ja küberkaitse magistriõppekavaladel on 2018. aasta seisuga kokku ligikaudu 230 tudengit, kellest pooled on välismaalased.**

2017. aastal võeti bakalaureuseõppesse vastu 37 ja magistrantuuri 63 üliõpilast. Kõige suurem oli vastuvõtt 2014/15 ja 2015/2016 õppeaastatel, kui magistrantuuri immatrikuleeriti 77 tudengit (Tabel 3). Seda aega meenutatakse keerulisena, kuivõrd õppeks vajalik ressurss ei kasvanud proportsionaalselt. Õppekava esindajate sõnul on 60 õpilase ringis selline õppemaht, mida suudetakse praeguse rahastuse juures tagada. Vastuvõtu kasvatamine eeldab lisaressurssi, et tagada piisava kvaliteediga õpe. Teisisõnu on tekkinud vastuolu riikliku tellimuse ja rahastuse vahel.

> *Kuigi TTÜs on küberturvalisuse õppe magistriprogramm olnud tegelikult vist juba üks esimese Euroopas ja väga pikka aega, siis mahult ei ole siiski sellised, mis seda turgu rahuldaks. (Riigiasutus)*

> *Nüüd suudame (ära õpetada). Tegime kaks aastat, kus võtsime peaaegu 80 tudengit vastu ja see oli raske. Läksime selle numbri peale tänu sellele, et riigi küberjulgeoleku strateegiasse kirjutati sisse, et peame aastaks 2017 jõudma 100 vastuvõtuni aastas. Meie eeldus oli, et riik vastavalt panustab, kui duubeldame vastuvõttu, siis duubeldub ka raha. Seda ei juhtunud sisuliselt. (Ülikool)*

TABEL 3. KÜBERKAITSE MAGISTRIÕPPEKAVA ÜLIÕPILASED (TALTECH)

Küberkaitse magister				
Õppeaasta	Üliõpilasi	Vastuvõetuid	Lõpetanuid	Katkestajaid
2009/10	27	27	0	9
2010/11	57	37	3	13
2011/12	85	42	21	12

2012/13	111	51	17	20
2013/14	133	52	23	28
2014/15	168	77	15	25
2015/16	208	77	36	39
2016/17	204	68	33	35
2017/18	204	63		

Allikas: EHIS

Õpetamiseks vajalik meeskond on üles ehitatud, kombineerides õpinguid TalTech ja Tartu Ülikooli vahel. Üksikute ainete puhul kasutatakse külalisõppejõude. Välismaalaste osakaal sisseastunutest on üle aastate suurenemas, ületades viimasel õppeaastal magistrantuuris kahe kolmandiku piiri. Seejuures ei ole välistudengite puhul ühte teistest selgelt enam levinumat päritolumaad, kümne aasta peale on küberkaitse õppekaval olnud üle 60 erineva kodakondsusega üliõpilase. Samas ei väljendu välistudengite suurenev osakaal küberettevõtete töötajate profiilides, kus töötab valdavalt vaid eesti-päritolu personal (vt pikemalt ptk „Eesti küberturbe ettevõtete ülevaade“).

> *Jämedalt pool lahkub neist välismaale tagasi koos oma teadmistega. Sellest ei ole Eestile konkreetselt mingit tolku (Küberturbe ettevõte)*

Naiste osakaal kõikidest tudengitest on nii eestlaste kui mitte-eestlaste seas üle aastate 20 – 25%.

2. **Küberturbe kõrghariduse õppekava valinud tudeng on sageli juba töötav IT spetsialist, kes soovib oma küberturbe oskusi täiendada.**

Suur osa tudengitest on õppekava esindajate sõnul IT hariduse taustaga, paljud on juba ka IT valdkonna töökogemusega. Põhjused küberturbe õppekava eriala valimiseks on nii töö leidmine kui küberturbe oskuste täiendamine. See annab võimaluse oma senist karjääri IT valdkonnas rohkem küberturbele suunata..

> *Nad on tulnud õppekavale minu hinnangul mitte saama küberturbe spetsialistiks, vaid saama endale küberturbe valdkonnas väga tugeva kõrvalvaate. Nad on spetsialiseerunud IT, kas arenemas IT juhiks või nad on juba IT juhid või IT-peaadministraatorid, nad tahavad aru saada rohkem küberturbest ja seetõttu tulevad /.../ Et oma karjääriteed kuidagi muuta või fokusseerida küberturbele. Pigem tulnud seda juurde õppima (Küberturbe ettevõte)*

> *After working for 2.5 years I just felt a kind of knowledge gap and I just try to go back to school and try to get more knowledge about cybersecurity /.../ most of my classmates are coming for finding a job, finding work here. So, some of them are just searching the Internet and they don't really find cybersecurity related positions (Küberkaitse magistriõppekava tudeng)*

3. **Küberkaitse magistriõppekava iseloomustab kõrge katkestajate määr, mis sarnaneb IKT erialade keskmisele. Samas ei tähenda katkestamine, et ollakse tööle asunud küberturbe ettevõttesse, kus töötavad vaid üksikud õppekava lõpetanud tudengid.**

EHISe andmetel katkestab iga teine küberkaitse õppekaval alustav tudeng õpingud enne lõpetamist, mis on kõrgem kogu kõrghariduse keskmisest näitajast (~40%). Seevastu ka info- ja kommunikatsioonitehnoloogiate õppekavadel katkestavad viimastel aastatel kolmest tudengist kaks. Küberkaitse lõpetanutest ligikaudu pooled läbivad magistrantuuri nominaalajaga, teistel pikeneb õppeaeg tüüpiliselt aasta võrra. Katkestamise põhjused on erinevad, muuhulgas seotud pere ja õppimise, töötamise ühildamisega.

> *Alati tuleb mingeid asju lugeda või kirjutada, sest me näeme, et see tulemuslikkus ei ole meil just väga hea. Kui inimesel on töistööaeg ja täiskooliaeg, siis ta tahab veel hobisid või perekonda, kuskilt peab kärisema. Ja käriseb lõpetamise juures. Praegu alla pooled jõuavad finišisse (Ülikool)*

4. Üliõpilased on küberkaitse õppekavaga üldiselt rahul.

Küberturbe valdkonna üliõpilased on ühisõppekavaga valdavalt rahul - kõrged hinnangud annavad nii üliõpilased kui vilistlased (TalTech, 2018a; Tartu Ülikool, 2018). TalTechi ja TÜ küberkaitse ühisõppekava 2018. a vilistlaste tagasiside põhjal (TalTech, 2018a) on õpiväljundid suuresti saavutatud. Lõpetajad hindavad, et nad on omandanud süsteemse ülevaate valdkonnas rakendatavatest meetoditest (keskmiselt 4,33 punkti 5st), tunnevad oma eriala arengusuundi (4,4), on suutelised omandatud teadmisi ja oskusi rakendama töös juhendaja abiga (4,8) ja iseseisvalt (4,3), oskavad määratleda erialaga seotud probleeme ning analüüsida võimalikke lahendusi (4,1). Järjepidevalt on kerkinud hinnang, et õppeainetes on loengute kõrval piisavalt praktilisi tegevusi tõstes hinnangud 2016. aasta 3,6-lt 3,83-ni (2017.a. oli 3,79).

Ühisõppekava vilistlaste üldine rahulolu oma õppekavaga on kõrgem kui TalTechi kõigi õppekavade keskmine (4,09 *vs.* 3,99). Lõpetanute rahulolu-uuring (TalTech, 2018a) tõid parendusvaldkondadena õppekorralduse paindlikkust (hinnang 3,7) ja praktikakoha leidmist (3,2). Õppekavagrupi 2013.a. hindamisotsuses tõstetakse esile mõlema ülikooli tugevusena koostööd ettevõtete ja ülikoolide vahel.

Kui õpingute sisuga ollakse valdavalt rahul, siis kitsaskohad joonistuvad välja seoses korraldusliku poolega. Vilistlaste hinnangul võiks õppekorralduslik info olla paremini kättesaadav; rahulolu hinnang 2018.a. on 3,98 ning see on aastate lõikes püsinud sarnasel tasemel. Võimalikule infovahetuse probleemile viidati ka õppekavagrupi hindamisotsuses, milles soovitati arendada välja ühtne ja arusaadavalt struktureeritud kommunikatsiooniplatvorm, tagamaks seda, et kahe haridusasutuse vahel jaotatud õpingutele paratamatult omasemate infolünkade teke oleks viidud miinimumini. Täiendavalt soovitati senisest parema koostöö saavutamist ka asutuste siseselt akadeemiliste töötajate ja üliõpilaste, aga ka instituutide ja teaduskondade vahel.

Samas hindavad õppekorraldusliku info kättesaadavust probleemseimaks ka küberturbe tehnoloogiate õppekaval õppivad bakalaureusetaseme üliõpilased (rahulolu info kättesaadavusega 3,41) (TalTech, 2018b). Seega ei seleta infotõrkeid TalTechis mitte ainult õpingute jagunemine mitme asutuse vahele, vaid teisedki tegurid, näiteks tase, millel õpitakse – bakalaureusetudengid on kõrgharidusõpingutes osalenud vähem aega kui magistrandid ning vajavad tõenäoliselt ka teistsugust informeerimist ja nõustamist. Toimiv infosüsteem on hea õppekorralduse aluseks, millele tuleks erilist tähelepanu pöörata kui tegemist on mitme ülikooli ühise ettevõtmisega nagu seda on küberkaitse magistriõppekava.

3.3. Spetsialistide värbamine ja täiendus- ning ümberõppe roll

Küberturbe spetsialistide karjääriteede kujunemisel mängivad olulist rolli ka spetsialistide värbamise praktikad ning täiendus- ja ümberõpe, pakkudes võimalust oskuste täiendamiseks küberturbe spetsialistide seas, aga vajadusel ka teiste valdkondade spetsialistidele küberturbe oskuste andmiseks.

1. **Küberturvalisusele spetsialiseeruvad ettevõtted värbavad töötajaid aastaringselt läbi koolide ja isiklike kontaktide.**

Selline muster toimib nii tudengite värbamisel ülikoolist kui spetsialistide otsimise puhul. Värbamisprotsess on aastaringselt pidev – sobiva kandidaadi leidmisel otsitakse või eraldatakse seejärel rahalised vahendid, mitte vastupidi. Tudengite puhul on iseloomulik, et ettevõtted osalevad õppeasutustes loengute, koolituste või seminaride andmisel, mille lõppedes tehakse valitud üliõpilastele koostööettepanek.

> *Kõigepealt on küsimus, et kust sa neid leiad. Sest tõesti neid ei ole leida ja inimesi võetakse otse ülikooli esimeselt, teiselt kursuselt juba ära (Küberturbe ettevõte)*

Avalike töökuulutuste ja konkurssidega küberkaitse spetsialiste valdavalt ei otsita. Tippspetsialiste on vähe ja küberturbe kogukond hoiab kontakti erinevate võrgustiku ürituste kaudu. Nende võrgustike kaudu toimib sageli ka tööpakkumiste tegemine.

> *Enamik inimesed tulevad ikkagi nii, et me teame kogukonda, selliseid inimesi, keda ma hoiame kogu aeg enda pildis. Et tegelikult nad mingit pidi ikka ringlevad (Elutähtsa teenuse ettevõte)*

Ehkki üleminekud toimuvad erasektorist avalikku ja vastupidi, on staaži tõustes iseloomulik liikumine riigiasutusest erasektorisse, mille peamiseks põhjuseks on kõrgem palgatase. Lisaks töötasule motiveeritakse töötajaid erasektorisse ka tehnilise baasi ja kompetentside laiendamise võimalustega.

> *Mis on ilmselgelt erasektoris omanikud otsustavad, kuidas nad oma raha kulutavad ja nad suudavad tõesti neid väga väärtuslikke inimesi üle kullata, mida riigisektoril ei ole võimalik kahjuks teha. Neil ei ole sellist paindlikust, et seetõttu ma julgen küll öelda, et riigisektoris on suured probleemid inimeste hoidmisega (Küberturbe ettevõte)*

Eriti just erasektoris ja väiksemate ettevõtete juures ei ole tööandjatele värbamisel määrav kindlalt suunitletud küberkaitse alased teadmised ning -haridus, vaid laiemaid infotehnoloogiaalased põhiteadmised ning pidev valmidus täiendõppeks. Viimane toimub ametikohale vastavalt töö spetsiifikast lähtudes. Formaalhariduse nõue võib pigem esineda avalikus sektoris. Üks võimalik viide potentsiaalse kandidaadi oskustest ja teadmistest on erinevate sertifikaatide omamine. Siiski näitavad intervjuud, et sertifikaatide tähtsustamine on erinev – on tööandjaid, kes päevas seda heaks indikaatoriks, kuid on ka neid, kes sertifikaatide põhjal oskuste ja teadmiste kohta otsuseid ei tee.

2. **Täiendkoolitustel on oluline osa küberturbe spetsialistide oskuste ja teadmiste kujunemisel.**

Koolitusi on laias laastus võimaliks liigitada kolmeks: koolitused tavakasutajale (küberhügieeni tase), koolitused IT spetsialistile ja nö spetsialisti koolitused (sageli toote- või teenusespetsiifilised koolitused).

Erinevatest teemadest, millel oma töötajaid koolitatakse on välja toodud näiteks: monitooring (ründaja ülesleidmine), logid ja logianalüüs; intsidentidele reageerimine, süsteemikaitse, *hands on hacking*; programmeerijatele turvaline programmeerimine; veebirakenduste turvalisus; võrguturbekoolitus, aga ka spetsiifilise tark- või riistvara koolitused. Vajadust nähakse ka laiema küberkaitse kursuse järele kui seda on praegu pakutud (hetkel pigem liidritele/ juhtidele). Palju viidatakse ka üldisemale küberturbealase teadlikkuse tõstmise koolitustele, sh ilma IT taustata inimestele.

Ühe eraldi teemana koolituste juures tuuakse välja osalemine küberõppustel. Kuigi maailma mastaabis olulistel õppustel osalemine on piiritletud väga kindlale seltskonnale (NATO *Locked Shields*), siis nähakse vajadust täiendavate küberõppuste järele, mis kaasaks rohkem ja suuremat ringi Eesti spetsialiste, sealhulgas ka elutähtsaid teenuseid pakkuvaid valdkondi.

> *Need [küberõppused] on väga, väga olulised selles mõttes, et nendel on need samad kaks aspekti – üks on see sama spetsialisti koolitamise vaade, suhteliselt hindamatu. Aga teine asi on ka see, mida tegelikult riik peaks edasi tegema, on edasi liikuma nende harjutustega ja võib-olla tegema neid valdkonna kaupa rohkem. Sest tegelikult selline Locked Shields, aga mitte militaar meeskondadele, vaid Eesti finantsasutuste meeskondades oleks tegelikult hindamatu väärtusega. (Küberturbe ettevõte)*

Koolituse viisidest on oluline ise õppimine/ ise lugemine, ettevõtte sisesed koolitused, konverentsid, võrgustiku üritused. Konverentsid annavad võimaluse nö viimaste trendidega kursis olemiseks. Koolituse teemasid lastakse sageli ettevõtetes inimestel ise valida, teatud eelarve piires (lisaks nö „kohustuslikele“ koolitustele).

Koolitusi peetakse üldiselt küllalt hästi kättesaadavateks. Samas on sageli huvi väga spetsiifiliste koolituste järele, mida Eestis ei pakuta, sest suunatud väga kitsale nišile. Seetõttu on oluline ka rahvusvaheline koolitusturg (sageli ka online kursused). Olulisem on aru saada, mis on koolitusvajadus ning uute trendide jälgimine

4. Küberturvalisuse tööjõuvajadus ja -prognoos

TÖÖJÕUVAJADUS ON TUGEVALT SEOTUD IKT SEKTORI VAJADUSTE JA STRUKTUURIGA

1. **Era- ja avaliku sektori peale kokku on tänane tööjõuvajadus hinnanguliselt 220 – 360 inimest, suurem puudus on laiemaid küberturvalisuse kompetentse nõudvatel ametikohtadel ja vähem vajatakse süvateadmisega tippspetsialiste.**

Tööjõuvajadus täpne sisu erineb sõltuvalt asutuse suurusest ning tegevusvaldkonnast. Paljusid väiksemaid kui viie töötajaga erasektori ettevõtteid iseloomustab, et süvaoskuseid nõudvate erialaste tööde puhul kasutatakse pigem kontakte oma võrgustikust ja otsest tööjõuvajadust mõne kindla kompetentsi järgi ei ole.

Suuremates ettevõtetes tuuakse teistest enam välja vajadust organisatsiooni küberturvalisuse valdkonna juhi, juristi või audiitori, krüptograafi ning süsteemiarhitekti järgi.

Elutähtsat teenust osutavate ettevõtete ja riigiasutuste puhul on eelkõige vajadus infoturbe valdkonnajuhtide järgi. Seejuures eeldatakse mitte süvateadmisi, aga piisavat IKT ja kübertuvalisuse tehnilist kompetensti arusaamaks organisatsiooni infoturbe sisulist ülesehitust, nõrkuste ja tulevaste nõrkuste paiknemist ning nende selget edastamist tehnilistele ekspertidele. Teisisõnu on vaja valdkonnas sisuteadlikke juhte, kes ei ole küll „*hands on* tegijad“, ent omavad sisulisi kompetentse nii viimastega kahepoolseks suhtemiseks kui samaaegset võimekust valdkonna eestvedamiseks.

Mõttehommikul osalejad on välja toonud, et **kõige suurem on vajadus küberjulgeoleku riskide analüüsi ja juhtimise kompetentside järele, sellele järgnevad küberturbe õpetajad erinevatel haridustasemetel ning küberturbe valdkonna juhid.**

> *„Üks probleem, mis täna on, on kindlasti juht .. et leida juhte valdkondadele, kes saaksid aru nii valdkonnast endast kui ka küberist kui ka ITst /…/ Väga suur osa (tänastest juhtidest) oskavad hooldada mingisuguses väga selges raamitud keskkonnas oma asju, nad isegi ei mõtle, et meil ei ole täna mitte midagi, aga homme võiks olla e-maksuamet .. kastist välja mõtlemist on suhteliselt vähe. (Riigiasutus)*

Küberturbe koolitajate ja õppejõudude puudus on oluline faktor, mis piirab küberturbe õppemahtude laiendamist, küberturbe alase õppe laiendamist teistele IT õppekavadele kui ka IT välistele õppekavadele, samuti küberturbe alase õppe / huvihariduse pakkumist gümnaasiumi tasemel. Sageli panustavad küberturbe valdkonna õpetamisse valdkonnas töötavad spetsialistid, kuid ka nende aeg ja võimalused käia aineid lugemas on sageli piiratud.

Ka süsteemiarhitektide vajadus kasvab seoses sellega, et erasektori nõudlus turvaliste infosüsteemide järele kasvab – ettevõtted investeerivad aina enam uutesse infosüsteemidesse ning kasvab teadlikkus nende investeeringute kaitsmise vajadusest. Ühtlasi on süsteemiarhitektide vajadus vanade süsteemide uuendamisel/ välja vahetamisel, seda ka avalikus sektoris, kus süsteemid on aegumas ning vajavad turvalisuse uuendusi.

Samaaegselt ettevõtete ja riigiasutustega on küberturvalisuse kompetentside puudus õpetajate seas, mis taandub laiemate digipädevuste puudumise taha[19]. Küberturvalisuse raamistikus on seejuures tegemist üheaegselt nii tööjõu puudusega (puudu on peamiselt haridustehnoloogid ja informaatikaõpetajad), kuivõrd juba olemasoleva töötajaskonna puuduliku küberhügieeni tasemega. Mõttehommikul osalenud ekspertide sõnul on võimalikud lahendused pigem pikaajalised - esmane meede oleks küberturvalisusega seotud kompetentside lisamine õpetajakoolitusse, et tagada uue õpetajaskonna kõrgem baasoskuste tase. Alternatiivsena on kiirem ja koolitasandil toimuv lahendus õpilaste kaasamine tundide läbiviimisse, mida on juba piloteeritud mitmetes üldhariduskoolides.

2. **Kõige lähematel aastatel mõjutab töötajate vajadust peamiselt valdkonna üldine kasv, mitte demograafilised muutused ega inimeste lahkumine kübersektorist.**

Küberturvalisuse kompetentsidega töötajaskond pigem noor või parimas tööeas ja suuremat pensionile siirdumist või suremust oodata ei ole. Küberturvalisuse spetsiifikaga ettevõttest lahkutakse mõnda teise (pigem erasektori) küberettevõttesse või välismaale. Vanuselist erinevust avaliku ning erasektori töötajate struktuuris ei ole ja mõlemal juhul on tööjõu asendusnõudlus madal.

3. **IKT alamsektoritest sarnaneb küberturvalisus tööjõu- ja palgastruktuuri poolest enim IKT hulgimüügi ja andmetöötlus-veebihostinguga.**

Kõrgem tööjõuelastus väljendab suuremat tööjõumahukust, mis käib kaasas näiteks IKT-ga seotud tootmises. Seevastu küberturvalisuse sektori madal käibeelastus (0,42) viitab eelkõige kapitalimahukusele, mis on iseloomulikum ka IKT teenindavale sektorile ja andmetöötlusele. Küberturvalisuse kontekstis väljendab madal käibeelastus pigem investeeringuid tarkvarasse, serveritesse jms.

Palgaelastus väljendab inimeste ja kapitali asendatavust – mida suurem (absoluutväärtuselt) on palgaelastus, seda lihtsamini on inimtööjõud ja kapital asendatavad. Küberturvalisuse elastuskoefitsient 0,07 viitab nende omavahelisele madalale asendusmäärale.

TABEL 4. KÄIBE- JA PALGAELASTSUSED KÜBERTURVALISUSE JA IKT SEKTORIS

		Küber-turvalisus	IKT kokku	IKT teenindus	IKT hulgimüük	Tarkvara-arendus	Andme-töötlus
Log(M)	Käibeelastus	**0,42**	0,62	0,51	0,34	0,62	0,42
		(0,04)	(0,02)	(0,02)	(0,04)	(0,03)	(0,05)
Log(PKTK)	Palgaelastus	**0,07**	-0.09	-0,05	0,06	-0,12	-0,03
		(0,05)	(0,02)	(0,02)	(0,06)	(0,03)	(0,07)
Konstant		**-4,3**	-4.5	-4,4	-3,7	-5,0	-5,0

**IKT hinnangud Praxise 2014. aasta uuringu põhjal*

4. **Lähimal viiel aastal on juurde vaja hinnanguliselt 270 – 870 küberturvalisuse kompetentsiga töötajat**.

[19] Jürgenson, A., Mägi, E., Pihor, K., Batueva, V., Rozeik, H., Arukaevu, R. (2013). Eesti IKT kompetentsidega tööjõu hetkeseisu ja vajaduse kaardistamine. Tallinn: Poliitikauuringute Keskus Praxis.

Vajaduse all mõistetakse mitte 270 – 870 erialast uut traditsioonilise küberturvalisuse ametikohta lisandumist, vaid eelkõige küberturvalisuse kompetentsiga inimesest, nagu on defineeritud peatükis 1.1. Tööjõuvajaduse hinnang sisaldab nii era- kui riigisektori töötajaid ja elutähtsate teenuste pakkumisega seotud ettevõtete personali. Siinses töös prognoositi viis stsenaariumi, mille nullaastaks on 2017 ehk viimane täisaasta, mille kohta on ettevõtetel uuringu teostamise hetkel esitatud majandusaasta andmed:

1) Baasprognoos - viimaste aastate müügimahu ja töötajate arvu kasvu jätk, kus struktuurseid arengumuutuseid ei toimu.
2) Ettevõtjate arvamus – ettevõtete ja avalike asutuste hinnatud uute töötajate nõudlus praegu ning lähiaastatel (10%/a).
3) Iduettevõtete kasv – kahe praeguse või loodava mikro-/iduettevõtte hüppeline kasv keskmise suurusega ettevõtteks
4) Konservatiivne hinnang – küberturvalisuse kompetentsiga inimeste madal ja lineaarne kasvuvajadus, mida täidavad väliskompetentsid.
5) IKT sektor – küberturvalisuse sektori praegused müügi – ning töötajate näitajate suurenemine 2014. aastal hinnatud IKT sektori elastsusega.

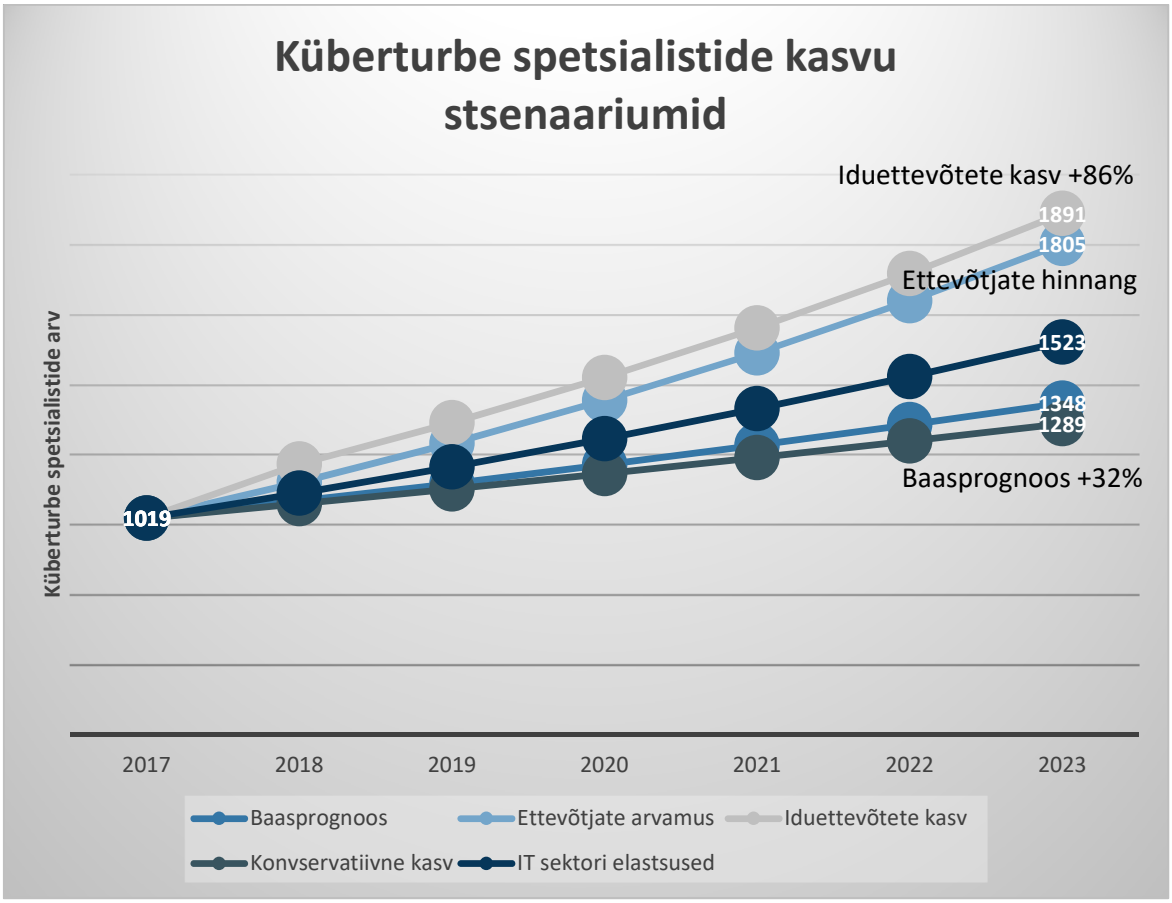
Baasstsenaarium näeb iga aasta ette ligikaudu 55 uue küberturbe kompetentsidega töötaja vajadust ehk aastaks 2023 on praeguste trendide jätkudes vaja kokku 330 selliste oskustega inimest. Tööjõu vajadus on kõige suurem, kui realiseerub stsenaarium „iduettevõtete kasv“, mis ennustab mitme praeguse mikroettevõtte kiiret laienemist prognoosiperioodi jooksul. Sellises variandis on era- ja avalikus sektoris viie aasta pärast kokku vaja 870 uut küberturvalisuse kompetentsiga töötajat.

TABEL 5. TÖÖJÕUVAJADUSE PROGNOOSID

	2018	2019	2020	2021	2022	2023
Baasprognoos	49	99	153	209	267	329
Ettevõtjate arvamus	102	214	337	473	622	786
Iduettevõtete kasv	155	273	402	544	700	872
Konvservatiivne kasv	41	83	127	173	221	270
IT sektori elastsused	71	146	227	313	405	504

Märkus - numbrid näitavad tööjõuvajadust võrreldes 2017 aastaga

JOONIS 2. TÖÖJÕUVAJADUSE KASVU STSENAARIUMID



TÖÖJÕUVAJADUSE KESKMES ON KÜBERTURBE KOMPETENTSIDE ANDMINE IKT VÄLISELE TÖÖJÕULE

5. **Küberspetsiifikaga üliõpilaste või tippspetsialistide osa tööjõuvajadusele vastamisel on väike, ent mitte puuduv. Küberkaitse magistri ühisõppekava täidab oma eesmärki kompetentside täiendamisel ja andmisel, mitte tööturule valmisspetsialistide pakkumisel.**

Koos äsjaavatud TalTechi küberturbe tehnoloogiate bakalaureusekavaga astub praeguste mahtude juures igal aastal küberturvalisuse õppekavadele 100 õpilast. Õppekavade aastane lõpetajate arv on 50, kellest hinnanguliselt pooled on välismaalased, kes omakorda praeguste trendidega Eesti küberettevõtetesse tööle ei asu.

> *Kuigi TTÜs on küberturvalisuse õppe magistriprogramm olnud tegelikult vist juba üks esimese Euroopas ja väga pikka aega. Siis mahult ei ole siiski sellised, mis seda turgu rahuldaks. (Riigiasutus)*

6. **Uutele küberturvalisuse kompetentsidele vastavad ehk tööjõuvajadust on senini täitnud eelkõige IKT tausta ja haridusega inimesed (töise) juurdeõppe ning täiendkoolitustega. Küberspetsiifikaga üliõpilaste või tippspetsialistide osa juurdekasvus on jäänud marginaalseks.**

Kõrghariduses võetakse kõigi riiklike IKT õppekavade peale lähiaastatel iga-aastaselt vastu ligikaudu 1200-1400 tudengit. IKTs vastukaaluks kogu kõrghariduse trendile on suurenenud ka bakalaureuse tasemel vastuvõtt. Näiteks TÜ arvutiteaduste instituudis on võrreldes 2013. aastaga suurenenud nii sisseasutunud eesti kui välismaise taustaga tudengite arv, seejuures on viimaste osakaal tõusnud 8 protsendipunkti võrra. Samas ei ole trend IKT õppekavade tudengite arvu suurenemisele demograafia põhjal kestev kümne või enama aasta perspektiivis kestlik.

Kui praegustes küberturvalisuse ettevõtetes on ligikaudu 80% personalist IKT haridustaustaga, siis küberkaitse magistrikava lõpetanuid on personaliankeetide osakaalude põhjal samades ettevõtetes või asutustes terves kübersektoris 20 – 30 inimest.

> *enda kogemuses, mis ma olen siin viimaste aastatega nagu omandanud, siis ma näen, et lihtsam on heale spetsialistidele nagu piisavalt ITd juurde õpetada, kuivõrd IT-inimesest teha head juhti (Riigiasutus)*

7. Suurim tulevikupotentsiaal tööjõuvajaduse lahendamises on väljaspool IT erialadel õppivate inimeste küberturvalisuse baaskompetentside omandamisel, mille esimeseks sammuks on küberturvalisuse kompetentsi viimine õpetajakoolitusse

Mida erialasemaks muutub ametikoht, seda enam eeldatakse lisaks IKT baasoskuste olemasolule küberturvalisuse valdkonna kogemust. Samas on uuringus täidetud personaliankeetide põhjal nii avalikus- kui erasektoris ligikaudu kuuendik küberturvalisuse kompetentse nõudvatest ametistest infotehnoloogia välise taustaga inimesed. Seejuures ei saa üldistusi teha vanuse, soo ega ametikoha põhiselt – IKT hariduseta töötajaid on nii juristi, infoturbe spetsialisti kui juhtivanalüütiku ülesannetes.

> *tegelikult see ampluaa meie ettevõtte töötajatest on väga-väga lai. Ja ütleme, et need, kes meil on projektijuhid ja valdkonnajuhid ja müügiinimesed, need ei pruugi olla üldse tehnilise taustaga inimesed, nad võivad olla tehnilise taustaga, aga mitte IT-ga /…/ küll aga kui sa oled programmeerija, siis 95% inimestest või 99% inimestest on meil ikkagi, või arendaja või arhitekt, on ikkagi IT lõpetanud. Analüütikud ka (Küberturbe ettevõte)*

IKT-väliste inimeste infoturbe kompetentside omandamine on keskseks võimaluseks tööjõuvajadusele vastamiseks. Selleni jõuavad nii riigiasutused, elutähtsate teenuste osutajad kui erineva suurusega eraettevõtted.

> *Täna on ikkagi nii, et ma pigem siis koolitan kohapeal juurde neid vajalikke küberoskusi .. küberturbeoskuste puudumine ei ole veel olnud takistuseks ühelegi ametikohale astumiseks (Küberturbe ettevõte)*

5. Soovitused

Küberturbe spetsialistide vajadus on pidevas kasvutrendis, seda nii küberturbe ettevõtetes kui ka elutähtsaid teenuseid pakkuvates ettevõtetes ja küberturbe laienemisega teistesse tegevusvaldkondadesse. Uuringu põhjal on esile tõstetud neli võtmevaldkonda, mis toetavad küberturbe spetsialistide järelkasvu:

1) IKT hariduseta täiskasvanute kaasamine küberturbe valdkonda (täiend- ja ümberõpe)
2) noorte küberturbe kompetentside arendamine
3) IT spetsialistide küberturbe kompetentside arendamine,
4) küberturbe talendipoliitika (koduste talentide hoidmine ja välisspetsialistide kaasamine).

Need neli võtmeteemat on poliitikavaldkondade ülesed, eeldades koordineeritud koostööd ja väljapaistvat eestkõnelejat nii protsessi juhtimisel, eesmärkide seadmisel kui tegevuskava loomes. Vajadust tervikliku juhtimise ja sidusa kogukonna kujundamise järgi on on esile toodud ka kehtivas küberturvalisuse strateegias[20]. Alljärgnevalt on igas võtmeteemas uuringu tulemuste põhjal valitud üks prioriteetne tegevus, mille rakendamist arutati valdkonna poliitikakujundajate, ekspertide ja ettevõtjatega Praxise Mõttehommikul.

I IKT hariduseta inimeste kaasamine küberturbe valdkonda

Miks on oluline? Küberturbesse jõutakse seni peamiselt IKT valdkonnast, kus spetsialistidest on juba praegu suur puudus. Tööjõuvajadusele vastamiseks on kriitiline kaasata järjest enam ilma IKT hariduseta inimesi, et laiendada küberpüramiidi aluseid ja tekitada lisaalternatiive IKT sektori koormamisele.

Prioriteetne tegevus: küberturbe karjäärivisioonide avardamine. Küberturbe valdkonnal on oht mõjuda nii IKT välistele kui ka seal juba tegutsevatele inimestele kinnise ning omaette seisva valdkonnana. Sisuliselt on tekkinud mulje suletud keskkonnast, kuhu teised oskused ei sobitu ning loodud seeläbi ka sisenemisbärjäär – teise taustaga inimesi valdavalt ei otsita ja samaaegselt ei soovita valdkonda IKT-formaalharidust omamata ka siseneda. Vajalik on väärtusloome ja teadlikkuse kasvatamine infoturbest ning selle tarvilikkusest laiemalt.

Selle rakendamist saavad toetada järgmised osapooled:

- **Ettevõtete** jagatud positiivne kogemus IKT hariduseta inimeste kaasamisel küberturbesse - tingituna nii tööjõupuudusest valdkonnas kui ka eesmärgipärasest meeskonna mitmekesistamisest - mõjub julgustavalt ka teistele ettevõtjatele ning suunab neid potentsiaalselt kaaluma teistsugust värbamismustrit. Algatus selleks peab tulema ettevõtjatelt, ent sõnumit saavad võimendada nii riik kui ülikoolid, kaasates ettevõtjaid riigi korraldatud sihtotstarbelistele seminaridele või toetades ettevõtjate suuremat kaasatust õppetöösse.
- **Kaitseministeeriumi** vedamisel on loodud toimiv küberajateenistuse süsteem koostöös formaalharidusega. Teisalt on üks soodustav mõjur küberturvalisusesse jõudmiseks varasem huvi riigikaitse vastu. Kui praegu on riigikaitsekursused valikainena järjest enam levimas gümnaasiumi tasemel, siis selle pakkumine ka **põhikoolides** võimaldaks potentsiaalselt suurendada tulevikus küberajateenistusse jõudvate noorte hulka.

[20] Küberturvalisuse strateegia 2019-2020. https://www.mkm.ee/sites/default/files/kuberturvalisuse_strateegia_2019-2022.pdf

- Kuigi küberturvalisuse alase koolitamise oluliseks takistuseks on peetud teema keerulisust ja tehnilisust, siis nutika **õppekavaarenduse kaudu on võimalik ülikoolidel ja kutsekoolidel** õppekavadesse tuua (valikulised) ainekursused, nt riskijuhtimine või turvaline programmeerimine. Need võimaldavad eelneva tugeva tehnilise baasita inimestele anda vastavasisulist kompetentsi, et nad huvi ja motivatsiooni korral saaksid kaaluda ja täita tehnoloogilisest kompetentsist arusaaja ülesandeid sisaldavat küberspetsialisti ametikohta.
- Pikaajaliselt on **ülikoolide õppekavaarendajate** jaoks kriitiline, kuidas lisada küberturbe komponent ülikoolide õpetajahariduse programmi, kus oleks teiste seas hõlmatud elementaarsed digipädevused (mh info kriitiline hindamine, digiõppevara kasutamine) ja (küber-)riskijuhtimine. Õpetajate küberturbe oskuste täiendamist saab suunata täienduskoolituste kaudu.
- **HTMi, MKMi ja Kaitseministeeriumi ning koolide ja ettevõtete** koostöös peaks olema loodud võimalused omandada esmaseid küberturbe alaseid baasteadmisi **ise õppides** atraktiivsete materjalide kaudu, nt videoloengud või arvutimängud huvilistele. Sarnaselt teistele valdkondadele peaks küberturbes koolituste ja iseõppimisega omandatud teadmisi olla võimalik sertifitseerida.

II Noorte küberturbe kompetentside arengu toetamine haridustasemeid läbivalt

Miks on oluline? Praegu toimub küberturbe kompetentside omandamine pigem formaalhariduse väliselt ja huvihariduse või iseseisva huvi kaudu (Koppel et al., 2018) ning noorte laiem teadlikkus ja motivatsioon küberturbe oskuste arendamiseks on pigem vähene või juhuslik. Selleks, et edendada küberturbe teadlikkust noorte seas, on tarvis süsteemsemalt erinevate osapoolte kaudu küberturbe huvilised radarile saada juba võimalikult noores eas. Lisaks on oluline järjepidev toetus küberturvalisuse kompetentsi arendamiseks erinevas eas ja tasemel.

Prioriteetne tegevus: „Küberprillide“ laiendamine läbi võimalikult varajase küberturbe huvi märkamise, toetamise ja suunamise ning teisalt teadlikkuse tõstmine märkajate, toetajate ja suunajate seas. Täiendavalt “küberprillide” teravdamine, et lõhkuda küberturvalisusele omistatud militaarset ja soostereotüüpset kuvandit ning lisada sellele mängulisust.

“Küberprillikandjate” ehk märkajate-edendajate võrgustik koosneks erinevatest osapooltest, kes oma võrgustatud tegevuse ja teadlikkusega noorte küberturvalisuse kompetentside arendamist toetavad.

Selle rakendamist saavad toetada järgmised osapooled:

- Mõtestatud ja järjekindel poliitikakujundamise protsess saab alata eesmärkide seadmisega. Teisisõnu peavad **HTM, MKM ja Kaitseministeerium omavahelises koostöös seadma ühiselt sõnastatud sihi noorte küberturvalisuse kompetentside arendamiseks** ja määratlema kaasneva tegevuskava koos selle täitmiseks vajalike ressurssidega (sh süstemaatilise rahastuse tagamine). See toetab üleminekut projektipõhiselt tegutsemiselt süsteemse valdkonna arendamiseni.
- **Formaalhariduses on keskne vastutus IT-õpetajatel ja haridustehnoloogidel,** kes saavad märgata õpilaste huvi ja võimekust, jagada õpilastele algtaseme küberturvalisuse alaseid teadmisi, korraldada koolis küberturvalisuse sisulisi üritusi, ergutada õpilasi varakult osalema kübervõistlustel ja/või töötubades, värvata neid koolis küberturbega tegelema või suunata õpilasi huvihariduse ning talendikamaid õpilasi sügavama õppe juurde. Lisaks saavad just nemad koolitada kooli teisi õpetajaid küberturvalisuse osas ning luua võimalused õpilaste kui ekspertide kaasamiseks, mis sillutab teed õpilaste ja õpetajate digikööstööks. Õpilaste ja õpetajate teadmiste vahetus on oluline eelkõige seetõttu, et mitmed digioskusi hindavad õpilased enda puhul oluliselt kõrgemaks kui õpetajad (Leppik, Haaristo ja Mägi 2017).

  - Inspireeriva praktika näitena toodi Mõttehommikul Gustav Adolfi Gümnaasiumi kogemus, kus 4.-12. klassi õpilased on kaasatud koolis IT-juhtimisse ja korraldusse, täites seda rolli roteeruvalt haridustehnoloogi toel. Õpilastel on praktilised ülesanded, mida lahendada, kusjuures vanemate klasside õpilased juhendavad nooremaid.
- Haridustehnoloogide ja IT-õpetajate toetamiseks **riiklikul tasandil** saavad **HTM, HITSA, Innove koostöös MKMi ja Kaitseministeeriumi** ning ülikoolide õpetajakoolituse õppejõududega integreerida küberturvalisust ja digipädevusi õppekava kohustuslikku osasse ja ainekavadesse. Täiendava ettepanekuna tõstatus Mõttehommikul küberturvalisuse teema lisamine esseeteemade hulka ja küberturbe teemade toomine matemaatika- ja inglise keele ülesannetesse.
- **HITSA**, kes suurendaks haridustehnoloogide koolituste tellimust ja mahtu, viies läbi nii küberturbe teemalisi baas- kui täienduskoolitusi, kaasates vajadusel eksperte küber(koolitus-)ettevõtetest, avalikust sektorist (RIAst ja ministeeriumitest) ning potentsiaalselt ka talendikamaid õpilasi, kellele viitaksid haridustehnoloogid. Samuti saab HITSA koostöös **haridustehnoloogide võrgustikuga** luua tugistriktuuri üldhariduskooli (õpetaja) ja teaduskooli koostööle.
- **Teaduskoolide töötajad** toetavad IT-õpetajaid ja teisi õpetajaid küberhuviliste ja –talentide märkamisel ja arendamisel, varustades neid teabega üritustest, sisuliste ülesannetega ning luues küberhuviliste õppurite võrgustikke. Siinkohal peeti oluliseks küberturbe õpetamise metoodika loomist ja testimist, et teada, mis toimib küberturbe õpetamisel üldhariduses ja milliseid metoodikaid küberturbe oskuste edendamiseks on kõige mõistlikum kasutada
- **Kooli muu personal** (eelkõige **õpetajad**) ja **huvihariduse õpetajad** saavad tuvastada küberhuvi ja talente ning vastavalt oma kompetentsile integreerida küberturvalisuse teemat õpetamisel või juhendamisel.
- **Lapsevanemad** saavad toetada lapse küberhuvi läbi iseenda teadlikkuse tõstmise (näiteks lasteaiaõpetaja või kooliõpetaja suunamise, Lapsevanemate liidu koolituste). Ka arvutimängude osas on oluline teadlik lähenemine – küberhuvi alged peituvad tihti just seal. Näiteks vanuses 10-13 on leitud positiivne seos küberentusiasmi ja arvutimängude vahel ning mängulisus ja lõbu on oluliseks motivaatoriks tagamaks küberhuvi püsimist (Koppel et al., 2018).
- **Kübervõistluste korraldajad** peaksid eristama kübervõistlustel osalejad, kelle jaoks võistlused on huvi tekitajad ja need, kelle jaoks on võistlused küberturbe oskuste arendajaks – ja sellele vastavalt suunama neid edasi. **Riiklikul tasandil** (MKMi ja Kaitseministeeriumi toel) tuleb tagada, et huvilistele oleks olenemata nende majanduslikust ja geograafilisest taustast tagatud ligipääs kübervõistlustele. Selleks saab kübervõistlusi ja töötube korraldada praegusest enam väljaspool Tallinnat ja Tartut ning viia neid läbi ka praegusega võrreldes nooremas vanuses lastele. Kübervõistlustel osalemiseks on tihti takistus hirm ja suur mõju on esimesel kogemusel – kui noor osaleb esimesel võistlusel põhikooli lõpuklassides ning kogemus osutub negatiivseks, on tõenäoline pettumus ja huvi kiire kadumine.
- **Karjäärinõustajate** teadlikkuse tõstmine täienduskoolitusega küberkarjäärivõimaluste osas on võtmetähtsusega stereotüüpide murdmisel küberturvalisuse valdkonnas. Lisaks küberturvalisusega seotud karjäärivõimaluste mitmekesisemate võimaluste nägemise ja valiku annab see võimaluse suuremal hulgal tüdrukuid kübervaldkonda kaasata. Küberturvalisuse Mõttehommikul toodi näitena kübervaldkonnaga seoste tutvustamine kriisikommunikatsioonis, küberpsühholoogias, õigusvaldkonnas ja üldkommunikatsioonis.

III IKT erialadele küberturbe kompetentside tihedam integreerimine

Miks on oluline? Küberturbe kompetentsid IKT erialadel on vajalikud kahest perspektiivist: 1) domineeriv karjääritee küberturbesse on IKT erialadelt, mistõttu aitab küberturbe komponent nendel õppekavadel küberturbe huvi soodustada ja esmast kokkupuudet valdkonnaga tekitada; 2) mitmetes valdkondades (nt elutähtsad teenused) kannavad ettevõtte/asutuse küberturbe eest vastutust IT meeskonnad – seetõttu on elementaarse küberturbe tagamiseks vajalik teadlike IKT töötajate koolitamine.

Prioriteetne tegevus: Küberturvalisuse integreerimine IKT ainetesse IKT õppekavadel nii kõrg- kui kutsehariduses. Eesmärk on integreerida sisseprojekteeritud turbe (*security by design*) põhimõtet - turbe vajadusi arvestatakse ja turvanõrkusi välditakse juba riist- või tarkvara ülesehitamise käigus. Infoturbe ained peaksid olema kättesaadavad nii õppivatele IKT tudengitele/õpilastele kui ka täienduskoolitusena juba töötavatele IKT spetsialistidele.

Selle rakendamist saavad toetada järgmised osapooled:

- **Majandus- ja Kommunikatsiooniministeerium** (valdkonna eestvedajana), **Haridus- ja Teadusministeerium** (haridussüsteemi kujundajana), **Kaitseministeerium** (olulise küberturbe kompetentside kasutajana ja kujundajana) saavad tegevuse rakendamist vedada näiteks **rakkerühma vormis**, kaasates teisi olulisi osapooli**.** Rakkerühma ülesanne on töötada välja raamistik, mis toetab osapoolte süsteemset koostööd, sisseprojekteeritud turbe rakendamise piloteerimisvõimalusi, heade praktikate ja metoodikate kohandamist või väljatöötamist.
- **IKT õppekavade arendajad ülikoolides** saavad õppekavasid täiendada infoturbe õppeainete loomise või sellealaste teemade integreerimisega olemasolevatesse ainekursustesse. Prioriteetsete teemadena IKT erialade õppekavas näevad eksperdid: riskihaldus, turvaline programmeerimine, riskijuhtimine, info- ja võrguturbe standardid (protsessidele ja toodetele), tehnoloogia ja õigus (nii Eestis kui rahvusvaheliselt). IKT õppekavadel omandatavate oskuste hulka peaks Mõttehommikul osalejate hinnangul kuuluma ka järgmised kompetentsid: süstematiseerimise oskus, infosüsteemi kui terviku nägemise oskus, (turbe)probleemi tuvastamise oskus ja selle keerukuse hindamise oskus, arusaamine turvaliste protokollide loomise protsessist (targa tellija kasvatamine).
- **IKT õppekavadel õpetavad** akadeemilised töötajad saavad õppekavaarenduses ja õpetamises täiendada küberturbe perspektiivi sisaldava **kogemusõppega,** st õppimist läbi reaalsete olukordade ja tegelike turvanõrkuste tagajärgede. Seda toetab vajalike õppematerjalide loomine koostöös küberturbe spetsialistide, ettevõtete ja erialaliitudega. Selle eelduseks on küberturbe intsidentidega seotud info kättesaadavus õppe eesmärgil.
- **Küberturbe üliõpilasi** saab kaasata IKT tudengite väljaõppes, sh praktikumide andmisel – nt juhendaks küberkaitse eriala tudeng äriinfotehnoloogia üliõpilaste seminare või praktikume.
- Küberturbe oskustega **IKT tudengeid** saab kaasata üldhariduse tasemel õpetamisse ja õpetajate mentorlusse, sh tundide ettevalmistusse ning õpetajate harimisse. Seda saaks toetada vastav stipendiumprogramm või praktikatasu kompenseerimine. Kaasamine toetab ka kooliõpetajate väljaõpet küberturbe teemades.
- **Küberturbe ettevõtted** ja **IKT erialaorganisatsioonid** peavad olema süstemaatiliselt kaasatud IKT-erialade küberturbe elemendi õppekavaarendusse (nt ainekursuste/moodulite sisustamise protsessi) ülikoolide esindajate eestvedamisel. Lisaks saavad nad osaleda ka ainekursuste õpetamisel ja täienduskoolituste läbiviimisel, rikastades õppeprotsessi infoturbega seotud praktikavõimaluste loomisega.

IV Küberturbe talentidele konkureerimine globaalsel tööjõuturul

Miks on oluline? Küberturbe tööjõuturg ületab riigipiire. Suutlikkus tuua Eestisse talente on oluline ettevõtetele tööjõu puuduse leevendamiseks, ekspordi toetamiseks ja riigile tervikuna küberturbe sektori arenguks. Talendipoliitika puudutab kohalike küberturbe spetsialistide hoidmist ja neile välismaalt naasmiseks sobivate tingimuste loomist kui ka välisriikidest pärit talentide Eestisse värbamist. Eriti oluliseks muutub välisvärbamine spetsiifiliste osksustega spetsialistide puhul, keda Eestis ei ole või on vähe leida.

Prioriteetne tegevus: Riikliku toe arendamine välistalentide värbamiseks toetava keskkonna loomiseks. Eesmärk on luua välistalentide värbamist soodustav keskkond ettevõtetele ja suurendada Eesti küberettevõtete tuntust rahvusvahelises perspektiivis.

Selle rakendamist saavad toetada järgmised osapooled:

- **Rahandusministeerium** saab töötada välisriikidest tippseptsialisti värbamiseks välja meetmeid (ajutiseks) maksukoormuse leevendamiseks – nt Mõttehommikul toodud idee vähendada välistööjõu eest makstavat sotsiaalmaksu pensioni esimese samba makse võrra. See eeldab ka poliitilist otsust.
- **Siseministeerium** toetab ettevõtteid välistööjõu taustakontrolli läbiviimisel. Vajalik on **Justiitsministeeriumi** tugi, kes loob seadusandliku baasi küberturbe sektoris vajalikuks taustakontrolliks ja sätestab kontrollitavad tingimused. Samuti on kaasatud **Politsei- ja Piirivalveamet** kui kontrolli teostaja. Eesmärk on, et ettevõte saaks enne välisspetsialisti värbamist kolmandatest riikidest küsida Politsei- ja Piirivalveametist kinnitust, kas inimene vastab küberturbe valdkonnas seatud turvanõuetele.
- **Majandus- ja Kommunikatsiooniministeeriumi, Välisministeeriumi, saatkondade ja valdkonnaga seotud poliitikute** koostöös Eesti küberturbe ettevõtete tuntuse suurendamine ning müümine. Vajalik on ka **Ettevõtluse Arendamise Sihtasutuse** panus välisturgudele suunatud tegevuste rahastajana. Maksimaalselt tuleks kasutada juba olemasolevaid programme (sh neisse küberturbe spetsiifika lisamine): nt Globaalse Digiühiskonna Fond[21], Eesti startup viisa võimaluste tutvustamine. Protsessi juures on kriitiline osapoolte tegevuste koordineerimine ja võimestamine, mis saaks olla MKMi kui valdkonna eestvedaja vastutus.
- **Ülikoolide ja ettevõtete esindajad** saavad senisest veelgi enam panustada keele- ja kultuuriruumi tutvustamisel välistudengitele ja värskelt saabunud välistööjõule. Toetuda saab olemasolevatele teenustele/tegevustele (nt Ettevõtluse Arendamise Sihtasutus ja Work in Estonia, tudengite suunamine Siseministeeriumi välismaalaste kohanemise programmi) ning koostöös partneritega (Haridus- ja Teadusministeeriumi, Siseministeeriumiga) vajadusel nende täiendav arendamine: nt õppega integreeritud eesti keele kursuste arendamine, mis soodustaksid Eesti tööturul kohanemist. Välistööjõu kohanemist saab toetada ka läbi küberturbe kogukonna ürituste ja välistööjõu kaasamise olemasolevatesse võrgustikesse.

[21] Hiljutistest algatustest on nt Majandus- ja Kommunikatsiooniministeerium ning EAS asutanud märtsis 2019 Globaalse Digiühiskonna Fondi, mis toetab Eesti digilahenduste eksporti, et luua uusi võimalusi Eesti IKT ettevõtjatele. Sihfond on plaanis käivitada 2020. aastal asukohaga Tallinnas. Sellised programmid toetavad ka küberturbe talendipoliitika arendamist. Vt täpsemalt https://www.err.ee/921589/globaalse-digiuhiskonna-fondi-asutamine-sai-allkirjad

Kasutatud kirjandus

Asia-Pacific Economic Cooperation. (2017). *Data Science and Analytics Skills Shortage: Equipping the APEC Workforce with the Competencies Demanded by Employers*. Salvestatud Asia-Pacific Economic Cooperation website: https://www.apec.org/Publications/2017/11/Data-Science-and-Analytics-Skills-Shortage

Australian Cyber Security Growth Network. (2017). *Cyber Security Sector Competitiveness Plan*. Salvestatud Australian Cyber Security Growth Network website: https://www.acsgn.com/wp-content/uploads/.../Cyber-Security-SCP-April2017.pdf

Australian Government. (2017). *Australia's Cyber Security Strategy: Enabling innovation, growth & prosperity, First Annual Update 2017*. Salvestatud https://cybersecuritystrategy.homeaffairs.gov.au/sites/all/themes/cybersecurity/img/cyber-security-strategy-first-annual-update-2017.pdf

Australian Information Security Association. (2016). *The Australian Cyber Security Skills Shortage Study 2016: AISA Research Report*. Salvestatud Australian Information Security Association website: https://www.aisa.org.au/Public/Training_Pages/Research/AISA%20Cyber%20security%20skills%20shortage%20research.aspx

BANKSETA. (2018). *Sector Skills Plan for the Fiscal Year 2018/2019: Enabling Skills Development In The Banking And Alternative Banking Sector*. Salvestatud BANKSETA website: https://www.bankseta.org.za/downloads/sector-skills-plan-2018-19.pdf

Bedding, K., & de Jongh, M. (2017). *Federal Workforce: Attracting and Retaining Talent in the Field of Cybersecurity*. Salvestatud Cornell Institute for Public Affairs website: https://ecommons.cornell.edu/handle/1813/52178

Burning Glass Technologies. (2015). *Job Market Intelligence: Cybersecurity Jobs, 2015*. Salvestatud Burning Glass Technologies website: https://www.burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

Buvat, J., Turner, M., Slatter, M., & Puttur, R. K. (2018). *Cybersecurity Talent: The Big Gap in Cyber Protection*. Salvestatud Capgemini website: https://www.capgemini.com/wp-content/uploads/2018/02/the-cybersecurity-talent-gap-v8_web.pdf

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, *75*, 24–35. https://doi.org/10.1016/j.cose.2018.01.015

Carr, M., & Tanczer, L. M. (2018). UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions. *Journal of Cyber Policy*, *3*(3), 430–444. https://doi.org/10.1080/23738871.2018.1550523

Center for Strategic and International Studies. (2016). *Hacking the Skills Shortage. A study of the international shortage in cybersecurity skills*. Salvestatud McAfee website: https://www.mcafee.com/us/resources/reports/rp-hacking-skills-shortage.pdf

Collins McNicholas. (2016). *Labour Market Review: Information & Communication Technology*. Salvestatud https://www.collinsmcnicholas.ie/wp-content/uploads/2016/07/The-ICT-Industry-in-Ireland-2016.pdf

Cyber Security Agency of Singapore. (2016). *Singapore's Cybersecurity Strategy*. Salvestatud https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf

Cybersecurity Ventures. (2017). *2017 Cybercrime Report*. Salvestatud https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Department for Business, Innovation and Skills (Government of the United Kingdom). (2014a). *Cyber Security Skills: Business Perspectives and Government's Next Steps*. Salvestatud Department for

Business, Innovation and Skills website: https://www.gov.uk/government/publications/cyber-security-skills-business-perspectives-and-governments-next-steps

Department for Business, Innovation and Skills (Government of the United Kingdom). (2014b). *Cyber Security skills: Business perspectives and Government's next steps: Supporting Evidence*. Salvestatud Department for Business, Innovation and Skills website: https://www.gov.uk/government/publications/cyber-security-skills-business-perspectives-and-governments-next-steps

Department for Digital, Culture, Media and Sport. (2018). *Identifying the Role of Further and Higher Education in Cyber Security Skills Development*. Salvestatud https://www.gov.uk/government/publications/the-role-of-further-and-higher-education-in-cyber-security-skills

Frost & Sullivan. (2017). *2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk*. Salvestatud https://iamcybersafe.org/gisws/

Griffith, M. K. (2018). A comprehensive security approach: bolstering Finnish cybersecurity capacity. *Journal of Cyber Policy*, *3*(3), 407–429. https://doi.org/10.1080/23738871.2018.1561919

Hague Security Delta. (2016). *Human Capital Actieagenda Cyber Security: 2016-2018*. Salvestatud https://www.thehaguesecuritydelta.com/media/com_hsd/report/109/document/20161208-HCA-Cyber-Security-DEF.pdf

Information and Communications Technology Council. (2016). *Critical Infrastructure in a Hyperconnected Economy*. Salvestatud https://www.ictc-ctic.ca/wp-content/uploads/2016/09/ICTC_Critical-Infrastructure-in-a-Hyperconnected-Economy_Sept13.pdf

International Data Corporation. (2014). *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things: Executive Summary*. Salvestatud https://estonia.emc.com/leadership/digital-universe/2014iview/executive-summary.htm

Kam, H.-J., Menard, P., Ormond, D., & Katerattanakul, P. (2018). Ethical Hacking: Addressing the Critical Shortage of Cybersecurity Talent. *PACIS 2018 Proceedings*, *321*. Salvestatud https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1320&context=pacis2018

Koppel, K., Tammsaar, H., Solnik, S., & Jaanits, J. (2018). *Tuleviku tegija teekond startup ökosüsteemi*. Salvestatud Rakendusliku Antropoloogia Keskus website: https://media.voog.com/0000/0037/5345/files/Raport%2015.11.18.pdf

Koppenjan, J. F. M., & Klijn, E.-H. (2004). *Managing uncertainties in networks: a network approach to problem solving and decision making*. London ; New York: Routledge.

Learning, Skills and Innovation Partnership. (2017). *Cardiff Capital Region Employment & Skills Plan 2017*. Learning, Skills and Innovation Partnership.

Leppik, C., Haaristo, H.-S., & Mägi, E. (2017). *IKT-haridus: digioskuste õpetamine, hoiakud ja võimalused üldhariduskoolis ja lasteaias.* Tallinn: Poliitikauuringute Keskus Praxis.

Libicki, M. C., Senty, D., & Pollak, J. (2014). *H4cker5 wanted: an examination of the cybersecurity labor market*. Santa Monica, CA: RAND.

Lingelbach, K. K. (2018). *Perceptions of Female Cybersecurity Professionals Toward Factors that Encourage Females to the Cybersecurity Field*. Salvestatud https://nsuworks.nova.edu/gscis_etd/1056/

Mets, U., & Leoma, R. (2016). *Tulevikuvaade tööjõu- ja oskuste vajadusele: info- ja kommunikatsioonitehnoloogia: uuringu terviktekst*. Salvestatud http://oska.kutsekoda.ee/wp-content/uploads/2016/04/IKT-Raport-loplik.pdf

Morgan, S. (2017). Cybersecurity Jobs Report 2018-2021. *Cybersecurity Ventures*. Salvestatud https://cybersecurityventures.com/jobs/

National Institute of Standards and Technology. (s.a.). *NICE Cybersecurity Workforce Framework*. Salvestatud https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (Nr NIST SP 800-181). https://doi.org/10.6028/NIST.SP.800-181

Nobles, C., & Burrell, D. (2018). The Significance of Professional Associations: Addressing the Cybersecurity Talent Gap. *MWAIS 2018 Proceedings*, *35*. Salvestatud https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1034&context=mwais2018

Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU). (2017). *Future demand and supply of ICT security competence* [Ingliskeelne kokkuvõte].

OECD. (2016). *School Leadership for Learning: Insights from TALIS 2013*. *TALIS*. https://doi.org/10.1787/9789264258341-en

Parrish, A., Impagliazzo, J., Raj, R. K., Santos, H., Asghar, M. R., Jøsang, A., … Stavrou, E. (2018). Global perspectives on cybersecurity education for 2030: a case for a meta-discipline. *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education - ITiCSE 2018 Companion*, 36–54. https://doi.org/10.1145/3293881.3295778

Pedley, D., McHenry, D., Motha, H., & Shah, J. N. (2018). *Understanding the UK cyber security skills labour market*. Salvestatud Department for Digital, Culture, Media and Sport website: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/767422/Understanding_the_UK_cyber_security_skills_labour_market.pdf

PricewaterhouseCoopers. (2016). *Unlocking the cybersecurity growth potential: Singapore's cybersecurity industry outlook*. Salvestatud https://www.pwc.com/sg/en/publications/assets/unlocking-cybersecurity-growth-potential.pdf

P&S Market Research. (2017). *Cyber Security Market by Component (Solution, Service), by Security Type (Application, Network, Endpoint, Cloud, Wireless), by Deployment Mode (On-Premises, Cloud), by Organization Size (Large Enterprises, Small and Medium Enterprises), by Industry (Aerospace and Defense, Government, BFSI, IT & Telecom, Healthcare, Retail, Manufacturing), by Geography (U.S., Canada, U.K., Russia, Ireland, China, Australia, India, South Korea, South Africa, Nigeria, Kenya, Morocco, Brazil, Mexico) – Global Market Size, Share, Development, Growth and Demand Forecast, 2013-2023*. Salvestatud https://www.psmarketresearch.com/market-analysis/cyber-security-market

Psience OÜ. (2017). *Tööandjate rahulolu uuring IKT õppekavade lõpetanutega.* Salvestatud Hariduse Infotehnoloogia SA website: http://media.voog.com/0000/0034/3577/files/RAPORT_T%C3%9C%20Informaatika%20bak_25.05%20l%C3%B5plik.pdf

Report Buyer. (2017). *Cyber Security Market by Component, by Security Type, by Deployment Mode, by Organization Size, by Industry, by Geography - Global Market Size, Share, Development, Growth and Demand Forecast, 2013-2023*. Salvestatud https://www.reportbuyer.com/product/5289039/cyber-security-market-by-component-by-security-type-by-deployment-mode-by-organization-size-by-industry-by-geography-global-market-size-share-development-growth-and-demand-forecast-2013-2023.html

SANS Institute. (2014). *Cybersecurity Professional Trends: A SANS Survey*. Salvestatud SANS Institute website: https://www.sans.org/reading-room/whitepapers/analyst/cybersecurity-professional-trends-survey-34615

Seath, S., & Drew, C. (2016). *Cyber Security Skills Report*. Salvestatud Greater Wellington Regional Council website: http://www.gw.govt.nz/assets/WRS-files/Cyber-security-skills-report-final.pdf

Silensec. (2017). *Addressing The Cyber Security Skills Gap*. Salvestatud http://www.silensec.com/downloads-menu/whitepapers/item/download/10_d3d9446802a44259755d38e6d163e820

Singapore's National Cybersecurity Masterplan 2018. (2018). Salvestatud https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/NationalCyberSecurityMasterplan%202018.pdf

TalTech. (2018a). *Lõpetajate rahulolu-uuring, küberkaitse õppekava.* Tallinn: TalTech.

TalTech. (2018b). *Üliõpilaste ÕIS-põhine tagasiside õppekava õppeainetele, õppeprotsessile ja õppejõududele, küberturbe tehnoloogiad.* Tallinn: TalTech.

Tartu Ülikool. (2018). *Viimase aasta üliõpilaste tagasiside, küberkaitse õppekava*. Tartu: Tartu Ülikool.

Tech Partnership. (2017). *Factsheet: Cyber Security Specialists in the UK*. Salvestatud Tech Partnership website: https://www.thetechpartnership.com/globalassets/pdfs/research-2017/factsheet_cybersecurityspecialists_feb17.pdf

Ter, K. L. (2018). Singapore's cybersecurity strategy. *Computer Law & Security Review*, *34*(4), 924–927. https://doi.org/10.1016/j.clsr.2018.05.001

United States Department of Labor. (2014). *Cybersecurity Industry Model*. Salvestatud United States Department of Labor website: https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx

University of Phoenix. (2014). *Cybersecurity Workforce Competencies: Preparing Tomorrow's Risk-Ready Professionals*. Salvestatud University of Phoenix website: https://www.isc2.org/-/media/1241294BA12145B6912309584E48C147.ashx

van Lakerveld, J. A., Broek, S. D., Buiskool, B. J., Grijpstra, D. H., Gussen, I., Tönis, I. C. M., & Zonneveld, C. A. J. M. (2014). *Arbeidsmarkt voor Cyber Security Professionals*. Salvestatud WODC, Ministerie van Veiligheid en Justitie website: https://www.wodc.nl/binaries/2486-volledige-tekst_tcm28-73679.pdf

Workforce Intelligence Network for Southeast Michigan. (2017). *Cybersecurity Skills Gap Analysis: National and Advance Michigan Data*. Salvestatud https://winintelligence.org/wp-content/uploads/2017/07/FINAL-Cybersecurity-Skills-Gap-2017-Web-1.pdf

Lisa 1. Küberturbe tööjõuvajaduse ja sektori uuringud

TABEL 1. KÜBERTURBE TÖÖJÕUVAJADUSE JA SEKTORI UURINGUD

Uuringu/ analüüsi nimi	Uuringu/ analüüsi geograafiline ulatus	Aasta	Allikas
2017 Cybercrime Report	Maailm	2017	(Cybersecurity Ventures, 2017)
Cybersecurity Jobs Report 2018-2021	Maailm	2017	(Morgan, 2017)
2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk	Maailm ja regioonid	2017	(Frost & Sullivan, 2017)
Hacking the Skills Shortage. A study of the international shortage in cybersecurity skills	Maailm. Kaheksa riiki: Austraalia, Prantsusmaa, Saksamaa, Iisrael, Jaapan, Mehiko, Ühendkuningriik ja USA	2016	(Center for Strategic and International Studies, 2016)
Cybersecurity Talent: The Big Gap in Cyber Protection	Maailm. Üheksa riiki: Prantsusmaa, Saksamaa, India, Itaalia, Holland, Hispaania, Rootsi, Ühendkuningriik ja USA	2018	(Buvat, Turner, Slatter, & Puttur, 2018)
Data Science and Analytics Skills Shortage: Equipping the APEC Workforce with the Competencies Demanded by Employers	APECi riigid	2017	(Asia-Pacific Economic Cooperation, 2017)
Tulevikuvaade tööjõu- ja oskuste vajadusele: info- ja kommunikatsioonitehnoloogia: uuringu terviktekst	Eesti	2016	(Mets & Leoma, 2016)
Human Capital Actieagenda Cyber Security: 2016-2018	Holland	2016	(Hague Security Delta, 2016)

Arbeidsmarkt voor Cyber Security Professionals	Holland	2014	(van Lakerveld et al., 2014)
Future demand and supply of ICT security competence	Norra	2017	(Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU), 2017)
Identifying the Role of Further and Higher Education in Cyber Security Skills Development	Ühendkuningriik	2018	(Department for Digital, Culture, Media and Sport, 2018)
Understanding the UK cyber security skills labour market	Ühendkuningriik	2018	(Pedley et al., 2018)
UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions	Ühendkuningriik	2018	(Carr & Tanczer, 2018)
„Cyber Security Skills: Business Perspectives and Government's Next Steps" koos lisaga „Cyber Security skills: Business perspectives and Government's next steps: Supporting Evidence"	Ühendkuningriik	2014	(Department for Business, Innovation and Skills (Government of the United Kingdom), 2014a, 2014b)
Factsheet: Cyber Security Specialists in the UK	Ühendkuningriik	2017	(Tech Partnership, 2017)
Cardiff Capital Region Employment & Skills Plan 2017	Cardiff pealinna piirkond (Wales)	2017	(Learning, Skills and Innovation Partnership, 2017)
Federal Workforce: Attracting and Retaining Talent in the Field of Cybersecurity	USA	2017	(Bedding & de Jongh, 2017)
Cybersecurity Workforce Competencies: Preparing Tomorrow's Risk-Ready Professionals	USA	2014	(University of Phoenix, 2014)
NICE Cybersecurity Workforce Framework	USA	2017	(National Institute of Standards and Technology, s.a.)
National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework	USA	2017	(Newhouse, Keith, Scribner, & Witte, 2017)
Cybersecurity Competency Model	USA	2014	(United States Department of Labor, 2014)
Job Market Intelligence: Cybersecurity Jobs, 2015	USA	2015	(Burning Glass Technologies, 2015)
Cybersecurity Professional Trends: A SANS Survey	USA	2014	(SANS Institute, 2014)
Cybersecurity Skills Gap Analysis:	USA	2017	(Workforce Intelligence

National and Advance Michigan Data			Network for Southeast Michigan, 2017)
Addressing The Cyber Security Skills Gap	USA	2017	(Silensec, 2017)
Critical Infrastructure in a Hyperconnected Economy	Kanada	2016	(Information and Communications Technology Council, 2016)
The Australian Cyber Security Skills Shortage Study 2016: AISA Research Report	Austraalia	2016	(Australian Information Security Association, 2016)
Cyber Security Sector Competitiveness Plan	Austraalia	2017	(Australian Cyber Security Growth Network, 2017)
Cyber Security Skills Report	Wellingtoni linna piirkond (Uus-Meremaa)	2016	(Seath & Drew, 2016)
Unlocking the cybersecurity growth potential: Singapore's cybersecurity industry outlook	Singapur	2016	(PricewaterhouseCoopers, 2016)
Sector Skills Plan for the Fiscal Year 2018/2019: Enabling Skills Development In The Banking And Alternative Banking Sector	Lõuna-Aafrika	2018	(BANKSETA, 2018)

Lisa 2. Uuringu metoodika

1. Ettevõtete kaardistus

Küberturbe tooteid ja teenuseid pakkuvate ettevõtete ja avaliku sektori asutuste kaardistamise aluseks on:

- Startup Estonia poolt kaardistatud küberturbe ettevõtted, start-upid;
- Eesti Kaitsetööstuse Liidu liikmed, kelle tegevusalade seas on loetletud küberkaitse;
- Äripäeva IT ettevõtete TOP100 sirvimine, selekteerides ettevõtted, kelle tegevused on seotud küberturbe/ andmekaitsega;
- ettevõtete otsing erinevate küberturbega seotud märksõnadega;
- valdkonna eksperdid (intervjueeritud eksperdid vaatasid ettevõtete loetelu, täiendasid vajadusel).

Osade ettevõtetega (mille puhul ei olndu kindlust nende tegutsemises küberturbe valdkonnas), võeti uuringu käigus täiendavalt ühendust, et täpsustada tegevusvaldkonnad.

Kõigi kaardistatud ettevõtete kohta tehti Äriregistri andmepäring. Äriregistri andmete põhjal eristati aktiivsed ettevõtted (st kellel on aktiivselt raporteeritud müügitulu ja tegutsevad 2016-2017 andmete järgi (omavad aktiivset müügitulu).

Riigile elutähtsaid teenuseid tagavate ettevõtete kaardistamise aluseks on:

- Riiklikusse haiglavõrku kuuluvad haiglad ning riikliku kiirabiteenuse pakkujad (Vabariigi Valitsuse määrus „Haiglavõrgu arengukava“)
- Eesti Panga Presidendi määruse alusel loetletud elutähtsat teenust osutavad krediidiasutused ja välisriikide krediidiasutuste filiaalid (3), teised Finantsinspektsiooni tegevusloa alusel Eestis tegutsevad krediidiasutused (5) ning Eesti Pank (1)
- Elektrituru seaduse mõistes elutähtsa teenuse osutajad (6 ettevõtet)
- Elektroonilise side seaduses nimetatud elutähtsa teenuse pakkujad (5 ettevõtet)

Kaardistamise tulemusel on uuringus identifitseeritud 52 aktiivset küberturbe tooteid ja teenuseid pakkuvat ettevõtet, 11 avaliku sektori asutust ja 43 elutähtsaid teenuseid pakkuvat ettevõtet.

2. Äriregistri andmepäring

Kõigi küberturbe tooteid või teenuseid pakkuvate ettevõtete kohta esitati Äriregistri andmepäring, järgmises koosseisus: ettevõtte registreerimise aeg, juriidiline staatus, tegevusala (põhitegevusala EMTAK ja kõrvaltegevusala EMTAK), töötajate arv kokku, kasumiaruande andmed, sh müügitulu/käive, puhaskasum/-kahjum, ärikasum/-kahjum, müügitulu riikide lõikes, müüdud teenuste kulud ja tegevuskulud, palgakulu/tööjõukulu ettevõttes, maksuvõlad, emaettevõte (olemasolu korral). Andmepäring esitati perioodi 2013-2017 kohta.

3. Veebiankeet

Kuivõrd puhtalt Äriregistri andmete põhjal ei ole võimalik selgeks teha, milline on küberturbe maht ettevõtte tegevuses ning avaliku sektori ja elutähtsate teenuste kohta vastavad andmed puuduvad, viidi läbi

veebiküsitlus uuringu sihtrühma seas. Eraldi küsitlusankeet koostati küberturbe ettevõtete jaoks ning eraldi avaliku sektori ja elutähtsate teenuste osutajate jaoks.

Kogutavad andmed olid:

- Ettevõtted: ettevõtte tegevusalad, küberturbe osakaal ettevõtte käibes, küberturbe oskuste ja teadmistega tööjõu otsimine 2017. aastal, küberturbe oskuste ja teadmistega töötajate lahkumine 2017. aastal (ja lahkunud töötajate arv), peamine põhjus töötajate lahkumiseks, küberturbe spetsialisti ühe kuu põhipalk, palgakasvu osakaal järgneva 12 kuu jooksul, spetsialistide vajadus 5 aasta möödudes
- Avalik sektor ja elutähtsad teenused: kulutused küberturbele 2017. aastal ja suuremad kuluallikad, küberturbe kulutuste muutus järgmise aasta jooksul, küberturbe töötajate arv 2013-2017, küberturbe oskuste ja teadmistega tööjõu otsimine 2017. aastal, küberturbe oskuste ja teadmistega töötajate lahkumine 2017. aastal (ja lahkunud töötajate arv), peamine põhjus töötajate lahkumiseks, küberturbe spetsialisti ühe kuu põhipalk, palgakasvu osakaal järgneva 12 kuu jooksul, spetsialistide vajadus 5 aasta möödudes

Kõigil vastanutel paluti täiendavalt täita ettevõtte või asutuse küberturbe spetsialistide kohta personaliankeet järgneva infoga iga küberturbe spetsialisti kohta: ametikoht, vanus, sugu, päritolu, kõrgeim omandatud haridustase, omandatud eriala ja lõpetatud haridusasutus.

Nende valimi liikmete osas, kes veebis täidetavale ankeedile ei vastanud, helistati uuringu käigus üle ja tuletati veebiankeedi täitmist meelde. Täiendavalt anti võimalus vastata samadele küsimustele ka telefoni teel.

Kokku laekus uuringus 57 täidetud ankeeti (veebis ja telefoni teel kokku, sh nii küberturbe ettevõtted kui avalik sektor ja elutähtsad teenused). Ka osaliselt täidetud ankeedid võeti uuringus arvesse.

4. Ettevõtete küberturbe osakaal ja soovitused edaspidiseks sektori analüüsiks

Selleks, et oleks võimalik hinnata küberturbe sektori mahtu tööjõu ja müügitulude ning ekspordi mahtude mõttes, on vaja ettevõtte andmed arvestada läbi küberturbe osakaalu koefitsiendiga. See tähendab, et suurem osa küberturbe ettevõtteid ei tegele küberturbe tegevustega 100% mahus ning seetõttu ei peegelda ettevõtte töötajate arv kokku küberturbe töötajate arvu või kogu müügimaht küberturbe müügimahtu.

Kuivõrd ettevõtete käest kõigi nimetatud andmete küsimine detailselt oleks liialt ressursimahukas ja ajamahukas ettevõtetele endile, on uuringus arvestatud küberturbe koefitsiendina ettevõtte küberturbe osakaalu. Seda osakaalu on laiendatud nii töötajate arvu andmetele kui ka müügitulude ja ekspordi müügitulude analüüsiks. Kuigi tegemist ei ole täpse hinnanguga, on see parim ligikaudne hinnang, mida on võimalik mõistlikult saavutada.

Juhul, kui MKMil on huvi uuringut korrata, soovitame sektori andmete uuendamiseks järgmisi samme:

a) Ettevõtete loetelu uuendamine peamiselt ekspertide toel, vajadusel kasutades ka siin uuringus kasutatud allikaid kaardistamiseks

b) Äriregistri andmetel ettevõtete andmete uuendamine, kasutades selles uuringus kaardistatud küberturbe koefitsenti

c) Ettevõtetele eeltäidetud ankeedi saatmine, palvega enda ettevõtte kohta käivad andmed üle kontrollida ja vajadusel kinnitada või parandada/ täiendada. Eeltäidetud andmed võiksid sisaldada:

ettevõtte küberturbe tegevusalad (vt ptk 1.1.1) ettevõtte küberturbe koefitsient, küberturbe oskuste ja teadmistega töötajate arv, koefitsiendi põhjal arvutatud küberturbe müügitulu, soovi korral ka ekspordi maht. Need on minimaalsed andmed, mis võimaldavad sektori arengute jälgimist praeguses uuringus loodud baasandmete jätkuna.

Sektori ülevaate uuendamine eeldab siiski ettevõtetega kontakteerumist, kuivõrd alternatiivset andmeallikat ei ole. Vastamise motivatsiooni suurendamiseks soovitame eeltäidetud ankeete, mis teeb ettevõtetele andmetest ülevaate saamise lihtsamaks ning eeldab väiksemat panust kui kõigile küsimustele nullist vastamine.

5. Kvalitatiivne andmekogumine

Uuringus mängivad olulist rolli kogutud kvalitatiivsed andmed. Uuringu käigus on läbi viidud järgmised intervjuud

a) 5 ettevalmistavat intervjuud valdkonna ekspertidega uuringu fookuse seadmiseks

b) 9 intervjuud küberturbe ettevõtete esindajatega, 6 intervjuud elutähtsaid teenuseid pakkuvate ettevõtetega

c) 3 rühmaintervjuud Põltsamaa Ühisgümnaasiumi juhtumi analüüsiks (sh juhtkonna, õpetajate ja õpilastega)

d) 3 intervjuud küberturbe üliõpilastega

Intervjuud tuginesid intervjuu kavadele. Siiski olu oluline, et intervjuu kava täienes intervjuust intervjuusse, võimaldades ka juba kogutud andmetele tagasisidet küsida ja tulemusi seeläbi verifitseerida.

6. Õppekavade märksõnaotsing

Töös viidi läbi andmekaeve kõikide Tartu Ülikooli ja TalTechi bakalaureuse- ning magistritaseme õppekavades ning -ainetes. Lõplikusse valikusse jäi 27 märksõna ja nende variatsiooni, mis valiti välja koos projekti kaasatud eksperdiga. Tulemustes eristati esinemist õppekava eesmärkides, õpiväljundites; õppemooduli eesmärkides ja väljundites ning kohustuslikes ainetes ja valikainetes.

Valikusse jäänud märksõnad: andmekaitse, andmeleke, autentimine, autoriseerimine, DDOS/teenustõkestus, digi-, e-hääl.., e-riik, infosüsteem, infoturve/andmeturve, isikusertifikaat, konfidentsiaalsus, krüpt-, kõrgtehnoloogiline sõda, küber, logi, lunavara, marsruuter, nimeserver, pahavara/kahjurvara, pilvetehnoloogia, privaatvõti räsi, süsteemiseire, tulemüür, turvaintsident, turvateadlikkus, viirustõrje.

7. Tööjõuprognoos

Tööjõuvajaduse prognoosimisel kasutatakse tööjõu nõudluse ja pakkumise prognoosimudelit, milles eristatakse tööjõu kasvu- ja asendusnõudlust. Kasvunõudlus on küberturvalisuse sektori arengust tingitud tööjõu vajaduse muutus, mis võib olla nii positiivne kui negatiivne. Asendusnõudlus tuleneb olemasoleva tööjõu asendamise vajadusest, kus peamised tööjõu asendamise põhjused on pensionile siirdumine, teisele tegevusalale tööle siirdumine ja suremus. Kuna küberturvalisuses sektori tööjõud on parimas tööeas ja märkimisväärset pensionile siirdumist ega suremust oodata ei ole, on siinses töös keskmes just kasvunõudluse hindamine.

Tööjõuvajaduse kasvunõudluse hindamiseks IKT sektoris kasutati klassikalist tööjõunõudluse hindamise mudelit, kus prognoosi jaoks on peamisteks komponentideks ettevõtte müügimaht, töötajate arv ja

palgakulu. Sellised näitajad saadi kõikide küberturvalisuse sektori ettevõtete viimase viie aasta majandustegevuse kohta päringuga Äriregistrist. Nende valideerimiseks ning küberturvalisusega seotud inimeste ja majandustegevuse osakaalu täpsustamiseks saadeti ettevõtetesse ka ankeetküsitlus või viidi läbi intervjuud, kogumaks lisaks eelnevale kolmele ka hinnanguid küberturvalisuse sektori tulevikuvajaduste kohta. Kui registris ja ettevõtete öeldud numbrites esines lahknevusi (nt töötajate arvus), loeti kehtivaks just ettevõttest öeldud suurus.

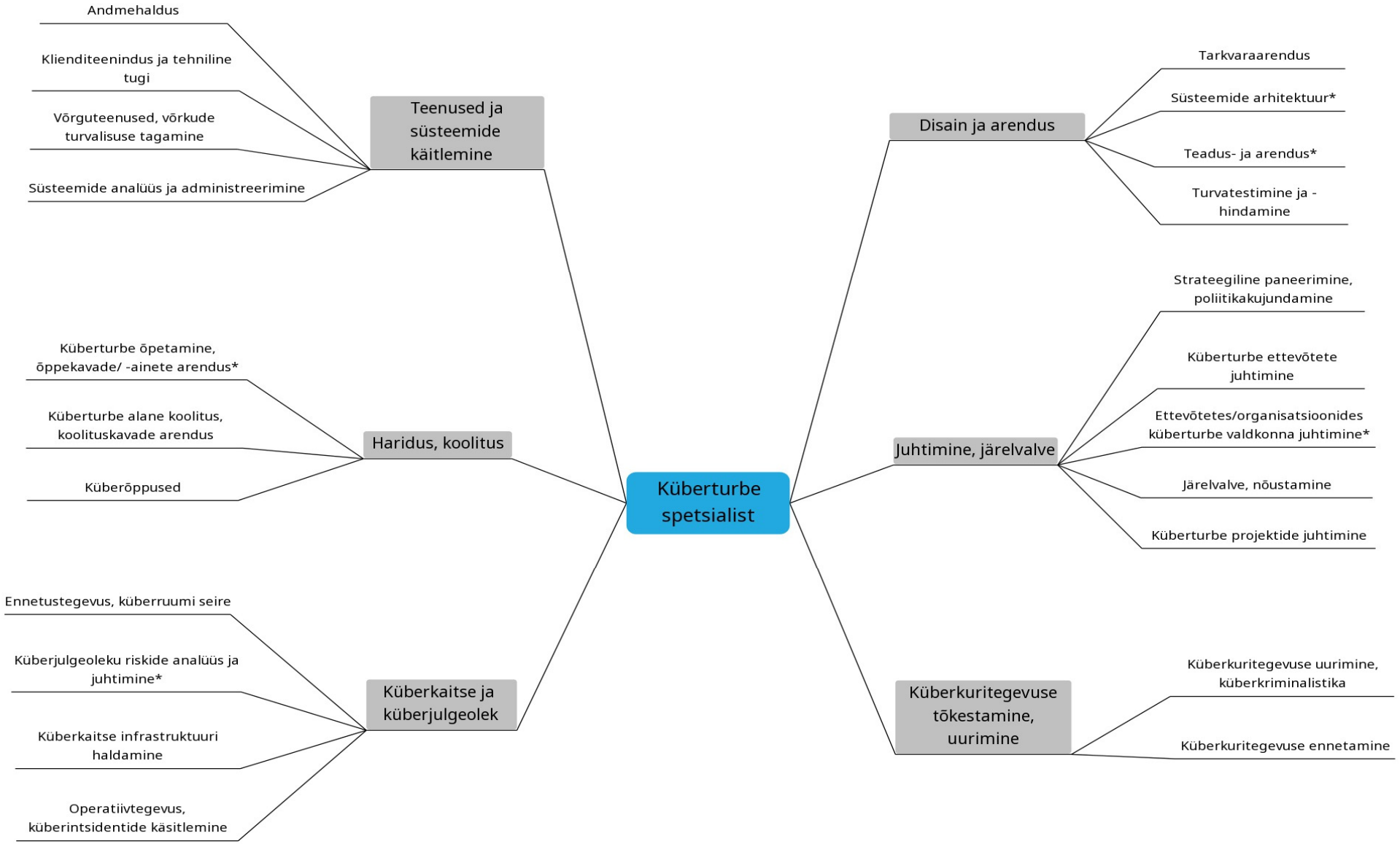
Kui klassikaliselt kasutatakse pika aegrea olemasolul tööjõunõudluse funktsiooni hindamiseks dünaamilist paneelandmete hindamismeetodit (nt Arellano-Bond), siis siinses analüüsis pole meetod rakendatav, kuna andmed on vaid viie aasta kohta ning ei olnud täidetud mudeli tehnilised eeldused. Seega viidi mudeli hindamine läbi vähimruutude meetodiga (OLS), mida rakendati muuhulgas IKT-kompetentsidega [22] tööjõuvajaduse prognoosimisel. Mudelis ei kasutata viiteajaga sõltumatut muutujat, et vältida nihketa hinnangu saamist[23]

Mudelis hinnatakse tööjõu nõudlust log-log kujul sõltuvana müügitulust ja palgakulust töötaja kohta, kontrollmuutujana kasutati IKT sektori SKP-d. Logaritmitud kuju võimaldab mudelist saadud koefitsiente tõlgendada elastsusena ehk näiteks hinnatud käibeelastsuse koefitsient 0,42 tähendab, et küberturvalisuse sektoris toob müügitulu üheprotsendiline kasv kaasa 0,42%-lise töötajate arvu kasvu muude tingimuste samaks jäädes. Kirjeldatud metoodikaga viidi läbi viie stsenaariumit, kus sisenditena varieerusid tööjõuvjaduse näitajad (nt viimaste aastate tööjõu muutus vs ettevõtjate hinnatud prognoos vs Praxise IKT sektori tööjõumuutus). Vt stsenaariumeid pikemalt ptk 4.

[22] Jürgenson, A., Mägi, E., Pihor, K., Batueva, V., Rozeik, H., Arukaevu, R. (2013). Eesti IKT kompetentsidega tööjõu hetkeseisu ja vajaduse kaardistamine. Tallinn: Poliitikauuringute Keskus Praxis

[23] Viiteajaga muutuja korral tekiks korrelatsioon vealiikmega, trendi sissetoomisel ajamuutuja ning teiste sõltumatute (x) muutujatega.

Lisa 3. Küberturbe kompetentsid



Selgitus: tärniga on märgitud need kompetentsid, mille vajadust peeti uuringu raames korraldatud aruteluseminaril osalejate poolt kõige suuremaks (kriitilised kompetentsid)