Sisekaitseakadeemia

Sisejulgeoleku instituut

Jevgenia Jakobson

KOHALIKU TASANDI POLITSEIUURIJATE DIGITAALSE KOMPONENDIGA KURITEGUDE UURIMISEKS VAJALIK KOMPETENTSIRAAMISTIK NING SELLE RAKENDUSVÕIMALUSED

Magistritöö

Juhendaja:

Jaanika Puusalu, PhD

Kaasjuhendaja:

Roger Kumm, MA

Tallinn 2023

SISEKAITSEAKADEEMIA MAGISTRITÖÖ ANNOTATSIOON

Kolledž/instituut: Sisejulgeoleku instituut	Kaitsmise kuu ja aasta: juuni 2023
Töö pealkiri eesti keeles: Kohaliku tasandi politseiuurijate digitaalse komponendiga kuritegude uurimiseks vajalik kompetentsiraamistik ning selle rakendusvõimalused	
Töö pealkiri võõrkeeles: *Competency Framework and its Implementation Possibilities for Investigating Crimes with a Digital Component by Local Police Investigators*	
Lühikokkuvõte: Magistritöö on kirjutatud eesti keeles, võõrkeelne kokkuvõte inglise keeles. Töö maht on 128 lk, millest põhiosa moodustab 80 lk ja 22 lk lisad. Magistritöö kirjutamisel on kasutatud 159 erinevat eesti-, inglise- ja venekeelset allikat. Töö sisaldab 14 tabelit, 2 joonist ja 8 lisa. Magistritöö uurimisstrateegiaks on juhtumiuuring (ingl k *case study*). Juhtumiks on kompetentsiraamistiku väljatöötamise ja valideerimise protsess. Teaduskirjanduse, välisriikide ja rahvusvaheliste organisatsioonide praktiliste materjalide alusel ja kompetentsimudeli metoodika elementide abil koostatud kohaliku tasandi politseiuurijate digitaalse komponendiga kuritegude uurimiseks vajalik kompetentsiraamistik valideeriti kvalitatiivse empiirilise uuringu käigus, mis seisnes ekspertintervjuude ja dokumendianalüüsi abil saadud andmete kodeerimises ja analüüsis. Eesmärgistatud valimisse kaasati Politsei- ja Piirivalveameti ja Sisekaitseakadeemia esindajad ning Põhja Ringkonnaprokuratuuri abiprokurörid. Dokumentide ja tekstide valimisel kasutati mugavusvalimi. Teoreetilise kompetentsiraamistiku ja empiirilise uuringu tulemuste sünteesi alusel esitati Politsei- ja Piirivalveametile ja Sisekaitseakadeemiale viis ettepanekut kompetentsipõhise lähenemise laiemas mõttes ning magistritöös välja töötatud kompetentsiraamistiku rakendusvõimaluste osas. Magistritööd saab kasutada PPA kogukonnasüütegude lahendamise, (digi-)kriminalistika ja koolitusteenuse arendamisel ning Sisekaitseakadeemias politseinikele ette nähtud õppekavade täiendamisel.	
Lisad:	
Võtmesõnad: digitaalse komponendiga kuriteod, politseiuurijad, kompetentsiraamistik, juhtumiuuring	
Võõrkeelsed võtmesõnad: *digital-component crime, police investigators, competency framework, case study*	
Säilitamise koht:	
Töö autor: Jevgenia Jakobson	
Olen koostanud lõputöö iseseisvalt. Kõik lõputöö koostamisel kasutatud teiste autorite tööd, seisukohad, kirjalikest allikatest ja mujal allikates saadud info on nõuetekohaselt viidatud. Olen nõus oma lõputöö avaldamisega elektroonilises keskkonnas.	
Allkiri:	Kommentaar (soovi korral)
Vastab lõputöö nõuetele	
Juhendaja: Jaanika Puusalu, PhD	Allkiri:
Kaasjuhendaja: Roger Kumm, MA	Allkiri:
Kaitsmisele lubatud	
Kolledži direktor/instituudi juhataja:	Allkiri:

SISUKORD

MÕISTETE JA LÜHENDITE SELGITUS

EL – Euroopa Liit

EMPACT – Euroopa multidistsiplinaarne kuritegevuse vastane platvorm (ingl k *European Multidisciplinary Platform Against Criminal Threats*)

EN – Euroopa Nõukogu

CEPOL – Euroopa Liidu õiguskaitsealase koolituse agentuur (ingl k *European Union Agency for Law Enforcement Training*)

CSIRT – küberturvalisuse intsidentidele reageerimise töörühm (ingl k *Computer Security Incident Response Team*)

ESCO – Euroopa Komisjoni mitmekeelne oskuste, kompetentside ja ametite klassifikatsiooni projekt (ingl k *European Skills, Competences, Qualifications and Occupations*)

EMPACT – Euroopa multidistsiplinaarne kuritegevuse vastane platvorm (ingl k *European Multidisciplinary Platform Against Criminal Threats*)

EU-STNA – CEPOL EL strateegiliste vajaduste hindamine (ingl k *CEPOL's European Union Strategic Needs Assessment 2022–2025*)

Digitaalkriminalistika – protsess, mille käigus kasutatakse teaduslikke põhimõtteid ja protsesse elektrooniliselt salvestatud teabe analüüsimiseks ja konkreetse juhtumini viinud sündmuste jada kindlaksmääramiseks süüteomenetluse raames (Raghavan, 2013, p. 91).

Digitaalse komponendiga kuriteod – kuriteod, mille toime panemisel kasutatakse IKT-d, digitaalset keskkonda, internetti ja/või mille tagajärjel jääb digitaalseid jälgi ja tõendeid.

DDoS rünnak – hajutatud teenuse tõkestusrünne (ingl k *Distributed Denial-of-Service (DDoS) Attack*) – küberrünnak, mille eesmärk on interneti serverite üleujutamine, et lammutada võrgu infrastruktuuri või veebisaite.

IKT – info- ja kommunikatsioonitehnoloogia

OSINT – avatud allikaga luure (ingl k *open-source intelligence*). OSINT – avatud allikatest kogutud teabe kogumise ja analüüsimise protsess, mille eesmärgiks on saada operatiivteavet, mis on vajalik riikliku julgeoleku ja õiguskaitse toetamiseks ja äriteabe levitamiseks. OSINT uurib avalikes (avatud) allikates mingil eesmärgil kogutud andmeid ning kasutab neid ümber hoopis teistel eesmärkidel varjatud teemade uurimiseks. OSINTi kontseptsioonist lähtuvalt kasutatakse avatud andmeid selle teabe paljastamiseks, mida tegelikult soovitakse salajas hoida. OSINTi toidavad allikad jaotatakse järgmistesse kategooriatesse: avalik meedia (trükitud ajalehed, ajakirjad ja televisioon); internet (võrguväljaanded ja blogid, arutelurühmad, näiteks foorumid, ja sotsiaalmeedia veebisaidid, näiteks YouTube, Twitter ja Instagram); avalikud valitsuse andmed (avalikud valitsuse aruanded, eelarved, pressikonverentsid, kuulamised ja kõned); erialased ja akadeemilised väljaanded (ajakirjad, konverentsid, akadeemilised tööd ja doktoritööd); kommertsandmed (kommertspildid, äri- ja finantshinnangud ning andmebaasid); hall kirjandus (tehnilised aruanded, patendid, äridokumendid, avaldamata tööd ja uudiskirjad). (European Commission, 2022)

OTNA – CEPOL operatiivkoolituse vajaduste analüüs (ingl k *Operational Training Need Analysis*)

PPA – Politsei- ja Piirivalveamet

PPA politseijaoskond (territoriaalne politseijaoskond) – PPA prefektuuri koosseisu kuuluv territoriaalne struktuuriüksus (PPVS § 5 lg 3)

SISSEJUHATUS

Tänu 1990ndatel hoogustunud interneti levikule ja internetikasutajate osakaalu pidevale kasvule on elanikkonna elustiil ja rutiinne tegevus tänasks oluliselt muutunud (Jewkes & Yar, 2011, p. 1; Tierney, *et al.*, 2018, pp. 3, 7-8; Caneppele & Aebi, 2019, p. 77). Üle poole maailma elanikest kasutab internetti ja peaaegu 45% on igapäevased sotsiaalmeedia kasutajad, mis omakorda muudab ühiskondade ja kommunikatsiooni toimimist. Prognooside kohaselt kasvab võrku ühendatud digiseadmete arv 2025. aastaks 25 miljardini, kusjuures veerand neist asub Euroopas (European Commission, 2020, p. 1). Eesti majandus ja ühiskonna toimimine sõltub suurel määral digitaalsest keskkonnast (Pernik, 2019, p. 73). Siin on on 1,28 miljonit internetikasutajat, mis vastab 98%-le kogu rahvastikust (Mesipuu, 2019).

Digitaliseerumine on muutnud ka kuritegevust (Jewkes & Yar, 2011, p. 1; Euroopa Ülemkogu, 2022; Euroopa Liidu Nõukogu, 2023). Digiseadmete ja IKT kasutamine kuritegude toime panemiseks on viimasel kümnendil järsult kasvanud ja nüüdseks muutunud tavaliseks (Vincze, 2016, p. 183; Tarter, 2017 p. 213; Holt & Bossler, 2016, pp. 2–4; Pernik, 2019, pp. 70–72). Paljud kuriteovormid, sh traditsioonilised kuriteod, sisaldavad digitaalset komponenti (Furnell & Dowling, 2019, p. 10; Euroopa Liidu Nõukogu, 2023).

Käesolevas töös on katuseterminiks **digitaalse komponendiga kuriteod**, mille uurimisega tegelevad regionaalsed, st kohaliku tasandi, politseiüksused. Digitaalse komponendiga kuritegude toime panemisel kasutatakse IKT-d, digitaalset keskkonda, internetti ja/või mille tagajärjel jääb digitaalseid jälgi ja tõendeid. Digitaalse komponendiga kuriteo mõiste sisustamiseks kasutatakse teaduskirjanduses (Leukfeldt, *et al.*, 2013, p. 3; McGuire & Dowling, 2013, p. 4; Furnell & Dowling, 2019, p. 2; Caneppele & Aebi, 2019, p. 71) toodud laias ja kitsas tähenduses küberkuritegevuse definitsioone. Nimetatud allikate kohaselt on digitaalse komponendiga kuritegudeks laiemas tähenduses kuriteod, mille toime panemisel mängib IKT olulist rolli. Kitsas tähenduses on IKT kübekuritegude toime panemisel nii vahendiks kui sihtmärgiks. Samas, nii teaduskirjanduses kui käesolevas töös digitaalse komponendiga kuriteole viidates kasutatakse ka selliseid mõisteid nagu küberkuritegu ja arvutikuritegu, kuna nende tähendus võib osaliselt kattuda.

Aastatel 2009–2017 Eestis kuritegevuse languse ja aastatel 2018–2021 stabiilsena püsimise perspektiivis (Justiitsministeerium, 2021a) on arvuti- ja küberkuritegude osakaal hoopis kasvanud (Justiitsministeerium, 2021b). 2021. aastal oli võrreldes 10 aasta taguse ajaga arvutikuritegude arv

kolmekordistunud (Justiitsministeerium, 2021a). IKT ja digiseadmete abil võimestatud süütegude tõusutrendi taustal on suure ühiskondliku mõjuga juhtumeid kõigist arvutikuritegudest vaid 3%. Nendeks on kohaliku tasandi politseiuurijate menetluspädevusse mittekuuluvad arvutisüsteemi vastu suunatud kuriteod, nagu DDoS rünnakud (st internetiserverite üleujutamine, et lammutada võrguinfrastruktuuri või veebisaite), pahavara valmistamine ja levitamine, teise inimese või organisatsioonide arvutitesse, serveritesse või võrku sisenemine). (Justiitsministeerium, 2021a) Esmakordne arvurikuritegude langus (25%) on toimunud 2022. aastal ning eelkõige arvutikelmuste arvelt. Samas, 2022. aastal oli levinumaks kuriteoks meili- ja sotsiaalmeedia kontode hõivamine, mis moodustas 57% kõigist arvurikuritegude juhtumitest. (Justiitsministeerium, 2022a)

Eespool toodud statistikast võib järeldada, et suur osa digitaalse komponendiga kuritegudest tuleb lahendada kohaliku tasandi politseiuurijatel. Digitaalse komponendiga lähisuhtevägivalla vormide uurimine on tüüpiline ja ilmekas näide kohaliku tasandi uurija tööst. Kaasaegne kuritegelik käitumine kätkeb (sh endiste) partnerite kontode hõivamist, digitaalse identiteedi kuritarvitamist maine rikkumise ja kahju tekitamise eesmärgil, digitaalset kiusu ning tööalast kättemaksu, mis seisneb kaaperdatud sotsiaalmeedia kontole kompromiteeriva informatsiooni postitamist, kontodele ligipääsu takistamist vms. (Justiitsministeerium, 2021c) Teiseks näiteks kohaliku tasandi uurija menetluspädevuses oleva digikomponendiga kuriteost on ahistava jälitamise juhtumid, millest 2021. aastal 75% ja 2022. aastal 55% juhtudel kasutati digivahendeid (Justiitsministeerium, 2021c, 2022b). IKT vahendeid kasutati samuti üle kolmandikus lähenemiskeelu rikkumise juhtumites (Justiitsministeerium, 2022a).

Euroopa Liidu õiguskaitsealase koolituse agentuuri (ingl k *European Union Agency for Law Enforcement Training* – CEPOL) hinnangul on digitaalse komponendiga kuritegevuse aina suureneva leviku tõttu digitoskuste alase erikoolituse vajadus oluline ja aktuaalne kõigile politseiametnike gruppidele (Coman & Alexa, 2022, p. 24). Eesti kriminaalpoliitika põhisuunad aastani 2030 seavad ootusi õiguskaitsetöötajate ettevalmistusele teadmiste ja oskuste osas, mis soodustavad tehnoloogia kasutamist (Justiitsministeerium, 2020). Küberkuritegevuse strateegia (Majandus- ja Kommunikatsiooniministeerium, 2019) eesmärke täpsustavast ja detailselt kirjeldavast Küberturvalisuse programmist aastateks 2021–2024 selgub vajadus järjepidevalt tegeleda erinevate sihtrühmade valdkondlike teadmiste ja digioskuste arendamisega. Kitsaskohtadena tuuakse välja küberturvalisuse valdkonna tööjõuvajadusest ja kompetentsidest täpse ülevaate ning prioriteetsete valdkondade spetsiifiliste küberoskuste vajadustest arusaama ning ka nende kompetentside kirjelduste

ja vastavatesse õppekavadesse lõimimise puudulikkuse. (Majandus- ja Kommunikatsiooniministeerium, 2020, lk 12–13)

Magistritöö teema on **aktuaalne** eespool toodud statistika, strateegiate ja tööjõu kompetentside defineerimise vajaduste valguses. Siseministeeriumi 2021. aasta prognoosi kohaselt ühiskonna ootus siseturvalisuse töötajate digikompetentsidele kasvab, sest vastavalt kuritegude digitaliseerumisele muutub politseinike töö sisu üha keerulisemaks ning neilt oodatakse muuhulgas rohkem IKT ja küberkuritegevuse uurimise oskuseid ning tehnilist taipu (SA Kutsekoda, 2019, lk 9; Siseministeerium, 2021, lk 4). Üha enam tuginevad õiguskaitseasutused kriminaaluurimises ja süüdistuste esitamisel elektroonilistele tõenditele, milleks on tekstisõnumid, e-kirjad või sõnumirakendused. Elektroonilisi tõendeid kasutatakse 85% kriminaaluurimistes ning enam kui 50% kriminaaluurimistes tehakse piiriülene taotlus juurdepääsuks elektroonilistele tõenditele (Euroopa Liidu Nõukogu, 2023). See tähendab, et digitaalse komponendiga kuritegude uurimine moodustab märkimisväärse tööülesannete osa mitte ainult küberkuritegevusele spetsialiseerunud funktsionaalüksustele, vaid ka kohaliku tasandi politseiüksustele nagu PPA politseijaoskonnad.

Käesolevas töös püstitatud teema on **uudne**. Kuigi varasemalt tehtud teadustööd ja uuringud sisaldavad järeldusi politseinike digikompetentside ja digikeskkonnas tõendite kogumise oskuste vajalikkuse ning selle puudulikkuse kohta (Kaha, 2017; Laats, 2017; Luuk, 2017; Raudsepp, 2018; Sepp, 2018; Pernik, 2019; Pillmann, 2021; Lall, *et al.*, 2021), pole Eestis põhjalikult käsitletud kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimiseks vajalikke kompetentse. Viidatud töödes keskenduti enamasti digitaalse tõendi kriteeriumidele ja lubatavusele (Kaha, 2017; Laats, 2017; Luuk, 2017; Lall, *et al.*, 2021), digitaalkriminalistika aspektidele (Sepp, 2018; Raudsepp, 2018; Lall, *et al.*, 2021), siseturvalisuse sektori küberturvalisuse-alasele haridusele (Pernik, 2019) ning siseturvalisuse vaates digiseadmete ja internetistasjade kasutamisest tulenevatele ohtudele (Pillmann, 2021).

Käesoleva magistritöö **uurimisprobleem** tuleneb PPA politseijaoskondade menetluspädevuses olevate kuriteoliikide digitaliseerumisest (Justiitsministeerium, 2021) ning ootustest politsei professionaalsusele (SA Kutsekoda, 2019, lk 9; Siseministeerium, 2021, lk 4; Coman & Alexa, 2022). Eestis varasemalt valminud küberkuritegevuse ja digitaalse komponendiga süütegude erinevatele aspektidele pühendatud uurimistöödes (Kaha, 2017; Laats, 2017; Sepp, 2018; Pernik, 2019; Pillmann, 2021; Lall, *et al.*, 2021) tehtud järelduste kohaselt on politseiuurijate teadmised ja oskused digitaalse

komponendiga kuritegude uurimiseks ebapiisavad ja neid tuleb arendada. **Uurimisprobleemi** sõnastatakse järgmiselt: kuidas süstematiseerida aktuaalseid kompetentse, mis on tänapäeval vajalikud kohaliku tasandi uurijatele digitaalse komponendiga kuritegude uurimisel?

Magistritöö eesmärgiks on välja töötada kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimiseks vajalike teadmisi ja oskusi süstematiseeriv kompetentsiraamistik ja esitada ettepanekud selle rakendusvõimaluste osas.

Eesmärgi saavutamiseks otsitakse vastuseid **uurimisküsimustele:**

1) Millised on ühiskonna digitaliseerumisest tingitud aktuaalsed väljakutsed kohaliku tasandi uurijatele digitaalse komponendiga kuritegude uurimisel?
2) Millised on digitaalse komponendiga kuriteod, mille lahendamisega tegelevad kohaliku tasandi politseiuurijad?
3) Kuidas süstematiseerida kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimiseks vajalikke teadmisi ja oskusi?
4) Kuidas hindavad PPA, Sisekaitseakadeemia ja prokuratuuri esindajad magistritöös välja töötatud kompetentsiraamistik asjakohasust ja rakendusvõimalusi?

Uurimisküsimustele vastuste leidmiseks on püstitatud **uurimisülesanded:**

1) Teadusallikatele põhinedes analüüsida ja süstematiseerida digitaalse komponendiga kuriteod ning nende uurimisel tekkinud väljakutsed ja kitsaskohad;
2) Analüüsida teoreetilised lähtekohad kompetentsiraamistik koostamiseks;
3) Välja töötada kohaliku tasandi uurijale digitaalse komponendiga kuritegude uurimiseks vajalik kompetentsiraamistik;
4) Viia läbi teoorias väja töötatud kompetentsiraamistikku valideeriv kvalitatiivne empiiriline uuring;
5) Teoreetilise kompetentsiraamistiku ja empiirilise uuringu tulemuste sünteesi alusel esitada PPA-le ja Sisekaitseakadeemiale ettepanekud magistritöös välja töötatud kompetentsiraamistiku rakendusvõimaluste osas.

Magistritöö on empiiriline uurimus ning empiirilise uuringu läbiviimiseks kasutatakse **juhtumiuuringu strateegiat,** mis sobib programmide, protsesside ja tegevuste uurimiseks, kus juhtum

on piiritletud aja ja tegevustega ning andmete kogumine toimub erinevate uurimisinstrumentide abil (Yin, 2003, p. 23; Creswell 2009, pp. 58, 227; Creswell & Poth, 2016, p. 74–75). Juhtumiks on kompetentsiraamistiku väljatöötamise ja valideerimise protsess.

Uurimisinstrumentideks on poolstruktureeritud ekspertintervjuud ja dokumendianalüüs (Flick, 2009, pp. 165, 255–259). Magistritöös välja töötatud kompetentsiraamistikku valideeritakse valdkonna asjatundjate ekspertintervjuude abil. Eesmärgistatud valimisse (Teddlie & Yu, 2007, pp. 77–79) kuuluvad 4 PPA strateegilise planeerimise tasandi eksperti, 3 Sisekaitseakadeemia õppeprogrammide arendamise ja valdkonna õppeainetega seotud eksperti ja 3 Põhja Ringkonnaprokuratuuri abiprokuröri, kelle ülesandeks on kogukonnakuritegude uurimise juhtimine. Dokumendianalüüsi mugavusvalimisse (Teddlie & Yu, 2007, pp. 77–79) valiti 10 teksti ja dokumenti, mis autori seisukohal sisaldavad uurimisküsimusele vastamiseks vajalikku informatsiooni kohaliku tasandi politseiuurija töö kirjelduse, kutsekvalifikatsiooni nõuete ja digitaalse komponendiga kuritegude uurimisel aktuaalsete kompetentside kohta. Dokumendianalüüsi valimisse kaastakse ka Eestis kasutusel olevad kompetentsiraamistiku koostamise metoodikaid sisaldavad dokumendid. Uuringu andmete analüüsimiseks kasutatakse **kvalitatiivset sisuanalüüsi** ja **kodeerimismeetodit** (Saldaňa, 2013, p. 22).

Magistritöö koosneb kahest peatükist: Esimeses peatükis esitatakse teoreetiline käsitlus aktuaalsetest väljakutsetest kohaliku tasandi uurijatele digitaalse komponendiga juhtumite uurimisel, digitaalse komponendiga kuritegude olemusest ning kompetentsimudeli väljatöötamise teooriast. Esimese peatüki lõpus jõutakse teoreetiliste materjalide alusel välja töötatud kompetentsiraamistikuni. Teine peatükk on pühendatud empiirilisele uuringule, mille raames analüüsitakse väljakutseid PPA kohaliku tasandi politseiuurijatele ning selleks vajalike kompetentside määratlemise ja arendamise praktikaid, võrreldes seda magistritöös välja töötatud kompetentsiraamistikuga. Uuringu ja teoreetilise kompetentsiraamistiku võrdluse ja sünteesi tulemustel tehtud järelduste alusel esitatakse ettepanekud kompetentsiraamistiku rakendusvõimaluste osas PPA-le ja Sisekaitseakadeemia.

1. ÜHISKONNA JA KURITEGEVUSE DIGITALISEERUMINE KOHALIKU TASANDI POLITSEIÜKSUSTE UURIJATE TÖÖ NING KOMPETENTSIDE PERSPEKTIIVIS

Käesoleva töö esimese peatüki ülesandeks on ette valmistada juhtumiuuringu teoreetiline käsitlus ja esitada juhtumi aspektid ja alateemad, mille alusel töötatakse välja kategooriad ja deduktiivsed koodid empiirilise uuringu käigus kogutavate andmete analüüsimiseks. Teadusallikate analüüs näitab seoseid erinevate kontseptuaalsete ideede vahel (Bryman, p. 2008, p. 57), millega piiritletakse juhtumiuuringu süsteemi. Teoreetilise peatüki koostamise metoodika on kirjeldatud metoodika ja valimi alapeatüki osas 2.1.1.

Teoreetilise peatüki esimene alapeatükk käsitleb väljakutseid kohalku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimisel ning annab ülevaate digitaalse komponendiga kuritegudest. Teises alapeatükis tuuakse välja politseiuurijatele digitaalse komponendiga kuritegude uurimiseks kompetentsiraamistiku konstrueerimiseks tarvilikke aspekte. Kolmandas alapeatükis sünteesitakse eeltoodu alusel kompetentsiraamistik.

1.1 Kuritegevuse mustrite muutused ühiskonna digitaliseerumise perspektiivis

Käesoleva alapeatüki ülesandeks on anda ülevaade digiajastuga kaasnenud kuritegevuse struktuuri muutustega kaasnenud väljakutsetest kohaliku tasandi politseiuurijatele ning digitaalse komponendiga kuritegude tüpoloogiatest. Peatükis otsitakse vastuseid kahele magistritöös püstitatud uurimisküsimusele:

1) Millised on ühiskonna digitaliseerumisest tingitud aktuaalsed väljakutsed kohaliku tasandi uurijatele digitaalse komponendiga juhtumite uurimisel?
2) Millised on digitaalse komponendiga kuriteod, mille lahendamisega tegelevad kohaliku tasandi politseiuurijad?

1.1.1 Kuritegevuse olemuse tehnoloogilistest muutustest tingitud väljakutsed kohaliku tasandi politseiüksuste uurijatele

Tänapäeva ühiskonda võib nimetada infoühiskonnaks, kuna IKT kasutusala on laienenud ka tavakasutaja tasemele. Internet, IKT ja sotsiaalmeedia kanalite küllus on oluliselt muutnud inimeste omavahelise suhtluse mustreid ja avaldanud mõju inimeste käitumisele (Grabosky, 2001, p. 244; Jewkes & Yar, 2011, p. 1; Holt & Bossler, 2016, pp. 2–5; Jarrahi & Eshraghi, 2019, p. 1051). Mobiiltehnoloogiate integreerimine internetti on veel enam suurendanud teabevahetuse ja kauplemise kõikehõlmavust inimeste elus (Holt ja Bossler, 2016, p. 2). Sampson (2014, p. 8) käsitleb digitaalset keskkonda sotsiaal-ruumilise dimensioonina, kus inimesed otsustavad elada, kaubelda, alustada ja lõpetada suhteid, suhelda, luua intellektuaalset omandit ja majanduslikku rikkust, panustada enesearengusse jms. Samas, see on ka keskkonnaks, kus inimesed võivad käituda mittekonventsionaalselt ja toime panna kuritegusid (Yar, 2005, p. 411; Wall, 2011, pp. 87, 100; Sampson, 2014, p. 8; Furnell & Dowling, 2019, p. 10; Lee, *et al*., 2021, p. 20).

Varasem ühiskonna digitaliseerumisega seonduv diskursus (Dunn & Brunner 2007, pp. 1–18 ref Dunn Cavelty, 2010, p. 181; Dunn Cavelty, 2010, p. 196) puudutas rahvusvahelist mõõdet ning enamasti riigi julgeolekule rahvusvahelisest kuritegevusest tulenevaid ohtusid. Käesoleval ajal digitaalse keskkonna võimaluste suurendamise ja kõigile inimestele kättesaadavuse valguses on digitaalse komponendiga kuriteod nihkunud indiviidi ja kogukondade tasemele, kelle turvalisuse tagamisega tegelevad kohaliku tasandi politseiüksused. (vt Dodge, & Burruss, 2020, p. 339) Nende muutuste valguses tuleb iga tasandi politseiuurijatel kohaneda digiajastu väljakutsetega kuritegude uurimise valdkonnas ja kohandada vastavalt sellele oma strateegiat, taktikat ning töövõtteid.

Uuringud (Hadlington *et al*., 2021, De Paoli, *et al*., 2021, p. 1446) on näidanud, et mitmes riigis tajuvad spetsialiseeritud (sageli kõrgtehnoloogilistele kuritegudele) üksustes töötavad ametnikud ja esmatasandi ametnikud sarnaseid väljakutseid digitaalse komponendiga kuritegude uurimisel. Varasemast Madalmaade uuringust (Leukfeldt, *et al*., 2013, pp. 12–13), mille tulemusi ja järeldusi kinnitas ka hiljem Austraalias läbi viidud uuring (Harkin, *et al*., 2018, p. 535–536) selgub, et mõne digitaalse komponendiga kuriteo uurimise keerukus võib ületada kohaliku tasandi politseiüksuste teadmisi, kompetentse ja tehnilisi ressursse, mille tõttu muutub kurjategija tuvastamine eriti raskeks ülesandeks.

Kuritegevuse struktuuri muutuste trendid viitavad sellele, et digitaalne komponent esineb tihti traditsiooniliste kuritegude sooritamisel. Samas teistest uuringutest selgub, et kohaliku tasandi üksuste politseinikud ei ole üldiselt huvitatud digitaalse komponendiga kuritegudele reageerimisest ja tunnevad end veebipõhiste juhtumite uurimisel vähem kindlalt, kui traditsiooniliste kuritegude uurimise korral (Bossler & Holt, 2012, p. 165; Lee, *at al.* 2021, pp. 38–39). Johnson, *et al.*, (2020, pp. 445–446) tõid välja, et kohaliku tasandi politseiuurijad tunnetavad, et digitaalse komponendiga kuritegude uurimisel on tugevaid erinevusi võrreldes traditsiooniliste kuritegude uurimise lähenemisega, mille tõttu peaks see olema spetsialiseeritud üksuste ülesanneteks. Selline lähenemine aga ei toeta ühiskonna vajadusi. Kuna IKT lahenduste kasutamisest on saanud elu igapäevane osa, siis on üheks ühiskonna ootuseks ka kohaliku tasandi politseiuurijate professionaalsus digitaalse komponendiga kuritegude uurimisel (Sampson, 2014, pp. 1, 5–6, Dodge & Burruss, 2020, p. 339).

Digitaalne keskkond tekitab uusi võimalusi nii juba varem eksisteerinud kui ka uute kuritegude toimepanemiseks (Grabosky, 2001, p. 248; Wall, 2007, pp. 185–186 tsit Caneppele & Aebi, 2019, pp. 70–71; Holt & Bossler, 2016 p. 2; Caneppele & Aebi, 2019, p. 75) ja võimaldab kurjategijatel kahjustada ohvrite õigushüvesid ning põhjustada isikutele ja organisatsioonidele kahju üle maailma, ületades riigipiire ja jurisdiktsioone (Sampson, 2014, pp. 1, 5–6; Johnson, *et al.*, 2021, p. 430). IKT on vahendiks ja keskkonnaks digitaalse komponendiga kuritegude toimepanemiseks või traditsiooniliste kuritegude kahjuliku efekti võimestajaks (Yar, 2005, p. 411; Wall, 2011, pp. 87, 100; Furnell & Dowling, 2019, p. 10). Digitaalse komponendiga lähisuhtevägivalla kuritegude näitel väidavad O´Hara, *et al.* (2020, pp. 1–2), et piir traditsiooniliste füüsiliste ja veebipõhiste kuritegude vahel hägustub, mistõttu kriminaaluurimine ja süüdistuse esitamine sõltub üha enam usaldusväärsetest kohtukõlbulikest digitaalsetest tõenditest. Pealegi, erinevalt traditsioonilistest isikuvastastest kuritegudest, nagu füüsiline ja seksuaalne rünnak, iseloomustab küberkuritegusid kurjategija digikompetentsus (Yar 2005, p. 411; Johnson, *et al*., 2020, pp. 430, 432), territooriumiülesus (Sampson, 2014, pp. 1, 5–6; Bossler & Holt, 2012, p. 167; Dodge & Burruss, 2020, p. 339) ja kurjategija anonüümsuse säilitamise võimalused (Furnel & Dowling, 2019, p. 13; Dodge & Burruss, 2020, p. 339; Curtis & Oxburg, 2022, p. 5).

Teadlaste ja politseiametnike sõnul on kohalikul tasandil digitaalse komponendiga kuritegude uurimist raskendanud sellised probleemid, nagu küberkuritegevuse ühtse definitsiooni puudumine, terminite mitmekesisus ja nende erinev tõlgendamine (Leukfeldt, *et. al*., 2013, p. 3; Furnell ja Dowling, 2019;

Caneppele & Aebi, 2019, pp. 69–70; Curtis & Oxburg, 2022, p. 1, De Paoli, *et al*., 2021 pp. 1444–1445); kohaliku tasandi politseiüksuste teadmiste ja metoodikate puudulikkus IKT hõlbustatud kuritegevuse uurimiseks (Leukfeldt, *et al*., 2013; Holt, *et al*. 2017 ref O'Shea, 2022, p. 12; Harkin, *et al*., 2018; Dodge & Burruss, 2020, p. 339; Lee, *et al.*, 2021; O'Shea, 2022, p. 12; Johnson, *et al.*, 2020); suutmatus hankida ja arendada ressursside puudulikkuse tõttu nende kuritegude uurimiseks vajalikku tehnoloogiat ning raskused ametnike koolitamisel (Dodge & Burruss, 2020, pp. 339, 347; Lee, *et al.*, 2021; O'Shea, *et al*., 2022, p. 3); juhtkonna toetuse puudulikkus (Johnson, *et al.*, 2020, p. 444). Järgnevalt käsitletakse neid kitsaskohti ja väljakutseid täpsemalt ning jaotatakse need viide kategooriasse.

Esiteks valmistab probleeme küberkuritegevusega seotud **teadmiste puudulikkus või ebajärjekindlus** (De Paoli, *et al*., 2021, p. 1430). Digitaalse komponendiga juhtumite uurimine eeldab politseiuurijate nõuetekohast ettevalmistust ja kompetentse. Nendega on kohaliku tasandi politseiüksustel probleeme üle maailma. Perniku (2019) ülevaatest Eesti, Soome, Saksamaa, Hollandi ja Norra politsei kõrgkoolide küberturvalisuse alasest haridusest, mille üheks alateemadest on ka digitaalse komponendiga kuritegude uurimine ja digitaalsete tõendite käsitlemine, selgus, et küberturvalisuse õppekavade tase Eestis ja välisriikides on ebaühtlane. Artikli ilmumise ajal, s.o 2019. aastal tehti ettepanek Sisekaitseakadeemias vastava õppekava väljatöötamiseks. (Pernik, 2019, pp. 77, 96–97) Politseikadettide digitaalse komponendiga kuritegude uurimiseks vajalike oskuste arendamisele suunatud õppekava muudatused hakati rakendama alates 2020/2021 õppeaastast, täiendusõppe kava on arendamisel (Sisekaitseakadeemia 18.12.2023 e-kiri, autori valduses).

Dodge & Burruss (2020, p. 339) juhivad samuti tähelepanu sellele, et vaatamata suurenenud nõudlusele digitaalse komponendiga juhtumitele reageerimise süsteemse lähenemise järgi puudub selgus selleks kohaliku tasandi politsejõududele vajalike ettevalmistuse, vahendite, täiendava koolituse ja adekvaatse reageerimisvõime hindamise osas. Lee, *et al*. (2021, p. 38–39), analüüsides Inglismaal ja Walesis kohaliku tasandi politseinike hinnanguid enda ettevalmistusele digitaalse komponendiga kuritegude uurimise ja juhtumite käsitlemise osas leiavad, et politseinikud omavad mõningaid otseseid kogemusi nende juhtumitega tegelemisel, kuid üle kahe kolmandiku valimi esindajatest märkis, et nad ei ole saanud koolitust veebipõhiste kuriteojuhtumite käsitlemiseks. Ühtlasi viidatakse politsei teemakohaste koolitusprogrammide väljatöötamise vajalikkusele, mis on kooskõlas ka Perniku (2019) küberturvalisuse õppe- ja koolituskavade uuringu tulemustest lähtuvalt tehtud ettepanekutega. Lee, *et*

al., (2021, pp. 38–39) uuringu üheks järelduseks on see, et kohaliku tasandi politseinikud leiavad, et digitaliseerumisest tingitud muutused on nende töös pigem tekitanud probleeme kui aidanud. De Paoli, *et al.*, (2021, p. 1446) uuringus seitsme Euroopa riigi ja Kanada küberkuritegevuse spetsialistidega läbi viidud ekspertintervjuude analüüs näitas samuti, et politseinikele pakutava ja planeerimisjärgus oleva koolituse kvaliteet ja ulatus ei ole piisav. See järeldus on kooskõlas ka varasemate uurimistulemustega (Hadlington *et al.,* 2021).

Üheks politsei erialaste teadmiste ja kompetentsusega tugevalt seotud teaduseks ja õppeaineks on kriminoloogia. Stratton, *et al.* (2017, p. 27) väidavad, et arvuti- ja küberkuritegusid ei käsitleta piisavalt ja täielikult kaasaaegse kriminoloogia distsipliini raames. Samas, digiühiskonna kriminoloogia nende autorite käsitluses on kiiresti arenev teadusvaldkond, mis rakendab kriminoloogilist, sotsiaalset, kultuurilist ja tehnilist teooriat ning meetodeid kuritegevuse, kõrvalekallete ja õigusemõistmise uurimiseks digiühiskonnas. (Stratton, *et al.*, 2017, p. 27) Eespool toodu kokku võttes võib järeldada, et kohalikul tasandi politseil puudub terviklik ja süsteemne teadmine digitaalse keskkonna toimimisest, digitaalse komponendiga juhtumite ja kuritegude võimalikest määratlustest, olemusest ning tüpoloogiatest.

Teiseks väljakutseks on **õiguslikud küsimused**, millega politsei küberkuritegevusega võitlemisel silmitsi seisab (De Paoli, *et al.*, 2021, p. 1430). Lisaks koondatakse selle valdkonna alla ka **protseduurilisi küsimusi, mis on seotud kohaliku tasandi politseiüksuste territoriaalsuse printsiibiga**. Õiguslikke probleeme on nii siseriiklikul kui rahvusvahelise koostöö tasandil ning need kätkevad nii materiaal- kui menetlusõigust (sh tõendite käsitlemise reegleid). Karie & Venter (2015, p. 8–10, 16) taksonoomia kohaselt on õigussüsteemi ja õiguskaitsealased väljakutsed seotud jurisdiktsiooni probleemidega; digitaalse komponendiga kuritegude menetlemise käigus süüdistuse esitamise protseduuridega; digitaalkriminalistika ja kohtuekspertiisi vahendite ja tehnikate lubatavuse küsimustega; kohtu ebapiisava toetusega kriminaal- või tsiviilvastutusele võtmiseks; eetiliste ja andmekaitsega seotud küsimustega. Käesolevas töös õiguslikke aspekte põhjalikumalt ei käsitleta, kuna seda temaatikat on mitmes magistritöös juba uuritud (vt Kaha, 2017; Laats, 2017).

Lisaks De Paoli, *et al*., (2021, p. 1430) poolt tähelepanu juhitud õiguslikele küsimustele on täiendavaks probleemiks veel kohaliku tasandi politseiüksuste töö protseduuride ja põhimõtete mittevastavus digitaalse komponendiga kuritegude piiriülesele iseloomule (vt. Burns *et al*., 2004, pp. 477, 488–491; Johnson, *et al*., 2020, p. 30; O'Shea, *et al*., 2022, p. 12). Digitaalse komponendiga kuritegude olemus

ei ole sageli vastavuses territoriaalsuse põhimõttel aastaid toiminud kohaliku tasandi uurijate töökorraldusega (Holt & Bossler, 2016, p. 17), mille kohaselt kohaliku tasandi politseiüksused vastutavad nende kuritegude ennetamise ja uurimise eest, milles nii kurjategija kui ohver on konkreetse politseiüksuse teenindusterritooriumi elanikud. Ka Eestis on politsei regionaalsete üksuste töökorraldus seotud konkreetse teenindusterritooriumiga (PPVS § 5; PPA, 2022). IKT lahenduste kättesaadavus ja nende hea kasutamise oskus aga suurendab kurjategijate võimekust ning õigusrikkumiste piiriülest toimepanemist (Johnson, *et al*., 2020, pp. 430, 432). Tihti ei kattu nende kuritegude uurimine ja juhtumite lahendamine territoriaalsuse põhimõtega (vt. Burns, *et al*., 2004, pp. 477, 488–491; Johnson, *et al*., 2020, p. 30; O'Shea, *et al*., 2022, p. 12). Kurjategijad, ohvrid, kuriteo toimepanemiseks kasutatud vahendid ja tegevused, kuritegelikul teel saadud kasum ja muud kuriteo tagajärjed võivad füüsiliselt asuda teineteisest kaugel, erinevates füüsilistes asukohtades ja isegi riikides (Johnson, *et al*., 2020, pp. 430, 432), mis eeldab rahvusvahelist koostööd, selle põhimõtete ja takistuste tundmist.

Kolmandaks probleemiks on (**digitaal-)kriminalistika väljakutse**, mis on seotud küberkuritegevuse lahendamiseks vajalike oskuste, koolituse ja varustusega (De Paoli, *et al*., 2021, p. 1430). Küberkuritegevus on tihedalt seotud digitaalsete tõendite, tehnoloogilise innovatsiooni ja infrastruktuuri ning suurandmete küsimustega (Moloney, *et al*., 2022), mistõttu selliste digitaalse komponendiga kuriteotunnustega juhtumite lahendamine on kohaliku tasandi õiguskaitseasutuste jaoks tõsine väljakutse.

Kuriteosündmuse uurimine on spetsiifiline kognitiivne tegevus, mille eesmärgiks on kuriteo asjaolude ja sellega seotud muude asjaolude väljaselgitamine, et anda uuritavale teole karistusõiguslik hinnang (Терехович, *et al*., 2019, lk 60, 72). Nende ülesannete lahendamisega tegeleb kriminalistika - „teadus tõendite tekkimise, kogumise, hindamise ja kasutamise seaduspärasustest ja nende seaduspärasuste tunnetamisel põhinevatest tõendite uurimise vahenditest ja meetoditest" (Öpik, 2009, lk 71). Kriminalistika moodustavad neli punkti, milleks on: 1) kuriteo toimepanemise mehhanismi seaduspärasused; 2) kuriteojälgede kujunemise seaduspärasused; 3) tõendite kogumise, uurimise, hindamise ja kasutamise seaduspärasused; 4) tõendite avastamise, kogumise, talletamise ja hindamise erivahendid, võtted ja meetodid (Белкин, 1987, с. 59, 1997, с. 112 ref Öpik, 2009, lk 71–72).

Digitaalses keskkonnas kuriteo kohta tõendite kogumine ja talletamine on spetsiifilisem, kuna digitaalse komponendiga kuriteosündmuse uurimiseks tuleb mõista digitaalse keskkonna toimeloogikat ja IKT vahendusel toime pandud tegude eripära. Digitaalse tõendi uuringu käigus

kasutatakse teaduslikke põhimõtteid ja käivitatakse protsesse elektrooniliselt salvestatud teabe analüüsimiseks ja konkreetse juhtumini viinud sündmuste jada kindlaksmääramiseks süüteomenetluse raames (Raghavan, 2013, p. 92). Seega, iga digitaalse tõendi uuringu staadium kätkeb menetlusi, reegleid ja nüansse, mistõttu tuleb määratleda, millised on politseiuurija roll ja ülesanded tõendusmaterjali käsitlemises.

Pamphlet (2010, p. 8) määratleb küberruumi digitaalse keskkonnana, mis koosneb kolmest dimensioonist või kihist: füüsilisest, loogilisest ja sotsiaalsest, ning viiest komponendist: geograafilisest asukohast, loogilisest võrgust, füüsilisest võrgust, isikust ja veebi-identiteedist (vt tabel 1). Nimelt, koosneb füüsiline kiht võrke toetavast riistvarast ja infrastruktuurist (internetist) ning riistvara geograafilisest asukohast. Loogiline kiht koosneb kõigist seadmetest, mis on ühendatud arvutivõrku. Sotsiaalne kiht koosneb inimlikest ja kognitiivsetest aspektidest, sealhulgas võrkude sees ja vahel suhtlevate inimeste digitaalsetest ja tegelikest identiteetidest (Pamphlet, 2010, p. 8–9). Seega digitaalse komponendiga kuriteosündmuse kohta informatsiooni ja tõendeid kogudes ja fikseerides tuleb arvestada kõigi nende dimensioonidega.

Tabel 1. Digitaalse keskkonna kihid ja komponendid (Pamphlet, 2010 p. 8 alusel autori koostatud)

KÜBERRUUM = DIGITAALNE KESKKOND		
Füüsiline kiht/ dimensioon	Loogiline kiht/dimensioon	Sotsiaalne kiht/dimensioon
➢ Geograafilised komponendid ➢ Füüsiline asukohtade võrgustik	➢ (toime-) loogiline võrgu komponent	➢ Isiku komponent ➢ Veebi identiteet (teisisõnu digitaalse identiteedi komponent)

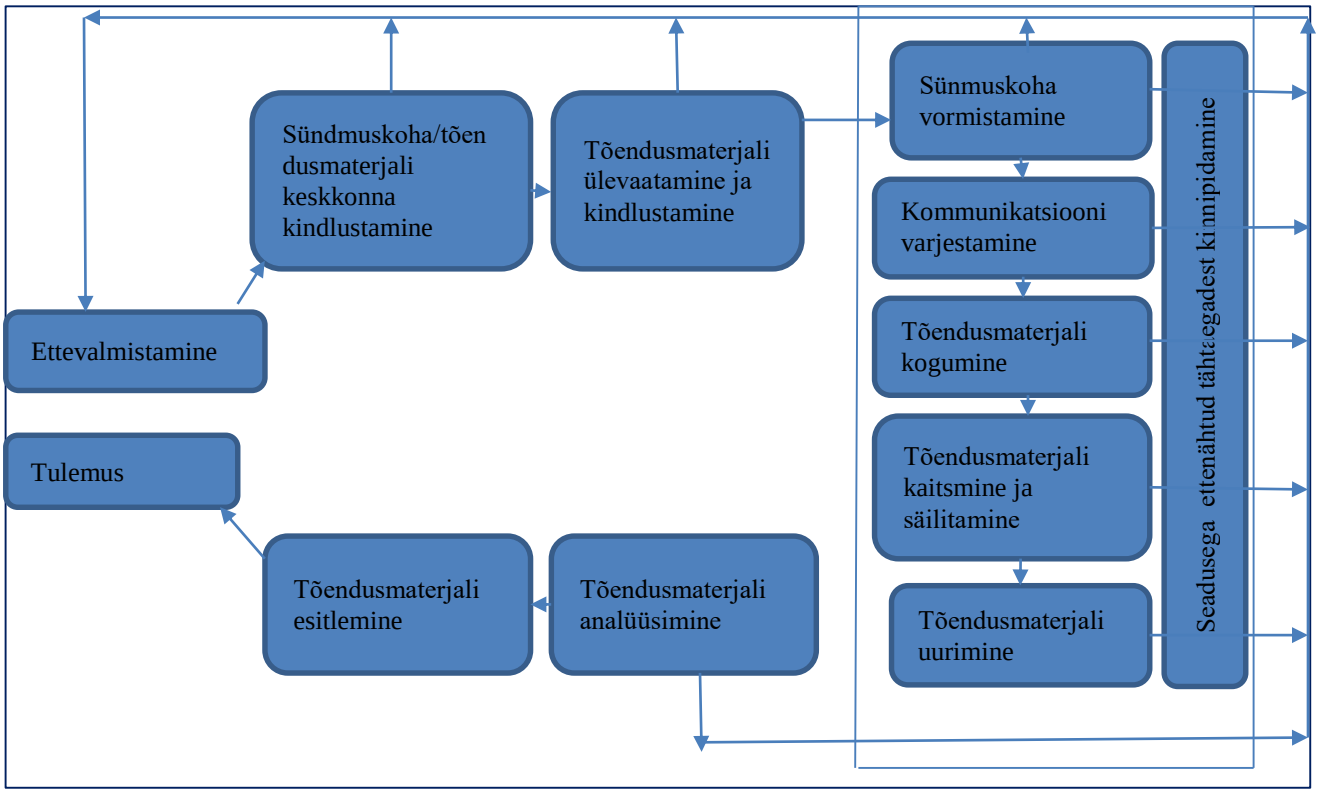
Digitaalsete tõendite kogumist ja talletamist käsitleb digitaalkriminalistika (ingl *digital forensics*). Tegemist on kriminalistika valdkonnaga, mis on IKT arengu ja maailma digitaliseerumise taustal viimase kolmekümne aasta jooksul välja kujunenud iseseisvaks haruks (Pollitt, 2010, pp. 12–14). Jones, *et al*., 2014 (p. 55) praktilise käsitluse kohaselt, mis ühtlasi langeb kokku ka Eesti eksperdite (Lall, *et al.*, 2021) seisukohtadega, on digitaalkriminalistika „kohtuekspertiisi haru, mis keskendub arvutisüsteemis, digiseadmes või muul andmekandjal salvestatud andmete tuvastamisele, hankimisele, töötlemisele, analüüsile ja aruandlusele". Maailmas kasvav teadusallikate ja praktikutele ette nähtud kirjanduse hulk viitab digitaalkriminalistika tähtsusele kriminaal- ja tsiviilkohtumenetluses (Pollitt,

2010, pp. 12–14; Lawton *et al*., 2014; Rogers 2017; Vincze, 2016; Belshaw, 2019; Wilson-Kovacs, 2019; Lall, *et al*., 2021). Eesti kriminalistika valdkonna eksperdid (Lall, *et al*., 2021), kes on koostanud ülevaate digitaalkriminalistika ja digitaalse kohtuekspertiisi hetkeseisust, väidavad et digitaalkriminalistika mõiste määratlemiseks ühte konkreetset terminit ei ole, kuid nimetatud valdkonna ülesanneteks on teaduslikke meetodite kasutamine digitaalsete tõendite lubatavuse tagamiseks kriminaalmenetluses. Tegemist menetlustehnika valdkonnaga ning tegevused on suunatud digitaalsete andmete avastamisele, analüüsimisele ja esitamisele selliselt, et neid saaks kasutada tõendina kohtumenetluses (Lall, *et al*., 2021).

Siit võib järeldada, et politsei tööde kirjeluses käsitletakse digitaalkriminalistikat kui menetlustehnikat ja eriteadmisi (sh tehnilisi, IT-spetsiifilisi) ja -tingimusi nõudvat distsipliini. Samas, enne tõendi digitaalkriminalistika laborisse jõudmist tegeleb sellega politseiuurija, kellel peab olema rida kompetentse digitaalse tõendi tuvastamiseks, talletamiseks, muude tõendite konteksti asetamiseks ja analüüsimiseks ning nendel eesmärkidel koostöö tegemiseks digitaalkriminalistika eksperdiga. Kuna digitaalsete tõendite osakaal süüteomenetlustes suureneb, sõltuvad õiguskaitseasutused üha rohkem tõenditele usaldusväärsuse ja õiglase kohtumõistmise nõuetele vastavuse tagamiseks digitaalkriminalistika meetoditest (Council of Europe, 2022). Seetõttu väidavad mõned autorid (Jones, *et al.*, 2014, p. 136; Humphries, *et al.*, 2021), et lisaks infotehnoloogilise ekspertiisi ja digitaalkriminalistika spetsialistide kompetentsile on vaja suurendada ka uurijate, esmareageerijate, kohtunike ja prokuröride teadlikkust ja kompetentsust digitaalsete tõendite käsitlemiseks.

Digitaalsed andmed on kergesti mõjutatavad ning ootus, et digitaalseid tõendeid võib koguda üksnes selleks ettevalmistatud ja eriteadmistega isik, oleks loogiline. Samas, Eesti kriminaalmenetluse seadustik ei reguleeri nõudeid menetlejale selleks vajaliku eriettevalmistuse osas analoogselt lastega menetlustoimingute läbiviimise tingimuste erisuste sätestamisega (Laurits, 2016, pp. 118–119, KrMS § 70). Sõltuvalt juhtumi ja digitaalse tõendi keerukusest ja mahust võib tegemist olla keerulise ja kauakestva protsessiga, kuhu võivad olla kaasatud digikriminalist ja kohtuekspert. Samas on ka selliseid juhtumeid, kus politseiuurija peaks ise toime tulema digitaalse tõendi tuvastamise ja talletamisega. Allpool on välja toodud Agarwal, *et al.,* (2011) digitaalse tõendi käsitluse skeem, mille väljatöötamisel analüüsiti ja sünteesiti erinevaid digitaalse tõendusmaterjali digitaalkriminalistikalise uurimise mudeleid (vt joonist 1, käesolev töö, lk 20). Skeemist nähtub, et digitaalse tõendi käsitlemine

peab olema hoolikalt ette valmistatud ja läbi mõeldud, mis on võimalik üksnes juhul, kui uurijal on süsteemne (baas-)teadmine digitaalse keskkonna toimeloogikast ja digitaalkriminalistika põhimõtetest.



Joonis 1. Digitaalse tõendusmaterjali käsitlemise protsess (Agarwal, *et al*., 2011, p. 124)

Neljandaks digitaalse komponendiga kuritegude uurimisel **ilmnenud väljakutseks on politsei organisatsioonisiseste takistuste ületamine**. Varasemate uuringute autorid märkisid, et sageli ei näe politsei juhtivtöötajad küberkuritegevust "päris" politseitööna (Jewkes ja Andrews, 2005, pp. 50–51, 53; Holt, *et al*., 2010 ref De Paoli, *et al*., 2020; Bossler & Holt, 2012). Kümmekond aastat hiljem juhivad Johnson, *et al*., (2020, p. 451) ikka tähelepanu sellele, et kõigil õigussüsteemi toimijatel, sh Inglismaa ja Walesi politseil, on raske kohaneda teaduse ja IKT arenguga ning ajakohaselt reageerida kriminoloogilistele muutustele. Vaatamata küberkuritegevusele reageerimiseks teadmiste, tegevuste, koostöö ja investeeringute laiendamisele, takistavad funktsionaalset kohanemisprotsessi ka sisemised institutsioonilised ja kultuurilised politseiorganisatsiooni probleemid. Nendeks on sügavalt juurdunud süüdistuskultuurina väljenduv riskide vältimise kultuur politseis, mis ohustab individuaalset karjääri ja võimalusi panustada uurimistöösse, olenemata sellest, kas välditav risk ja sellest tulenev süüdistus on isiklik hinnang või käitumine, õiguslik viga või oht mainele (nii isiklik kui organisatsiooniline). Riskide vältimine on juhtidele omane ka tavapärase politseitöö puhul, kuid küberkuritegevuse puhul on see

tendents tugevam, kuna tegemist on ebatraditsioonilise keskkonnaga ja mittetraditsioonilise politseitöö tavade ja mustritega. (Johnson *et al.*, 2020 p. 444) .

1.1.2 Digitaalse komponendiga kuritegevuse määratlus ja kategooriad

Analüüsides küber-, arvuti- ja digitaalse komponendiga kuritegevuse määratlusi, selgub, et valdkonnas valitseb terminite ja nende tähenduste mitmekesisus. Seda kinnitab ka üks värskematest uuringutest (De Paoli, *et al*., 2021, p. 1444–1445), milles intervjueeriti 13 küberkuritegude uurimise spetsialisti ja politsei eksperti Kanadast, Soomest, Taanist, Norrast, Rootsist, Madalmaadest, Poolast ja Šotimaast. Nimetatud uuringuga toodi välja, et politseiasutustel on kasutusel mitmeid alternatiivseid küberkuritegude määratlusi, mis muudab raskeks aruandlus-, registreerimis- ja uurimisstatistika süsteemse võrdlemise nii riigisiseselt kui riigiti. See omakorda viib muuhulgas politseiametnike kompetentsuse hindamiseks ja selle suurendamiseks vajalike strateegiate ja instrumentide väljatöötamise puudulikkuseni. De Paoli, *et al.*, 2021 väidavad, et tehtud on vähe edusamme alatest esmaste sisukate uuringute ajast (Holt *et al*., 2015; Stambaugh *et al*., 2001) ja puudub sisuline politsei statistika küberkuritegude osas.

Käesolevas töös süstematiseeritakse digitaalse komponendiga kuriteo mõiste sisustamiseks küberkuritegude tüpoloogiaid. Kuigi varasemalt tehti vahet küberkuritegevuse ja IKT abil toime pandud kuritegude vahel asjakohase taksonoomia koostamise eesmärgil, siis IKT arengu ja kiire leviku perspektiivis hõlmavad nüüd paljud kuriteovormid digitaalset komponenti (Furnell & Dowling, 2019, p. 10) ning IKT ja digitaalse keskkonna kasutamine kuritegude toimepanemiseks on muutunud tavaliseks (Vincze, 2016, p. 183; Tarter, 2017 p. 213; Holt & Bossler, 2016, pp. 2–4; Pernik, 2019, p.71–72; Council of Europe, 2022). Ülevaade küberkuritegude iseloomust ja tüpoloogiatest aitab paremini mõista, milliste digitaalse kuritegude liikide uurimine kuulub kohaliku tasandi (Eesti konteksti kohaselt politseijaoskondade – vt PPVS § 5 lg 3) politseiuurijate menetluspädevusse. Järgnevalt esitatakse ülevaade digitaalse komponendiga kuritegude tüpoloogiatest, mida koondatakse kokkuvõtva tabeli kujul (Tabel 2, käesolev töö, lk 24).

Ühena esimestest võttis termini „küberkuritegevus“ kasutusele Wall (1998, pp. 202–203), pidades selle all silmas interneti abil toime pandud kuritegusid, millised ta liigitas teo iseloomu tunnuste alusel nelja gruppi. Esimese gruppi moodustavad **küber-sissetungid** (ingl k *cybertrespass*), mis seisnevad loata tungimises kaitstud küberruumi ning hõlmavad tegusid alates kahjutust sissetungist kuni riikide

vahelise infosõjani. Sinna kuuluvad samuti kübervandalism, spionaaž ja terrorism. Teisse gruppi kuuluvad **kübervargused** (ingl k *cyber thefts*), mis viitab erinevatele digitaalses keskkonnas toime pandud omastamisviisidele. Eristatakse kolme liiki kübervargusi: küberkrediidi, küberraha ja intellektuaalse omandi omastamisi. Kolmas grupp on **küber-rõvedused** (ingl k *cyberobscenity*), mis seisnevad ropu ja sündsusetu sisuga materjalidega kauplemises küberruumis, kuhu näiteks liigitub lapsporno. Küberrõveduste kohased arusaamad ja määratlused võivad eri õigusruumides olla erinevad. Neljas rühm on **kübervägivald** (ingl k *cyberviolence*), mis kirjeldab digitaalses keskkonnas indiviidile või sotsiaalsele grupile kuritegelikku vägivaldset mõju avaldavaid viise. Selline tegevus ei pea väljenduma otseses füüsilises vägivallas, piisab sellest, kui ohver tunnetab sellist tegevust vägivallana või sellega ähvardamisena. Kübervägivalla näideteks on küberjälitamine (Eesti kontekstis tegemist on ahistava jälitamise vormidega), vihakõne ja pommiähvardus (Wall, 1998, pp. 202–203).

Wall (2007, p. 185 ref Caneppele & Aebi, 2019, pp. 70–71) liigitab küberkuritegevust lähtuvalt IKT rollist teo toimepanemisel kolmeks võimaluste rühmaks. Esimesed kaks võimaluste rühma on seotud traditsiooniliste kuritegudega, mille toimepanemiseks kasutavad kurjategijad IKT ja digitaalset keskkonda oma tegude tõhustamiseks (nt kasutades suhtlemiseks selliseid rakendusi nagu Whatsapp või Google kaardid, et enne kuriteo toimepanemist kontrollida asukohta) või võimestavad tegude ulatust ja tagajärgi, kasutades ära uusi veebipõhiseid võimalusi (nt finantspettused, küberjälitamine, küberkiusamine, lapsporno internetis). Teine võimaluste rühm vastab „kolmanda põlvkonna tõelistele küberkuritegudele /.../, mille toimepanemine on võimalik üksnes digitaalses keskkonnas (nt intellektuaalomandi vargused internetis, spämmimine)“ (Wall, 2007, pp. 185–186 tsit Caneppele & Aebi, 2019, pp. 70–71) Seega, rõhutas Wall (2007) küberkuritegude klassifitseerimisel IKT rolli *modus operandi* kirjeldamisel, liigitades neid **küber-seotud** (ingl k *cyber-related*), **küber-põhiseks** (ingl k *cyber-enabled*) ning **küber-sõltuvateks** (ingl k *cyber-dependent*) kuritegudeks, kusjuures viimased moodustavad nn ehtsate küberkuritegude kategooria, mille toimepanemine on võimalik üksnes IKT vahendusel ja digitaalses keskkonnas (Wall, 2007 ref Akdemir & Lawless, 2020, pp. 1667–1668).

Leukfeldt, *et al.*, (2013, p. 3), McGuire & Dowling (2013, p. 4), Suurbritannia tõsise ja organiseeritud kuritegevuse vastane strateegia (Home Office, 2013, p. 18); Furnell & Dowling, (2019, p. 2) ja Caneppele & Aebi, (2019, p. 71) määratlevad küberkuritegevust samuti kui kõikvõimalikke kuritegusid, mille puhul IKT mängib kuriteo toimepanemisel olulist rolli, kusjuures eristatakse kahte

kategooriat. Esimesse kategooriasse kuuluvad kitsamas tähenduses **küberkuriteod**, mille puhul on IKT nii vahendiks kui sihtmärgiks. Teise kategooriasse kuuluvad aga laiemas tähenduses **digitaalse komponendiga kuriteod**, mille puhul on IKT kuriteo toimepanemisel põhimõtteliselt oluline (nt digitaalne keskkond on teo toimepanemise vahendiks), kuid ei ole sihtmärgiks. Esimese kategooria puhul on tegemist **küber-sõltuvate kuritegudega**, mida saab toime panna ainult arvuti, arvutivõrgu või muu IKT abil. Ründeobjektideks on peamiselt arvutid või võrguressursid, kuigi rünnakutel võib olla ka teiseseid tagajärgi, näiteks pettus. Nende tegude hulka kuuluvad viiruste ja muu pahatahtliku tarkvara levitamine, häkkimine ja DDoS rünnakud. **Küber-põhised kuriteod** on traditsioonilised kuriteod, mille ulatust ja tagajärge võimestatakse digiseadmete ja IKT kasutamise tulemusel. Erinevalt kübersõltuvatest kuritegudest võib neid toime panna ka ilma IKT kasutamiseta. Näidetena võib tuua pettused, sh andmepüük ja muud võrgupettused, vargused ja laste vastu suunatud seksuaalkuriteod. (Home Office, 2013, p. 22; Furnell & Dowling, 2019, p. 2)

Caneppele & Aebi (2019, p. 71) täiendavad, et eespool toodud küberkuritegevuse klassifikatsioonid vajavad siiski täpsustamist ja täiendamist, kuna küberkuritegevus võib omandada hübriidvorme ja kombineerida veebipõhiseid ja võrguväliseid käitumisviise. Nimelt, kaasaegse kuritegevuse liigitamisel tuleb eristada **veebiväliseid kuritegusid** ehk teisisõnu traditsioonilisi kuritegusid, **hübriidkuritegusid**, mis ühendavad veebi- ja vebivälist komponenti, ning **küberkuritegusid**, mille toimepnemine on võimalik üksnes internetis. Isikuvastaste kuritegude valdkonna võrguväliste käitumisviiside illustreerimiseks tuuakse küberkiusamise või -seksuaalse ahistamise näiteid, mille puhul võib osa kurjategija ahistava käitumise episoode toimuda ka füüsilises keskkonnas. (Caneppele & Aebi 2019, p. 71)

Digitaalne keskkond hõlbustab inimeste omavahelist seotust ja suhtlemist ning suurendab lähisuhtevägivalla (Dragiewicz *et al.*, 2018; Yar & Drew, 2019) või muude naistevastaste vägivalla tegude toimepanemise vahendite valikuid või võimestab ohvrit kahjustavat efekti (Yar, 2005, p. 411; Henry & Powell, 2015, p. 759; Yar & Drew, 2019). Mõnel veebipõhisel varavastasel kuriteol, nagu identiteedivargusel või krediitkaardipettusel, on sageli ka veebiväline komponent, mis on seotud viisiga, kuidas hangitakse kuriteo toimepanemiseks kasutatav teave. Kurjategijal võib olla juurdepääs sellele teabele nn „prügikastisukeldumise“, postkastidest vargusest või sugulaste isikuandmete paberdokumentide varastamise kaudu (Allison *et al.*, 2005, p. 19; Copes & Vieratis, 2009, pp. 245–250; White & Fisher, 2008, p. 3; Morris, 2010, pp. 186, 193–196; Tcherni *et al.*, 2016, p. 892).

Küberkuritegevuse uurimise ja digitaalsete tõendite käsitlemise ühtsed rahvusvahelised standardid on toodud Euroopa Nõukogu Arvutikuritegude Vastases Konventsioonis (Budapesti Konventsioon), mis võeti vastu 23.11.2001.a Budapestis ning Eesti ratifitseeris selle 2004. aastal. Konventsiooniga on ühinenud 66 riiki, sh 26 EL liikmesriiki. (Paukštys, 2021; Council of Europe, 2022) Vastavalt Euroopa Nõukogu (edaspidi EN) definitsioonile küberkuritegevuseks on arvutisüsteemide vastu suunatud ja nende abil toime pandud õigusrikkumised, kuid lisaks sellele rõhutatakse, et iga kuritegu võib hõlmata arvutisüsteemis asuvaid tõendeid, mida vajatakse kriminaalmenetluse käigus. (Council of Europe, 2022) Sellest võib järeldada, et konventsioon lähtub ehtsa küberkuritegevuse määratlusest (**küberpõhised** teod) ja liigitab küberkuritegusid nelja valdkonda. Esimesse valdkonda kuuluvad arvutiandmete ja -süsteemide konfidentsiaalsuse, terviklikkuse ja kättesaadavuse vastased õigusrikkumised (nt häkkimine); teise valdkonda kuuluvad arvutiga seotud õigusrikkumised (nt arvutivõltsimine ja -pettus); kolmandasse valdkonda kuuluvad sisuga seotud (ingl k *content-related*) õigusrikkumised (nt lapsporno); neljandasse valdkonda kuuluvad autoriõiguse ja sellega seotud õiguste vastased õiguserikkumised (nt digitaalne autoriõiguste rikkumine).

Tabel 2. Digitaalse komponendiga kuritegude tüpoloogiad, autori koostatud

Digitaalse komponendiga (küber-) kuriteod		
Autor (-id)/ organisatsioonid	liigitamise alus	liigitus
Wall, 1998	Kitsas tähenduses küberkuriteod, Kuriteoliigi alusel, valdkonniti	➢ küber-sissetungid (ingl k *cybertrespass*) ➢ kübervargused (ingl k *cyber thefts*) ➢ küber-rõvedused (ingl k *cyberobscenity*) ➢ kübervägivald (ingl k *cyberviolence*)
Euroopa Nõukogu Arvutikuritegude Vastane Konventsioon (Budapesti Konventsioon)	Kitsas tähenduses küberkuriteod, kuriteoliigi alusel, valdkonniti	➢ arvutiandmete ja -süsteemide konfidentsiaalsuse, terviklikkuse ja kättesaadavuse vastased õigusrikkumised (nt häkkimine) ➢ arvutiga seotud õigusrikkumised (nt arvutivõltsimine ja -pettus) ➢ sisuga seotud (ingl k *content-related*) õigusrikkumised (nt lapsporno) ➢ autoriõiguse ja sellega seotud õiguste vastased õiguserikkumised (nt digitaalne autoriõiguste rikkumine)
Wall, 2007	Digitaalse komponendiga kuriteod ja küberkuriteod, lähtuvalt IKT rollist teo toimepanemisel	➢ -küber-seotud kuriteod (ingl k *cyber-related*) ➢ -küber-põhised kuriteod (ingl k *cyber-enabled*) ➢ -küber-sõltuvad kuriteod (ingl k *cyber-dependent*)

Leukfeldt, *et al.*, 2013 McGuire & Dowling, 2013 Suurbritannia tõsiste ja organiseeritud kuritegevuse vastane strateegia (Home Office), 2013 Furnell & Dowling, 2019	Digitaalse komponendiga kuriteod ja küberkuriteod, lähtuvalt IKT rollist teo toimepanemisel	➢ küber-sõltuvad kuriteod (toimepanemise viis on arvuti, arvutivõrgu või muu IKT abil ja ründeobjektideks on peamiselt arvutid või võrguressursid, kuigi rünnakutel võib olla ka teiseseid tagajärgi, näiteks pettus) ➢ küber-põhised kuriteod (traditsioonilised kuriteod, mille ulatust ja tagajärge võimestatakse digiseadmete ja IKT kasutamise tulemusel, erinevalt kübersõltuvatest kuritegudest võib neid toime panna ka ilma IKT kasutamiseta)
Caneppele & Aebi, 2019	Digitaalse komponendiga uriteod ja kõberkuriteod, veebipõhiseid ja võrguväliseid käitumisviisid ja/või nende kombinatsioon	➢ veebivälised kuriteod (traditsioonilised kuritegusid) ➢ hübriidkuriteod (ühendavad veebi- ja veebivälist komponenti) ➢ küberkuriteod (ainult internetis)

Kokkuvõtteks, analüüsides küber-, arvuti- ja digitaalse komponendiga kuritegevuse määratlusi (vt tabel 2) selgub, et valdkonnas valitseb terminite ja nende tähenduste mitmekesisus, mida kinnitab ka üks värskematest uuringutest (De Paoli, *et al*., 2021, p. 1444–1445). Vaatamata digitaalse komponendiga kuritegude mitmekesisusele ning nende toimepanemisel IKT rolli erinevusele, on nende kuritegude ühiseks tunnuseks IKT lahenduste ja digiseadmete kasutamine ning digitaalsete tõendite ja jälgede olemasolu. Käesolevas töös katuseterminina kasutatav **digitaalse komponendiga kuriteo** mõiste (käesolev töö lk 7) sisaldab eespool kirjeldatud küberkuritegude liikide tunnuseid. USA autorid Moloney, *et al*. (2022) võtavad asjakohaselt kokku, et küberkuritegevus on üks kõige kiiremini arenevaid ja eksponentsiaalselt kasvavaid globaalseid sotsiaalseid probleeme, mis hõlmab mitmesuguseid digitaalses keskkonnas toimuvaid või IKT poolt hõlbustavaid tegevusi. Samas, territoriaalsete politseiüksuste ja kohaliku tasandi politseiuurijate tegevus ongi suunatud teenindusterritooriumi põhimõttel kogukonnakuritegude ja sotsiaalsete probleemide lahendamisele. Moloney, *et al*. (2022) definitsioon kinnitab ka varasemat Leukfeldt, *et al.*, (2013, p. 3) esitatud küberkuritegevuse määratluse, milleks on „kõikvõimalike kuritegude üldmõiste, mille puhul IKT mängib kuriteo toimepanemisel olulist rolli“. Sõltuvalt kohalikust seadusandlusest ja võttes arvesse eri riikide politseiorganisatsiooni struktuuri eripära võib suurem osa eespool loetletud kuritegude liikidest kuuluda kohaliku tasandi politseiüksuste uurijate menetluspädevusse.

1.2 Kompetentsimudeli konstrueerimise põhimõtted

Antud alapeatükis keskendutakse politseiuurijatele digitaalse komponendiga kuritegude uurimiseks kompetentsiraamistiku konstrueerimiseks vajalike aspektide tutvustamisele. Esmalt täpsustatakse kompetentsi ja kompetentsuse määratlused. Järgnevalt tutvustatakse kompetentsimudeli väljatöötamise põhimõtteid. Selles ja ka järgnevas alapeatükis otsitakse vastust kolmandale uurimisküsimusele: kuidas süstematiseerida kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimiseks vajalikke teadmisi ja oskusi kompetentsiraamistiku kujul?

1.2.1 Kompetentsi ja kompetentsuse määratlused

Kui kompetentsid (ingl k *competency*) on inimese sooritusvõimet kirjeldavad eraldiseisvad komponendid, siis nende kogum ja inimese võimekus moodustavad kompetentsuse (ingl k *competence*) (Rowe, 1995, p. 12; Leigh, *et al*., 2007, p. 464). Kompetentsuse mõiste defineerimisel peetakse olulisteks elementideks nii isiklike tunnuseid kui ka spetsiifilisi teadmisi ja oskusi, mis tagavad sooritusvõime ja on vajalikud teatud ülesande täitmiseks (Boyatziz, 1982 ref Bellini, *et al.*, 2021, p. 604; Plamínek & Fišer 2005, p. 17; Klieme, *et al*., 2008, p. 6; Blaškova, *et al*., 2014, p. 459).

Teadmised on teadlikkus või arusaamine faktidest, reeglitest, põhimõtetest, suunistest, kontseptsioonidest, teooriatest või protsessidest, mis on vajalikud ülesande edukaks täitmiseks. Teadmisi omandatakse õppimise ja kogemuste kaudu. (Mirabile, 1997, p. 73–74) Teadmised võivad olla konkreetsed, spetsiifilised ja kergesti mõõdetavad või keerulisemad, abstraktsemad ja raskesti hinnatavad (Lucia & Lepsinger, 1999 ref Stacy, 2000, p. 140).

Oskus on võime sooritada vaimseid või füüsilisi ülesandeid, millel on kindel tulemus (Marrelli, 1998, p. 27). Kui teadmised tähendavad teoreetilist arusaamist kontseptsioonist, siis oskused seisnevad teadmiste praktilises rakendamises (Murawski & Bick, 2017, p. 723). Mõisteid kompetents ja kompetentsus kasutatakse eespool toodud autorite käsitlustele sarnases tähenduses ka Eestis kasutusel olevas juhendmaterjalis kutsestandardi koostajale, tasemeõppe ja täienduskoolituse õppekava koostajale ning karjäärinõustajale (Jamnes, *et al.*, 2013, käesoleva töö lisa 1, lk 106) ja Eesti siseturvalisuse hariduse mudeli analüüsisis (Haaristo, *et al.*, 2015, lk 6). Kompetentsust, st võimeid ja oskusi, saab aja jooksul teadliku harjutamise abil parendada (Klieme, *et. al*, 2008, p. 7; Shavelson, 2013, p. 74–75). Kompetentsuse terviklik käsitlus rõhutab asjaolu, et kompetentside sisemine struktuur

koosneb teadmistest, oskustest, hoiakutest, mis ühendab kõik need osad konkreetsetele olukordadele reageerides erilisel viisil (Sultana, 2009, p. 25).

Klieme, *et al.,* (2008, p. 8) määratluse kohaselt on kompetentsuseks „kontekstispetsiifiliste saavutuste dispositsioon, mida saab omandada õppimise kaudu ja mis on funktsionaalselt seotud olukordade ja nõudmistega konkreetsetes valdkondades“. Shavelsoni (2013, p. 85) käsitluses hõlmab kompetentsuse mõiste lisaks soorituse ja tunnetuse aspektidele ka motivatsiooni ja emotsioone. Motiveeritud isikute sooritused on kompetentsed, kuna nende isikute eesmärk on sooritada tööülesanne maksimaalselt hästi. See tähendab ka inimese identiteedi seotust ülesannetega milles ta on kompetentne.

Kompetentsid on kompetentsust tõendatavad komponendid, mis peegeldavad tõhusat sooritust ja mida saab hinnata tunnustatud standardite alusel (Kaslow *et al.,* 2004, p. 708, Marrelli, *et al.*, 2005, pp. 534–535). Tuginevalt konstruktivistlikule paradigmale on kompetentsus ühiskonna poolt loodud konstruktsioon, mis ei ole otseselt vaadeldav, vaid tuletatav ülesannete sooritamise jälgimisest (Shavelson, 2013, p. 74–75).

Sultana (2009, p. 20–21), analüüsides erinevaid kompetentse ja kompetentsuse mitmemõõtlemisi määratlusi erinevate paradigmade vaates, väidab, et nendel terminitel on palju erinevaid tõlgendusi ja tähendusi ning seega on kompetentsipõhine lähenemine sattunud kriitika alla. Näiteks, detailselt määratletud ja käitumisviisidele rajanevad kompetentsiraamistikud tõstatavad küsimusi selle kohta, mil määral need toetavad või õõnestavad kaalutlusõigust ja loovust tööülesannete täitmisel (Sultana 2009, p. 25). Samas, kompetentsipõhine lähenemine on kesksel kohal inimressursi arengut ja hariduse tootlikkust käsitlevates empiirilistes uuringutes. Nimelt, kompetentsipõhise lähenemise kohaselt inimressurssi arendamise kaudu soodustatakse organisatsiooni arengut ja edukust. Kuna organisatsioonide üks keskseid eesmärke on tõhususe ja tootlikkuse parendamine, siis kompetentsimudeleid kasutatakse laialdaselt organisatsiooni tõhususe suurendamise vahendina. (Salman, *et al.,* 2020, p. 717;.Bellini, *et al.* 2021, p. 603) Organisatsiooni perspektiivis määratletakse erialast kompetentsust kui “peamiste kutsealaste ja isiklike oskuste, annete ja käitumismustrite kogumit, mida töötaja peab omama ja näitama talle määratletud kutsealaste eesmärkide saavutamiseks ja sellega seotud kutsealaste ülesannete ning kohustuste täitmiseks” (Blašková, 2011, p. 108 ref Blašková, *et. al*, 2014, p. 459). Plamínek ja Fišer (2005, p. 17 ref Blašková, *et. al,* 2014, p. 459) määratlevad organisatsiooni kompetentsust kui “saavutatud tulemuslikkuse (st inimtöö) ja loodud

potentsiaali (st inimressursi) kogumit, kusjuures neist ühe komponendi puudumise korral puudub ka kompetentsus tervikuna.”

Klieme, *et al*., (2008, pp. 10–11) juhivad tähelepanu kompetentsuse konstruktsioonide keerukusele ning sellega seonduvalt kompetentside uurimisel ja hindamisel eristavad nad kahte liiki kompetentsimudeleid, mis käsitlevad kompetentside struktuuri ja tasemeid, samuti rõhutavad nad ka kompetentsuse arengu võimalusi. Nimetatud mudelid peaksid üksteist ideaalis täiendama. Kompetentside **struktuuri mudelites** keskendutakse sellele, millistest elementidest teatud kompetents koosneb. (Klieme, *et al*., 2008, pp. 10–11) Näiteks, USA teadlane Boyatzis (1982), kes esimesena kasutas 1970. aastate lõpus mõistet "kompetentsus" juhtide kontekstis, määratles kompetentsust kui sooritusvõimet ja määras empiiriliselt kindlaks juhtide kompetentside loetelu, mis hõlmab isiksuseomadusi, kognitiivseid oskusi ja interpersonaalseid/sotsiaalseid oskusi (Boyatzis, 1982 ref Bellini, *et al.*, 2021, p. 604).

Kompetentside **tasememudelid** aga kirjeldavad erinevaid kompetentside astmeid, mis erinevad kvalitatiivselt selle poolest, millist ülesannet inimene on võimeline täitma konkreetse kompetentsi taseme juures. Arengu aspekti silmas pidades näevad mõned kompetentsimudelid ette kompetentsuse täiendamist pideva arenguna, mis eeldab järjestikku liikumist madalamast kõrgeimale kompetentside tasemele. Pikaajalise praktika tulemusel võib kompetents üle kasvada vastava valdkonna eksperdi teadmisteks ja kogemuseks ehk ekspertiisiks (ingl k *expertise*). (Klieme *et al*., 2008, pp. 7, 10–11)

Eespool käsitletu lühidalt kokku võttes saab väita, et kompetentsid on õpitavad (Klieme, *et al.*, 2008, p. 8; Shavelson, 2013, pp. 74–75); organisatsiooni vaates on kompetentsus tihedalt seotud nii indiviidi isiklike ja kogniktiivsete tunnustega (Roth, 1971, p. 180 tsit Klieme, *et. al*, 2008 p. 6; Boyatziz, 1982 ref Bellini, *et al.*, 2021, p. 604; Plamínek & Fišer 2005, p. 17; Klieme, *et al*., 2008, p.; Blaškova, *et al.*, 2014, p. 459) kui kutsekvalifikatsiooni nõuete- ja sooritusvõime hindamiskriteeriumitega (Boyatzis, 1982 ref Bellini, *et al.*, 2021, p. 604; Blašková, 2011, p. 108 ref Blašková, *et. al*, 2014, p. 459). Kompetentside kirjeldused on mõõdikuteks mitte ainult indiviidi sooritusvõime hindamiseks, vaid need on vajalikud organisatsiooni tõhususe suurendamiseks (Plamínek & Fišer, 2005, p. 17 ref Blašková, *et. al*, 2014, p. 459; Bellini, *et al.* 2021, p. 603). Kompetentse saab paigutada horisontaalsetesse (Boyatzis, 1982 ref Bellini, *et al.*, 2021, p. 604) ja vertikaalsetesse (Klieme, *et al.*, 2008, p. 7) mudelitesse, mida nimetatakse vastavalt kompetentside taseme- ja struktuurimudeliteks (Klieme, *et al.*, 2008). Neid mudeleid saab omakorda omavahel integreerida. Konkreetsele tasemele vastavat kompetentside loetelu

saab nimetada ka kompetentsiraamistikuks, mille eesmärgiks on toetada koolitusprogrammide arendamist, tuvastada kompetentsilüngad, edendada enesearengut ja tagada ühised standardid (Sultana, 2009, pp. 15–16). Järgnevas alapeatüki osas käsitletakse kompetentsimudeli konstrueerimist.

1.2.2 Kompetentsimudeli ja -raamistiku konstrueerimine

2017. aastast toimiv Euroopa Komisjoni mitmekeelne oskuste, kompetentside ja ametite klassifikatsiooni projekt European Skills, Competences, Qualifications and Occupations (ESCO) on näide kompetentsipõhise lähenemise populaarsusest ja praktilisusest. ESCO eesmärk on toetada Euroopa integreeritust ja tõhusamat tööturgu ning tööjõu liikumist, pakkudes ühiseid standarte ametite ja oskuste kohta, mida erinevad sidusrühmad saavad kasutada tööjõu värbamisel, tööalase koolituse korraldamisel ning hariduse valdkonnas. ESCO pakub 2942 ameti ja 13 485 kutseala (sh politseiniku, politsei- ja kriminaaluurija eriala) kirjeldust, mis on tõlgitud 27 keelde (Euroopa Komisjon, 2022). Eestis toovad Haaristo, *et al*. (2015, lk 78–79) analüüsides PPA politseijaoskonna töötajate ametijuhendeid välja, et kompetentside puudulik kajastamine ametijuhendites viib selleni, et tööülesannete täitmiseks vajalikud kompetentsid ei võeta arvesse tööjõu värbamisel, koolitamisel ja spetsialiste ettevalmistavas õppeasutuses vastavate õppeprogrammide väljatöötamisel ja ajakohastamisel. Nad soovitavad kasutada läbivalt ühte kompetentsimudelit ja üldkompetentside määratlemisel tugineda Eestis kasutatavale Jamnes, *et al.* (2013) universaalsele käsitlusele.

Kompetentsuse valiidsed mõõdikud peavad põhinema empiiriliselt usaldusväärsetel ja testitud kompetentsimudelitel (Koeppen, *et al.*, 2008, p. 63), mis on organisatsiooni strateegilisi eesmärkide saavutamise vahendiks ja on vajalikud organisatsioonis konkreetses töörollis tööülesannete tõhusa täitmise tagamiseks (Lucia & Lepsinger, 1999 ref Stacy, 2000, p. 140). Kompetentsimudelitega määratletakse rollid ja tööülesannete täitmiseks vajalikud oskused, teadmised, isiksuseomadused ning käitumisviisid. See tagab läbipaistvuse töö tulemuslikkuse ootuste ja meetmete vahel, kuna mudeliga paika pandud töö tegemiseks vajalikel oskustel, teadmistel ning käitumisviisidel on kõige otsesem mõju töö tulemuslikkusele. (Lucia & Lepsinger, 1999 ref Stacy, 2000, pp. 140–142) Mirabile (1997, p. 75) ja Marrelli, *et al*., (2005, p. 538) käsitluses on kompetentsimudel korralduslik raamistik, milles loetletakse konkreetsel töökohal, töökoha perekonnas (st seotud töökohtade rühmas), organisatsioonis, funktsioonis või protsessis tõhusaks tööks vajalikud kompetentsid.

Sultana (2009, p. 23) eristab kahte kompetentsiraamistiku korraldamise viisi. Esimesel juhul on tegemist **ülevalt-alla viisil** koostatud kompetentsiraamistikega. Nõnda koostavad neid tippjuhid või akadeemilisse keskkonda kuuluvad eksperdid, tuginedes teoreetilistele teadusallikatele, mudelitele ning valdkonnas tunnustatud standarditele ja strateegilistele dokumentidele. Teine kompetentsiraamistike loomise võimalus põhineb valdkonna tunnustatud praktikute seas parimate praktikate vaatlemisele **alt-üles viisil** ja sellele tuginedes vajalike kompetentside väljatoomises. Mõlemal lähenemisviisil on omad tugevused ja nõrkused. Neid tuleks kombineerida, et tagada tundlikkus kiiresti muutuvas keskkonnas nii töörollide kui ka tööülesannete aktuaalsuse määratlemise osas. Kompetentsiraamistike nõrkuseks on see, et aktuaalsuse tagamiseks tuleb neid pidevalt ajakohastada. Üksnes ülevalt-alla või alt-üles viisil koostatud kompetentsiraamistik ei ole suuteline tuvastama muutvaid ja arenevaid kompetentsinõudeid ja hõlmama ning õiglaselt arvesse võtma konteksti.

Koeppen (2008, p. 67) toonitab, et ilmse hindamisvajadusega kompetentsuse valdkondades on eelkõige vajalik määratleda nii teoreetiliselt kui ka empiiriliselt põhjendatud kompetentsuse struktuuri, kompetentsuse taseme- ja arengumudeleid. Marrelli, *et al*. (2005), Mirabile (1997) ja Shavelson (2013, pp. 74–75) eristavad madala, keskmise ja kõrgema taseme sooritusvõimet kirjeldavaid kompetentsimudelite vorme. Kui Marrelli, *et al*., (2005, p. 537) arvates määravad optimaalse raamistiku organisatsiooni vajadused, siis Shavelson (2013, p. 74–75) rõhutab, et kompetentsimudel sõltub andmete kogumiseks kasutatud meetoditest, klientide nõuetest ja mudeli koostajate konkreetsetest eelarvamustest.

Kompetentsiraamistiku väljatöötamisel on oluliseks sammuks valdkonna, töörolli ja -sisu analüüs. Vastavalt Eestis kasutatavale üldkompetentside juhendmaterjalile (Jamnes, *et al*., 2013), mille mõisteid kasutatakse ka Eesti siseturvalisuse hariduse mudeli analüüsisis (Haaristo, *et al*., 2015, lk 6), liigitatakse kompetentse lähtuvalt ülekantavuse põhimõttest üldisteks ja kutsespetsiifilisteks kompetentsideks. „**Üldkompetentsid** (ingl k *soft skills*) sisaldavad suures ulatuses kõikidele kvalifikatsioonidele ülekantavaid käitumuslikke kompetentse, mis on seotud hoiakutega ja inimese võimega oma oskusi rakendada (nt suhtlemine). Samuti kuuluvad üldiste kompetentside hulka keskmise ja suure ülekantavusega teadmistel ja oskustel põhinevad kompetentsid (nt IKT-teadlikkus). **Kutsespetsiifilised kompetentsid** (ingl k *specific hard skills*) on tööosade ja tööülesannetega otseselt seotud kompetentsid. Neid omandatakse esialgse väljaõppe käigus ja nende kohandamine muutub

elukestvaks protsessiks, kuna kutsespetsiifiliste kompetentside vajadus sõltub kontekstist ja olukorrast (Leigh, *et al*., 2007, p. 464). Kutsespetsiifilised ehk tehnilised kompetentsid on madala ülekantavusega ning nende puudumisel ei ole võimalik ametikohal ettenähtud tööülesandeid täita. (Jamnes, *et al*., 2013, Haaristo, *et al*., 2015, lk 6, 27)

Marrelli *et al*., (2005, pp. 539–559) pakub 7-astmelist kompetentsimudeli, mis koosneb järgnevalt kirjeldatud etappidest. **Esimeseks etapiks on** kompetentsimudeli abil soovitud **eesmärkide määratlemine**. Selles etapis täpsustatakse kompetentsimudeli vajalikkust, valitakse analüüsi üksuseid, määratletakse ajavahemik, mille raames tuleb kompetentse täpsustada ja/või ajakohastada, ning lõpuks määratletakse kohaldamisala (nt kas seda mudelit kasutatakse tööjõu strateegilisel planeerimisel, töötajate värbamisel, edutamisel, tulemuslikkuse juhtimisel, koolitamisel ja arendamisel, sertifitseerimisel, järelkasvu planeerimisel, tasustamisel, premeerimisel ja tunnustamisel või karjääri planeerimisel).

Teiseks etapiks on toetaja ja rahastaja leidmine, mis kindlustab uurimiseks vajalikku tuge lobitöö tegemiseks, ligipääsu sihtgrupile jms. Toe saamiseks tuleb selgitada kompetentsimudelis käsitletavad organisatsioonilised vajadused ning kuidas neid rahuldatakse; mudeli võimalik rakendusala; sidusrühmade, spetsialistide ja ekspertide kaasamise võimalused ja viisid; mudeli väljatöötamisel kaasnevad probleemid ja takistused ning nende ületamise võimalused; mudeli arendamisel kaasnevad materiaalsed ja mittemateriaalsed (nt kaasatud inimeste aeg) kulud.

Kolmandas etapis töötatakse välja ja rakendatakse **kommunikatsiooni- ja teavituskava,** mille peamiseks ülesandeks on veenda kompetentsimudeli väärtuses neid, kes selles osalevad või keda see mõjutab. Selleks eristatakse sidusrühmad ja isikud, kes ühel või teisel määral panustavad kompetentsimudeli väljatöötamisse. Esimesse kategooriasse kuuluvad vabatahtlikud osalejad, kelle osavõtt on hädavajalik – nende kaudu kogutakse andmeid või viiakse läbi pilootkatseid, samuti võivad nad mõjutada teisi, kaasates neid uuringust osa võtma, toetama rahaliselt või suunata ressursse muul viisil.

Neljanda etapina kavandatakse metoodika kompetentsimudeli väljatöötamiseks. See hõlmab sobivatest inimesest valimi moodustamist ning andmete saamiseks ja analüüsimiseks kasutatavate uurimisinstrumentide valimist. Ametikohtade perekonna, ametikoha sisese spetsialiseerumise või erifunktsiooni kohta (edaspidi kasutatakse kõigi nende mõistete tähistamiseks terminit „töö kirjeldus“)

andmete kogumiseks soovitatakse uurida mitu gruppi, kombineerides erinevaid meetodeid. Tervikliku pildi saamiseks on oluline koguda andmeid tööks nõutavate vajalike oskuste kohta nii ametikohal vahetult töötavatelt, kui ka teistelt tööga tuttavatelt isikutelt (nt juhtidelt, valdkonna ekspertidelt, poliitika kujundjatelt ning teaduskirjandusest). Nõnda võetakse arvesse erinevaid aspekte ja vajadusi. See lähenemine on kooskõlas Sultana (2009, pp. 23–25) teadusartiklis toodud ülevalt-alla ja alt-ülesse kompetentsiraamistiku kirjeldatud viiside kombineerimisega (vt käesolev töö, lk 30).

Viienda etapi käigus **luuakse kompetentsimudel**. Kuna kompetentsid on seotud töö sisuga, ei saa tööülesannete edukaks sooritamiseks nõutavaid kompetentse kindlaks määrata enne, kui on määratletud töö sisu. Seejärel kaardistatakse iga töö elemendi või ülesande täitmiseks vajalikud teadmised, oskused, võimed ja isiksuseomadused. Edaspidi rühmitatakse neid vastavalt kategooriatele ning sageli mainitud kategooriatest moodustatakse esialgne kompetents. Järgnevalt nimetatakse kõigi tasandite ühised kompetentsid ning märgitakse iga tasandi spetsiifilised kompetentsid. Seejärel võrreldakse selle protsessi tulemused läbitöötatud kirjanduse ülevaatega ja kättesaadava võrdlusinformatsiooniga. Lõpuks koostatakse kompetentside esialgne määratlus, mida hiljem võib jaotada tasemeteks, mille kaudu eristatakse tipptasemel ja algtasemel töötajale vajalikke kompetentse. Valmis kompetentsimudeli valideeritakse koostöös töövaldkonna asjatundjatega, kellel on ulatuslik kogemus sihttööga ja teadmised töö sisu kohta. Kompetentsimudeli valideerimisel täpsustatakse definitsioonid ja antakse hinnangud mudeli rakendusvõimaluste osas. Valmis kompetentsimudel sisaldab kompetentside loetelu, mis on liigitatud tüübi järgi, koos iga kompetentsi määratluse ja mitme käitumisnäidisega erineval tasemel.

Kuuendas etapis kontrollitakse loodud **kompetentsimudel selle rakendamise** käigus. Kompetentsimudeli väärtus on maksimaalne, kui seda rakendatakse kõigis inimressursside juhtimise aspektides. Täielikult integreeritud kompetentsipõhises inimressursi juhtimise süsteemis kasutatakse kompetentsimudeli töötajate värbamisel, arendamisel, juhtimisel, premeerimisel ja tõhusa töö tagamisel. Töötajad teavad täpselt, milline on tööandja kompetentsuse ootus, millele peab vastama ning millised on selle hindamiskriteeriumid ja -instrumendid.

Seitsmendas etapis toimub **kompetentsimudeli hindamine ja ajakohastamine**, mis seisneb nii kompetentsimudeli väljatöötamise protsessi kui ka organisatsiooni jaoks saadud mudeli väärtuse hindamises. Kompetentsi modelleerimine on pidev protsess organisatsiooni strateegiate, keskkonnatingimuste, töökoha eripära muutuse, eeskirjade ja kutsealaste tavade pidevate muutuste

perspektiivis. Seetõttu on kompetentsimudelite või üksikute kompetentside kehtivusaeg erinev. Näiteks tehnilised (st kutsespetsiifilised) kompetentsid aeguvad tavaliselt ennem, kui isikliku tõhususe või juhtimiskompetentsid (st üldkompetentsid). (Marrelli *et al*., 2005, pp. 539–559)

Täies mahus esitatud kompetentsimudeli koostamise ja kompetentsuse hindamise metoodika on toodud laiahaardelise lähenemisviisi tutvustamise ning selle tugevuste ja nõrkuste väljatoomise eesmärgil. Nõnda luuakse eeldusi teema edasiarendamiseks teiste uurijate poolt, näiteks kompetentsipõhise lähenemise kaalumisel kogu politseiorganisatsiooni vaates, kompetentsuse hindamiseks vajalike instrumentide väljatöötamiseks jms. Käesolevas töös keskendutakse siiski vaid kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimseks vajaliku kompetentsiraamistiku väljatöötamisele, tuginedes mõnele Marrelli, *et al.,* (2005) mudeli etapile ja Sultana (2009) artiklis toodud kompetentsiraamistiku korraldamise ülevalt-alla viisile (käesolev töö lk 30).

1.3 Kohaliku tasandi politseiüksuste uurijate kompetentsiraamistik digitaalse komponendiga kuritegude uurimiseks

Kohalikul tasandi uurijate poolt digitaalse komponendiga kuritegude uurimine kuulub mingil määral küberturbe sektori ülesannete piiridesse. PPA on üheks avaliku sektori asutustest, mis tegeleb küberturbe valdkonnas siseturvalisuse tagamisega, mis seisneb küberkuritegude ennetamises ja nende uurimises. Melesk, *et al*., (2019), koostanud küberkompetentside loetelu, tuginedes USA põhisele kompetentside kaardistusele NICE ja kohandades seda Eesti kontekstile, määratleb küberkriminalistikat ja kitsamas mõttes digitaalset kriminalistikat kui küberkuritegevuse tõkestamise ja uurimise valdkonda (Melesk, *et al.*, 2019, lk 6, 11, 16). Kübervaldkond on arvutiteaduse, matemaatika, majanduse, õiguse, psühholoogia ja tehnika multidistsiplinaarne ühendamine (Dawson, & Thomson, 2018).

Dawson ja Thomson (2018) väidavad, et küberturbe sektoris tegutsevad inimesed vajavad edu saavutamiseks kombinatsiooni tehnilistest oskustest, valdkondlikest teadmistest ja sotsiaalsest intelligentsusest, mis on kooskõlas ka eespool toodud seisukohtadega (Roth, 1971, p. 180 tsit Klieme, *et. al*, 2008 p. 6; Boyatziz, 1982 ref Bellini, *et al.,* 2021, p. 604; Rowe, 1995, p. 12; Plamínek & Fišer 2005, p. 17; Leigh, *et al*., 2007, p. 464; Klieme, *et al*., 2008, p. 6; Blaškova, *et al.*, 2014, p. 459; Sultana 2009, pp. 23–25). Teisisõnu, kompetentsiraamistikku koondatud kompetentsid saab jagada kolme

kategooriasse: ristkasutatavad üldkometentsid ja üld-digikompetentsid ning kutsespetsiifilised kompetentsid (vt ka käesoleva töö lk 30–31).

Vajalike kompetentside täpsustamiseks tuleb eelkõige määratleda konkreetse töötaja rolli, töö, ametikoha sisese spetsialiseerituse või selle erifunktsiooni sisu. Kompetentside määratlemine järgneb otseselt töö sisu määratlemisele (Marrelli, *et al.,* 2005, pp. 553–554). Ka teised autorid (Dawson, & Thomson, 2018) toovad välja küberturbe sektori näitel, et meeskonnakorralduse optimeerimiseks, et see vastaks ülesannete soorituse nõudmistele, tuleb eelkõige mõista erinevaid tööülesandeid, s.h organisatsiooni iga spetsialisti rolli vaates. Selleks anti käesoleva töö alapeatükis 1.1 ülevaate digitaalse komponendiga kuritegude uurimisega takistustest ja väljakutsetest ning digitaalse komponendiga kuritegude olemusest. Lisaks käsitletakse siin politseiuurija töö ja selleks vajalikke kompetentside soovituslikke kirjeldusi (European Commission, 2016; Euroopa Komisjon, 2022).

Käesolevas alapeatükis määratletakse digitaalse komponendiga kuritegude uurimiseks töö elementidega seotud üld- ja kutsespetsiifilisi kompetentse ning samuti täpsustatakse digikompetentside iseloomu ja kohta nende kahe kompetentside kategooria vahel. Alapeatükk on jaotatud kolmeks osaks. Esmalt antakse ülevaade üld- ja digikompetentside raamistikest. Teisena keskendutakse politseiuurija kutsespetsiifilistete kompetentsidele digitaalse komponendiga kuritegude uurimisel. Viimasena esitatakse kohaliku tasandi uurija digitaalse komponendiga kuritegude uurimiseks vajalik kompetentsiraamistik.

1.3.1 Üld- ja digikompetentsid

Politseinike (st ka uurijate) ettevalmistamisel, värbamisel ja täiendkoolituse kavandamisel tuleb tähelepanu pöörata üldkompetentside arendamisele. Neid nimetatakse ühtlasi ka 21. sajandi oskusteks (Van Laar, *et al*., 2021). Analüüsides küberturbe sektoris tööjõu arendamise, küberhariduse uuringuid, jõudsid USA autorid Dawson ja Thomson (2018) järeldusele, et peamine rõhuasetsus on neis enamasti tehnilistel oskustel. Samas ei pöörata piisavalt tähelepanu potentsiaalse küberspetsialisti isiksuse ja sotsiaalsete oskuste, s.o üldkompetentside, kontekstile. Sellele lüngale viidates aga rõhutatakse, et lisaks tehnilistele võimetele on oluline ka spetsialisti organisatsiooniline ja sotsiaalne sobivus. „Kriminaaluurimine on üheks haruks üleüldises kübervaldkonnas, mis on nii tehniline kui ka uurimuslik (Ono, *et al*., 2011 ref Dawson, & Thomson, 2018) ja tugineb rohkem sotsiaalsetele oskustele

kui toorele kognitiivsele võimekusele“. (Dawson, & Thomson, 2018) USA-s läbi viidud kohalike politseiakadeemiate õppekavade ja õppemeetodite uuringu (Blumberg, *et al.,* 2019) järeldused kinnitavad Dawson ja Thomson (2018) uuringu tulemusi selles osas, et kognitiivsed, emotsionaalsed, sotsiaalsed ja moraalsed oskused on oluliseks kompetentsuse ja professionaalsuse komponendiks. Neid kompetentse aga ei saa otseselt seostada kutsespetsiifiliste kompetentsidega ning neid ei omandata formaalse politseihariduse raames. Blumberg, *et al.,* (2019) peavad oluliseks kriitilise mõtlemise oskust, suhtlemisoskust ja head emotsionaalset intelligentsust. Nende tunnuste olemasolu ja pidev arendamine tagab politseiniku vastavuse kutsesobivusnõuetele, töötõhususe ja on vajalikud nii ühiskonna vaates kui politseinikule endale emotsionaalse heaolu ja vaimse tervise säilitamiseks. Kuigi neis uuringutes ei analüüsita otseselt üldkompetentside raamistikke, viidatakse siiski üldkompetentside vajalikkusele.

Nüüdisaja tööjõud seisab silmitsi üha keerulisemate interaktiivsete ülesannetega. Van Laar, *et al.*, (2017) analüüsides asjakohast teaduskirjandust süstemaatilise ülevaate meetodil rõhutavad oskuste laia spektrit ja väidavad, et 21. sajandi oskused ja digikompetentsus on omavahel seotud ning osaliselt kattuvad mõisted, kuid alati ei hõlma üldkompetentsid digitaalset aspekti. Üldkompetentside raamistikud sisaldavad reeglina koostöö oskust, suhtlemisoskust, probleemide lahendamise oskust, kriitilise mõtlemise ja anlüüsimise oskust, infohaldusoskust, digitaalkirjaoskust, digikompetentse ning käitumisega ja isiksuse omadusega seotud kompetentse, mis viitavad hoiakutele ja inimese võimele rakendada oma oskusi (eetilisus, paindlikkus, enesejuhtumine, pingetaluvus jne) (Voogt & Roblin, 2012; Binkley, *et al.,* 2012; Jamnes, *et al.*; 2013 Van Laar, *et al.*, 2017). Ülevaade pehmete ehk ülekantavate üldkompetentside raamistikest on toodud tabelis 3 (käesolev töö, lk 36).

Eestis on tööandjatele personali kvalifikatsiooninõuete täpsustamiseks ja värbamisel kasutamiseks ning õppeasutustele tulevaste spetsialistidele õppekavade väljatöötamiseks ja õpiväljundite määratlemiseks soovituslik rakendada eespool käsitletud raamistikele sarnast üldkompetentside raamistikku (Jamnes, *et al.*, 2013). Kõnealune raamistik on piisavalt detailne, kuid samas universaalne. Käesolevas töös seda võetakse arvesse uurijatele digitaalse komponendiga kuritegude uurimiseks vajalike kompetentside määratlemisel.

Tabel 3. Üldkompetentside raamistikud, autori koostatud

Autor/institutsioon	Sisu
Voogt & Roblin, 2012	● koostööoskus ● suhtlemioskus ● digitaalne kirjaoskus ● kodanikualgatus ● probleemide lahendamise oskus ● kriitilise mõtlemise oskus ● loovus ● tootlikkus
Binkley, *et al*., 2012	➢ **mõtlemisviisidega seotud oskused** (loovus ja innovatsioon; kriitiline mõtlemine, probleemide lahendamine ja otsuste tegemine; õppimine ja metakognitsioon) ➢ **tööviisidega seotud oskused** (suhtlemine; koostöö ja meeskonnatöö), ➢ **töövahendite kasutamise oskused** (infokirjaoskus; infotehnoloogia ja kommunikatsioonialane kirjaoskus) ➢ **üldised toimetuleku oskused** (elu ja karjääri planeerimisoskus; isiklik ja sotsiaalne vastutus)
Jamnes, *et al*., 2013 (vastavuses Eesti kvalifikatsiooniraamistikuga) + viide digikompetentside kirjedusele standardites, mis on koostatud DigComp alusel	**4 kompetentsigruppi: 8 kompetentside kategooriat, 23 kompetentsi, mis mingil määral sisaldavad ka digikompetentse (lisaks tegevusnäitajad ja EKR kutsekvalifikatsioonile vastavuse nr):** ➢ **suhtlemine** 1) suhtlemine ja esitlemine 1. suhtlemine 2. teabe esitamine 3. klientide teenindamine 2) koostöö ja toetamine 4. koostöö 5. väärtustest lähtumine ja põhimõtete järgimine 6. mõjutamine ja veenmine ➢ **juhtimine** 3) juhtimine ja eestvedamine 7. otsustamine ja tegevuste algatamine 8. inimeste juhtimine 9. protsesside juhtimine 10. juhendamine ➢ **mõtlemine** 4) analüüs ja tõlgendamine 11. kirjutamine ja aruannete koostamine 12. analüüsimine ja tõlgendamine 5) loovus ja üldistusoskus 13. teadmiste ja tehnoloogiate kasutamine 14. õppimine ja enesearendamine 15. loovus ja uuenduslikkus 16. kontseptuaalne ja strateegiline mõtlemine ➢ **enesejuhtimine** 6) kohanemine ja toimetulek 17. avatus ja paindlikkus 18. toimetulek pinge ja tagasilöökidega 7) ettevõtlikkus 19. isiklikele tööalastele eesmärkidele pühendumine 20. ettevõtlikkus

	8) organiseerimine ja tegutsemine 21. juhiste ja reeglite järgimine 22. planeerimine ja organiseerimine 23. tulemuste saavutamine ➢ **Digikompetentsidele on viidatud eraldi:** IKT-kompetentside kirjeldamisel mitte-IKT valdkonna kutsestandardites lähtutakse kolmest dimensioonist: ● baasdigioskused ● erialased IKT-kompetentsid ● eriala +IKT-kompetentsid
Van Laar, *et al.*, 2017	Kombinatsioon 21. saj oskustest ja digioskustest: ➢ **tehnilised oskused:** ● infohaldus ● kommunikatsioon ● koostöö ● loovus ● kriitiline mõtlemine ● probleemide lahendamine ➢ **kontekstuaalsed oskused**: ● eetiline teadlikkus ● kultuuriteadlikkus ● paindlikkus ● enesejuhtimine ● elukestev õpe

Digiühiskond sõltub arvutisüsteemide turvalisusest ja terviklikkusest, kuna digitaalne komponent on sotsiaalse tegelikkuse element, mis oluliselt muudab ja võimestab inimeste, organisatsioonide ja institutsioonide interaktsiooni ulatust ja vorme (Jewkes & Yar, 2011, p. 1; Tierney, *et al.*, 2018, pp. 7–8). See eeldab inimestelt tugevaid digikompetentse elus hakkama saamiseks, mis omakorda seab politseiuurijatele võrreldes tavainimestega veel kõrgemaid nõudmisi. Juba kümmekond aastat tagasi täheldasid Yewkes ja Yar (2012, p. 602), et küberkuritegude vastases võitluses on üheks oluliseks komponendiks kõigil tasanditel (st riiklikul, juhtimis-, piirkondlikul ja kohalikul tasandil) politseinike info- ja arvutioskuste vastavusse viimine. Nende arvates on digikomkompetentsuse taseme tõstmisel seos küberkuritegevusega seotud politseitööl. Dodge ja Burrus (2020, p. 351) jagavad eespoool toodud seisukohti, konkretiseerides, et kui ametnik ei ole piisavalt digikompetentne, võib ta teenistusülesannete täitmisel jätta tähelepanuta olulist teavet või kaotada olulisi tõendeid.

IKT kasutamise vajadus muudab põhjalikult töökohtade kvalifikatsiooni profiili ja eeldab nii üld- kui digikompetentside pidevat kaasajastamist (Van Laar, *et al.*, 2017; Dawson, & Thomson, 2018; OECD, 2019). Vaatamata nii 21. sajandi oskuste (st üldkompetentside) kui ka eraldi digikompetentside

olulisusele, ei ole nende kombinatsioon veel piisavalt määratletud. Samas, need on tähtsad nii inimeste kui ka organisatsioonide jaoks protsesside, toodete ja teenuste arenguga sammu pidamiseks (Van Laar, *et al.*, 2017; Sillat, *et al*., 2020, p. 1).

Kuigi digikompetentsid kuuluvad üldkompetentside hulka, moodustavad nad eraldi täpsustamist vajava kategooria. Nagu ka küberkuritegude puhul, valitseb siin terminoloogia mitmekesisus. Digikompetentside määratlemiseks kasutatakese erinevaid mõisteid: digioskused, digikompetents(-pädevus), meediakompetents(-pädevus), infokompetents(-pädevus), transversaalsed oskused, uusmeediapädevus, e-oskused, e-kompetentsus ja isegi digitaalne intelligentsus (Van Laar, *et al*., 2017; Sillat, *et al*., 2020, p. 2). Kozanoglu ja Abedin (2021, p. 2) rõhutavad digikompetentside organisatsioonilise dimensiooni tähtsust. Ühtlasi leiavad nad, et üksikisikute digioskuste kujunemisel ja arengul on seos nende suhtlemisega teiste töötajatega organisatsioonis. Selleks, et samaaegselt haarata individuaalset ja organisatsioonilist mõõdet, kontseptualiseerivad nad digitaalkirjaoskust kui organisatsioonilist võimekust. See seisukoht on sarnane ka Jarrahi ja Eshraghi (2019, p. 1066) uuringu järeldustega, mille kohaselt toovad töötajad oma individuaalsed identiteedid ja eelistused töösse, sh tehnoloogia kasutamise mustrite ja harjumuste osas, mistõttu individuaalsete ja tööga seotud valdkondade ristumiskohas tekivad uued kasutuspraktikad. Samuti täiendatakse, et digikompetentsus kujuneb ja areneb eelkõige isiklikust suhtlusest ja kogemustest tehnoloogiaga (Jarrahi ja Thomson, 2017 ref Jarrahi & Eshraghi, 2019, p. 1066)

Kokkuvõttev ülevaade digikompetentside erinevatest käsitlustest (Alkali & Amichai-Hamburger, 2004; Claro, *et al*., 2012; Ferrari, 2012; Van Deursen, *et al.*, 2016; Jamnes, *et al*., 2013; Carretero, *et al.,* 2017) on toodud tabelis 4 (käesolev töö, lk 39). Kui Alkali ja Amichai-Hamburger (2004) on ühena esimestest pakkunud viiest komponendist (fotovisuaalne, reproduktiivne, infokirja-, hargnenud ja sotsiaal-emotsionaalne kirjaoskuse komponent) koosneva digitaalkirjaoskuse kontseptsiooni indiviidi vaates, siis tabelis 3 viimasena toodud raamistik – DigComp 2.1 (Carretero, *et al.*, 2017) kirjeldab mitmemõõtmelist ja -tasandilist süsteemi, mida rakendatakse tööjõu üldkompetentside raamistikes.

DigComp 2.1 sisaldab viit olulist osaoskust, millel on omakorda 8 kompetentsi astet. Osaoskusteks on: 1) **info haldamine** – digitaalse info eesmärgipärane otsimine, sirvimine, hindamine, salvestamine ja taasesitamine; 2) **suhtlemine digikeskkondades** – teadlik suhtlemine veebipõhistes keskkondades, info ja sisu jagamine, osalemine ühiskonnaelus ning koostöö digivahendite toel; 3) **sisuloome** – digitaalse sisu loomine, olemasoleva digitaalse materjali muutmine ja lõimimine, loominguline

eneseväljendus ja programmeerimine ning intellektuaalse omandi õiguste ja litsentside järgimine; 4) **turvalisus** – identiteedi, tervise ning keskkonna kaitsmine; IKT turvaline ning kestlik kasutamine; 5) **probleemilahendus** – vajaduste väljaselgitamine ja lahenduste leidmine sobivate digivahenditega, tehnoloogia loov kasutamine ning digikompetentsuse arendamine (Carretero, *et al.*, 2017). Magistritöös digikompetentside loetelu koostamise aluseks võeti DigComp 2.0 (Vuorikari, *et al*., 2016) raamistikus loetletud digioskuste sisu, mis on ühtlasi toodud kehtivas kohtukriminalsitika eksperdi tase 8 kutsestandardis (SA Kutsekoda, 2019), eristamata kompetentsuse tasemeid, nagu seda on tehtud DigComp 2.1 (Carretero, *et al.*, 2017, vt käesoleva töö lisa 2, lk 107) ja DigComp 2.2 (Vuorikari, *et al*., 2022) raamistikes.

Tabel 4. Digioskuste kontseptuaalsed raamistikud (koostatud Van Laar, *et al.*, 2017 alusel, autori kohandatud)

Autor/institutsioon	**Oskuste liigitused**
Alkali & Amichai-Hamburger, 2004	➢ fotovisuaalne kirjaoskus ➢ reproduktiivne kirjaoskus ➢ infokirjaoskus ➢ hargnenud kirjaoskus ➢ sotsiaal-emotsionaalne kirjaoskus
Claro *et al*., 2012	➢ IKT-rakenduste valdamine kognitiivsete ülesannete lahendamiseks tööl ➢ oskused, mis ei ole tehnoloogiapõhised, kuna need ei viita ühegi konkreetse tarkvaraprogrammi kasutamisele ➢ oskused, mis toetavad kõrgema taseme mõtlemisprotsesse ➢ töötajate pidevat õppimist soodustavad oskused, mis on seotud kognitiivsete protsessidega
Ferrari, 2012	➢ infohaldus ➢ koostöö ➢ suhtlemine ja informatsiooni jagamine ➢ sisu ja teadmiste loomine ➢ eetika ja vastutus ➢ probleemide lahendamise oskus ➢ tehnilised toiminguid
Van Deursen, *et al.*, 2016	➢ **tehnilised või meedia aspektid** ➢ **sisulised aspektid (sisuga seotud oskused):** - operatiivsed oskused - formaalsed oskused - informatsioonilised oskused - kommunikatsiooni alased oskused - sisu loomise oskus

	- strateegilised oskused
Jamnes, *et al*., 2013 (vastavuses Eesti kvalifikatsiooniraamistikuga): + lisa **digikompetentside kirjedustest kutsestandardites**	IKT-kompetentside kirjeldamisel mitte-IKT valdkonna kutsestandardites lähtutakse kolmest dimensioonist: - baasdigioskused (DigComp alusel) - erialased IKT-kompetentsid - eriala +IKT-kompetentsid
Carretero, *et al.*, 2017 (DigComp 2.1 alusel koostatud)	sisaldab 8 kompetentsiastet ja näiteid nende kasutamise kohta alljärgnevates kompetentsivaldkondades: ➢ info- ja andmekirjaoskus ➢ suhtlemine ja koostöö ➢ probleemide lahendamine ➢ sisu loomine ➢ turvalisus

Eespool toodu kinnitab üld- ja digikompetentside omandamise, arendamise ja pideva kaasajastamise vajadust nii indiviidi kui organisatsiooni vaates. Politseiuurija töös on IKT-l kaksikroll: ühelt poolt suurendab ja toetab see uurimistegevuse tõhusust, samas suurendab see aga ka kurjategijate potentsiaali (European Commission, 2016, p. 69–70). Politseiuurija ametil tuleb arvestada üld- ja digikompetentside keskmisest kõrgema tasemega, kuna töö on seotud suhtlemise ja informatsiooni töötlemisega, mis hõlmab selle otsimist, süstematiseerimist ja analüüsi. Palju infot hangitakse ja töödeldakse digitaalsel kujul. Soovituslikus politseiuurija töö analüüsi (European Commission, 2016, p. 69–70) kohaselt on politseitöö keeruline teabepõhine tegevus, mis eeldab erinevate andmeallikate integreerimist ning seda sageli lühikese aja jooksul. Üldkompetentsid kätkevad osa digikompetentse, võttes arvesse digiajastu vajadusi. Tugevad üldkompetentsid on aga eelduseks digi- ja kutsespetsiifiliste kompetentside edukaks arendamiseks. Järgnevalt käsitletakse digitaalse komponenidga kuritegude uurimiseks vajalikke kutsespetsiifilisi kompetentse.

1.3.2 Kohaliku tasandi politseiuurija kutsespetsiifilised kompetentsid

Lisaks üld- (sh digi-)kompetentsidele eeldatakse politseiuurijatelt kuritegude uurimiseks vajalikke kutsepetsiifilisi kompetentse, mis hõlmavad teadmisi õigusest (sh valdkonna rahvusvahelisest koostöö õigusküsimustest), kriminoloogiast ja (digitaal-)kriminalistikast. Seda kinnitab käesoleva töö esimeses alapeatükis antud ülevaade digitaalse komponendiga kuritegude uurimise valdkonnast, selle spetsiifikast ja väljakutsetest. Politsei organisatsioonides on erinevate üksuste uurijate rollid, tasandid, spetsialiseerumine ja sellest tulenevalt ka tööülesannete ning selleks vajalike kompetentside sisu ja

maht erinevad (Beesley, 2021; CEPOL, 2022). Aktuaalsete digitaalse komponendiga kuritegude uurimiseks vajalike kompetentside määratlemiseks kasutatakse käesolevas töös kaardistavaid uuringuid, mis on pühendatud politseiuurijate koolitusvajaduse hindamisele nii rahvusvaheliselt (nt CEPOL) kui siseriiklikult (nt Kanada). Järgnevalt tuuakse näiteid politseiuurijate kutsepetsiifiliste kompetentside määratlemise praktikast, mida saab arvesse võtta käesolevas töös kompetentsiraamistiku väljatöötamisel.

Kooskõlas Marrelli, *et al*. (2005) kompetentsimudeli neljanda etapiga (käesolev töö, lk 31–32) on oluline määratleda uurija tasand organisatsioonis, sest erinevate üksuste uurijate tööülesannete ulatus ja spetsiifika erinevad. Tuleb koostada kirjeldus ametikoha spetsialiseerumise või erifunktsiooni kohta. Heaks näiteks politseiametnike rollide ja tasandite, ning seega nende kompetentside piiritlemise kohta on Kanadas välja töötatud maatriksi kujuline kompetentsipõhine juhtimisraamistik. See lähenemine keskendub inimressursside juhtimisele, määratledes oskused, teadmised ja omadused, mis aitavad kaasa töö tõhususele ja tulemuslikkusele konkreetsel ametikohal (töörollis) töötamiseks. (Beesley, 2021, pp. 1–2)

Kanada politsei kontekstis klassifitseerib kompetentsipõhine raamistik põhilisi käitumis-, tehnilisi ja juhtimiskompetentse, mis on seotud üldiste ülesannete, uurimis- ja juhtimisülesannetega. Kanada raamistikus on määratletud kümme digikompetentsi, millel on omakorda viis taset. Raamistikus kirjeldatakse põhikompetentsid, nende tasemed 1–5 ning kompetentsiprofiilid soovitatavate kompetentside kombinatsiooni- ja tasemetega. Konkreetsele töökohale (-rollile) on ette nähtud vajalikel tasemel kompetentside kombinatsioon. Kanada õiguskaitseasutuste digikompetentside eelnõu koostamseks tehti kirjanduse ja praktika ülevaate ja ühendati konsultatsioonifaasi ja arendusetapi käigus kogutud teave ja teadmised. Raamistikku kuuluvad järgmised kompetentside valdkonnad: 1) digitaalkirjaoskus ja internet; 2) küberhügieen ja küberturvalisus; 3) küberkuritegevuse alane teadlikkus, ennetamine ja ohvriabi; 4) avatud allikaga luure (OSINT) ja tõendite kogumine; 5) küberruumiga seotud õigusalased küsimused (sh rahvusvahelise koostöö osas); 6) küberandmed ja luureanalüüsid; 7) krüptoraha ja plokiahelad; 8) programmeerimine ja skriptimine; 9) digitaalne kohtueksperтiis; 10) võrgu kohtueksperтiis. (Canadian Police Knowledge Network, 2020, pp. 1–4 ref Beesley, 2021, p. 4; Greenwood, 2020 ref Beesley, 2021, p. 4) Nagu näha kuuluvad osa eespool nimetatud kompetentside valdkondasid üldkompetentside alla (nt digitaalkirjaoskus ja internet, küberhügieen ja küberturvalisus).

Kanada politsei digikompetentsiraamistiku koostamisel võeti arvesse EL-s ja USA-s kasutusel olevatest politseinike eri rollide ja tasandite digikompetentside loetelusid (CEPOL Cybercrime Training and Education Group (ECTEG), 2020; USA National White Collar Crime Center (NW3C, 2021) ja analüüsiti neid Kanada konteksti vaates. Arvesse on võetud ka CEPOL ECTEG välja töötanud E-FIRST esmareageerijate koolituspaketti, mille abil loodetakse koolitada tuhandeid esmareageerijaid järgmiste kompetentside omandamiseks: 1) võime tuvastada ja konfiskeerida võimalikke elektroonilisi tõendeid, sealhulgas reaalajas andmeid kohtuekspertiisi jaoks; 2) teadlikkus küberkuritegevusest, internetist, krüpteerimisest, tumedast veebist ja krüptovaluutadest; 3) tehnoloogia abil hõlbustatud kuritegude ohvrite abistamine (kuriteo-)kaebuse esitamisel ja kriminaalmenetluse algatamisel (CEPOL ECTEG, 2021; Beesley, 2021, pp. 1–4). CEPOL ECTEG-maatriksi digitaalsed pädevused on kokkuvõtlikult esitatud tabelina lisas 3 (käesolev töö, lk 109). Ameerika Ühendriikides on küberkuritegude uurijatele mõeldud erialased sertifikaadid, mis kinnitavad konkreetselt sõnastatud nõudmistele vastavust vajalike teadmiste ja oskustele osas (USA National White Collar Crime Center (NW3C), 2021 ref Beesley, 2021 pp. 15–16, vt tabel 5).

Tabel 5. NW3C sertifikaadi saamiseks nõutavate teadmiste kogum (USA NW3C, 2021 ref Beesley, 2021, pp. 15–16)

Sertifitseeritud küberkuritegude uurija roll ja ülesanded (3CE)	**Sertifitseeritud küberkuritegevuse uurija roll ja ülesanded (3CI)**
kohaldada digitaalse kohtuekspertiisi (digitaalkriminalistika) parimaid tavasid usaldusväärsete digitaalsete tõendite fotografeerimisel, dokumenteerimisel ja nende kohta aruannete esitamisel	avastada küberkuritegusid ja veebipõhiseid kuritegusid, nendele reageerida ja neid uurida, Suhelda nendel teemadel asjassepuutuvate isikutega.
3CE teadmiste kogum:	**3CI teadmiste kogum:**
1. tehnoloogiad 2. digitaalsete tõendite käsitlemine 3. kohtuekspertiisi pildistamine 4. failisüsteemi kohtuekspertiis 5. kohtuekspertiisi mõisted 6. seadusandlik, õiguslik ja regulatiivne raamistik	1.teooria ja ajalugu 2.levinumad küberkuritegude ja interneti vahendusel toimepandud kuritegude vormid 3.elektrooniliste teenuste pakkujate valduses olevate tõendite kogumine ja analüüs 4.küberkuritegevuse ja interneti vahendusel toimepandud kuritegude uurimine 5.küberturvalisus, küberkuritegevuse vähendamine ja küberhügieen 6.seadusandlik, õiguslik ja regulatiivne raamistik

Kompetentside ja (sh digi-) oskuste vajaduste hindamiseks tehti veel mitu politseiuurija töö soovituslikku kirjeldust, mille kohaselt teevad uurijad üldist klassikalist politseitööd, sh kuritegude uurimist. Kuriteo uurimisel põhitegevusteks on vastavalt õigusnormidele tõendusmaterjali kogumine, analüüsimine, süstematiseerimine ja ettevalmistamine juhtumis lahendi tegemiseks. Vajadusel tehakse koostööd teiste õiguskaitseasutuste- ja muude koostööpartneritega. (European Commission, 2016; Euroopa Komisjon, 2022) Sellest võib järeldada, et kriminaaluurimise raames informatsiooni ja tõendite kogumine toimub nii digitaalselt kui ka füüsiliselt.

EL uues strateegilises vajaduste hindamises (ingl k *European Union Strategic Training Needs Assessment* – edaspidi EU-STNA) määratletakse õiguskaitseametnike strateegilised ELi tasandi koolitusprioriteedid nelja-aastaseks tsükliks (2022–2025) kooskõlas Euroopa multidistsiplinaarse kuritegevuse vastase platvormi (ingl k *European Multidisciplinary Platform Against Criminal Threats* – järgnevalt EMPACT) prioriteetidega, rõhutades digioskuste ja uute tehnoloogiate kasutamise tähtsust ühe peamise horisontaalse aspektina, mida tuleks käsitleda kõigis koolitustegevustes. Võttes arvesse EU-STNA protsessi tulemusi, on CEPOL 2021. aastal käivitanud struktureeritud koolitusvajaduste analüüsi (ingl k *Operational Training Need Analysis* – järgnevalt OTNA) digitaaloskuste ja uute tehnoloogiate kasutamise kohta, et määratleda õiguskaitse digitaliseerimist käsitlev koolitusportfell aastateks 2023–2025. Tulemused näitavad, et nõudlus koolituse järele on teemade ja potentsiaalsete koolitatavate arvu poolest suur ning õiguskaitseametnike edasiseks ettevalmistamiseks digitaalajastuks on vaja paindlikke õppelahendusi (CEPOL, 2022; Coman & Alexa, 2022).

Prioriteetsemateks koolitusteemadeks on digitaalsed uurimised, uute tehnoloogiate kasutamine ja digitaalne kohtuekspertiis (kriminalistika), mistõttu tuleks neid lülitada õiguskaitsealasesse koolitustegevusse (Coman & Alexa, 2022, p. 23) Seoses õiguskaitseametnike põhivõimekuse tagamiseks vajalike digioskuste puudujäägiga kuuluvad koolitusvajaduste loetellu erinevad teemad: digioskused ja uute tehnoloogiate kasutamine; küberturbe alused ELi ametnike igapäevaseks kasutamiseks (küberhügieen, küberturbe suunised, turvaline teabevahetus, füüsiline turvalisus); teadlikkuse tõstmine kõige olulisematest küberohtudest (e-posti-põhised rünnakud, veebipõhised rünnakud, DDoS-rünnakud, sotsiaalmeedia pettused); kaasaegsetest tehnoloogiatest (nt tehisintellekt või 5G) ja nendest tulenevate küberturvalisuse probleemide mõistmine. Digitaalse uurimise valdkonda on omakorda koondatud järgmised alateemad: avatud allikaga luure (OSINT), tumedad võrgud,

küberohtude luure, teadmiste haldamine, dekrüpteerimine, tehisintellekti kasutamine, suurandmete analüüs, kvantitatiivsed ja kvalitatiivsed analüüsimeetodid, asjade internet, kaamerasüsteemide, droonide, eksoskelettide ja kõneprotsessorite täiustatud kasutamine, suurandmete analüüs kuritegeliku käitumise prognoosimiseks, krüptovaluutade kasutamine, digitaalne kohtueksperтiis/digitaalkriminalistika, ohvrite kaitse, põhiõigused ja andmekaitse. (CEPOL, 2022; Coman & Alexa, 2022)

Seega, nii käesoleva töö peatükkides käsitletud teadusallikad kui praktikud on ühel meelel selles, et politsei esmareageerijate ja traditsiooniliste kuritegude ja/või kohaliku tasandi politseiuurijate töös tekkinud ja hoogsalt kasvanud digitaalse komponendiga kuritegude osakaalu tõttu tuleb otsida lahendusi selles valdkonnas ametnike kompetentsuse tõstmiseks. Viimases alapeatükis esitatakse kompetentsiraamistik.

1.3.3 Kohaliku tasandi politseiüksuse uurija kompetentsiraamistik digitaalse komponendiga kuritegude uurimiseks

Politseinike (digi-)kompetentsid peavad ulatuma kaugemale küberkuritegevuse laiast määratlusest (Beesley, 2021, p. 9). Sultana, (2009, p. 21), rõhutades kompetentsuse määratlemisel teadmiste, tegemiste ja suhtumise kombineerimise terviklikku lähenemist, väidab, et kompetentne inimene on võimeline kombineerima oma teadmiste ja oskuste erinevaid aspekte, et reageerida konkreetsetes kontekstides tekkivatele väljakutsetele ja olukordadele (Sultana, 2009, p. 21). Kontekstiks on üldine ühiskonna digitaliseerumine ja sellest tulenev kuritegevuse struktuuri muutus (käesolev töö, lk 7–8, 13–14)

Arvestades politseis lahendatavate digitaalse komponendiga kuritegude levikut (Vincze, 2016, p. 183; Tarter, 2017 p. 213; Holt & Bossler, 2016, pp. 2–4; Furnell & Dowling, 2019, p. 10; Pernik, 2019, p.71–72), on ebarealistlik oodata, et kõrgelt kvalifitseeritud ja küberkuritegevusele kitsalt spetsialiseeritud politsei funktsionaalüksused reageeriks igale digikomponendiga juhtumile ja on mõistlik eeldada, et igal politseiametnikul on digikompetentside baastase (Beesley, 2021, pp. 9–11). Baastaseme, ehk kohaliku tasandi politseiuurija oskuste taseme määratlemiseks kastutatakse magistritöös välja töötatud kompetentsiraamistikus SA Kutsekoda kvalifikatsiooniraamistiku tasemekirjeldusi vahemikus 3–5 (SA Kutsekoda, 2023, käesoleva töö lisa 5, lk 118).

Kompetentsiraamistikul või -mudelil põhinev terviklik lähenemine organisatsioonis annab valdkonnale peamised kontseptuaalsed kategooriad või ehitusplokid, samuti aluseks oleva filosoofia, teadmiste olemuse ja komponentide vaheliste suhete kohta (Sultana, 2009, p. 22; Beesley, 2021, pp. 9–11) Kompetentsiraamistikus määratletakse rollid ja tööülesannete täitmiseks vajalikud oskused, teadmised, isiksuseomadused ning käitumisviisid (Lucia & Lepsinger, 1999 ref Stacy, 2000).

Käesoleval juhul kasutatakse raamistikupõhist (horisontaalset) lähenemist (Boyatzis, 1982 ref Bellini, *et al.*, 2021, p. 604, käesolev töö lk 28),mis põhineb ametikoha tasemel. Kompetentsid jaotatakse üld- ja kutsespetsiifilisteks (Jamnes, *et al.*, 2013, Haaristo, *et al.*, 2015, lk 6, 27, käesolev töö lk 30–31). Teoreetiliselt (Marrelli, *et al.*, 2005, pp. 537–539) on kompetentside modelleerimise protsessis vaja paindlikkust, mis vähendab õiguslikke riske organisatsioonile mudeli rakendamise korral. Ranguse ja täpsuse tase määratletakse selle järgi, kui oluline on organisatsiooni jaoks tuvastatud kompetentside täpsus ja põhjalikkus.

Käesolevas töös lähtuti kompetentsiraamistiku eesmärgi sõnastamisel ja selle vajalikkuse põhjendamisel Marrelli, *et al.*, (2005, pp. 539–559) kompetentsimudeli koostamise metoodikast. Enne kompetentsimudeli koostamist tuleb määratleda kompetentsimudeli eesmärk, põhjendada selle vajalikkust, täpsustada kohaldamisala, valida analüüsiüksused ning määratleda ajavahemik kompetentside kehtivuse ja ajakohastamise osas (vt tabel 6). Käesolevas magistritöös välja töötatud kompetentsiraamistik on esitatud lisas 4 (käesolev töö, lk 112).

Tabel 6. Kompetentsiraamistiku eesmärgistamine (Marrelli, *et al.*, p. 239 alusel, autori koostatud)

Vajaduse välja toomine ja põhjendamine	Nõuded kohaliku tasandi uurija kompetentsidele on viimastel aastatel oluliselt muutunud ühiskonna digitaliseerumise ja kuritegudel digitaalse komponendi tekkimise ja selle kasvu tõttu. Järgmise aastate jooksul on oodata digitaalse komponendiga kuritegude arvu suurenemist ja mitmekesistumist (käesoleva töö alapeatükk 1.1)
Sihtgrupp ja parameetrid (analüüsi üksus ja ajaline perspektiiv)	Tuleb määratleda kohaliku tasandi uurijate kompetentsid, mis on olulised tõhusaks tööks digitaalse komponendiga kuritegude uurimisel. Need on vajalikud juba praegu ning järgneval 3 aastal.

Rakendamine/kohaldamine	Välja töötatud kompetentsiraamistiku võimalik rakendusala: ➢ uurijate praegused arenguvajaduste kindlaks tegemisel digitaalse komponendiga kuritegude uurimiseks ja politsei organisatsiooni siseste koolitusprogrammide ja -materjalide väljatöötamisel nende vajaduste katteks ➢ kohaliku tasandi uurijate värbamisel ➢ koostöös haridusasutusega, kes tegeleb spetsialistide ettevalmistamisega, asjakohase riikliku tellimuse kujundamiseks

Kokkuvõtteks, esimeses peatükis toodi välja digitaalse komponendiga kuritegude uurimisel tekkinud väljakutsed ja kitsaskohad, defineeriti digitaalse komponendiga kuriteo mõistet ja toodi sellest näiteid, kasutades küberkuritegude terminoloogiat ja liigitusi. Seejärel esitati teoreetiline käsitlus organisatsioonis kompetentsipõhise lähenemise kasutamisest ning tugevustest ja nõrkustest kompetentsiaamistiku rakendamisel organisatsiooni ja indiviidi (töötaja) vaates. Tuginedes teoreetilistele lähtekohtadele, koostati kohaliku tasandi politseiuurijate digitaalse komponendiga kuritegude uurimiseks vajalik kompetentsiraamistik, süstematiseerides kompetentse kolme kategooriasse, milleks on üld-, üld-digi- ja kutsespetsiifilised kompetentsid. Kuna käesoleva töö valmimisel selgus, et 2022. aastal ilmusid SA Kutsekoda poolt tööelu ja üldoskuste kaasajastatud kontseptsioon (Leemet, *et al.*, 2022) ja DigComp 2.2 (Vuorikari, *et al*., 2022), mida teoreetilises osas arvesse ei võetud, analüüsitakse neid empiirilise uuringu raames, et välja tuua asjakohaseid valdkonna edasiarendusi.

Võttes arvesse magistritöö formaati ja PPA uurimistöö loa (PPA e-kiri, reg. 23.02.2023 nr 1.1-14/41-2, autori valduses) piiranguid, kasutatati kompetentsiraamistiku väljatöötamisel ja selle valideerimise kavandamisel vaid mõningaid Marrelli, *et al*. (2005) metoodika elemente. Nendeks on eesmärkide määratlemine, oluliste aspektide arvesse võtmine, kompetentsiraamistiku koostamise metoodika väljatöötamine, teoreetilise kompetentsimudeli loomine ja selle hindamine ning kohandamine pärast empiirilise uuringu käigus saadud andmete analüüsi. Järgnevalt valideeritakse magistritöös välja töötatud kompetentsiraamistikku empiirilise uuringu raames.

2. KOHALIKU TASANDI POLITSEIUURIJATELE DIGITAALSE KOMPONENDIGA KURITEGUDE UURIMISEKS VAJALIKU KOMPETENTSIRAAMISTIKU VALIDEERIMINE

2.1 Metoodika ja valim

Käesolevas alapeatükis esitatakse eelkõige uuringut ettevalmistava teaduskirjanduse ülevaate koostamise metoodika, mis võimaldas luua kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimiseks vajaliku teoreetilise kompetentsiraamistiku. Järgnevalt tutvustatakse empiirilise uuringu metoodikat.

2.1.1 Teoreetilise käsitluse koostamise metoodika

Käesoleva töö esimese etapina analüüsiti relevantset teaduskirjandust ja teiste riikide praktikaid, et ette valmistada alus juhtumi igakülgseks uurimiseks ja leida vastused uurimisküsimustele 1–3 (käesoleva töö lk 10). Kirjanduse ülevaade on teoreetiline alus ja uurimiskava koostamise vahend (Yin, 2003, p. 9), mis on vajalik uuringu fookuse ja ulatuse täpsustamiseks (Gray, 2018, p. 6) ning ühtlasi on põhjenduseks uuringule valitud lähenemisele ja metoodikale (Levy & Ellis, 2006, p. 183–184). Varasemad uuringud analüüsiti ja süstematiseeriti vastavalt püstitatud uurimisküsimustele (Yin, 2003, p. 9, 30–31; Gray, 2018, p. 6).

Käesoleva töö ja juhtumiuuringu epistimoloogiline orientatsioon tuleneb interpretivistlikust traditsioonist, mille kohaselt püütakse mõista, kuidas inimesed tähendusi loovad ja sündmusi tõlgendavad (Õunapuu, 2014, lk 32). Ontoloogiline küsimus lahendatakse konstruktivistlikust seisukohast lähtuvalt (Õunapuu, 2014, lk 32, 53–54), mille kohaselt sotsiaalseid nähtusi ja nende tähendusi luuakse ning ka pidevalt töötatakse ümber sotsiaalses interaktsioonis (Berger & Luckmann, 1991, pp. 69–70). Konstruktivistid usuvad, et inimesed konstrueerivad oma tähendust erinevalt, isegi ühe ja sama nähtuse suhtes. (Robson, 2002 ref Poni, 2014, p. 410) Uuringu üheks raamteemadest on kompetentsid ja nende süstematiseerimise viis. Kompetentsuse mõiste näol on tegemist ühiskonna poolt loodud konstruktsiooniga, mis ei ole absoluutne, vaid see kätkeb tõlgendusi ja tähenduste kogumi (Shavelsoni, 2013, p. 74). Süsteem, mille alusel kompetentsust määratletakse ja skriptitakse, on sotsiaalselt läbiräägitav ja lahtine, tegemist on ajas muutuva ja killustunud konstruktsiooniga (Kosmala 2013, p. 578)

Käesolevas töös kasutati meta-etnograafilist kirjandusülevaate koostamise meetodit, mis seisneb kvalitatiivsete uuringute ja muude sekundaarsete allikate tõlgendavas sünteesis. Eelkõige määratleti käesoleva töö uurimisväli ja fookus, milleks on kompetentsiraamistiku väljatöötamise ja valideerimise protsess konkreetse töövaldkonna või funktsiooni näitel. Seejärel otsiti relevantseid allikaid ja nende vahelisi seoseid. Sünteesis keskenduti kirjanduse ülevaatesse kaasatud uuringutes pakutavatele tõlgendustele ja selgitustele, mitte üksnes andmetele, millel need uuringud põhinevad. (Bryman, 2008, p. 89)

Kirjanduse ülevaate koostamiseks relevantsete allikate leidmiseks kasutati mitut ringi Kimberley ja Croslingu (2012, p. 24–25 ref Õunapuu, 2014, lk 97) metoodikat, mis seisnes järgnevas seitsmes etapis:

1) Fikseeriti uurimisteema/-väli: kohaliku tasandi politseiuurijate kompetentsid digitaalse komponendiga kuritegude uurimiseks, kompetentsiraamistiku koostamine.
2) Määrati kindlaks töö alateemadele vastavad põhimõistete plokid ja otsingusõnad: **digitaalse komponendiga kuritegu** – ingl k otsingusõnad: *cybercrime, cyber-dependant crime, cyber-enabled crime, online-crime)*; **politseiuurijate kompetentsus/kompetentsid** – ingl k otsingusõnad *police investigators/detectives kompetence/competency, digital competence/competency, general competence, professional competence*. **Kompetentsimudel/-raamistik** – ingl k *competence/competency model, competence framework.* **Politseiuurijatele digitaliseerumisest tingitud väljakutsete** kohta allikate otsimiseks tugineti küberkuritegevuse ja digitaalkriminalistika teemalistele teadusartiklitele, need allikad liigitati digitaalse komponendiga kuriteo kategooria alla.
3) Koostati nimekirja lähedastest mõistetest, mis väljendavad põhimõistet pisut teisiti ja teemaplokkidega seotud mõistetest (vt tabel 7, käesolev töö, lk 49).
4) Google Scholar platvormilt, elektroonilistest repositooriumitest, teadusallikate andmebaasidest (EBSCOHost, Proquest, SAGE, ScienceDirect, HeinOnline jt) teostati laiendatud otsingut põhimõistete ja nende lähedaste mõistete ühendamine loogikaoperaatoriga OR (või) otsingu laiendamiseks.
5) Seejärel ühendati põhimõistete ja nende lähedaste mõistete kombinatsioone loogikaoperaatoriga AND (ja), et saada otsingutulemus, mis sisaldab vähemalt ühe kombinatsiooni terminitest.
6) Hinnati otsingutulemusi.

7) Muudeti algset päringut ja hinnati uusi otsingutulemusi.

Tabel 7. Teadusallikate infootsingu märksõnadega lähedased ja teemaplokile vastavad mõisted

digitaalse komponendiga kuritegu(juhtum)	**politseiuurijate kompetentsus/kompetentsid**	**kompetentsimudel/-raamistik**
Ingl k - *digital forensics; digital forensics challenges; digital forensics policy ,forensics readiness; computer forensics; software forensic; database forensics; multimedia forensics; device forensics; network forensics; internet policing, etc*	Ingl k - *police officers´ skills; skills; knowledge; digital skills; digital literacy; soft skills; hard skills; human resources management; century skills; organizational competences professional profiles; concept of competence, employee competence; professional competence; professional practice; professionalism; police training and expertise, etc*	Ingl k – *Competency/competence frameworks; expert evaluation; competence modeling; competence assessment; European Qualification Framework-EQF*

Lisaks eespool toodud metoodikale pöörati tähelepanu ka valitud allikate bibliograafiatele, kus samuti valiti kirjandusülevaate teemade plokidega haakuvaid teadus- ja muid allikaid. Kirjandusülevaate valimisse valiti teemaplokkide kohta huvipakkuva informatsiooni sisaldavad eelretsenseeritud teadusallikad ja praktilise suunitlusega dokumendid. Otsing toimus järjepidevalt ajavahemikus august 2022.a – veebruar 2023.a, kirjanduse ülevaade täiendati jooksvalt selle koostamise vältel. Töö fookus ja teemaplokid ning empiirilise uuringu metoodika täpsustusid lõplikult 2022. aasta novembriks, kuid seda tuli muuta ja kohandada lähtuvalt PPA 23.02.2023 saadud uurimistöö loa (reg. 23.02.2023 nr 1.1-14/41-2, e-kiri, autori valduses) piirangutest.

2.1.2 Empiirilise uuringu metoodika ja valim

Käesolevas töös kasutatakse **juhtumiuuringu uurimisstrateegiat** (Yin, 2003, p. 23), mis on sobiv viis programmide, protsesside ja tegevuste süvitsi uurimiseks (Creswell 2009, pp. 58, 227; Creswell & Poth, 2016, p. 74–75) ja uurimisküsimustele „kuidas“, „millised, missugused, mis“ vastuste leidmiseks (Yin, 2003, p. 7). Uurimisprobleem on sõnastatud küsimusena: kuidas süstematiseerida aktuaalseid kompetentse, mis on tänapäeval vajalikud kohaliku tasandi uurijatele digitaalse komponendiga kuritegude uurimisel? Kuigi juhtumiuuringu võib seostada nii induktiivse kui deduktiivse lähenemise kasutamisega (Bryman, 2008, p. 57; 373), lähtuti käesolevas töös juhtumiuuringu läbiviimisel konstruktivistlikust paradigmast, kus esineb tugev deduktiivne element (Blatter 2008, pp. 69–71). Uuring algas teooriaga ja uurimisprobleemi lahendamise võimalusi hinnati teoreetilises käsitluses

tooduga võrdlevalt. Magistritöö empiirilise uuringu raames andmete kogumisel ja analüüsimisel lähtuti teoreetilise käsitluse alateemadest (Yin 2009, p. 131), kontseptualiseerides juhtumi "piiratud süsteemi" (Rule & John, 2015). Juhtumiuuringus saadud andmete analüüsimisel kategooriate ja deduktiivsete koodide moodustamisel tugneti teooriale, kuid uuringus saadud andmete põhjal tuletati ka induktiivsed koodid.

Juhtumiks on kompetentsiraamistiku väljatöötamise ja valideerimise protsess. Kompetentsiraamistiku valideerimisel täpsustatakse, kuidas on hetkel korraldatud PPA-s ja Sisekaitseakadeemias kohaliku tasandi politseiuurijate digitaalse komponendiga kuritegude uurimiseks vajaliku kompetentsuse kriteeriumide korraldamisega seonduv ning millised on magistritöös välja töötatud kompetentsiraamistiku tugevused, nõrkused ja rakendusvõimalused. Protsessi käsitleti terviklikult, kus uuritav nähtus ei eristu selgelt juhtumi kontekstist (Yin, 2003, pp. 13–14), et saada vastust kõigile töös püstitatud uurimisküsimustele. Kontekstiks on kohaliku tasandi politseiuurijate tasandi kompetentsivajadus digitaalse komponendiga kuritegude uurimiseks ja selleks vajalike oskuste süstematiseerimise lähenemised.

Uurimisinstrumentideks on **poolstruktureeritud ekspertintervjuud** ja **dokumendianalüüs** (Flick, 2009, pp. 165, 255–259). Kvalitatiivsed uurimismeetodid on eelistatud põhjusel, kuna neid peetakse eriti kasulikuks juhtumi intensiivse ja üksikasjaliku uurimise loomisel (Bryman, 2008, p. 53). Uuringus teineteist täiendavate teabeallikate kasutamisega taotleti terviklikku lähenemist ja uurimistulemuste valiidsust (Lub, 2015, p. 3) Uuringu andmete analüüsimiseks kasutati **kvalitatiivset sisuanalüüsi** ja **kodeerimismeetodit** (Saldaña, 2013, p. 22).

Magistritöös välja töötatud kompetentsiraamistikku valideeriti valdkonna asjatundjate **ekspertintervjuude abil**. Empiirilise uuringu andmed koguti loomulikus keskkonnas vesteldes nende osalejatega, kellel on kogemusi uuritava teemaga ja kes on otseselt seotud selle kontekstiga (Creswell 2009, p. 175) **Eesmärgistatud valimisse** (Teddlie & Yu, 2007, pp. 77–79) kuuluvad 4 PPA strateegilise planeerimise tasandi eksperti, 3 Sisekaitseakadeemia õppeprogrammide arendamise ja valdkonna õppeainetega seotud eksperti ja 3 Põhja Ringkonnaprokuratuuri abiprokuröri, kelle ülesandeks on kogukonnakuritegude uurimise juhtimine. Nende isikute valimisse kaasamine põhineb uurimisküsimustele vastamisega seotud konkreetsete eesmärkidega (Teddlie & Yu, 2007, p. 77–79). Valimi moodustamise viisi valikut põhjendab asjaolu, et ekspertide arv, keda on lubatud PPA poolt uuringusse kaasata (PPA uurimistööde kooskõlastamise komisjoni uuringu läbiviimise luba, reg.

23.02.2023, nr 1.1-14/41-2, autori valduses) ja PPA väliste spetsialistide ring, kes on pädevad ja nõus uuringu spetsiifilistel teemadel kaasa rääkima, on piiratud. Ekspertide valimi moodustamise põhimõtted on ühtlasi osaliselt kooskõlas Sultana (2009) ülevalt-alla viisil kompetentsiraamistiku koostamisega (käesolev töö, lk 30) ja Marrelli, *et al.* (2005), kompetentsimudeli konstrueerimise metoodika neljandas ja viiendas etapis kirjeldatud erinevatest asjasse puutuvatest isikutest valimi moodustamise põhimõtetega (käesolev töö, lk 31–33).

Ekspertide valimi moodustamisel arvestati nende kogemust ja kokkupuudet kohaliku tasandi politseiuurijatega ning digitaalse komponendiga kuritegude uurimisega seonduvaga. PPA ekspertideks on kogukonnasüütegude lahendamise, kriminalistika ning värbamis- ja koolitusteenuse omanikud ja digikriminalistika keskuse juht. Sisekaitseakadeemia ekspertideks on politsei eriala õppekavade koostamise, arendamise ja vastavate õppeainete õpetamisega seotud spetsialistid. Täiendava väärtuse annab kolme Põhja Ringkonnaprokuratuuri abiprokuröride panus, kuna viimased puutuvad tööalaselt kokku kohaliku tasandi politseiuurijatega ning nende menetlusasjades olevate digitaalsete komponentidega. Ekspertide valimi ja intervjuude läbiviimise tehnilisi andmeid kirjeldav tabel sisaldub lisas 7 (käesolev töö, lk 127).

Dokumendianalüüsi mugavusvalimisse (Teddlie & Yu, 2007, pp. 77–79) valiti 10 teksti ja dokumenti, mis autori seisukohal sisaldavad uurimisküsimusele vastamiseks vajalikku informatsiooni kohaliku tasandi politseiuurija töö kirjelduse, kutsekvalifikatsiooni nõuete ja digitaalse komponendiga kuritegude uurimisel aktuaalsete kompetentside kohta. Dokumendianalüüsi valimisse kaastakse ka Eestis kasutusel olevad kompetentsiraamistiku koostamise metoodikaid sisaldavad dokumendid. Käesoleva töö valmimisel selgus, et 2022. aastal ilmus SA Kutsekoda poolt tööelu üldoskuste edasiarendatud ja kaasajastatud kontseptsioon (Leemet, *et al.*, 2022) ja uus digikompetentside raamistik DigComp 2.2 (Vuorikari, *et al.*, 2022), mida teoreetilises osas ja ekspertintervjuude läbiviimisel arvesse ei võetud. Samas, üld- ja digikompetentsid moodustavad magistritöös väljatöötatud kompetentsiraamistiku eraldi kategooriad. Seega, tuleb antud kontseptsioonid analüüsida empiirilise uuringu raames, et välja tuua edasiarendusi üld- ja digikompetentside vaates. Dokumendianalüüsi valim on toodud tabelis 8 (käesolev töö, lk 52).

Nii ekspertintervjuude transkriptsioonide analüüsimisel kui dokumendianalüüsis kasutati kodeerimise meetodit (Saldaña, 2009, p. 22) ning uurimisküsimuste põhjal moodustatud ühise kategooriate ja koodide süsteemi (käesoleva töö lisa 8, lk 128). Kuna dokumendianalüüsi eesmärgiks oli täpsustada ja

täiendada ekspertintervjuude käigus kogutud andmed, siis sel põhjusel dokumendianalüüsis kasutati vaid osa koode ja kategooriad (käesoleva töö lisa 8, lk 128). Intervjuude transkriptsioonid ja dokumendianalüüsiks valitud tekstid analüüsiti NVivo14 andmetöötlusprogrammi abil.

Tabel 8. Dokumendianalüüsi valimisse kuuluvad tekstid ja dokumendid

Dokumendile viitamisel kasutatav tunnus	**Tekst/dokument**
D1	PPA vastus kohaliku tasandi uurijate (st. politseijaoskondade uurijate) taustainfo kohta (e-kiri 30.03.2023, autori valduses)
D2	ESCO kriminaaluurija tööülesannete ja funktsioonide kirjeldus (Euroopa Komisjon, 2022)
D3	Politseiametniku ning Politsei- ja Piirivalveameti struktuuriüksuse juhi ametikohal teenistuses oleva ametniku kutsesobivusnõuded, nende kontrollimise tingimused ja kord (Siseministri määrus, 2013, RT I, 29.08.2019, 7)
D4	Sisekaitseakadeemia vastus selgitustaotlusele (päring seoses magistritöö koostamisega; vastus 6.1-17/3250-1 – autori valduses), milles viidatakse politsei eriala õppekavadele: ➢ Politseiametniku õppekava (kutseõppe esmaõpe, statsionaarne õpe ja mittestatsionaarne õpe), kinnitatud Sisekaitseakadeemia rektori 31.05.2021 käskkirjaga nr 6.1-5/319, EHIS kood 170157 ➢ Süüteomenetleja õppekava (kutseõppe jätkuõpe, mittestatsionaarne õpe), kinnitatud Sisekaitseakadeemia rektori 26.05.2020 käskkirjaga nr 1.1-5/151, EHIS kood 187017 ➢ Politseiteenistuse eriala õppekava (kõrgharidus), kinnitatud Sisekaitseakadeemia nõukogu istungi 20.05.2021 protokolli nr. 1-1-5/160 protokollilise otsusega, EHIS kood 108771
D5	OSKA ülevaade valdkonnaspetsiifiliste IKT-oskuste vajadusest (SA Kutsekoda, 2020a)
D6	Tulevikuvaade tööjõu- ja oskuste vajadusele: Siseturvalisus ja õigus. Siseturvalisuse alavaldkond (SA Kutsekoda, 2020b)
D7	OSKA põhikutsealade hõive muutuse prognoos ning hinnang tööjõu nõudluse ja koolituspakkumise tasakaalule (OSKA, 2022)
D8	Tööelu üldoskuste klassifikatsioon ning tulevikuvajadus. Uuringu terviktekst. Tallinn: SA Kutsekoda (Leemet & Ungro, 2022)
D9	DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes (Vuorikari, *et al*., 2022)
D10	Kohalike omavalitsuste kompetentside põhise koolitusvajaduse hindamise metoodika ja analüüs: Lõpparuanne (Õunapuu, *et al.*, 2021)

2.2 Uuringu käik ja tulemused

Ekspertintervjuude küsimustikud koostati kolmes variandis, võttes arvesse ekspertide tegevusvaldkonna erisusi ja kokkupuudet kohaliku tasandi politseiuurijatega. Küsimused on jaotatud teemaplokideks. PPA ekspertidele ettenähtud küsimustik A koosneb 17 küsimusest ning Sisekaitseakadeemia ekspertidele ja prokuröridele koostatud küsimustikud B ja C koosnevad 14

küsimusest (käesoleva töö lisa 6, lk. 120). Intervjuud toimusid ajavahemikus 10.03–05.04.2023. Need toimusid suunatud vestluse formaadis, vajadusel küsimused täpsustati. Enamus eksperte, v.a üks intervjueeritav, ei soovinud käesolevas uuringus enda nime kajastamist, kuid kõik olid nõus tegevusvaldkonnale ja ametile viitamisega. Seetõttu ei kasutata käesolevas töös ekspertide isikuandmeid, tagades võrdne lähenemine (lisa 7, käesolev töö lk 127).

Enne intervjuude läbiviimist saadeti ekspertidele uuringu ja magistritöö eesmärki kirjeldava kutse ja intervjuus arutelu objektiks olevad kompetentsiraamistiku ja kompetentside tasemekirledusi sisaldavad materjalid (lisad 4–5, käesolev töö lk 112–119). Neile, kes soovisid põhjalikumalt tutvuda intervjuu teema ja küsimustega, edastati ka vastavale ekspertide grupile ettenähtud küsimustik (lisa 6, käesolev töö lk 120). Vahetult enne intervjuu läbiviimist täpsustas autor uuesti uuringu teemat ja kompetentsiraamistiku koostamise põhimõtteid ja komponente. Keskmine intervjuu kestvus oli 1 tund 9 minutit (v.a sissejuhatav ja kompetentsiraamistiku tutvustav osa). Intervjuud salvestati ekspertide nõusolekul ning seejärel transkribeeriti kõnetuvastuse süsteemi tekstiks.ee (Olev & Alumäe, 2022) abil ning seejärel helisalvestised kuulati ja redigeeriti trandkriptsioonide tekstid. Kodeerimiseks kasutati andmetöötlusprogrammi NVivo14.

2.2.1 Ekspertintervjuude kokkuvõte ja analüüs

Esimesele uurimisküsimusele „Millised on ühiskonna digitaliseerimisest tingitud uued väljakutsed kohaliku tasandi uurijatele kuritegude uurimise perspektiivis?“ (UK1) vastuse saamiseks moodustati kategooria „**1. Väljakutsed ja võimalused**“ (Ka1), mille alla kuulub neli koodi: „**1.1 politseiorganisatsiooni sisesed tegurid**“ (Ko1.1), „**1.2 politseiorganisatsiooni välised tegurid**“ (Ko1.2), „**1.3 takistuste ja kitsaskohtade ületamise võimalused**“ (Ko1.3) ja „**1.4 digitaliseerumisega kaasnevad positiivsed muutused**“ (Ko1.4). Mõne koodi alla moodustati rohkem alamkoode, et piiritleda probleemid ja kitsaskohad, mis on tekkinud kohaliku tasandi uurija töös digitaalse komponendiga kuritegude uurimisel ja selleks vajalike kompetentside omandamisel. Ko1.4 aitab samuti leida vastuseid UK1-le, kuna lahenduste väljapakkumisel eeldatakse probleemide ja kitsaskohtade olemasolu. Selleks, et tasakaalustada vastuseid kitsaskohtade ja digitaliseerumise negatiivse mõju kohta, koondati ka ekspertide mõtteid digitaliseerumise positiivsete mõjude kohta kohaliku tasandi politseiuurija töö vaates. Eksperdid kirjeldasid tihti kõik nimetatud väljakutsed ja probleemid omavahel seostatuna ühe ja sama arutluse käigus, mille tõttu ühele intervjuu

transkriptsiooni tekstilõigule võib korraga vastata mitu koodi. UK1 vastamiseks moodustatud kategooria ja koodid, koodide esinemine ja esinemissagedus intervjuudes on esitatud tabelis 9.

Tabel 9. UK1 vastamiseks moodustatud kategooria ja koodid, koodide esinemine ja esinemissagedus intervjuudes, (NVivo faili põhjal autori koostatud)

1. **KATEGOORIA** / 1.1 kood / - alamkood	koodi esinemine intervjuudes	esinemissagedus intervjuudes
1. VÄLJAKUTSED JA VÕIMALUSED		
1.1 Politseiorganisatsiooni sisesed tegurid		
- digikriminalistika väljakutse	7	19
- inimressursside puudulikkus	6	14
- motivatsiooni ja huvi probleemid	8	22
- muu	7	19
- **personalile ettevalmistuse tagamise väljakutse**	**9**	**40**
- toetava keskkonna ja töövahendite puudulikkus	6	7
- töö mahu ja koormuse suurenemine	7	17
- uurija vanus (nn digiimmigrandid)	7	18
- uurijate ebakindlus ja hirmud	5	14
- **uurijate teadmiste ja oskuste puudulikkus**	**10**	**43**
- valdkonna arendamiseks vajalike rahaliste ressursside puudulikkus	9	23
1.2 Politeiorganisatsiooni välised tegurid		
- digimaailmas anonüümsuse tagamise võimalused ja kurjategija tuvastamise väljakutse	2	3
- **IKT valdkonna ja digitaalsete lahenduste kiire areng ja sellega kohanemise väljakutse**	**10**	**44**
- õiguslikud probleemid	3	9
- piiriülesus ja rahvusvahelise koostöö probleemid	5	9
- kuritegude toimepanemiseks võimaluste suurenemine	6	10
1.3 Takistuste ja kitsaskohtade ületamise võimalused	10	85
1.4 Digitaliseerumisega kaasnevad positiivsed muutused	8	16

Uuringu tulemusel selgus, et **Ko1.1** all tõid kõik küsitletud eksperdid välja, et kõige kaalukamateks probleemideks ja politseiorganisatsiooni sisesteks teguriteks on uurijatel digitaalmaailmas hakkama saamiseks ja digikomponendiga kuritegude uurimiseks vajalike **teadmiste ja oskuste puudulikkus** ja **personalile vajaliku ettevalmistuse tagamise väljakutse,** mis on ühtlasi kooskõlas teooriaga (käesolev töö, lk 15–16). Enamuses intervjuudes viidati uurijate seas nii üld-digikompetentside kui ka kutsespetsiifiliste oskuste puudulikkusele, milleks on näiteks digivahendite ja tarkvara kasutamise oskus ja digitõendite tuvastamise ja käsitlemise oskus.

Kuna ekspertide eesmärgistatud valim on tagasihoidlik ja koosneb kolmest väikesest grupist, siis alamkoodi „**personalile ettevalmistuse tagamise**“ all juhtisid eksperdid tähelepanu väga erinevatele

aspektidele, mis on seotud ühtlasi ka Ko1.1 teiste alamkoodide all tooduga. Olulisel kohal on nii inim- kui tehniliste ressursside arendamiseks vajaliku optimaalse rahastamise puudulikkuse tegur, mis on ühtlasi kooskõlas teooriaga (käesolev töö lk 15). Kui teoorias ei lahatud rahastamise tegurit detailselt, siis ekspertide tähelepanu sellele aspektile oli märkimisväärne. Politseiorganisatsioonil valdkonna arendamiseks vajalike **rahaliste ressursside puudulikkust** toodi olulise takistusena välja kõigis ekspertide gruppides ja umbes võrdses osakaalus.

„Noh, ega organisatsiooni sisemised tegurid ongi seesama, et esiteks meie... me ei pakku ametnikele teadmisi. Noh, selles, selles suhtes, et suur risk on see, et meie ei pakku teadmisi, kuidas ainuüksi käidelda neid asju, neid, kasvõi neid seadmeid, mis võivad digitaalset komponenti sisaldada. Või kuidas vormistada. Ehk põhimõtteliselt see on üks pool, et me ei paku teadmisi ise organisatsioonina, ja ei paku siis ka kool. See on üks suur risk. /.../ Noh, pigem jah, jääb selle juurde, et me pakume liiga vähe seda võimalust. Ja me toetame küll igasugust õppimisvõimalust ja nii edasi. Aga selle jaoks pean ma ise minema, otsima, tegema. /.../Aga, aga see, et me tööks spetsiifilist koolitust, millega kompetentsi arendada, seda pakume me ikkagi vähesel... noh, me teeme teatud teemadel. Meie eelarve on piiratud, väike ja nii edasi... Meie võimalused on väikesed. ” (Ekspert 4)

Üheks takistavaks teguriks nägid PPA eksperdid samuti politseiorganisatsiooni võimaluste piiratust erinevatele sihtgruppidele arendamisvajaduste tagamises organisatsioonis tervikuna, mitte ainult politseiuurijate digikomponendiga kuritegude uurimiseks vajalike kompetentside osas. Põhjuseks on PPA-s pädevate koolitajate arvu vähesus ja nende töökoormus. Ka Sisekaitseakadeemial on murekohaks digi- ja kübersuunitlusega teemade õpetamiseks asjatundlike õppejõudude leidmine. Koolituste ja õppekavade arendus on aega ja ressursse nõudev tegevus, koolituste arv ja nende kättesaadavus kõigile sihtgruppidele, kes seda vajavad, on piiratud. Need tähelepanekud on kooskõlas teooriaga (käesolev töö, lk 15–16).

“Noh, eks, olekski nagu koolitused, et... Noh, et inimesed sellest IT-st rääkides, ongi see, et oleks programmi koolitusi rohkem ja kõike muid asju. Aga seda nagu sisse osta on väga raske, aga meie lihtsalt koormuse tõttu ei jõua kõiki koolitada. /.../ Isegi, noh, kui raha oleks, ta on väga raske sisse osta. Seda ei tee keegi teine, noh.“ (Ekspert 3, PPA)

Sageli ja vastavalt teooriale kitsaskohtadena mainiti uurijate digikomponendiga kuritegude uurimiseks ja selleks vajaliku ettevalmistuse arendamiseks uurijatel **motivatsiooni ja huvi puudumise probleemi**

(käesolev töö, lk 14) ja **digikriminalistika väljakutset** (käesolev töö, lk 17–20). Teoorias käsitlemata aspektidest toodi Eesti üldisest demograafilisest olukorrast tulenevaid probleeme ja kohaliku tasandi uurijate **kuulumist üleesindatud vanusegruppi 40+ aastat** ning sellega seonduvate nn „digi-immigrantide" põlvkonna probleeme; **töö mahu ja -koormuse suurenemist**. Veel ühe märkimisväärse tegurina toodi välja politseiuurijate **hirme ja ebakindlust** seoses IKT lahenduste integreerimisega tööprotsessi ja digikomponendiga juhtumite lahendamisel.

"... Noh, et järgmise etapina on siis see, et me /st digikriminalistika keskuse eksperdid/ kopeerime ja siis tuleb uurija vaatlus. Et sellega nad /st uurijad/ on tihtipeale hädas. Sest et andmeid on palju, ei oska programmi käsitleda, puudub siis, vahel puuduvad lihtsad teadmised, kuidas kasvõi Excelit kasutada. See on täiesti... See üllatab, aga kus inimene ei oska isegi Office´i korrektselt kasutada.../.../ Noh, et seal, okei, õpetame nad selgeks, et kuidas siis nii öelda vaadelda seda, aga siis on tulnud juhtumeid, kus nad, noh, siis aitame eksportida ja siis olenevalt siis piirkonnast, kas vormistame meie ise, nii öelda, ja või siis see uurija. Aga see on väga suur probleem nende jaoks. Tuuakse välja seda, et nad ei oska vormistada iseseisvalt. Nad ise ka tunnistavad seda… Ja seda on väga palju. /.../ Ja seda on nagu väga raske õpetada, kui inimene, noh /paus/ ei taha seda endale võtta." *(Ekspert 3, PPA)*

Erinevalt teooriast kõige vähem mainiti intervjuudes kohaliku tasandi uurija digitaalse komponendi juhtumite käsitlemiseks ja kuritegude uurimiseks vajaliku **toetava keskkonna** ja **töövahendite puudulikkuse tegurit** (käesolev töö lk 14). Ühtlasi toodi välja ka digitaalse komponendiga kuritegude uurimisel ning selleks vajalike kompetentside arendamisel tekkinud mõned üksikud kitsaskohad, millel ühisosa puudus. Need koondati alamkoodi **„muu"** alla. Üksikutel juhtudel toodi välja uurija soo ja vanusega seotud tegnoloogioalembelisuse puudumise; digikompetentsemaks saanud uurijate ülemineku funktsionaalsetese üksustesse või lahkumist politseisüsteemist; uurijate oskuste hindamissüsteemi puudumist, mille alusel saaks planeerida enesearendamist ja saada erinevale tasemele vastavaid koolitusi; digitaalsuse taha vahetu suhtlemisega kaasnevat inimlikku komponendi vähenemist ja kadumist; keskmisest digikompetentsema ametniku poolt politsei infosüsteemide kuritarvitamise riski.

Välised tegurid on tihedalt seotud teiste eespool kajastatud väljakutsetega. Ka1 alla Ko1.2 „**politseiorganisatsiooni välised tegurid**" all eristati 4 alamkoodi, millest alamkood „**IKT valdkonna ja digitaalsete lahenduste kiire areng ja sellega kohanemise väljakutse**" oli esindatud kõigis ekspertintervjuudes. Kõigis ekspertide gruppides toodi välja, et digikomponendiga juhtumite osakaal on kasvutrendis ning käesoleval ajal peaaegu iga juhtum ja kuritegu, mida lahendab kohaliku tasandi

politseiuurija, sisaldab ühel või teisel moel digitaalset komponenti (käesolev töö, lk 8–9, 13). Kõik eksperdid tõid välja, et ühiskonna digitaliseerumise kiirus on seadnud rida väljakutseid kuritegude uurimise vaates nii indiviidi tasandil kui PPA-le laiemalt. Digitaliseerumise kiirus ületab PPA ja Sisekaitseakadeemia võimekust sellele adekvaatselt reageerida ja arendada politseinikud vastavale tasemele. Kitsaskohaks on ka asjaolu, et juba omandatud teadmised ja oskused aeguvad kiiresti ja IKT arenguga paralleelselt, mille tõttu tuleb neid pidevat kaasajastada. Enamus eksperte täheldasid, et digikomponendiga kuritegude uurimiseks vajaliku ettevalmistuse tagamine on keeruline tehnoloogia kiire ja hüppelise arengu perspektiivis, mida teoorias on küll käsitletud, kuid pealiskaudselt (nt käesolev töö, lk 19).

"Sest et noh, see digitaliseerumine ainult kiireneb ja erinevates suundades korraga ka. Et täna, täna on meil asjad nagu hoopis teistmoodi ja keerulisemad kui juba 10 või 5 aastat tagasi. Et ja, ja ma arvan, et see aeg on nüüd muutunud kiiremaks. Ja uurijad hakkavad, nad peavad oskama noh, kõik võimalikke sotsiaalvõrgustikke kasutada, kuidas sealt neid tõendeid kätte saada. Noh, kõik igasugused erinevad videoformaadis, et noh, see on nagu lõputu, lõputu nimekiri tegelikult. Vähemalt, et ma arvan, et, et see on nagu suur kitsaskoht. Et kui kiiresti see areneb ja kui hästi uurijad oskavad selle arenguga nagu kaasas käia." (*Ekspert 8, prokuratuur)*

Ko1.2 olevad alamkoodid **„kuritegude toimepanemiseks võimaluste suurenemine"** (käesolev töö, lk 15) ja **„piiriülesus ja rahvusvahelise koostöö probleemid**" (käesolev töö, lk 16) olid esindatud vastavalt kuues ja viies intervjuus. Eksperdid tõid välja, et kiire digitaliseerumine suurendab kurjategijate võimalusi ja laiendab nende tööriistade valiku kuritegude toimepanemiseks (käesolev töö, kl 14). Samas, alamkood „digimaalimas anonüümsuse tagamise võimalused ja kurjategija tuvastamise väljakutse", oli esindatud oodatust vähem (käesolev töö, lk 14). Samuti tekivad uued süütegude liigid, mida varem ei olnud, mis vastab teooriale (käesolev töö, lk 13–14). Hetkel nende uurimiseks vajalikud metoodikad ning kohtupraktika on alles kujunemas.

"Negatiivse külje pealt on see, et tänu digitaliseerumisele on meil tekkinud täiesti uued kuriteoliigid, mida ennem ei olnud. Nüüd meil on võimalik, või ütleme siis teatud kuritegusid varem ei olnud, võimalik toime panna, näiteks kelmust üle internetti või muude digitaalsete vahenditega. Ja, ja nüüd on. Et selles mõttes on nagu, nagu teiselt poolt jällegi negatiivne on see digitaliseerumine. Ja, või noh, ütleme veel lihtsam näide minu valdkonnast, lähisuhtevägivallast on see, et meil on eraldi kuriteokoosseis ahistav jälitamine. Ehk siis, kui keegi kuskil tülitab süstemaatiliselt. Et tänu digitaliseerumisele on, on nüüd veel

rohkem igasuguseid võimalusi inimest, kannatanute, siis kannatanu suhtes selle teo toime panna. Et on võimalik teda kõnedega, kuidagi kiusata või siis, või siis sõnumite teel. Või kuidas iganes. Selles mõttes, et tänu digitaliseerumisele on neid tööriistu on tegelikult oluliselt rohkem kui vanasti." (Ekspert 8, prokuratuur)

Digitaliseerumise vaates muutub ja areneb ka õigusruum, millega uurijatel tuleb ennast pidevalt kurssi viia. Toodi välja, et õiguslike regulatsioonide ajakohastamine ei jõua IKT võimaluste arengutele järgi, nagu ka inimeste kompetentsid, mis tekitab täiendavat ajakulu ja töö sisu keerulisemaks muutmist (käesolev töö, lk 13–14). Näiteks, kriminaalmenetluses suure mahuga andmekandja asitõendina vaatlustoimingu läbiviimine ja vormistamine eeldab rohkem tugevaid digikompetentse ja aega kui mõne füüsilise asitõendi vaatlus. Õiguslikke probleeme mainisid kaks eksperti Sisekaitseakadeemiast ja üks prokurör.

„...Sest ennem seda nähtust ei olnud, nagu digitaalne maailm ja seal toime pandavad kuriteod... Ja pole, noh… Siin tuleb loominguliselt läheneda… Seadusandlus ei jõua õigeaegselt need reeglid kuidagi sätestada, et, ütleme… Alguses on kuidagi… Ütleme, alguses kuidagi näib see digitaalne maailm kaootiline. Siis tuleb… siis, siis tulevad need kirja pandud siis seadused ja reeglid. Ja neil puudub lihtsalt… eee… menetluse poolt kohaldamise praktika… Et tuleb rajada seda uut rada, mille järgi siis järglased juba menetlevad asju. Teerajajad oleme selles mõttes." *(Ekspert 10, prokuratuur)*

Ka1 Ko1.3 „**Takistuste ja kitsaskohtade ületamise võimalused**" alla koondati ekspertide ettepanekuid kõigi eespool toodud väljakutsete lahendamiseks ja kitsaskohtade ületamiseks. Tegemist on kontrollkoodiga, kuna see aitab veelkord esile tuua erinevate probleemide ja väljakutsete olemasolu, ning seega kinnitada ka käesoleva töö aktuaalsust. Kõik uuringus osalenud eksperdid pakkusid oma lahendusi ja ettepanekuid.

Kõik eksperdid rääkisid uurijatele digitaalse komponendiga kuritegude uurimiseks vajalike kompetentside arendamist toetavate koolituste ja täiendusõppe tagamise vajalikkusest. Samas, pöörati tähelepanu erinevatele aspektidele nii uurija isiku kui politseiorganisatsiooni vaates. Nimelt, ekspertide arvates peab politseiorganisatsioon otsima ja pakkuma lahendusi kõigi uurijate kompetentside arendamiseks. Kolm eksperti pidasid oluliseks enne lahenduste pakkumist ka sihtgrupi vajaduste ja taseme hindamist ja mitmele eri tasandile vastavate koolituskavade arendamist. Kaks PPA eksperti ja kõik Sisekaitseakadeemia eksperdid tõid lahendusena välja Sisekaitseakadeemias tänaseks kolm aastat

kestnud politsei eriala õppekavadesse digi- ja küberteemade integreerimist ja arendamist, mis võimaldab tagada baasteadmiste pakkumist uuele politseinike põlvkonnale. Samuti rõhutati täna tööl olevatele uurijatele nende tasemele sobiva põhjaliku täiendusõppe tagamise vajalikkust. Tööl olevate uurijate täiendusõppekava oli intervjuude läbiviimise hetkel arendamisel ning seda plaanitakse rakendama hakata käesoleval aastal.

Digitaalse komponendiga kuritegude uurimiseks vajalike kompetentside arendamise võimalusi nähakse ka politseijaoskonna tasandil töökorralduslike muudatuste abil. Näiteks, ühe võimalusena pakuti kohaliku tasandi politseiuurijate sihtgrupi seast tehnilise taibuga inimeste motiveerimist ja arendamist sellele tasemele, et nendest saaksid oma jaoskonnas digitõendite käsitlemise temaatika eestvedajad. Võimalusi nähakse ka enda seast edasikoolitajate ettevalmistamises, teiste partnerite kaasamises (ülikoolid õppekavade ja digilahenduste väljatöötamiseks, finantsinspektsiooni koolitus krüptoraha teemal). Need lahendused eeldavad töökoormuse ülevaatamist ja sellise inimese põhitööst vabastamist, mis on keeruline inimressursside vähesuse vaates. Digitaalse komponendiga kuritegude uurimiseks vajalikest töövõtetest ja praktikatest ülevaate saamiseks nägid kolm PPA eksperti ühe võimaliku lahendusena kohaliku tasandi uurijatele töövarju- ja praktikapäevade korraldamist politsei funktsionaalüksustes. Kaks Sisekaitseakadeemia eksperti pidasid oluliseks omandatud kompetentside kinnistamise protsessi, ühel juhul toodi välja ka uurijate grupijuhi rolli selles.

„Kui me seda õpet ei kinnista, siis sellisel juhul on see jällegi selles mõttes selline maha visatud aeg, et me õpetame. Aga tegelikult läheb mingi aeg mööda ja see õppija on juba kõik ära unustanud, mis tähendab seda, et sisuliselt peaks, näiteks, grupijuht leidma sellise võimaluse, näiteks, et mitte jätta siis, ütleme, neid vanema generatsiooni inimesi, kes võib-olla seda digivaldkonda pelgavad. Ütleme, et nad on selle õppe läbinud ja siis peale seda, kui nad tööle naasnud, siis tegelikult võikski grupijuht leida vähemalt ühe või kaks juhtumit sellist... Noh, ütleme, ühes kuus, ütleme, et üks-kaks juhtumit... sellist, mis eeldavadki nende digioskuste kasutamist, ma arvan. See, see kindlasti päästaks päeva.“ (Ekspert 9, Sisekaitseakadeemia)

Mitmes intervjuus kõlas ettepanekuid enesearendamist toetava keskkonna või selle komponentide loomise kohta. Kesksesse keskkonda saaks koondada ja pidevalt kaasajastada ülesannete täitmist selgitavad videojuhendid, erinevate kuriteoliikide menetlusmetoodikad, heade praktikate jagamise kanalid, digilahenduste vahendusel korraldatud ja järelvaadatavad nn 25-minutised „õpiampsud“, jms.

Intervjuudes kõlas ka teisi kauge perspektiiviga ja rahalisi investeeringuid eeldavate lahenduste ettepanekuid, nagu üksikute tehnilise taibuga andekate kolleegide eriharidust (IT) omandamiseks organisatsiooni poolt õppima suunamine. Kõik prokurörid ja kaks Sisekaitseakadeemia eksperti pakkusid välja digitõendite või üksikute keerulisemate digikomponendiga toimingute teostatmiseks ja üleüldse digiteemalistes küsimustes abi pakkuvat politseijaoskondades toimiva tugi- ja nõustamisteenuse korraldamist. Kaks PPA eksperti rääkisid arendamisel oleva küber- ja digikomponendiga juhtumite menetlemiseks tööriistade komplekti kasutamisala laiendamisest kohaliku tasandi uurijale. Üks intervjueeritav pakkus välja seadusemuudatust eeldavat lahendust ehk politseinikele seadusega kehtestatud füüsiliste katsete nõuete ülevaatamist ja üksikjuhtudel nendele nõuetele mittevastavate, kuid sobiva haridusega ja heade digikompetentsidega inimeste politseiteenistusse võtmist.

Ka1 Ko1.4 „**digitaliseerumisega kaasnevad positiivsed muutused**“ abil toodi välja ekspertide tähelepanekud uurija töös ilmunud positiivsete momentide osas. 7 eksperti tõid positiivsena välja tõendite kogumise võimaluste suurendamist, aga kolm intervjueeritavat täiendasid, et need võimalused realiseeruvad vaid uurijatel vastavate oskuste ja teadmiste olemasolul. Kaks eksperti rääkisid ka aja kokkuhoiust ja tööprotsessi lihtsustamisest.

“Jah, võimalused on. Tegelikult on ju lihtne, ainult taevas on laeks. Et nii palju kui sa oskad, nii palju sa leiad. Noh, võtame täna OSINTi võimekuse või võimalused, siis iga täiendav võimekus annab sulle väga suure edumaa jälle. Sest noh, täna on, täna midagi ei ole teha. On edukad need, kes suudavad, suudavad töödelda läbi suuri andmemahtusid. Ja noh, ennekõike leida need andmed, et eristada neid suuri andmemahtusid. Ja leida sealt siis üles see komponent, mis sul parajasti mingisuguses menetluses kas siis tähendab või, või siis edasi aitab.” (Ekspert 6, Sisekaitseakadeemia)

Teisele uurimisküsimusele „Millised on digitaalse komponendiga kuriteod, mille lahendamisega tegelevad kohaliku tasandi politseiuurijad?“ (UK2) vastamiseks moodustati kategooria „**2. Digikomponendiga kuriteod**“ (Ka2), mille alla kuulub kolm koodi: „**2.1 digikomponendi näited**“ (Ko2.1), „2.2 **juhtumid ja kuriteod**“ (Ko2.2) ja „**2.3 menetluspädevuse ja kompetentside ootuse erinevus kohalik tasand vs funktsionaalüksused**“ (Ko2.3). UK2 vastamiseks moodustatud kategooria ja koodid, koodide esinemine ja esinemissagedus intervjuudes on esitatud tabelis 10 (käesolev töö, lk 61).

Tabel 10. UK2 vastamiseks moodustatud kategooria ja koodid, koodide esinemine ja esinemissagedus intervjuudes, (NVivo faili põhjal autori koostatud)

2. **KATEGOORIA** / 2.1 kood / - alamkood	koodi esinemine intervjuudes	esinemissagedus intervjuudes
2. DIGIKOMPONENDIGA KURITEOD		
2.1 Digikomponendi näited		
- digitaalne tõend ja jälg	9	29
- IKT kui kuriteo toimepanemise vahend ja keskkond	10	12
- IKT vahendid kuriteo uurimiseks	8	11
- suhtlemisviis menetluse raames	4	6
2.2 Juhtumid ja kuriteod		
- digikomponendiga kuriteod	8	15
- küberkuriteod	8	15
2.3 Menetluspädevuse ja kompetentside ootuse erinevus kohalik tasand vs funktsionaalüksused)	9	33

Ko2.1 alla koondati neli alamoodi, milleks on: „**digitaalne tõend ja jälg**“ „**IKT kui kuriteo toimepanemise vahend ja keskkond**“, „**IKT vahendid kuriteo uurimiseks**“ ja digitaalne komponent kui „**suhtlemisviis menetluse raames**“.

Enamus eksperte rääkisid digitaalsest komponendist kui digitaalsest tõendist ja elektroonilisest jalajäljest. Selle all peeti silmas nii politsei, eraisikute ja ettevõtete valduses olevaid digitaalseid andmekandjaid ja seadmeid ning nende abil salvestatud andmeid. Samuti on tõendiks avalikus veebis olevad digitaalsed andmed (sh sotsiaalvõrkudes olevate kontode ja seal tehtud toimingute kohta), mida saab päringu tegemise teel või digitaalset seadet uurides. (käesolev töö, lk 21–25)

IKT kui kuriteo toimepanemise vahendit või keskkonda seostasid kõik eksperdid küberkuritegude toimepanemisega, mis on võimalik üksnes IKT vahendusel või digitaalsel kujul eksisteeriva objekti ehk andmete vastu. Samuti pidasid 8 eksperti digitaalse komponendi all silmas IKT vahendite ja lahenduste kasutamist kuriteo uurimiseks ja menetluse läbiviimiseks ning menetluse andmete digitaalsel kujul salvestamist ja esitlemist. Siia alla kuuluvad kaugülekuulamine, kaugkohtuistungid, elektroonilistesse infosüsteemidesse salvestatud menetlusandmed. Kõige vähem mainiti, et IKT-d kasutatakse menetluse raames suhtlemiseks. Need aspektid ei ole seotud kuriteokoosseisu tunnustega, kuid nõuavad uurijatel üld-digikompetentside olemasolu (käesolev töö, lk 34–40).

Ko2.2 alla kuulub kaks alamkoodi, milleks on „**digikomponendiga kuriteod**“ ja „**küberkuriteod**“. Mõlemad alamkoodid esinevad 8 intervjuus. Digikomponenidga kuritegude iseloomustamisel toodi

välja, et tegemist on misiganes kuriteoga, kus mõneks elemendiks on digitaalne komponent (v.a IKT vahendid kuriteo uurimiseks ja digitaalne komponent kui suhtlemisviis). Küberkuriteo mõiste sisustamisel juhiti tähelepanu sellele, et see on spetsiifiline kuritegu, mille toimepanemine on võimalik üksnes digitaalses keskkonnas või on suunatud tehnoloogia vastu, kus IKT või digiseade on kuriteo toimepanemise vahendiks või objektiks, mis on vastavuses teooriaga ja seostub küber-sõltuvate kuritegude määratlusega. (käesolev töö, lk 21–25)

"Küberkuriteo puhul minu jaoks on see selline... Kas see on toime pandud siis arvutivõrgus, on see suunatud konkreetselt mingisuguse infotehnoloogilise vahendi suhtes. Ehk, on see häkkimine, on see andmete kogumine sealt lihtsalt, või misiganes, näiteks, läbi Trooja hobuste või mingite selliste asjade. Et see on küberkuritegu. Digitõend võib olla tavalises menetluses ka täiesti igapäevane. Aga küberi puhul mina eristan, mina eristan need enda jaoks niimoodi. Ehk ongi need, need, mis on pandud toime infotehnoloogilisest seadmest või tema vastu kasutades." (Ekspert 4, PPA)

Ko2.3 „**2.3 menetluspädevuse ja kompetentside ootuse erinevus kohalik tasand vs funktsionaalüksused**" abil toodi välja kohaliku tasandi politseiuurija rolli digitaalse komponendiga kuritegude uurimisel politseiorganisatsiooni vaates vastavalt kompetentsiraamistiku koostamise teoreetilisele käsitlusele (käesolev töö, lk 30–31, 33–34, 40–41). Koodi esines 9 ekspertintervjuus ning kõige rohkem oskasid sellest rääkida PPA eksperdid ja üks Sisekaitseakadeemia ekspert. PPA vaates kohaliku tasandi ja funktsionaalüksuse tööülesanded ja menetluspädevus on jaotatud erinevalt, võttes arvesse iga prefektuuri tööpiirkonna geograafilist asukohta, elanikkonna suurust ning sellest tulenevat prefektuuri töökorralduslikku eripära.

Ühisosana toodi välja, et kohaliku tasandi politseiuurija menetleb kogukonna turvatunnet riivavaid ja mõjutavaid ja/või ilmsiks tulnud juhtumeid, kus puuduvad raske ja organiseeritud (sh peit-)kuritegevuse tunnused. Üldjuhul ei menetle kohalik tasand ka kitsa suunitlusega kuritegusid (nt küberkuriteod, narkokuriteod, majanduskuriteod), mille uurimiseks eeldatakse spetsiifilisemaid oskusi ja metoodikaid. Ühlasi toodi välja, et kohaliku tasandi uurijate menetluspädevuses olevad juhtumid on reeglina vähem mahukad. Eeldatakse, et nendes juhtumites tõendite kogumiseks ja vormistamiseks piisab heal tasemel baasdigioskuste ja üldkompetentside olemasolust. Samas, on kogukonnasüütegude valik väga lai: alates liiklusrikkumisest kuni tapmiseni. Osa nendest kuritegudest nimetatakse ka masskuritegevuseks (nt kauplusevargused, liiklussüüteod). Teoreetilises osas kohaliku tasandi politseiuurijate menetluspädevuse erisust käsitletakse kaudselt ja seostatakse kohaliku tasandi politseiüksuste

territoriaalsuse printsiibiga (käesolev töö, lk 16).

"Üldiselt /uurija roll/ ei erinegi. Üleüldiselt lihtsalt, on lihtsalt töö spetsiifilisusest tulenevalt jaotatud... Tehtud mingi tööjaotuskava. Ehk nagu ma ütlesin ennem ka, et see tegu, mis mõjutab kogukonda kõige enam... Ehk mis on noh, ütleme, et seesama vargus näiteks. Seda menetleb meil ikkagi jaoskonna tasand. Kui nüüd selge... ja funktsionaalsed üksused on jaotatud pigem selliseks mingite, mingite kuriteoliikide põhiseks. Ehk, näiteks, küberkuriteod, näiteks, narkokuriteod, organiseeritud kuritegevus. Nagu sellised ongi funktsionaalsetes. Ehk see, mida välja ei paista tavainimesele. See, mis toimub kuskil a-la teises maailmas. Ehk võib olla, et sellega tegelevad siis funktsionaalsed. Ülejäänud kõik, mis puudutab seda nimetatud nähtavat osa, menetleb siis kohalik tasand. Et kohalik tasand põhimõtteliselt menetleb siis, kuidas ma ütlen, kõige pisemast vargusest kuni lõpetades tapmiseni. Kõik, mis, vahet ei ole, sinna kuulub, välja arvatud, siis... võib menetleda väiksemaid narkoasju seal, laste seksuaalkuritegusid, selliseid... Ka väiksemaid niinimetatud küberkuritegusid, mis on seal kohalikul tasandil toime pandud. Aga ülejäänud, jah, menetletakse.... näiteks korruptsioon, kus kasutatud digitõendite osakaal on suurem... võib olla korruptsioon, küber-, narko-, organiseeritud kuriteod, see on siis funktsionaalsete üksuste menetluses." (Ekspert 4, PPA)

Kolmandale uurimisküsimusele: „Kuidas süstematiseerida kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimiseks vajalikke teadmisi ja oskusi?" (UK3) vastamiseks moodustati kaks kategooriat**: „3a. kompetentsiraamistiku väljatöötamise meetod" (Ka3a)**, mille all eristati kolm koodi, ja kategooria „**3b. kohaliku tasandi uurija oodatavad kompetentsid" (Ka3b)**.

Koodi „**3.1a tegelik olukord**" **(Ko3.1a)** sooviti välja tuua, kuidas on seni lähenetud PPA-s eri üksuste ametnike rolli, tööülesannete jaotamisele ja selleks vajalike kompetentside määratlemisele ning arendamisele. Koodiga „**3.2a kompetentsiraamistiku korraldamise viis**" **(Ko3.2a)** abil sooviti esile tuua ekspertide arvamusi ja mõtteid, kuidas peaks kompetentsiraamistikku korraldama ja keda tuleks selleks kaasata. Kood **„3.3a raamistiku koostamise etapid, elemendid" (Ko3.3)** kondab ekspertide mõtteid teoreetilises käsitluses kirjeldatud kompetentsiraamistiku korraldamise viisi (käesolev töö, lk 30) ja koostamise etappide perspektiivis (käesolev töö, lk 31–34).

Kategooria **„3b. kohaliku tasandi uurija oodatavad kompetentsid" (Ka3b)** all on kolm koodi: „**3.1b üldkompetentsid" (Ko3.1b), „3.2b üld-digikompetentsid" (Ko4.2) ja „3.3b kutsespetsiifilised kompetentsid" (Ko3.3b).** Kategooria ja selle all moodustatud koodide abil sooviti koondada ekspertide

mõtteid magistritöös välja töötatud kompetentsiraamistiku (käesoleva töö lisa 4, lk 112) kompetentside jaotuse kohta üld-, digi- ja kutsespetsiifilisteks (käesolev töö, lk 34–46). UK3-le vastamiseks moodustatud kategooriad ja koodid, koodide esinemine ja esinemissagedus intervjuudes on esitatud tabelis 11.

Tabel 11. UK3 vastamiseks moodustatud kategooriad ja koodid, koodide esinemine ja esinemissagedus intervjuudes, (NVivo faili põhjal autori koostatud)

3. **KATEGOORIA** / 3.1a kood / - alamkood	koodi esinemine intervjuudes	esinemissagedus intervjuudes
3a. KOMPETENTSIRAAMISTIKU VÄLJATÖÖTAMISE MEETOD		
3.1a Tegelik olukord	7	62
3.2a Kompetentsiraamistiku korraldamise viis	6	13
3.3a Raamistiku koostamise etapid, elemendid	6	14
3b. KOHALIKU TASANDI UURIJA OODATAVAD KOMPETENTSID		
3.1b Üldkompetentsid	10	48
3.2b Üld-digikompetentsid	8	27
3.3b Kutsespetsiifilised kompetentsid	10	70

PPA-s ja Sisekaitseakadeemias kompetentsipõhise lähenemise vaates **tegeliku olukorra** esile toomisel (Ko3.1a) selgus, et intervjuude läbiviimise hetkel formaliseeritud kujul kompetentsipõhist lähenemist ei rakendata. Igale põhitööle kompetentside komplekti detailselt lahti kirjutatud ei ole ja ametijuhendis seda ei kajastata, vaid lähtutakse üldistest põhimõtetest. PPA ja Sisekaitseakadeemia eksperdid selgitasid, et PPA-s põhineb ressursside (sh inimressursside) juhtimine teenuspõhisel lähenemisel. Kompetentside arendamiseks vajalikud koolitused planeeritakse keskselt vastavalt strateegilise eesmärgi kaudu määratletud koolitusvajadusele, kuid samas igaastase tööplaani raames kogutakse prefektuuri teenuse koordinaatori korraldamisel tagasisidet erinevates üksustes tekkinud koolitusteemade soove, nii valmis oleva loetelu alusel, kui ka vabas vormis. Viimase variandi korral täpsustatakse ning kaalutakse nendel teemadel koolituste korraldamise otstarbekust.

"Nemad /PPA ennetus- ja süüteomenetluse büroo/ on praegu alustanud sellist, erinevate põhitööde kompetentsimudelite loomist… Ja see tähendab siis seda, et erinevale põhitööle, näiteks uurija põhitööle planeerivad nad kirjeldada... eee, kompetentsid, mis on uurija põhitöö kriitilised kompetentsid. Ja nüüd siis me hakkame arendama neid konkreetseid kompetentse, eks ju.../.../ Et täna on see niimoodi, see arendamine pigem, et teenus sõnastab endale strateegilised eesmärgid ja püüab

siis läbi arengutoe nende strateegiliste eesmärkideni jõuda.../.../ Täna ei ole see kompetentsidest lähtuv.“ (Ekspert 1, PPA).

PPA-s eeldatakse süütegude uurimiseks vajalike kompetentside olemasolu olenemata uurimissituatsioonidest ja tõendite liigist. Kompetentse täiendatakse vajaduspõhiselt koolituste kaudu. Politseijaoskonna menetlusgruppi uue ametniku värbamise korral ja grupile vajaliku kompetentsivõimekuse otsimisel lähenetakse juhtumi- ja vajaduspõhiselt, intuitiivselt. Uurijaks sobiva kandidaadi valimisel võetakse arvesse grupi hetkeseisu. Hindamine toimub kandidaadiga toimuva vestluse raames. Konkreetse juhtumi lahendamiseks või toimingu tegemiseks menetlusgrupis puuduva kompetentsi korral pöördutakse digikriminalistika keskuse või funktsionaalüksuse poole. Sellist paindlikku lähenemist kasutatakse üksikjuhtudel, sest üldjuhul peaks menetlusgrupis kohaliku tasandi uurijale ette nähtud kompetents eeldatavalt olemas olema.

Politsei hariduse kaasajastamise ja arendamise vaates alates 2020/2021. õppeaastast täiendati Sisekaitseakadeemia politsei eriala õppekavades olevad õppeained küber- ja digikompetentside teemadega. Tulevasest kompetentsivajadusest teavitavad Sisekaitseakadeemiat PPA arendusosakond ja teenuseomanikud. Sisekaitseakadeemias küber- ja digiteemadel saadud teadmised ja nende töös kasutamise tulemusel tekkinud oskused moodustavad kohaliku tasandi uurija baaskompetentside komplekti.

Koodiga Ko3.2 abil sooviti esile tuua ekspertide arvamusi ja mõtteid, **kuidas peaks kompetentsiraamistikku korraldama** ja keda selleks kaasama. Üldjuhul pakkusid eksperdid hinnata sihtgrupi tööülesandeid ja arenguvajadusi ning seejärel koostada kompetentside loetelu, mis on kooskõlas teooriaga (käesoleva töö lk 31–33). Samas, intervjuudes kõlas ülevalt-alla viisil tegelikult rakendatava lähenemise näiteid, kus hinnangu koostavad strateegilise tasandi eksperdid ning hinnatava sihtgrupi panus on vähene ja formaalne (käesolev töö, lk 30). Siiski leidus igast ekspertide rühmast üks esindaja, kes mainis, et eelkõige tuleb uurida konkreetset sihtgruppi, kellele kompetentsikomplektid määratletakse. Sellisel juhul uurimisobjektideks võiksid olla nende inimeste taust ja üldine digiteadlikkuse tase ning ajas muutuv töösisu just nende inimeste silmade läbi. Näiteks, vastava uurimisinstrumendi abil saaks tuvastada konkreetsed muret tekitavad uurimissituatsioonid ja tööülesanded. See lähenemine on kooskõlas alt-üles viisil kompetentsiraamistiku koostamisega (käesolev töö, lk 30).

Ko3.3 all toodi **kompetentsiraamistiku elementidena** välja organisatsioonis konkreetse sihtgrupi rolli täpsustamist, selle sihtgrupi vastutusalasse kuuluvate tööülesannete ja tüüpiliste lahendatavate juhtumite iseloomu hindamist, millega määratletakse selle sihtgrupi tasand politseiorganisatsiooni vaates. Tulenevalt sellest saab juba hinnata, milliseid teadmisi ja oskusi on sihtgrupil vaja töös püstitatud ülesannetega edukaks hakkama saamiseks.

„Ja noh, eks, eks kõigepealt peab jällegi noh, alustame sellest samast definitsioonist, mis, millest me alguses rääkisime, eks ole. Et mis on see üldse digitaalse komponendi definitsioon. Ja siis järgmine, vaatame, et okei, millised on need juhtumid, kus on see, see digitaalkomponent on sees. Ja mida on vaja teha selleks, et noh, nüüd ma… Siis on kolmas küsimus, mida on vaja teha selleks, et see digitaalne komponent seal uurida sama hästi selle juhtumi juures ära, kui ütleme, siis, ma ei tea, analoogkomponent. Et ja, ja kui me sellele küsimusele same vastatud, mida vaja teha, mis on need toimingud, mis on need… Ongi, missugused toimingud on vaja teha. Et siis me saame hakata kokku panema seda, mida peaks oskama teha." (Ekspert 8, prokuratuur)

Üheks reaalseks kompetentsivajaduse hindamise elemendi näiteks on PPA digikriminalistika keskuse ekspertide 2017–2018. aastal läbi viidud koolituskavade planeerimiseks uurimissituatsioonidest ja digitõendite käsitlemise olukordadega seonduvast ülevaate koostamine, kuhu oli kaasatud ka politseijaoskondade tasand. Andmete kogumine toimus kõrgema taseme juhtide ja menetlusgruppide juhtide kaasamisel 15–20 küsimust sisaldanud struktureeritud küsimustiku abil. Saadud andmete põhjal töötati välja digitõendite käsitlemise koolituse materjalid ning see koolitus kuulub eespool mainitud iga-aastase tööplaani raames pakutavate koolituste hulka. Veel üheks elemendiks saab pidada eespool mainitud koolitussoovide kaardistamist, mille abil saab teha järeldusi puuduva või täiendamist nõudvate kompetentside osas.

„Noh, ma võin siis mõned küsimused ette lugeda: millised digitaalsed seadmed, arvutid, välikettad, nutiseadmed, nuppudega telefonid – need, kas üldse ära võetakse; kas on menetlusi, kus üldse digitaalseid seadmeid ära ei võeta või võetakse ainult telefon; millised toimingud... toimingute raames seadmeid ära võetakse; milline on maht seadmetel, mis ära võetakse; kellelt on saadud digikriminalistika teenust; eee… pilveandmetest on siin juttu, EKEI-st on siin juttu; vaatlusjärjekordadest; kuidas toimub selle teostamine, vormistamine; kuidas edastatakse leitud materjalid; kõik muud asjad." (Ekspert 3, PPA)

Kõik eksperdid pidasid **üldkompetentse** (Ko3.1a) oluliseks kompetentsuse komponendiks, kuid selle tähtsust rõhutasid vaid kolm eksperti. Enamus eksperte pidasid üldkompetentse loomulikuks politsei kutsesobivusnõuete osaks, mis isegi ei vääri esiletoomist. Samas, intervjuudes muudele küsimustele vastamisel osutati korduvalt politseinikel enesearengu, pideva enesetäiendamise, iseseisva õppimise, tehnilise taibu, heal tasemel digitaalkirjaoskuse, leidlikkuse, kriitilise mõtlemise ja muu säärase vajalikust, kuna digimaailm pidevalt muutub ja areneb, tuues kaasa uusi nähtusi ja trende, millega tuleb ennast pidevalt kurssi viia ja kaasas käia. Võttes ekspertide mõtteid kokku selgub, et kõrgel tasemel üldkompetentsidega inimene õpib kergesti ka kutsespetsiifilisi teadmisi ja omandab ükskõik mis valdkonnast vajalikke oskusi pidevalt juurde. Tugevad üldkompetentsid on aluseks teiste oskuste omandamiseks, nende kinnistamiseks ja ajakohastatuna hoidmiseks, mis on ühtlasi koosõlas teooriaga (lk 34–38). Enamusest intervjuudest selgub, et uurijatele on seatud suured ootused üldkompetentside osas, eeldatakse nende aktiivsust ja enesearengule orienteerumist.

"...Noh, kui me võtame siin üldkompetentsidest, mis on veel olulisem digiteemas, siis on kindlasti see elukestev õpe ja enesejuhtimine... /.../ Ehk kui sul ei ole neid tugevat tahet, pühendumist, mõtlemsvõimet, kõike seda asja, enesejuhtimise oskusi, noh, siis sa seda ei omanda... seda tulpa /näitab kompetentsiraamistikus sisalduvatele kutsespetriifilistele kompetentsidele/. Nii lihtne see tegelikult ongi." (Ekspert 2, Sisekaitseakadeemia)

Üld-digikompetentsid (Ko3.2b) on toodud eraldi välja, vaatamata eeldusele, et osa neist (näiteks, digitaalkirjaoskus, MS Office arvutiprogrammide alustasemel kasutamie oskus jms) peaks tänapäeval kuuluma tavaliste üldkompetentside alla. See on üheks kutsesovivusnõudeks enamuses tööturu valdkondades, mis on kooskõlas teooriaga (käesolev töö lk 37–40). Üld-digikompetentside osas 4 eksperti pöörasid tähelepanu uurijatel küberturvalisuse ja küberhügieeni oskuste ja teadmiste vajalikkusele. 7 eksperti rääkisid erinevate digiseadmete käsitlemise oskustest, arvuti kasutamise baasoskustest, nt MS Office ja muude programmide kasutamise oskusest. Digikriminalistikaliste toimingute abistamise raames on ilmsiks tulnud asjaolu, et mõnel uurijal on need põhioskused puudulikud. Samas, intervjuudes üld-digioskuste piiritlemise detailidesse ei süvenetud. Teadmiste tõstmiseks küberturvalisuse ja küberhügieeni osas korraldab PPA regulaarselt kõigile töötajatele õppematerjalidega tutvumist ja ettevalmistust eeldava kohustusliku kübertesti läbimist.

„Noh,ideaalis ta peaks olema nii, et need politseijaoskonna uurijad peaksid: punkt üks - olema ja suures plaanis küberteadlikud, küberturbe teadlikud. Kindlasti peavad nad oskama digitaalseid seadmeid käidelda.“ (Ekspert 6, Sisekaitseakadeemia)

Kohaliku tasandi uurijate digitaalse komponendiga kuritegude uurimiseks vajalike **kutsespetsiifiliste kompetentisde** (Ko3.3b) osas tõid kõik eksperdid välja, et kohaliku tasandi uurijal on vaja heal tasemel teadmisi ja oskuseid digitõendite otsimiseks, käsitlemiseks ja talletamiseks, kuid nende oskuste sisu jäi enamusel juhtudel täpsustamata. Enne intervjuud tutvustatud kompetentsiraamistiku osas toodu jäid eksperdid eriarvamustesse: osa pidas raamistikus sisalduvate kutsespetsiifilisi kompetentse liiga detailseks ja kohaliku tasandi uurijale vajaliku taseme ületavaks, osa oli sellega nõus.

„Tõenäoliselt baaskompetentsid on samad kõigile, aga, aga ka siis tundub, et ei ole realistlik… mõistlik, et jaoskonna tasanil uurijal oleksid väga erilised digitaalsed kompetentsid eripärased... Aga see, eksju, et ta suudaks talletada, või... eee, käsitleda digitõendeid, eksju, kindlasti oluline.” (Ekspert 2, Sisekaitseakadeemia)

“Eee... (mõtleb). Nii, siin on jah, kõik sihukesed vajalikud. Lihtsalt, noh. Need on enamus need, mis ma ise ka rääkisin. Mmm... /vaatab läbi/ Ja, et selles mõttes, üldiselt ma nõustun nendega, noh. Küll, ei kujuta ette, kuidas kõigile sihukest mahukust suudaks selgeks teha.” (Ekspert 3, PPA)

Neljandale uurimisküsimusele: „Kuidas hindavad PPA, Sisekaitseakadeemia ja prokuratuuri esindajad magistritöös välja töötatud kompetentsiraamistiku asjakohasust ja rakendusvõimalusi?“ (UK4) vastamiseks moodustati kategooria „**4. kompetentsiraamistiku rakendusvõimalused**“, mille alla kuulub kolm koodi: **„4.1 kompetentsipõhise lähenemise tugevused“ (Ko4.1),** mis esineb 8 intervjuus**, „4.2 kompetentsipõhise lähenemise nõrkused“ (Ko4.2),** mis esineb 7 intervjuus**,** ja **„4.3 hinnangud ja arvamused magistritöös välja töötatud kompetentsiraamistiku kohta“,** mis esineb kõigis intervjuudes. UK3-le vastamiseks moodustatud kategooriad ja koodid, koodide esinemine ja esinemissagedus intervjuudes on esitatud tabelis 12 (käesolev töö, lk 69).

Tabel 12. UK4 vastamiseks moodustatud kategooria ja koodid, koodide esinemine ja esinemissagedus intervjuudes, (NVivo faili põhjal autori koostatud)

4. **KATEGOORIA** / 4.1 kood / - alamkood	koodi esinemine intervjuudes	esinemissagedus intervjuudes
4. KOMPETENTSIRAAMISTIKU RAKENDUSVÕIMALUSED		
4.1 Kompetentsipõhise lähenemise tugevused	8	27
4.2 Kompetentsipõhise lähenemise nõrkused	7	11
4.3 Hinnangud ja arvamused magistritöös välja töötatud kompetentsiraamistiku kohta, rakendusvõimalused	10	27

Ko4.1 all kompetentsipõhise lähenemise **tugevustena** tõi enamus eksperte välja selgust ja arusaadavust kriteeriumide osas, millele politseiuurija kompetentsus peab vastama ning seda politseiorganisatsiooni kui politseiuurija isiku perspektiivis. Kompetentsiraamistik koondab endasse selged ja arusaadavad kriteeriumid, millele peab politseiuurija töökohale kandideeriv isik vastama või mis oskused ja teadmised tuleb arendada tööl oleval uurijal ja Sisekaitseakadeemias õppival politseikadetil, et ta vastaks politseiorganisatsiooni ootustele. See aitab organisatsiooni vaates arendustegevuste kavandamisel ja politseiuurija vaates oma karjääri planeerimisel. Need ekspertide seisukohad vastavad teoreetilisele käsitlusele (käesolev töö, lk 29–30, 41)

„Tugevus on see, et väga selge süsteem, loogiline süsteem, peakski olema need kompetentsid vastavalt kas põhitöödele või tööde gruppidele ära kirjeldatud. Vastavalt sellele on siis need, eee, ka haridusprogrammid. Vähemalt sinna. Eee, inimese jaoks on selge ka, eks ju, kuidas tema selles süsteemis saab karjääri teha. Muidu, ja seda, ja ma isegi ütleks, et inimese vaates on ta kõige selgem ja parem. Et mitte ainult süsteemi on lihtsam niimoodi juhtima, onju. Et teame need kompetentsid, siis teeme haridusprogrammid, onju, aga eelkõige me, see ... See ongi, et ma tean, et ma tahan sinna töökohale liikuda, või seda tööd teha. Okei, milline ma siis peaksin olema, on ju. Mis ma peaks juurde õppima, mida ma peaks omandama juurde.“ (Ekspert 2, Sisekaitseakadeemia)

Ko4.2 all kompetentsipõhise lähenemise suurimaks **nõrkuseks** peeti paindumatust raamistiku liigse detailsuse korral ning pidevat kompetentsiraamistiku ajakohastamise vajadust mõnede kompetentside aegumise tõttu. See seisukoht on kooskõlas teooriaga (käesolev töö lk 31, 33). Teised ekspertide hinnangud olid väga erinevad, ühisosa nendel puudus. PPA eksperdid tõid välja personali kompetentsiraamistikus toodud kompetentside arenguvajaduse kaardistamise ja organisatsiooni poolt arenguvõimaluste pakkumist problemaatiliseks nende paljususe tõttu, kuna arvesse tuleb võtta mitte

üksnes uurija, vaid ka teisi PPA põhitöid, milliseid on üle 70. Probleeme võib tekkida ka PPA personali liikumisel ühelt ametikohalt teisele. Sisekaitseakadeemia eksperdid rõhutasid et uurija vaates seab see raamistik konkreetsed nõudmised ning tuleb kaaluda, kuida võiks selle rakendamisel pehmemalt läheneda juba töötavate ametnike vaates.

Ko4.3 alla koondati **ekspertide hinnanguid ja arvamusi kompetentsiraamistiku** ja magistritöös püstitatud uurimisprobleemi kohta. Kõik eksperdid kinnitasid, et kompetentsiraamistikust oleks kasu, kuid tähelepanu pöörati erinevatele aspektidele. Sisekaitseakadeemia eksperdid tõid välja magistritöös läbi töötatud teadusallikate alusel koostatud teooria väärtuse, mida saab kasutada õppeprogrammide täiendamisel, samuti huvitavaks leiti kompetentsitasemete hindamiskriteeriumide välja toomist (lisa 5, lk 118). PPA eksperdid tõid välja, et konkreetset töövaldkonda kompetentsiteooria vaates seni analüüsitud ei ole ning kompetentsiraamistik võiks mingis osas olla kasulik kompetentsivajaduse kaardistamisel. Politseinike digi- ja küberkompetentside arendamine on prioriteediks ning hetkel on PPA-s mitu vastavasisulist projekti töös. Prokurörid olid arvamusel, et uurijate digitaalse komponendiga kuritegude uurimiseks vajalike kompetentside teema on aktuaalne ning kompetentsiraamistik võiks olla vahendiks uurijate kompetentsilünkade tuvastamiseks ja koolitusmaterjalide kavandamiseks (käesolev töö, lk 29, 41).

2.2.2 Dokumendianalüüs

Käesolev magistritöö on empiiriline uurimus, mis ühendab teadmist politseiuurija tööst digitaalse komponendiga kuritegude uurimise valdkonnast ning kompetentsiteooriast. Dokumendianalüüsi abil taotleti ekspertintervjuudega saadud uurimistulemuste täiendamist UK1 ja UK3 vastuste leidmise osas (vt tabel 13), tagades sellega uurimistulemuste valiidsust. Põhjuseks on asjaolu, et valimisse kaasatud eksperdid ei ole kompetentsiteooria spetsialistid.

Tabel 13. Dokumendianalüüsi käigus täiendavalt uuritud uurimisküsimused

Uurimisküsimus (UK)	**Dokumendianalüüsi allikad valim (vt valimi tabelist 8, käesolev töö, lk 52)**
Millised on ühiskonna digitaliseerumisest tingitud aktuaalsed väljakutsed kohaliku tasandi uurijatele digitaalse komponendiga juhtumite uurimisel? (UK1)	Dokumendianalüüsi allikad D6, D7, D9
Missugust meetodit rakendades saab välja töötada konkreetsele sihtgrupile vajaliku kompetentsiraamistiku? (UK3)	Dokumendianalüüsi allikad D1–D10

Dokumendianalüüsiga sooviti täpsustada, kuidas on dokumentides kajastatud väljakutsed kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude lahendamisel, kuidas on reguleeritud kompetentsinõudega seonduv, milliseid kompetentsipõhise lähenemise praktikad kasutatakse Eestis, milline on nende praktiline väärtus. Dokumentide kodeerimisel kasutati lisas 8 (käesolev töö, lk 128) käesoleva uuringu ühise kategooriate ja koodide süsteemi.

Mahukamate dokumentide tekstid vaadati üle sihistatult, otsides neist vasteid kategooriate **„1. väljakutsed ja võimalused“** (Ka1), **„3a. kompetentsiraamistiku väljatöötamise meetod**“ (Ka3a), **„3b. kohaliku tasandi uurija oodatavad kompetentsid“** (Ka3b) ja Ka4 all olevatele koodidele, v.a. koodid Ko1.4 (vt tabel 9 – lk 55, tabel 11 – lk 65, tabel 12 – lk 69). Mõne dokumendi sisu on väiksema mahuga ja kitsama suunitlusega (nt D1–D4, vt tabel, käesolev töö, lk 52). Dokumendianalüüsi raames kasutati ka UK4-le vastamiseks moodustatud koodi „ **4.3 Hinnangud ja arvamused magistritöös välja töötatud kompetentsiraamistiku kohta, rakendusvõimalused**“ (Ko4.3), tõlgendades seda laiemalt, et otsida dokumentidest vasteid kompetentsipõhise lähenemise rakendusvõimaluste kohta. Dokumendianalüüsis ei taotletud koodide esinemissageduse täpse osakaalu väljatoomist, vaid pöörati tähelepanu dokumendis koodi esinemisele ja selle tekstis paiknemisele, s.o kontekstile. Erinevalt ekspertintervjuude transkriptsioonide analüüsist, kus tulemused kajastati täpselt kategooriate ja koodide ja alamkoodide kaupa esitatakse dokumendianalüüsi tulemused üldistavalt.

Sarnaselt ekspertintervjuude uurimistulemustega koodi „**1.1 politseiorganisatsiooni sisesed tegurid**“ (Ko1) all on dokumentidest kõige enam silma paistnud alamkoodi „**digitaliseeruvas maailmas personalile ettevalmistuse tagamise väljakutse**“ esinemine. Muutustega kohanemiseks on soovitatav tagada senisest paremad arengu- ja karjäärivõimalused, sh töötavale personalile täiendusõpe digi- ja muude uurijatele vajalike kompetentside arendamiseks. Kasvava tähtsusega on siseturvalisuse töötajate elukestva õppe väljakutse (D6) ja tugevad üldkompetentsid (D2, D3, D8, D9). Samuti on palju tähelepanu pööratud inimressursside vähesusele, mis on tingitud Eesti demograafilistest probleemidest. Teravalt tuntakse puudust IKT-kompetentsidega töötajatest (D7). Tugevalt on esindatud Eesti demograafilise olukorraga seotud alamkood **„uurija vanus“.** Personali voolavus on suurenenud töötajaskonna vananemise, noore põlvkonna väiksema esindatuse ning noorte inimeste väärtuste ja töökultuuri suhtumisest tingitud muutuste tõttu. Tööjõu pealekasv on tagasihoidlikum kui nende inimeste osakaal, kellel lähiajal tekib õigus suunduda pensionile (D1, D6, D7, D8). Hetkel on keskmine PPA kohaliku tasandi uurija politsei- või õigusalase haridusega naisterahvas, kelle keskmine

vanus on 41,2 aastat (D1). Uurijate vanuse tegurit on sageli mainitud ka ekspertintervjuudes (käesolev töö, lk 57), kuid seda aspekti ei käsitletud teoorias.

Koodi „**1.2 politseiorganisatsiooni välised tegurid**“ osas saab dokumendianalüüsi alusel välja tuua **IKT kiiret levikut** (D6), mis avaldab mõju kogu elanikkonna elustiilile ja seab kõrged ootused siseturvalisuse valdkonna töötajate, sh politseiuurijate kompetentsidele. Samuti on esile toodud õigusnormide ajakohastamise ja IKT muutustega kohanemise probleemi, süüteomenetluste keerukamaks ja mahukamaks muutumist ning ka kuritegevuse rahvusvahelisust ja piiriülesust (D6), mis on kooskõlas teooriaga (käesolev töö, lk 15).

Töötajasokonna perspektiivis digiajastu väljakutsete lahendustena nähakse (Kood **„1.3 takistuste ja kitsaskohtade ületamise võimalused“)** kõigil haridusastmel õppetegevuse käigus üldkompetentside kujundamisele ja arendamisele suunatud tegevuste kavandamist. Üldkompetentsid tuleb hoida kaasajastatuna ja arendada neid elukestva õppe kaudu, sh tööprotsesside raames. (D6, D8) Ka eksperdid väljendasid arvamusi, et digitaalse komponendiga kuritegude uurimiseks vajalikke kompetentse saab arendada üksnes pideva juurdeõppimise ja tööprotsesside raames uute oskuste kinnistamise kaudu (käesolev töö, lk 58–59).

Kategooria **„3a. Kompetentsiraamistiku väljatöötamise meetod“** alla koondatud koodide abil otsiti dokumentidest vasteid, et iseloomustada **tegelikku olukorda kompetentsipõhise lähenemise kasutamise osas**, erinevate kompetentsiraamistike korraldamise vise ja metoodikaid. Hetkel PPA-s ei kasutata formaliseeritud kompetentsipõhist lähenemist ja standardiseeritud kompetentside hindamisinstrumente, politseiuurija kutsestandard puudub. Politseiametniku kutsesobivuse nõuetele vastavuse hindamisel lähtutakse õigusaktidega sätestatud nõuetest. Üldkompetentside- ja haridusnõuetele vastavust hinnatakse politseiametniku kandidaadiga kutsesobivusvestluse või töötava politseiniku arenguvestluse ajal. (D3) EQF üldisem kriminaaluurija kvalifikatsiooninõuete kirjeldus näeb ette, et kriminaaluurija peab analüütiliselt mõtlema ja erinevaid suhtluskanaleid kasutama (D2). D6 tuuakse lisaks välja, et uurijal ja politseinikul peab olema suhtlemis-, meeskonnatöö (-sh võõrkeeltes) ning mitmekultuurilises keskkonnas töötamise oskus. Digikompetentse on vaja iseseisva kasutaja tasemel ning nende sisu ja tasemete kirjeldamisel viidatakse DigComp kehtivale versioonile. Seega, informatsiooni kohaliku tasandi politseiuurija kompetentsinõuete kohta leidub süstematiseerimata kujul erinevatest allikatest, kus kasutatakse erinevat terminoloogiat.

Kompetentsiraamistike koostamise viisi osas saab välja tuua, et enamusel neist kasutatakse käesoleva töö mõistes ülevalt-alla viisil raamistiku koostamise metoodikaid (käesolev töö, lk 30, D6, D8, D9). Ainult kohalike omavalitsuste ametnike koolitusvajadust kaardistavas uuringus lähtuti kompetentsiraamistiku koostamisel ülevalt-alla ja alt-ülesse viisi kombinatsioonist, kaasates uuringusse sihtgruppi, kelle kompetentse hinnati (D10). Kõigi analüüsitud kompetentsiraamistike (D6, D8, D9, D10) osas rakendatakse nende pidevat ülevaatamist ja ajakohastamist. Näiteks, DigComp igal järgneval ülevaatmisel muutub kompetentsiraamistiku metoodika keerulisemaks ja raamistiku struktuur mitmemõõtlemiseks: 1. dimensioon kirjeldab kompetentsivaldkondi laiemalt; 2. dimensioonis on kajastatud kompetentside kirjeldused; 3. dimensiooni kasutatakse tasemekirjelduseks; 4. dimensioonis sisaldub tehisintellekti, kaugtöö ja digitaalse juurdepääsetavusega seotud näiteid; 5. dimensioon pakub näidisjuhtumeid õppimise ja hariduse kontekstide kohta. Ühtlasi sisaldab DigComp raamistik enesehindamisel põhinevat hindamisinstrumenti kompetentsitaseme kontrollimiseks. (D9) Edasiarenduse on saanud ka üldoskuste kontseptsioon (D8), mille kohaselt on üldkompetentsid jaotatud kolme jaotuskategooriasse: enesejuhtimis-, mõtlemis- ja lävimisoskusteks, kus igas valdkonnas on rida üldoskusi. Kokkuvõtteks, eespool kirjeldatud kompetentsiraamistike metoodikate elemendid on saranased Marelli, *et al.,* (2005) kajastatud metoodikaga (käesolev töö, lk 31–33) Sellega võrreldes on magistritöös välja töötatud raamistik lihtsakujulisem, kus kompetentsid on jaotatud kolme valdkonda ja nende hindamiseks pakutakse tasemeid.

Dokumendianalüüsi põhjal paistab **Kohaliku tasandi uurijate oodatavate kompetentsidest** (Ko3b.) enam silma ootus politseinikele üld- ja digikompetentsidele, mis on ühtlasi kooskõlas ka ekspertide seisukohtadega (käesolev töö, lk 67). Samas, kui enamus interjueeritavaid ei osanud digikompetentside teemal pikemalt rääkida ja selgitada nende tähtsust, siis dokumentides on üldkompetentse käsitletud põhjalikult ja erineval viisil. Viimane universaalne üldkompetentside käsitlus, millel on tugev seos Eesti kvalifikatsiooniraamistikuga, ilmus 2022. aastal (D8). Selle kohaselt üld-digikompetentsid ehk baasdigioskused kuuluvad lävimisoskuste jaotuskategooriasse ning siseturvalisuse valdkonna töötajatel peavad need olema iseseisva kasutaja tasemel.

Politsei tööülesannete täitmisel on hulk kutsealaseid tegevusi, mille keskseks tegevuseks on üldoskuste rakendamine. Näiteks, uurija tööülesannetega hakkama saamiseks on vaja nii enesejuhtimis-, lävimis- kui mõtlemisoskusi. (D8) Üldoskused on osa politseiniku kutsesobivusnõuetest, kuid nende kirjeldamisel on kasutatud teisi termineid: kõrge stressitaluvus, meeskonnatöö oskus,

kohusetundlikkus, otsustus- ja vastutusvõime, iseseisvus, analüüsivõime, probleemilahendus- ja suhtlemisoskus. (D3) Tänapäeval kätkevad lävimisoskused ka baasdigioskusi, mis on kirjeldatud kehtivas DigComp2.2 versioonis (D8, D10). Üldoskused on eelduseks valdkonnaspetsiifiliste oskuste omandamiseks (D6, D8). Kuigi **üld-digikompetentsid** (Ko3.2b) moodustavad magistritöös välja töötatud kompetentsiraamistikus eraldi kategooria, kuuluvad nad kaasaegse lähenemise kohaselt (D8) üldkompetentside lävimisoskuste alla.

Digitaalse komponendiga kuritegude uurimiseks vajalike **kutsespetsiifiliste oskuste (Ko3b)** väljatoomiseks analüüsiti Sisekaitseakadeemia vastust selgitustaotlusele (päring seoses magistritöö koostamisega; vastus 6.1-17/3250-1 – autori valduses) (D4), sest võrreldes kompetentsiraamistikus toodud kutsespetsiifiliste kompetentside loeteluga on kutsespetsiifilised teadmised ja oskused enamuses analüüsitud dokumentides sõnastatud üldisemalt. Neid kompetentse nimetatakse valdkondlikeks IKT-oskusteks: tööalaste andmekogude, infosüsteemide ja programmide kasutamine, digitõendite käitlemine, suurandmete analüüsimine, tulemuste tõlgendamine ja kasutusvõimaluste tundmine; küberturvalisus jne. (D5, D6, D7) Kõrvutades Sisekaitseakadeemia õppekavade teemasid ja õpiväljundeid kompetentsiraamistikus kajastatud kutsespetsiifiliste oskustega olulisi erisusi välja ei toodud. Sisekaitseakadeemia ekspertide sõnul moodustavad õppekavades kirjeldatud digi- ja küberteemalistel õppeainete raames omandatud teadmised ja oskused kohaliku tasandi uurijatelele vajalikku erialast baaskompetentsi. Samas osa kompetentse on omandatav vaid kriminaalpolitsei süvaõppe suunal (vt tabel 14). PPA töötajaskonnale ette nähtud täiendusõppekava on hetkel arendamisel (D4, käesolev töö, lk 31, 66).

Tabel 14. Digitaalse komponendiga kuritegude uurimiseks vajalikud kompetentsid vastavalt Sisekaitseakadeemia politsei eriala õppekavadele

Sisekaitseakadeemia politsei eriala õppekavad	
Politseiametniku õppekava (kutseõppe esmaõpe, statsionaarne õpe ja mittestatsionaarne õpe) Moodul „Väärtegude menetlemine ja kriminaalmenetluse alustamine“: ➢ digitaalsed tõendid, digiinfokandjate liigid, digitaalsete tõendite kogumine ja käitlemine	**Süüteomenetleja õppekava (kutseõppe jätkuõpe, mittestatsionaarne õpe)** Moodul „Kriminaalmenetluse läbiviimine“: ➢ digitaalsed tõendid, võimalike digitaalsete tõendite äratundmine, talletamine, säilitamine; ➢ digiinfokandjate kasutamine tavakuritegude toimepanemisel. Internetikelmused; ➢ tehnoloogiline pool (operatsioonisüsteemid, WIFI, IP aadressid, VOIP, logid, nutitelefonid, krüpteeritud andmeside, VPN, pilved, pime ja süvaveeb);

	➢ Infokandjate tüübid, salajane andmeside monitoorimine, IP-jälitamine; andmekaitsereeglite järgimine menetlustoimingute läbiviimisel. Moodul „Väärtegude menetlemine ja kriminaalmenetluse alustamine“: ➢ digitaalsed tõendid, digiinfokandjate liigid, digitaalsete tõendite kogumine ja käitlemine.
<u>Politseiteenistuse õppekava</u> (kõrgharidus) Moodul „Kogukonnakeskne politseitöö“: ➢ OSINT, sotsiaalmeedia Moodul „Piiriülene koostöö“: ➢ küberturvalisus (riigisisese ja rahvusvahelise koostöö olulisus) Moodul „Kriminaalmenetluse läbiviimine“: ➢ digitaalsed tõendid, võimalike digitaalsete tõendite äratundmine, talletamine, säilitamine; ➢ digiinfokandjate kasutamine tavakuritegude toimepanemisel, internetikelmused; ➢ tehnoloogiline pool (operatsioonisüsteemid, WIFI, IP aadressid, VOIP, logid, nutitelefonid, krüpteeritud andmeside, VPN, pilved, pime ja süvaveeb); ➢ infokandjate tüübid, salajane andmeside monitoorimine, IP-jälitamine; andmekaitsereeglite järgimine menetlustoimingute läbiviimisel.	**<u>Politseiteenistuse õppekava</u> (kõrgharidus)** Moodul „Raskete kuritegude menetlemine“ (üksnes kriminaalpolitsei süvaõppe): ➢ küberkuritegevus (sh globaalne ja Eesti statistika, trendid, majandusliku kahju määr; kurjategija sotsioloogiline ja psühholoogiline profiil; ➢ pahavarad, krüptorahad, krüpteeritud suhtluskanalid; ➢ politsei ülesanded küberkuritegevuse ennetamisel ja uurimisel ning koostöö teiste riigisiseste asutustega (kohtud, prokuratuur, Riigi Infosüsteemide Amet); ➢ küberkuritegude uurimise metoodika (karistusõiguslik iseloomustus, tüüpilised uurimissituatsioonid ja sellest tulenev uurija tegevus uurimise esialgsel etapil, esialgsete versioonide ja uurimise planeerimine, uurimis- ja jälitustoimingute tegemise eripära; ➢ tüüpilised määratavad ekspertiisid ja nendega lahendatavad küsimused).

Dokumendianalüüsi tulemused (D8, D9, D10) kategoorias **„4. Kompetentsiraamistiku rakendusvõimalused“** on kooskõlas teooriaga (käesolev töö, lk 27–29, 32, 42, 45) ja ekspertide arvamustega (käesolev töö, lk 69), et kompetentsipõhise lähenemise tugevusteks on selgus ja konkreetsus uurija kompetentsi kriteeriumide osas nii indiviidi kui ka politseiorganisatsiooni vaates ja kompetentsilünkade tuvastamise ning arendustegevuste kavandamise vahendiks (käesolev töö, 30–31, 41, 68–69).

2.3 Järeldused ja ettepanekud

Käesoleva empiirilise uurimuse raames uurimisprobleemi: „kuidas süstematiseerida aktuaalseid kompetentse, mis on tänapäeval vajalikud kohaliku tasandi uurijatele digitaalse komponendiga kuritegude uurimisel?“ lahendamiseks koostati vastavalt magistritöö eesmärgile teoreetiline kompetentsiraamistik (vt lisad 4, 5, käesolev töö lk...) mida valideeriti ekspertintervjuude

ja dokumendianalüüsi abil. Uuringus saadud tulemused kinnitavad digitaalse komponendiga kuritegude uurimiseks vajalike kompetentside arendamise aktuaalsust. Järeldused esitatakse vastavalt magistritöös püstitatud uurimisküsimustele vastamisel saadud tulemustest.

Esimesele uurimisküsimusele: „Millised on ühiskonna digitaliseerumisest tingitud aktuaalsed väljakutsed kohaliku tasandi uurijatele digitaalse komponendiga kuritegude uurimisel?“ vastamisel selgus, et PPA-s on olulisemateks politsei organisatsioonisisesteks väljakutseteks digitaalse komponendiga kuritegude uurimisel uurijatel vajalike teadmiste ja oskuste puudulikkus ja politseiorganisatsiooni võimaluste piiratus vastava ettevalmistuse tagamiseks rahaliste ressursside ja pädevate koolitajate vähesuse tõttu, mis on ühtlasi kooskõlas teooriaga (käesolev töö, lk 15–17).

Väljakutsetena toodi välja ka uurijate endi huvi ja motivatsiooni probleeme (käesolev töö, lk 14), seostades seda tegurit keskmise politseijaoskonna uurija vanusegruppi 40+ aastat kuulumisega, tehnilise taibu puudumisega ja hirmudega IKT lahenduste kasutusele võtmise ees. Viimaseid tegureid teoorias ei käsitletud. Dokumendianalüüsis on kinnitust leidnud, et keskmine PPA politseijaoskonna uurija on politsei- või õigusalase kõrgharidusega 41-aastane naine. Välisteks väljakutseteks on IKT kiired muutused, millele PPA ei jõua järgi ametnikele ettevalmistuse tagamise osas. IKT kiired muutused soodustavad uute käitumisvormide (sh kuritegelike) tekkimist (käesolev töö, lk 13, 21–25). Samas, digitaalse komponendiga kuritegude uurimise metoodikad ja kohtupraktika on alles kujunemas (käesolev töö, lk 14–15) ning nende juhtumite uurimiseks eeldatakse uurijate initsiatiivi ja loomingulise lähenemise kasutamist. Uuringu käigus selgus, uute oskuste ja teadmiste omandamiseks eeldatakse politseiuurija initsiatiivi ja iseseisvust, millest tegelikult on sageli puudu. Motivatsiooni puudumine ja digihirmud võivad olla seotud üld- ja digioskuste puudulikkusega ning nende oskuste arendamine inimestel vanuses 40+ aastat on tõsine väljakutse, mis eeldab erilist lähenemist.

Seega, tulenevalt sellest **esimene ettepanek** PPA-le on tegeleda kohaliku tasandi uurijate sihtgrupiga, pöörates täiendavalt tähelepanu üleesindatud vanusegrupile. Välja tuleks töötada nendele sobiv metoodika kompetentsivajaduse hindamiseks ja selle täiendamiseks. Motivatsiooni puudumise ja digihirmude korral on oluline rakendada mitmekülgset lähenemisviisi, mis hõlmab teadlikkuse tõstmist, koolitusi, mentorlust ning toetava keskkonna loomist organisatsiooni poolt.

Uuringus on eksperdid esitanud erinevad ettepanekud digitaalse komponendiga kuritegude uurimise protsessi parendamise ja uurijate toetamise kohta. Autori seisukohal oleks teostatavaks lahenduseks

politseijaoskondades motiveeritud ametnike arendamine tasemeni, et nemad saaksid vastutada jaoskonnas menetluses digiteemade arendamise eest ning suunata ja abistada kolleege keerulisemate menetlustoimingute teostamisel digitaalse komponendiga kuritegude uurimisel. Sellisel juhul tuleb kaaluda nende vabastamist põhitööst osaliselt või täielikult. Selliste initsiatiivikate ametnike arendamist toetaks vastava väljaõppe saamise võimalus, stažeerimine funktsionaalüksustes, jms, mida eksperdid on soovitanud. (käesolev töö, lk 58–60)

Sellest tulenevalt on **teiseks ettepanekuks** PPA-le toetada ekspertide ideed luua jaskonnapõhine mentorluse süsteem. Üle tuleks vaadata töökoormuse jaotamine politseijaoskonnas, tagades 1–2 ametniku pühendumine digitaalse komponendiga kuritegude uurimiseks tingimusel, et need ametnikud võtavad vastutuse oma jaoskonnas süüteomenetluslike digiteemade eestvedamise eest.

Teisele uurimisküsimusele: „Millised on digitaalse komponendiga kuriteod, mille lahendamisega tegelevad kohaliku tasandi politseiuurijad?“ vastamisel selgus, et PPA-s on kohaliku tasandi uurijate menetluspädevus jaotatud erinevalt, võttes arvesse iga prefektuuri tööpiirkonna geograafilist asukohta, elanikkonna suurust ja sellest tulenevat prefektuuri töökorralduslikku eripära. Üldplaanis menetleb kohaliku tasandi uurija kogukonna turvatunnet riivavaid ja mõjutavaid ning avalikkusele nähtavaid juhtumeid, kus puuduvad raske ja organiseeritud (sh peit-)kuritegevuse tunnused. Üldjuhul ei tegele politseijaoskonna uurija kitsa suunitlusega kuritegude (nt küberkuriteod, narkokuriteod, majanduskuriteod) uurimisega, kus eeldatakse spetsiifilisemaid oskusi ja metoodikate kasutamist. Samas võib piirkonniti selles osas olla erinevusi. Ühlasi toodi välja, et kohaliku tasandi uurijate menetluspädevuses olevad juhtumid on reeglina vähem mahukad. Nendes juhtumites piisab tõendite kogumiseks ja vormistamiseks, kui kohaliku tasandi uurijal on olemas baasdigioskused ja üldkompetentsid. Teoorias kohaliku tasandi politseiuurijate menetluspädevuse erisust käsitleti kaudselt, seostades seda kohaliku tasandi politseiüksuste territoriaalsuse printsiibiga (käesolev töö lk 17). Erinevalt teooriast territoriaalse printsiibi alusel kohaliku tasandi uurijate töö ülesehitusest kaasnevaid geograafilisi probleeme, mis on seotud digitaalse komponendiga kuritegevuse piiriülesusega (käesolev töö lk 17), uuringus välja ei toodud.

Digitaalse komponendiga kuritegude määratlus vastab magistritöös katuseterminina kasutatavale digitaalse komponendiga kuriteo mõistele (käesolev töö lk 7, 26). Digitaalse komponendiga kuritegude toimepanemisel kasutatakse IKT-d, digitaalset keskkonda, internetti ja/või mille tagajärjel jääb digitaalseid jälgi ja tõendeid. Eksperdite arvamusel ja dokumendianalüüsi kohaselt esineb digitaalset

komponenti peaaegu igas kuriteos, mille uurimisega tegeleb kohalik tasand, mis on kooskõlas teooriaga (käesolev töö, lk 21). Seega uurivad kohaliku tasandi politseiuurijad nii digitaalse komponendiga traditsioonilisi kuritegusid, kui ka mõningaid ehtsaid küberkuritegusid (käesolev töö, lk 21–26). Samas toodi erinevalt teooriast digitaalse komponendina välja ka IKT lahenduste kasutamist menetluse läbiviimisel, tõendite vormistamisel ja menetluse raames suhtluse tagamisel.

Ühtlasi võib järeldada, et hetkel puudub täpsem ülevaade muret tekitavatest uurimissituatsionidest ja ametlikku statistikat digitaalse komponendiga juhtumitest uurijate kompetentsivajaduse täpsustamise eesmärgil ei koguta (käesolev töö, lk 21). Eeldatakse, et kohaliku tasandi politseiuurijal piisab üldoskustest ja baasdigioskustest misiganes uurimissituatsioonidega toime tulemiseks, sh digikomponendiga juhtumites. Esimene ja viimane kaardistamine toimus 2017–2018. aastal digitõendite koolituse materjalide koostamise eesmärgil, kuid võttes arvesse IKT kiiret arengut ja selle mõju kuriteovormide mitmekesistumisele (käesolev töö, lk 14–15) ja uurijate vajalike teadmiste ja oskuste puudulikkusele (käesolev töö, lk 54), tuleb seda praktikat aeg-ajalt kaasajastada ja korrata.

Kolmas ettepanek PPA-le on tihedalt seotud esimese ettepanekuga: kohaliku tasandi uurijate kompetentsivajaduse hindamisel ja selle täiendamisel välja töötada või ajakohastada uurimisinstrument aktuaalsete muret tekitavate uurimissituatsioonide täpsustamiseks. See aitab orienteeruda, milliseid kompetentse tuleb arendada.

Vastustest esimesele ja teisele uurimisküsimusele võib seega järeldada, et kohaliku tasandi politseiuurijate kompetentsid digitaalse komponendiga kuritegude uurimiseks on aktuaalne teema. Üld-, digi- ja kutsespetsiifiliste kompetentside arendamine on politseiuurijate jaoks oluline, et nad saaksid tõhusalt tegeleda digitaalse komponendiga kuritegude uurimisega. Kompetentside sisu täpne määratlemine sõnastamine ning süstematiseerimine võib aidata mõista, millised on kohaliku tasandi politseiuurijate kompetentsilüngad, edendada enesearengut ja toetada koolitusprogrammide arendamist vastavalt standardiseeritud lähenemisele (käesolev töö, lk 29).

Kolmandale uurimisküsimusele: „Kuidas süstematiseerida kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimiseks vajalikke teadmisi ja oskusi?“ vastamisel lähtuti kompetentsiraamistiku koostamise teooriast, jaotades kompetentse kolme valdkonda: üldkompetentsideks, üld-digikompetentsideks ja kutsespetsiifilisteks kompetentsideks, mida on vaja

spetsiifiliselt digitaalse komponendiga kuritegude uurimiseks (käesolev töö lk 46). Välja töötatud kompetentsiraamistiku materjalid paiknevad lisades 4 ja 5 (käesolev töö, lk 112–19).

Uuringu tulemusel selgus, et hetkel formaliseeritud kujul süsteemset kompetentsipõhist lähenemist PPA-s ei rakendata, mis sarnaneb ka teoorias toodud probleemkohtadele (käesolev töö lk 15). Inimressursside juhtimisel, sh nende kompetentsi täiendamisel lähtutakse PPA-s teenuspõhise juhtimise põhimõtetest. Igale põhitööle kompetentside komplekti detailselt lahti kirjutatud ei ole ja ametijuhendis seda ei kajastata, vaid lähtutakse üldistest põhimõtetest. PPA personali kompetentside arendamiseks vajalikud koolitused planeeritakse keskselt vastavalt strateegilise eesmärgi kaudu määratletud koolitusvajadusele. Samas igaastase tööplaani raames kogutakse prefektuuri teenuse koordinaatori korraldamisel tagasisidet erinevates üksustes tekkinud koolitusteemade soove, nii valmis oleva loetelu alusel, kui ka vabas vormis. Vabas vormis esitatud koolitusteemade ettepanekute osas täpsustatakse ja kaalutakse nendel teemadel koolituste korraldamise otstarbekust.

PPA-s eeldatakse süütegude uurimiseks vajalike kompetentside olemasolu olenemata uurimissituatsioonidest ja tõendite liigist. Kompetentse täiendatakse vajaduspõhiselt koolituste kaudu. Politseijaoskonna menetlusgruppi uue ametniku värbamise korral ja grupile vajaliku kompetentsivõimekuse otsimisel lähenetakse juhtumi- ja vajaduspõhiselt, intuitiivselt. Uurijaks sobiva kandidaadi valimisel võetakse arvesse grupi hetkeseisu. Hindamine toimub kandidaadiga vestluse raames. Konkreetse juhtumi lahendamiseks või toimingu tegemiseks menetlusgrupis puuduva kompetentsi korral pöördutakse digikriminalistika keskuse või küberkuritegevusele spetsialiseeritud funktsionaalüksuse poole. Sellist paindlikku lähenemist kasutatakse üksikjuhtudel, sest üldjuhul peaks menetlusgrupis kohaliku tasandi uurijale ette nähtud kompetents eeldatavalt olemas olema.

Samas näevad eksperdid probleemi selles, et kohaliku tasandi uurija ei ole sageli võimeline iseseisvalt digikomponendi vormistamisega toime tulema ning ta ei ole huvitatud vajalike teadmiste oskuste omandamisest (käesolev töö, lk 56). Motivatsiooni puudumisest rääkisid ka teised eksperdid (käesolev töö, lk 55–56). Selline vastuolu tõstatab küsimuse kohaliku tasandi politseiuurijate üldkompetentside ja baasdigioskuste soovitud tasemele vastavuse kohta, sest üldoskused eeldavad initsiatiivikust ja motivatsiooni. Teooriast selgub, et tunded ja motivatsioon on kompetentsuse komponendiks ning motiveeritud töötaja on reeglina kompetentne töötaja (käesolev töö lk 27). Lisaks, vastavalt teooriale, toovad töötajad oma isiksuse ja isikuomadused töösse ja kujundavad sellega teineteise tööharjumusi,

olles omavahelises interaktsioonis (käesolev töö, lk 38). Selest võib järeldada, et tuleb tegeleda uurijate motivatsiooni tõstmisega ja digihirmude maandamisega (vt ettepanek 1, käesolev töö, lk 76)

Positiivne areng on see, et alates 2020/2021. õppeaastast täiendati Sisekaitseakadeemia politsei eriala õppekavas olevad õppeained küber- ja digikompetentside teemadega ning saadud teadmised ja nende töös kasutamise tulemusel tekkinud oskused moodustavad kohaliku tasandi uurija baaskompetentside komplekti. See tagab digikompetentsemate kolleegide järelekasvu ja eeskuju kogenud kohaliku tasandi uurijatele. Vastavalt teooriale töötajate identiteedid segunevad ja muutuvad tööalase kokkupuute ja suhtluse käigus ning sellest tekivad uued praktikad (käesolev töö, lk 38). PPA töötajaskonnale ettenähtud vastavasisuline täiendusõppe kava on hetkel arendamisel ja seda plaanitakse rakendama hakata käesoleval aastal (Sisekaitseakadeemia 18.12.2023 e-kiri, autori valduses).

Kompetentsiraamistiku valideerimisel selgus, et eksperdid ei süvenenud üldkompetentside, üld-digikompetentside ja kutsespetsiifiliste kompetentside detailidesse, vaid rääkisid üldisemalt ja laiemalt, märkides, et need komponendid on vajalikud. Intervjuude käigus keskenduti peamiselt tehnilistele ehk kutsespetsiifilistele oskustele, rõhutades vaid seda, et uurija peab olema võimeline käitlema digitõendeid ja tulema toime nende vormistamisega. Võib järeldada, et kompetentsiteooria terminoloogia vähene kasutamine ja sellele keskendumise puudumine tuleneb sellest, et ekspertidel on teadmised ja kogemused konkreetses töövaldkonnas või funktsioonis (digitaalse komponendiga kuriteod), kuid samal ajal puuduvad neil sügavad teadmised kompetentsiteooria valdkonnas. Sellest võib järeldada, et politseiorganisatsioonis pööratakse vähe tähelepanu kompetentsiteooria terminoloogiale ning seetõttu ei osata detailselt kirjeldada, millistest konkreetsetest teadmistest ja oskustest on puudu, et saavutada soovitud tulemus. Samas ei saa välistada, et enne kompetentsiraamistiku valideerimist ei selgitanud autor ekspertidele piisavalt arusaadavalt, kuidas üldoskused on seotud digitaalse komponendiga kuritegude uurimisega.

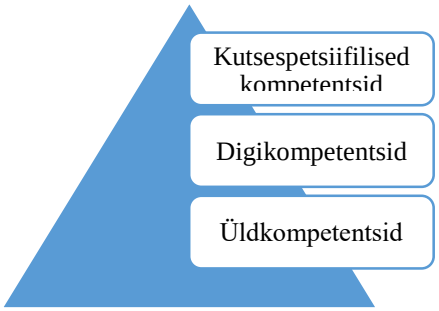
Seega, **neljandaks ettepanekuks PPA-le ja Siseaitseakadeemiale** on tõsta kõigi ametnike teadlikkust üldkompetentside ja baasdigioskuste kehtivatest kontseptsioonidest ning kasutada läbivalt ühte kompetentsiteooria terminoloogiat koolitus- ja õppekavade koostamisel, ametijuhendites ja tööde kirjelduses, kutsesobivus- ja arenguvestluste planeerimisel ning läbiviimisel jms.

Kompetentsiraamistiku valideerimisel selgus, et võttes arvesse IKT valdkonna kiireid muutusi, mida nimetati sageli tõsise väljakutsena digitaalse komponendiga kuritegude uurimisel ja

kompetentsinõuete vastavusse viimisel (käesolev töö lk 18, 20, 56), tuleb kompetentsiraamistiku kontseptsiooni muuta paindlikumaks. Nii teoorias kui ka empiirilise uuringu tulemusel selgus, et kompetentsiraamistikud tuleb aeg-ajalt ajakohastada (käesolev töö lk 30–31, 33).

Seega, viiendaks ja üldisemat laadi ettepanekuks PPA-le ja Sisekaitseakadeemiale on võtta kasutusele üldisem kompetentsiraamistik, eristades seal kolm kompetentsivaldkonda (üldkompetentsid, digikompetentsid, kutsespetsiifilised kompetentsid) ja viidates kaasajastatud kehtivatele ja üldtunnustatud üldkompetentsidele (Leemet, *et al.*, 2022) ja DigComp 2.2 (Vuorikari, *et al*., 2022) kompetentsiraamistikule (käesolev töö, lk 35). Kutsespetsiifiliste kompetentside loetelu tuleb samuti hoida kaasajastatuna, kogudes regulaarselt tagasisidet praktikutelt ja hoides end kursis CEPOL koolitusvajaduse kaardistusega, jms. Nõnda lähenedes põhineb kompetentsiraamistik nii teaduslikul kui ka praktilisel alusel, mis võimaldab paremini mõista ja täita kohaliku tasandi uurijate kompetentsivajadusi digitaalse komponendiga kuritegude uurimisel.

Nii teooriast kui ka uuringu läbiviimisel selgus, et kohaliku tasandi politseiuurija töö tegemise aluseks on tugevad üldkompetentsid, mis on eelduseks kutsespetsiifiliste kompetentside omandamiseks ja kinnistamiseks. Osa üldkompetentse (nt suhtlemis-, probleemilahendus- ja analüüsioskust) rakendab kohaliku tasandi politseiuurija oma igapäevases töös ning nende oskusteta töötamine ei ole võimalik. (käesolev töö, lk 40) Üldkompetentside mõistete korrektne sõnastamine on seega oluline mõistmisel, milliste teadmiste ja oskuste arendamisele tuleb tähelepanu pöörata. Kuigi digikompetentsid on mingis osas muutunud üldkompetentside osaks, tuleb neid siiski eristada, sest üld- ja digikompetentside üldtunnustatud raamistikud võivad muutuda teineteisest sõltumata ning erineval ajal. Nõnda lähenedes tagatakse kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimiseks vajaliku kompetentsiraamistiku paindlikkus ja pideva täiendamise võimalus (vt joonis 2).



Joonis 2. Kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimiseks vajaliku kompetentsiraamistiku struktuur

Neljandale uurimisküsimusele: „kuidas hindavad PPA, Sisekaitseakadeemia ja prokuratuuri esindajad magistritöös välja töötatud kompetentsiraamistiku asjakohasust ja rakendusvõimalusi?“ vastamisel selgus, et kõik eksperdid leidsid kompetentsiraamistiku mingis osas kasulikuna. Kompetentsipõhise lähenemise tugevusteks on selgus ja konkreetsus uurija kompetentsi kriteeriumide osas nii indiviidi kui ka politseiorganisatsiooni vaates, mis on ühtlasi kooskõlas teooriaga (käesolev töö, lk 30–31, 41, 68–69). Sellest võib järeldada, et magistritöös välja töötatud kompetentsiraamistik on näide universaalsest tööriistast nii politseiorganisatsioonile, politsei õppeasutusele, samuti uurijale, mis aitab tuvastada ja arendada kompetentse konkreetses töövaldkonnas. See pakub struktuuri ja suuniseid kompetentside jaotamiseks kategooriatesse ning nende kirjeldamiseks, arendamiseks ja hindamiseks. Organisatsiooni vaates aitab kompetentsiraamistik mõista, millised kompetentsid on vajalikud, et saavutada soovitud tulemusi ja eesmärke. Indiviidi vaates tagab kompetentsiraamistik selgust, milliseid oskusi, teadmisi ja omadusi on vaja konkreetsel töökohal tööülesannetega toime tulemiseks.

Kompetentsiraamistikku võib seega kasutada alljärgnevatel eesmärkidel:

- abimaterjalina kompetentsilünkade tuvastamiseks ning arendustegevuste kavandamisel PPA-s;
- sisendina Sisekaitseakadeemias õppekavade täiendamisel, määratledes kohaliku tasandi uurijale oodatavad kompetentsid;
- uurija või uurijaks kandideeriva inimese enesearendamisel ja karjääri planeerimisel;
- uurijaga arenguvestluse ja uurijaks kandideeriva inimesega kutsesobivusvestluste läbiviimisel.

Kokkuvõtteks, käesolevas töös välja töötatud kompetentsiraamistiku roll on aluse loomine kohaliku tasandi uurija arenguks ja politseijaoskonna menetlusgrupi edukaks toimimiseks. Kompetentsiraamistik toetaks nii uurija individuaalset arengut kui ka menetlusgrupi ja politseijaoskonna tulemuslikkust.

KOKKUVÕTE

Magistritöö on empiiriline uurimus, kus kasutati juhtumiuuringu strateegiat. Juhtumiks oli kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimiseks vajaliku kompetentsiraamistiku väljatöötamise ja valideerimise protsess, kus esimese etapina analüüsiti teemakohast teaduskirjandust ja teiste riikide praktikaid. Empiirilise uuringu uurimisinstrumentidena kasutati poolstruktureeritud ekspertintervjuusid ja dokumendianalüüsi. Intervjueeritavate eesmärgistatud valimisse kuulusid 4 PPA strateegilise planeerimise tasandi eksperti, 3 Sisekaitseakadeemia õppeprogrammide arendamise ja valdkonna õppeainetega seotud eksperti ja 3 Põhja Ringkonnaprokuratuuri abiprokuröri, kelle ülesandeks on kogukonnakuritegude uurimise juhtimine. Uuringu andmeid täiendati dokumendianalüüsiga. Dokumendianalüüsi mugavusvalimisse valiti kümme uurimisküsimusele vastamiseks vajalikku informatsiooni sisaldavat teksti ja dokumenti.

Magistritöös küsimusena sõnastatud uurimisprobleemi: „kuidas süstematiseerida aktuaalseid kompetentse, mis on tänapäeval vajalikud kohaliku tasandi uurijatele digitaalse komponendiga kuritegude uurimisel?“ lahendamiseks püstitati eesmärk välja töötada kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimiseks vajalike teadmisi ja oskusi süstematiseeriv kompetentsiraamistik ja esitada ettepanekud selle rakendusvõimaluste osas.

Eesmärk täideti leides vastuseid neljale uurimisküsimusele viie uurimisülesande lahendamise kaudu. **Esimesele uurimisküsimusele**: „Millised on ühiskonna digitaliseerumisest tingitud aktuaalsed väljakutsed kohaliku tasandi uurijatele digitaalse komponendiga kuritegude uurimisel?“ ja **teisele uurimisküsimusele**: „Millised on digitaalse komponendiga kuriteod, mille lahendamisega tegelevad kohaliku tasandi politseiuurijad?“ nii teoreetilises osas kui empiirilise uuringu raames analüüsiti ja süstematiseeriti digitaalse komponendiga kuriteod ning nende uurimisel tekkinud väljakutsed ja kitsaskohad. Uuringu tulemusel selgus, et PPA-s on olulisemateks organisatsioonisisesteks väljakutseteks digitaalse komponendiga kuritegude uurimisel uurijatel vajalike teadmiste ja oskuste puudulikkus ja politseiorganisatsiooni võimaluste piiratus vastava ettevalmistuse tagamiseks rahaliste ressursside ja pädevate koolitajate vähesuse tõttu, mis sarnaneb teoorias välja toodud teiste riikide probleemkohtadega. Väljakutsetena toodi välja ka uurijate endi huvi ja motivatsiooni probleeme, seostades seda tegurit keskmise politseijaoskonna uurija vanusegruppi 40+ aastat kuulumisega, tehnilise taibu puudumisega ja hirmudega IKT lahenduste kasutusele võtmise ees. Neid tegureid teoorias ei käsitletud. Motivatsiooni puudumine ja digihirmud võivad olla seotud üld- ja digioskuste

puudulikkusega ning nende oskuste arendamine inimestel vanuses 40+ aastat on tõsine väljakutse, mis eeldab erilist lähenemist.

PPA-s ei peeta täpsemat ülevaadet muret tekitavatest uurimissituatsionidest ja eraldi statistikat digitaalse komponendiga juhtumite osas ei koguta. Eeldatakse, et kohaliku tasandi politseiuurijal piisab üldoskustest ja baasdigioskustest nende situantsioonidega toime tulemiseks. Esimene ja viimane kaardistamine toimus 2017–2018. aastal digitõendite koolituse materjalide koostamise eesmärgil, kuid võttes arvesse IKT kiiret arengut ja selle mõju kuriteovormide mitmekesistamisele oleks mõistlik seda praktikat aeg-ajalt kaasajastada ja korrata.

Kolmandale uurimisküsimusele: „Kuidas süstematiseerida kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimiseks vajalikke teadmisi ja oskusi?“ analüüsiti teoreetilisi lähtekohti kompetentsiraamistiku koostamiseks ja loodi kohaliku tasandi uurijale digitaalse komponendiga kuritegude uurimiseks vajalik kompetentsiraamistik, süstematiseerides kompetentse kolme kategooriasse, milleks on üld-, üld-digi- ja kutsespetsiifilised kompetentsid. Kompetentsiraamistiku valideerimisel selgitati välja ekspertide seisukohtad kompetentsipõhise lähenemise ja konkreetselt magistritöös välja töötatud kompetentsiraamistiku rakendusvõimaluste kohta. Uuringu tulemusel selgus, et hetkel formaliseeritud kujul süsteemset kompetentsipõhist lähenemist PPA-s ei rakendata, vaid lähtutakse teenuspõhise juhtimise põhimõtetest. Igale põhitööle kompetentside komplekti detailselt lahti kirjutatud ei ole ja ametijuhendis seda ei kajastata, vaid lähtutakse üldistest põhimõtetest. PPA personali kompetentside arendamiseks vajalikud koolitused planeeritakse keskselt vastavalt strateegilise eesmärgi kaudu määratletud koolitusvajadusele.

Neljandale uurimisküsimusele: „Kuidas hindavad PPA, Sisekaitseakadeemia ja prokuratuuri esindajad magistritöös välja töötatud kompetentsiraamistiku asjakohasust ja rakendusvõimalusi?“ leiti vastused kompetentsiraamistikku valideeriva kvalitatiivse empiirilise uuringu käigus. Kõik eksperdid leidsid kompetentsiraamistiku mingis osas kasulikuna. Toodi välja, et kompetentsipõhise lähenemise tugevusteks on selgus ja konkreetsus uurija kompetentsi kriteeriumide osas nii uurija kui ka politseiorganisatsiooni vaates, mis on ühtlasi kooskõlas teooriaga. Kompetentsiraamistik pakub struktuuri ja suuniseid kompetentside jaotamiseks kategooriatesse ning nende kirjeldamiseks, arendamiseks ja hindamiseks. Organisatsiooni vaates aitab kompetentsiraamistik mõista, millised kompetentsid on vajalikud, et saavutada soovitud tulemusi ja eesmärke. Indiviidi vaates tagab kompetentsiraamistik selgust, milliseid oskusi, teadmisi ja omadusi on vaja konkreetsel töökohal

tööülesannetega toime tulemiseks. Kompetentsiraamistikku võib kasutada abimaterjalina kompetentsilünkade tuvastamiseks ning arendustegevuste kavandamisel PPA-s; sisendina Sisekaitseakadeemias õppekavade täiendamisel, määratledes kohaliku tasandi uurijale oodatavad kompetentsid; uurija või uurijaks kandideeriva inimese enesearendamisel ja karjääri planeerimisel; uurijaga arenguvestluse ja uurijaks kandideeriva inimesega kutsesobivusvestluste läbiviimisel.

Teoreetilise kompetentsiraamistiku ja empiirilise uuringu tulemuste sünteesi alusel esitati PPA-le ja Sisekaitseakadeemiale viis ettepanekut kompetentsipõhise lähenemise laiemas mõttes ning magistritöös välja töötatud kompetentsiraamistiku rakendusvõimaluste osas.

Magistritööd saab kasutada PPA kogukonnasüütegude lahendamise, (digi-)kriminalistika ja koolitusteenuse arendamisel ning Sisekaitseakadeemias politseinikele ette nähtud õppekavade täiendamisel. Ühtlasi saab kaaluda kompetentsipõhise lähenemise kasutamist organisatsioonis tervikuna. Käesoleva töö uurimistulemustest lähtuvalt võiks järgmised uurimistööd pühendada politseiuurijate seas üleesindatud vanusegrupi 40+ üld- ja digikompetentside arendamise võimaluste uurimisele ning kompetentsuse hindamismetoodika ning -instrumentide väljatöötamisele.

SUMMARY

The title on this master thesis is: „Competency Framework and its Implementation Possibilities for Investigating Crimes with a Digital Component by Local Police Investigators“ and it focuses on the development and implementation of a competency framework for local police investigators to effectively investigate crimes with a digital component.

The thesis consists of two chapters: the theoretical approach and the empirical study. The theoretical chapter explores the current challenges faced by local investigators in handling digital-component cases, the nature of crimes with a digital component, and the theory behind developing a competency model. Based on the theoretical findings, a competency framework is constructed. The empirical chapter presents a case study that analyzes the challenges encountered by local police investigators and their practices in defining and developing the necessary competences. A comparison is made between these practices and the competency framework developed in the thesis. Conclusions and suggestions for applying a competency-based approach are derived from the synthesis of the study and the theoretical competency framework.

The research problem addressed in this master thesis is how to systematize the competences required by local investigators for investigating crimes with a digital component. The aim of the study is to develop a competency framework that organizes the knowledge and skills needed by local police investigators and propose its practical application. Four research questions are formulated, which are addressed through five research tasks. The research methodology employs a case study strategy, analyzing relevant literature and practices from other countries. Semi-structured interviews with experts from the Estonian Police and Border Guard Board strategic planning level, Estonian Academy of Security Sciences curriculum development specialists, and assistant prosecutors from Northern District Prosecutor's Office, along with document analysis, are utilized for the empirical study.

The synthesis of the theoretical competency framework and the findings from the empirical study contribute to the development of five proposals for the Estonian Police and Border Guard Board and Estonian Academy of Security Sciences. These proposals aim to enhance the broader concept of a

competency-based approach and suggest potential applications of the competency framework developed in the master thesis.

Overall, this research offers valuable insights into the challenges of investigating crimes with a digital component at the local level and provides a comprehensive competency framework to guide local police investigators in acquiring the necessary knowledge and skills. The practical implications of implementing a competency-based approach are discussed, emphasizing the importance of general competences and digital competences in effectively addressing digital-component crimes.

Viidatud allikate loetelu

Agarwal, A., Gupta, M., Gupta, S. & Gupta, S. C., 2011. Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, 5(1), pp. 118–131.

Akdemir, N. & Lawless, C., 2020. Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: a lifestyle routine activities approach. *Internet research*, 30(6), pp. 1665–1687.

Alkali, Y. E. & Amichai-Hamburger, Y., 2004. Experiments in digital literacy. *CyberPsychology & Behavior*, 7(4), pp. 421–429.

Allison, S. F. H., Schuck, A. M. & Lersch, K. M., 2005. Exploring the crime of identity theft: Prevalence, clearance rates, and victim/offender characteristics. *Journal of Criminal Justice*, 33(1), pp. 19–29.

Beesley, P., 2021. *Competency-based management framework for digital competencies in Canadian policing: A component of the Canadian Police Knowledge Network's Cybercrime Training and Digital Competency Development for Canadian Law Enforcement project*. Public Safety Canada [Võrgumaterjal] Leitav: https://www.cpkn.ca/wp-content/uploads/final_CBMF_Digital_Competencies_Report_June17_2021-1.pdf [Kasutatud 28.12.2022].

Bellini, D., Cubico, S., Favretto, G., Noventa, S. A., Ardolino, P., Gianesini, G., Ciabuschi, F., Leitao, J. & Jain, A. K., 2021. A metamodel for competence assessment Co.S.M.O.© competences software management for organizations. *European Journal of Training and Development*, 45(6-7), pp. 603–616.

Belshaw, S. H., 2019. Next generation of evidence collecting: The need for digital forensics in criminal justice education. *Journal of Cybersecurity Education, Research and Practice*, 1(3), pp. 1–20.

Berger, P. L. & Luckmann, T., 1991. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*. London: Penguin Books.

Binkley, M., Erstad, O., Herman, J., Raizen, S., Ripley, M., Miller-Ricci, M. & Rumble, M., 2012. Defining twenty-first century skills. Rmt: P. Griffin, B. McGaw, & E. Care, toim-d. *Assessment and teaching of 21st century skills: Methods and approach*. Dordrecht: Springer, pp. 17–66.

Blatter, J. K., 2008. Case Study. Rmt: L. M. Given, toim-d. *The Sage encyclopedia of qualitative research methods*. Vol 1. Los Angeles, London, New Delhi: Sage Publications, pp. 68–71.

Blašková, M., Blaško, R. & Kucharčíková, A., 2014. Competences and competence model of university teachers. Procedia-Social and Behavioral Sciences, 159, pp. 457–467.

Bossler, A.M. & Holt, T.J., 2012. Patrol officers' perceived role in responding to cybercrime. *Policing*, 35(1), pp. 165–181.

Bryman, A., 2008. *Social research methods*. 3d ed. Oxford, New York: Oxford University Press.

Burns, R.G., Whitworth, K.H. & Thompson, C.Y., 2004. Accessing law enforcement preparedness to address internet fraud. *Journal of Criminal Justice*, 32(5), pp. 477–493.

Caneppele, S. & Aebi, M. F., 2019. Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes, *Policing: A Journal of Policy and Practice*, 13(1), pp. 66–79.

Carretero Gomez, S., Vuorikari, R. & Punie, Y., 2017. *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*. Luxembourg: Publications Office of the European Union.

CEPOL European Cybercrime Training and Education Group, 2020. *Cybercrime Training Competency Framework: Cybercrime Training Competencies Framework Introduction*. [Võrgumaterjal] Leitav: https://www.ecteg.eu/tcf/co/TCG_OpaleModule_4.html [Kasutatud 15.02.2023].

CEPOL, 2022. *Operational Training Needs Analysis Digital Skills and the Use of New Technologies* [Võrgumaterjal] Leitav: https://www.cepol.europa.eu/training-education/training-needs-analysis/training-needs-analyses [Kasutatud 22.01.2023].

Claro, M., Preiss, D. D., San Martín, E., Jara, I., Hinostroza, J. E., Valenzuela, S., Cortes, F. & Nussbaum, M., 2012. Assessment of 21st century ICT skills in Chile: Test design and results from high school level students. *Computers & Education,* 59(3), pp. 1042–1053.

Coman, I. M., & Alexa, N., 2022. EU Law Enforcement Training Needs on Digital Skills and the Use of New Technologies. *European Law Enforcement Research Bulletin*, 22(6), pp. 23-30. [Võrgumaterjal] Leitav: https://bulletin.cepol.europa.eu/index.php/bulletin/article/view/561 [Kasutatud 22.01.2023].

Copes, H. & Vieraitis, L. M., 2009. Bounded rationality of identity thieves: Using offender-based research to inform policy. *Criminology & Public Policy*, 8(2), pp. 237–262.

Council of Europe, 2022. *Actions against cybercrime.* [Võrgumaterjal] Leitav: https://www.coe.int/en/web/cybercrime/home [Kasutatud 24.09.2022].

Council of Europe, 2022. *Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. Treaty Series. No. 224*

Curtis, J., & Oxburgh, G., 2022. Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal: Theory, Practice and Principles*, 0(0), pp. 1–20.

Dawson, J. & Thomson, R., 2018. The future cybersecurity workforce: going beyond technical skills for successful cyber performance. *Frontiers in psychology*, 9. [Võrgumaterjal] Leitav: https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00744/full [Kasutatud 24.01.2023].

De Paoli, S., Johnstone, J., Coull, N., Ferguson, I., Sinclair, G., Tomkins, P., Brown, M. & Martin, R., 2021. A qualitative exploratory study of the knowledge, forensic, and legal challenges from the perspective of police cybercrime specialists. *Policing: A Journal of Policy and Practice*, 15(2), pp. 1429–1445.

Dodge, C., & Burruss, G., 2020. Policing cybercrime: Responding to the growing problem and considering future solutions. Rmt: R., Leukfeldt, T. J. Holt, toim-d. *The human factor of cybercrime*, Routledge, pp. 339–358.

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N., Woodlock, D. & Harris, B., 2018. Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, 18(4), pp. 609–625.

Dunn Cavelty, M. D., 2009. Cyber-threats. Rmt: M., Dunn Cavelty & V., Mauer, toim-d. *The Routledge handbook of security studies.* London and New York: Routledge, pp. 180–189.

Euroopa Komisjon, 2022. *Kriminaaluurija*. *3355.1*. ESCO 1.1.0 27.01.2022. [Võrgumaterjal] Leitav: https://esco.ec.europa.eu/et/classification/occupation_main [Kasutatud 29.03.2022].

Euroopa Komisjon, 2022. *Mis on ESCO? Current version: ESCO v1.1.0 (Last update 27/01/2022)* [Võrgumaterjal] Leitav: https://esco.ec.europa.eu/et/about-esco/what-esco [Kasutatud 12.01.2023].

Euroopa Ülemkogu Euroopa Liidu Nõukogu, 2023. *Elektroonilistele tõenditele juurdepääsu parandamine kuritegevuse vastu võitlemiseks*. [Võrgumaterjal] Leitav: https://www.consilium.europa.eu/et/policies/e-evidence/ [Kasutatud 06.01.2023].

European Commission, 2020. *The EU's Cybersecurity Strategy for the Digital Decade. Brussels*. [Võrgumaterjal] Leitav: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 [Kasutatud 06.01.2023].

European Commission, 2022. *Open-source intelligence.* [Võrgumaterjal] Leitav: https://data.europa.eu/en/publications/datastories/open-source-intelligence [Kasutatud 07.04.2023].

European Commission, 2016. Police detective: The context: the use of ICT in police work. *The impact of ICT on job quality: evidence from 12 job profiles: An intermediate report from the study "ICT for work: Digital skills in the workplace – SMART 2014/0048*". INTERMEDIATE REPORT Prepared for the European Commission DG Communications Networks, Content & Technology, pp. 69–76.

European Union Agency for Cybersecurity, 2023. National Cyber Security Strategies. [Võrgumaterjal] Leitav: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-ncss [Kasutatud 11.01.2023].

Ferrari, A., 2012. *Digital competence in practice: An analysis of frameworks*. Seville: European Commission Joint Research Centre, Institute for Prospective Technological Studies.

Flick, U., 2009. *An Introduction to Qualitative Research*. London, California, New Dehli, Singapore: SAGE Publications Ltd.

Furnell, S. & Dowling, S., 2019. Cyber crime: a portrait of the landscape. *Journal of Criminological Research, Policy and Practice*, 5(1), pp. 13–26.

Grabosky, P. N., 2001. Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, 10(2), pp. 243–249.

Gray, D. E., 2018. *Doing Research in the Real World* (4th ed.). London: Sage.

Haaristo, H. S., Kirss, L., Mägi, E., Rell, M. & Rozeik, H., 2015. *Siseturvalisuse hariduse mudeli analüüs*. Tallinn: Poliitikauuringute keskus PRAXIS.

Hadlington, L., Lumsden, K., Black, A. & Ferra, F., 2021. A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing: A Journal of Policy and Practice*, 15(1), pp. 34–43.

Harkin D., Whelan C. & Chang L., 2018. The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research*, 19, pp. 519–536.

Henry, N. & Powell, A., 2015. Embodied harms: Gender, shame, and technology-facilitated sexual violence. *Violence against women*, 21(6), pp. 758–779.

Holt, T. J. & Bossler, A. M., 2016. *Cybercrime in progress: Theory and prevention of technology-enabled offenses.* London and New York: Routledge Taylor & Francis Books.

Home Office, 2013. *Serious and Organised Crime Strategy.* UK: The Stationery Office Limited [Võrgumaterjal] Leitav: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/248645/Serious_and_Organised_Crime_Strategy.pdf [Kasutatud 17.10.2022].

Humphries, G., Nordvik, R., Manifavas, H., Cobley, P. & Sorell, M., 2021. Law Enforcement educational challenges for mobile forensics. *Forensic Science International: Digital Investigation*, 38 [Võrgumaterjal] Leitav:

https://reader.elsevier.com/reader/sd/pii/S2666281721000275?token=A28FE930B5B040374E336FA92281E775B3C452C0714A9F2EE467D72F8088A199CF8A8C5C2B8F6D3D3AD9EA463A4DC9C6&originRegion=eu-west-1&originCreation=20220921140249 [Kasutatud 14.09.2022].

Jamnes, P., Elenurm, T., Murre, S., Kerem, M.-K. & Randma, T., 2013. *Üldised kompetentsid: kvalifikatsiooniga seonduvad terminid. Juhendmaterjal kutsestandardi koostajale, tasemeõppe ja täienduskoolituse õppekava koostajale ning karjäärinõustajale*. SA Kutsekoda: Iloprint. [Võrgumaterjal] Leitav: https://www.kutsekoda.ee/wp-content/uploads/2019/KS/Uldised-kompetentsid.pdf [Kasutatud 06.03.2023].

Jarrahi, M. H. & Eshraghi, A., 2019. Digital natives vs digital immigrants: A multidimensional view on interaction with social technologies in organizations. *Journal of Enterprise Information Management*, 32(6), pp. 1051–1070.

Jarrahi, M.H. & Thomson, L., 2017. The interplay between information practices and information context: the case of mobile knowledge workers, *Journal of the Association for Information Science and Technology*, 68(5), pp. 1073–1089.

Jewkes, Y. & Andrews, C., 2005. Policing the Filth, the Problems of Investigating Online Child Pornography in England and Wales. *Policing and Society* 15(1), pp. 42–62.

Jewkes, Y. & Yar, M., 2012. Policing cybercrime: emerging trends and future challenges. Rmt: T. Newburn, toim-d. *Handbook of policing*, Dewon: Willan Publishing, pp. 608–634.

Jewkes, Y., & Yar, M., 2011. Introduction: The Internet, cybercrime and the challenges of the twenty-first century. Rmt: Y. Jewkes & M. Yar, toim-d. *Handbook of internet crime*. London & New York: Routledge, pp. 1–8.

Johansson, R., 2003. Case Study Methodology. *A key note speech at the International Conference "Methodologies in Housing Research.* Stockholm: the Royal Institute of Technology in cooperation with the International Association of People–Environment Studies. [Võrgumaterjal] Leitav: https://d30037385.purehost.com/HTMLobj-3839/Case_Study_Methodology-_Rolf_Johansson_ver_2.pdf [Kasutatud 02.01.2023].

Johnson, D., Faulkner, E., Meredith, G. & Wilson, T. J., 2020. Police functional adaptation to the digital or post digital age: Discussions with cybercrime experts. *The Journal of Criminal Law*, 84(5), pp. 427–450.

Jones, N., George, E., Merida, F. I., Ramussen, U. & Volzow, V., 2014. Electronic Evidence Guide - A Basic Guide for Police Officers, Prosecutors, and Judges. Version 2.0. [Võrgumaterjal] Leitav: https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-annex_4_-_electronic_evidence_guide_2.0_final-complete.pdf [Kasutatud 24.09.2022].

Justiitsministeerium, 2020. *Kriminaalpoliitika põhialused aastani 2030.* [Võrgumaterjal] Leitav: https://www.just.ee/kuritegevus-ja-selle-ennetus/kriminaalpoliitika-pohialused [Kasutatud 03.09.2022].

Justiitsministeerium, 2021a. *Kuritegevus Eestis 2021. Arvutikuriteod.* [Võrgumaterjal] Letav: https://www.kriminaalpoliitika.ee/kuritegevus2021/arvutikuriteod_page.html
[Kasutatud 03.09.2022].

Justiitsministeerium, 2021b. *Kuritegevus Eestis 2021. Kuritegevuse üldvaade.* [Võrgumaterjal] Letav: https://www.kriminaalpoliitika.ee/kuritegevus2021/
[Kasutatud 12.10.2022].

Justiitsministeerium, 2021c. *Kuritegevus Eestis 2021. Perevägivald.* [Võrgumaterjal] Leitav: https://www.kriminaalpoliitika.ee/kuritegevus2021/perevagivald_ja_ahistamine_page.html [Kasutatud 03.09.2022].

Justiitsministeerium, 2022a. *Kuritegevus Eestis 2022. Arvutikuriteod*. [Võrgumaterjal] Letav: https://www.kriminaalpoliitika.ee/kuritegevus2022/arvutikuriteod/
[Kasutatud 11.02.2023].

Justiitsministeerium, 2022b. *Kuritegevus Eestis 2022. Perevägivald*. [Võrgumaterjal] Letav: https://www.kriminaalpoliitika.ee/kuritegevus2022/perevagivald-ja-ahistamine/ [Kasutatud 11.02.2023].

Kaha, H., 2017. *Elektroonilise sõnumi saladuse problemaatika kriminaalmenetluses. Magistritöö.* Tallinn: Tallinna Tehnikaülikool.

Karie, N. M. & Venter, H. S., 2015. Taxonomy of challenges for digital forensics. *Journal of forensic sciences*, 60(4), pp. 885–893.

Kaslow, N. J., 2004. Competencies in Professional Psychology. *American Psychologist*, 59(8), pp. 774–781.

Klieme, E., Hartig, J. & Rauch, D., 2008. The concept of competence in educational contexts. Rmt: J., Hartig, E., Klieme & D., Leutner, toim-d. *Assessment of competencies in educational contexts.* Göttingen: Hogrefe, pp. 3–22.

Koeppen, K., Hartig, J., Klieme, E. & Leutner, D., 2008. Current issues in competence modeling and assessment. *Zeitschrift für Psychologie/Journal of Psychology*, 216(2), pp. 61-73.

Kosmala K, 2013. Scripting shifts in the regulatory structures: Professional competence constructed as a lack. *Organization* 20(4), pp. 577–595.

Kozanoglu, D. C. & Abedin, B., 2021. Understanding the role of employees in digital transformation: conceptualization of digital literacy of employees as a multi-dimensional organizational affordance. *Journal of Enterprise Information Management*, 34(6), pp. 1649-1672.

Laats, M., 2017. *Piiriüleste jälitustoimingute läbiviimine digitaalkeskkonnas. Magistritöö.* Tallinn: Sisekaitseakadeemia.

Lall, A., Tohter, M. & Öpik, R., 2021. Some aspects of digital forensics in the Republic of Estonia. *Criminalistics and forensic expertology: science, studies, practice*. Bratislava, pp. 133–146. [Võrgumaterjal] Leitav: https://www.etis.ee/Portal/Publications/Display/548fdba6-c4c4-41c1-926e-48cb7cbf5efa [Kasutatud 22.09.2022].

Laurits, E., 2016. Criminal procedure and digital evidence in Estonia. *Digital Evidence and Electronic Signature Law Review*, 13, pp. 113-120.

Lawton, D., Stacey, R. & Dodd, G., 2014. *eDiscovery in Digital Forensic Investigations. Technical Report,* CAST Publication 32/14, Home Office: London. [Võrgumaterjal] Leitav: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/394779/ediscovery-digital-forensic-investigations-3214.pdf [Kasutatud 25.09.2022].

Lee, J. R., Holt, T. J., Burruss, G. W. & Bossler, A. M., 2021. Examining English and Welsh detectives' views of online crime. *International Criminal Justice Review*, 31(1), pp. 20–39.

Leemet, A. & Ungro, A., 2022. Tööelu üldoskuste klassifikatsioon ning tulevikuvajadus. Uuringu terviktekst. Tallinn: SA Kutsekoda. [Võrgumaterjal] Leitav: https://oska.kutsekoda.ee/wp-content/uploads/2022/03/Tooelu-uldoskused_-terviktekst.pdf [Kasutatud 29.03.2023].

Leigh, I. W., Smith, I. L., Bebeau, M. J., Lichtenberg, J. W., Nelson, P. D., Portnoy, S., Rubin N. J. & Kaslow, N. J., 2007. Competency assessment models. *Professional Psychology: Research and Practice*, 38(5), pp. 463–473.

Leukfeldt, R., Veenstra, S. & Stol, W., 2013. High volume cyber crime and the organization of the police: The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology*, 7(1), 1. [Võrgumaterjal] Leitav: https://www.researchgate.net/profile/Eric-Leukfeldt/publication/280013987_High_Volume_Cyber_Crime_and_the_Organization_of_the_Police_The_results_of_two_empirical_studies_in_the_Netherlands/links/575ec73b08ae414b8e545953/High-Volume-Cyber-Crime-and-the-Organization-of-the-Police-The-results-of-two-empirical-studies-in-the-Netherlands.pdf [Kasutatud 22.10.2022].

Levy, Y. & Ellis, T. J., 2006. A systems approach to conduct an effective literature review in support of information systems research. *Informing Science Journal*, 9, pp. 181-212.

Luuk, M., 2017. *Digitaalsete tõendite kasutamise erisused, Magistritöö.* Tartu: Tartu Ülikool.

Majandus- ja Kommunikatsiooniministeerium, 2019. Küberturvalisuse strateegia aastateks 2019-2022. [Võrgumaterjal] Leitav: https://www.mkm.ee/media/700/download [Kasutatud 11.01.2023].

Majandus- ja Kommunikatsiooniministeerium. 2020. Küberturvalisuse programm aastateks 2021-2024. [Võrgumaterjal] Leitav: https://www.fin.ee/media/1040/download [Kasutatud 11.01.2023].

Marrelli, A. F., 1998. An introduction to competency analysis and modeling. *Performance Improvement*, 37(5), pp. 8–17.

Marrelli, A. F., Tondora, J. & Hoge, M. A., 2005. Strategies for developing competency models. *Administration and Policy in Mental Health and Mental Health Services Research*, 32(5), pp. 533–561.

McGuire, M. & Dowling, S., 2013. *Cyber crime: a review of the evidence. Summary of Key Findings and Implications.* Home Office Research Report, 75. London: Home Office. [Võrgumaterjal] Leitav: file:///C:/Users/jevge/Downloads/Cyber-crime-a-review-of-the-evidence-chapter-1-cyberdependent-crimes.pdf [Kasutatud 19.09.2022].

Melesk, K., Mägi, E., Koppel, K., Michelson, A. & Praxis, P., 2019. *Küberturbe valdkonna tööjõuvajaduse ja hariduse uuring: Uuringu aruanne 29.03.2019*. Tallinn: Poliitikauuringute Keskus Praxis.

Mesipuu, B., 2019. *Suur uuring - eestlaste internetikasutus aastal 2019.* [Võrgumaterjal] Leitav: https://milos.ee/eestlaste-internetikasutus-aastal-2019/ [Kasutatud 07.01.2023].

Mirabile, R., 1997. Everything you wanted to know about competency modeling. *Training and Development*, 51(8), pp. 73–78.

Moloney, C. J., Unnithan, N. & Zhang, W., 2022. Assessing Law Enforcement's Cybercrime Capacity and Capability. *FBI, Law Enforcement Bulletin. Retrieved July*, *30*, 2022. [Võrgumaterjal] Leitav: https://leb.fbi.gov/articles/featured-articles/assessing-law-enforcements-cybercrime-capacity-and-capability- [Kasutatud 13.01.2023].

Morris, R. G., 2010. Identity thieves and levels of sophistication: Findings from a national probability sample of American newspaper articles 1995-2005. *Deviant Behavior*, 31(2), pp. 184–207.

Murawski, M. & Bick, M., 2017. Digital competences of the workforce–a research topic? *Business Process Management Journal*, 23(3), pp. 721–734.

O'Hara, A. C., Ko, R. K., Mazerolle, L., & Rimer, J. R., 2020. Crime script analysis for adult image-based sexual abuse: a study of crime intervention points for retribution-style offenders. *Crime Science*, 9(1), pp. 1–26.

O'Shea B., Asquith N. L. & Prichard J., 2022. Mapping cyber-enabled crime: Understanding police investigations and prosecutions of cyberstalking. *International Journal for Crime, Justice and Social Democracy*, 10(4), pp. 1–15.

OECD, 2019. *OECD Skills Outlook 2019: Thriving in a Digital World*. Publishing, Paris. [Võrgumaterjal] Leitav: https://read.oecd-ilibrary.org/education/oecd-skills-outlook-2019_df80bc12-en#page19 [Kasutatud 19.11.2022].

Olev, A. & Alumäe, T., 2022. Estonian Speech Recognition and Transcription Editing Service. *Baltic J. Modern Computing*, 10(3), pp. 409–421.

OSKA 2022. *OSKA põhikutsealade hõive muutuse prognoos ning hinnang tööjõu nõudluse ja koolituspakkumise tasakaalule*. [Võrgumaterjal] Leitav: https://oska.kutsekoda.ee/uuring/oska-pohikutsealade-toojouvajaduse-prognoos-ning-hinnang-noudluse-ja-pakkumise-tasakaalule/ [Kasutatud 29.03.2023].

Pamphlet, T., 2010. *The United States Army's cyberspace operations concept capability plan 2016-2028*. [Võrgumaterjal] Leitav: https://apps.dtic.mil/dtic/tr/fulltext/u2/a516590.pdf [Kasutatud 25.10.2022].

Paukštys, P. 2021. Rahvusvaheline koostöö küberkuritegude uurimisel. Prokuratuuri aastaraamat 2021. [Võrgumaterjal] Leitav: https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2021/rahvusvaheline-koostoo-kuberkuritegude-uurimisel [Kasutatud 22.10.2022].

Pernik, P., 2019. Cybersecurity education in Estonia: building competences for internal security personnel. *Proceedings Estonian Academy of Security Sciences*, 18. pp. 71–108.

Pillmann, H., 2021. *Asjade interneti tehnoloogia kasutusega seonduvad turvalisuse riskid ning nende maandamine inimeste tavakasutuses olevate tehnoloogiate näitel*. *Magistritöö*. Tallinn: Sisekaitseakadeemia.

Politsei- ja Piirivalveamet, 2022. Põhja prefektuuris alustas tööd kaks uut jaoskonda. [Võrgumaterjal] Leitav: https://www.politsei.ee/et/uudised/pohja-prefektuuris-alustas-toeoed-kaks-uut-jaoskonda-2754 [Kasutatud 02.04.2023].

Politsei- ja piirivalveseadus (2009), RT I, 20.06.2022, 47.

Pollitt, M., 2010. A history of digital forensics. Rmt: K. P. Chow & S. Shenoi, toim-d. *Advances in digital forensics*, 6, Berlin: Springer-Verlag, pp. 3–15.

Poni, M., 2014. Research paradigms in education. *Journal of Educational and Social Research*, 4(1), pp. 407–413.

Raghavan, S., 2013. Digital forensic research: current state of the art. *CSI Transactions on ICT*, 1(1), pp. 91–114.

Raudsepp, G., 2018. *Digitaalsete tõendite kogumise ja kasutamise perspektiivikus kriminaalmenetluses. Magistritöö.* Tartu Ülikool.

Rogers, M., 2020. Forensic Evidence and Cybercrime. In: Holt, T., Bossler, A., ed. *The Palgrave Handbook of International Cybercrime and Cyberdeviance.* Palgrave Macmillan, pp. 425–445.

Rowe C., 1995. Clarifying the use of competence and competency models in recruitment, assessment and staff development. *Industrial and Commercial Training*, 27(11), pp. 12–17.

Rule, P. & John, V. M., 2015. A necessary dialogue: Theory in case study research. *International Journal of Qualitative Methods*, 14(4), pp. 1-11. [Võrgumaterjal] Leitav: https://journals.sagepub.com/doi/pdf/10.1177/1609406915611575 [Kasutatud 02.01.2023]

SA Kutsekoda, 2019. *Tulevikuvaade tööjõu- ja oskuste vajadusele: siseturvalisus ja õigus. Siseturvalisuse alavaldkond. Uuringu tervikteks*t. Tallinn: SA Kutsekoda [Võrgumaterjal] Leitav: https://oska.kutsekoda.ee/wp-content/uploads/2017/10/OSKA_%C3%B5iguse-alavaldkond_terviktekst_l%C3%B5plik.pdf [Kasutatud 02.09.2022].

SA Kutsekoda, 2019. *Kutsestandardid: Kohtukriminalistikaekspert, tase 8.* [Võrgumaterjal] Leitav: https://www.kutseregister.ee/ctrl/et/Standardid/vaata/10723669 [Kasutatud 06.03.2023].

SA Kutsekoda, 2020a. OSKA ülevaade valdkonnaspetsiifiliste IKT-oskuste vajadusest. [Võrgumaterjal] Leitav: https://oska.kutsekoda.ee/wp-content/uploads/2021/01/OSKA-ulevaade-valdkonnaspetsiifiliste-IKT-oskuste-vajadusest_16.06.2020.pdf [Kasutatud 29.03.2023].

SA Kutsekoda, 2020b. Tulevikuvaade tööjõu- ja oskuste vajadusele: Siseturvalisus ja õigus. Siseturvalisuse alavaldkond. [Võrgumaterjal] Leitav: https://oska.kutsekoda.ee/wp-content/uploads/2017/10/OSKA_siseturvalisus_aruanne_l%C3%B5plik.pdf [Kasutatud 29.03.2023].

SA Kutsekoda, 2023. *Kvalifikatsiooniraamistiku tasemekirjeldused*. [Võrgumaterjal] Leitav: https://www.kutsekoda.ee/kvalifikatsiooniraamistiku-tasemekirjeldused/ [Kasutatud 06.03.2023].

Saldaňa, J., 2013. *The Coding Manual for Qualitative Researchers*. 2nd ed. Los Angeles, London, New Delhi, Singapore, Washington: SAGE

Salman, M., Ganie, S. A. & Saleem, I., 2020. The concept of competence: a thematic review and discussion. *European Journal of Training and Development*, 44(6/7), pp. 717–742.

Sampson, F. 2014.Cyberspase: The new frontier for policing? Rmt: B. Akhgar, A. Staniforth, F. Bosco, toim-d. *Cyber crime and cyber terrorism investigator's handbook*. Elsevier Science & Technology Books.

Sepp, P., 2018. *Digitaalsete tõendite käitlemine Politsei- ja Piirivalveametis. Magistritöö.* Tallinn: Sisekaitseakadeemia.

Shavelson, R. J., 2013. On an approach to testing and modeling competence. *Educational Psychologist*, 48(2), pp. 73–86.

Sillat, L. H., Tammets, K. & Laanpere, M., 2021. Digital competence assessment methods in higher education: A systematic literature review. *Education Sciences*, 11(8), pp. 1-13.

Siseministeerium, 2021. *Politseinike ja päästjate tulevikuvajaduse ning töötasu analüüs,* Tallinn: Sisemimisteerium, [Võrgumaterjal] Leitav: file:///C:/Users/jevge/Downloads/politseinike_ja_paastjate_tulevikuvajadus_ning_tootasu_analuus_2021%20(3).pdf [Kasutatud 02.09.2022].

Siseminister, 2013. *Politseiametniku ning Politsei- ja Piirivalveameti struktuuriüksuse juhi ametikohal teenistuses oleva ametniku kutsesobivusnõuded, nende kontrollimise tingimused ja kord. Määrus. RT I, 29.08.2019, 7*

Stacy, V. W., 2000. The art & science of competency models: Pinpointing critical success factors in organizations. *HRMagazine,* 45(1), pp. 140–142.

Stambaugh, H., Beaupre, D. S., Icove, D. J., Baker, R., Cassaday, W. & Williams, W. P., 2001. Electronic Crime Needs Assessment for State and Local Law Enforcement. U.S. Department of Justice: National Research Report. [Võrgumaterjal] Leitav: https://books.google.ee/books?hl=ru&lr=&id=qYvaAAAAMAAJ&oi=fnd&pg=PR9&dq=Stambaugh,+H.,+Beaupre,+D.+S.,+Icove,+D.+J.+et+al.+(2001).+%E2%80%98Electronic+Crime+Needs+Assessment+for+State+and+Local+Law+Enforcement.%E2%80%99+National+Institute+of+Justice+Research+Report.+&ots=HJKrY8DUy7&sig=NnRe-xDqYNcbok_7OkswGgC0fbg&redir_esc=y#v=onepage&q&f=false [Kasutatud 19.01.2023].

Stratton, G., Powell, A. & Cameron, R. 2017. Crime and justice in digital society: Towards a 'digital criminology'? *International Journal for Crime, Justice and Social Democracy*, 6(2), pp. 17–33.

Sultana, R. G., 2009. Competence and competence frameworks in career guidance: complex and contested concepts. *International Journal for Educational and Vocational Guidance,* 9, pp. 15–30.

Tarter, A., 2017. Importance of Cyber Security. Rmt: Bayerl, P. S., Karlović, R., Akhgar, B., G. Markarian, toim-d. *Community Policing – A European Perspective Strategies, Best Practices and Guidelines*. pp. 213–230.

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

Tierney, W. G., Corwin, Z. B. & Ochsner, A., 2018. *Diversifying Digital Learning : Online Literacy and Educational Opportunity*. Baltimore: Johns Hopkins University Press. [Võrgumaterjal] Leitav: ProQuest Ebook Central. [Kasutatud 10.10.2022].

Терехович, В. Н., Ниманде, Э., В., 2019. Криминалистическая методика в системе теории криминалистики, Rmt: О. М. Клюєв, В. Ю Шепітько, toim-d. *Теорія та практика судової експертизи і криміналістики*, 19, Харків: Право, с. 58–73.

USA National White Collar Crime Center, 2021. *NW3C Certifications*. [Võrgumaterjal] Leitav: https://www.nw3c.org/certifications/AssessmentResults#certificationassessment [Kasutatud 15.02.2023].

Van Deursen, A. J., Helsper, E. J. & Eynon, R., 2016. Development and validation of the Internet Skills Scale (ISS). *Information, Communication & Society*, 19(6), pp. 804–823.

Van Laar, E., Van Deursen, A. J., Van Dijk, J. A., & De Haan, J., 2017. The relation between 21st-century skills and digital skills: A systematic literature review. *Computers in human behavior*, 72, pp. 577–588.

Vincze, E. A., 2016. Challenges in digital forensics. *Police Practice and Research,* 17(2), pp. 183–194.

Voogt, J. & Roblin, N. P., 2012. A comparative analysis of international frameworks for 21st century competences: Implications for national curriculum policies. *Journal of Curriculum Studies,* 44(3), pp. 299–321.

Vuorikari, R., Kluzer, S. & Punie, Y., 2022. *DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes*. Publications Office of the European Union, Luxembourg.

Vuorikari, R., Punie, Y., Carretero Gomez, S. & Van Den Brande G,. 2016. *DigComp 2.0: The Digital Competence Framework for Citizens*. Luxembourg: Publications Office of the European Union.

Wall, D. S., 2011. Criminalising cyberspace: the rise of the Internet as a ‘crime problem’. Rmt: Y. Jewkes, M. Yar, toim-d. *Handbook of Internet Crime*. London and New York: Routledge, pp. 88–103.

White, M. D. & Fisher, C., 2008. Assessing our knowledge of identity theft: The challenges to effective prevention and control efforts. *Criminal Justice Policy Review,* 19(1), pp. 3–24.

Wilson-Kovacs, D., 2019. Effective resource management in digital forensics: An exploratory analysis of triage practices in four English constabularies. *Policing: an international journal*, 43(1), pp.77–90.

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

Õunapuu, T., Tambur, M., Noorkõiv, R., Kivistik, K., Tatar, M. 2021. *Kohalike omavalitsuste kompetentside põhise koolitusvajaduse hindamise metoodika ja analüüs. Lõpparuanne*. Rahandusministeerium, Riigi Tugiteenuste Keskus. [Võrgumaterjal] Leitav: https://www.ibs.ee/publikatsioonid/kohalike-omavalitsuste-kompetentside-pohise-koolitusvajaduse-hindamise-metoodika-ja-analuus/ [Kasutatud 30.03.2023].

Öpik, R., 2009. Kriminalistika sisejulgeoleku valdkonna teaduse ja õppeainena. Rmt: L. Tabur & A. Talmar, toim-d. *Sisekaitseakadeemia toimetised. Teadmistemahukas turvalisus, 8*. Tallinn: Sisekaitseakadeemia, lk 70–87.

Yar, M. & Drew, J., 2019. Image-based abuse, non-consensual pornography, revenge porn: A study of criminalization and crime prevention in Australia and England & Wales. *International Journal of Cyber Criminology*, 13(2), pp. 578–594.

Yar, M., 2005. The novelty of "cybercrime": An assessment in light of routine activity. *European Journal of Criminology*, 2. pp. 407–427.

Yin, K. R., 2009. *Case Study Research. Design and Methods.* (4th ed.). Thousand Oaks: Sage Publications.

Yin, R., 2003. *Case study research: Design and methods.* (3rd ed.). Thousand Oaks, London, New Delhi: Sage Publications.

*Blašková, M., 2011. *Rozvoj Ďudského potenciálu. Motivovanie, komunikovanie, harmonizovanie a rozhodovanie.* Žilina: Publishing of University of Žilina.

*Boyatzis, R.E., 1982. *The Competent Manager: A Model for Effective Performance*. New York: Wiley.

*Dunn Cavelty, M. & Brunner, E., 2007. Information, power, and security: An outline of debates and implications. In: Dunn Cavelty, M., Mauer, V. & Krishna-Hensel, S.-F. ed. *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. Aldershot: Ashgate, pp. 1–18.

*Holt, T. J., Bossler, A., and Fitzgerald, S., 2010. Examining State and Local Law Enforcement Perceptions of Computer Crime. Rmt: T. J Holt, toim-d. *Crime On-line: Correlates, Causes, and Context*. Raleigh, NC: Carolina Academic, pp. 221–246.

*Kimberley, N. & Crosling, G., 2016. Student Q Manual (5th ed.) Australia: Monash University. Faculty of Business and economics.

*Lucia, A. D. & Lepsinger, R., 1999. *The Art and Science of Competency Models: Pinpointing Critical Success Factors in Organizations*. San Francisco: Jossey-Bass Pfeiffer.

*Ono, M., Sachau, D. A., Deal, W. P., Englert, D. R., and Taylor, M. D., 2011. Cognitive ability, emotional intelligence, and the big five personality dimensions as predictors of criminal investigator performance. *Criminal Justice and Behavior*, 38(5), pp. 471–491.

*Plamínek, J. & Fišer, R., 2005. *Řízení podle kompetencí*. Prague: Grada.

*Robson, C., 2002. *Real world research: a resource for social scientists and practitioner-researchers* (2nd ed.). Oxford: Blackwell.

*Stake, R.,1995. *The Art of Case Study Research*. Thousand Oaks, London, New Delhi: Sage.

*Wall, D., 2007. *Cybercrime: The transformation of crime in the information age*. Cambridge: PolityPress.

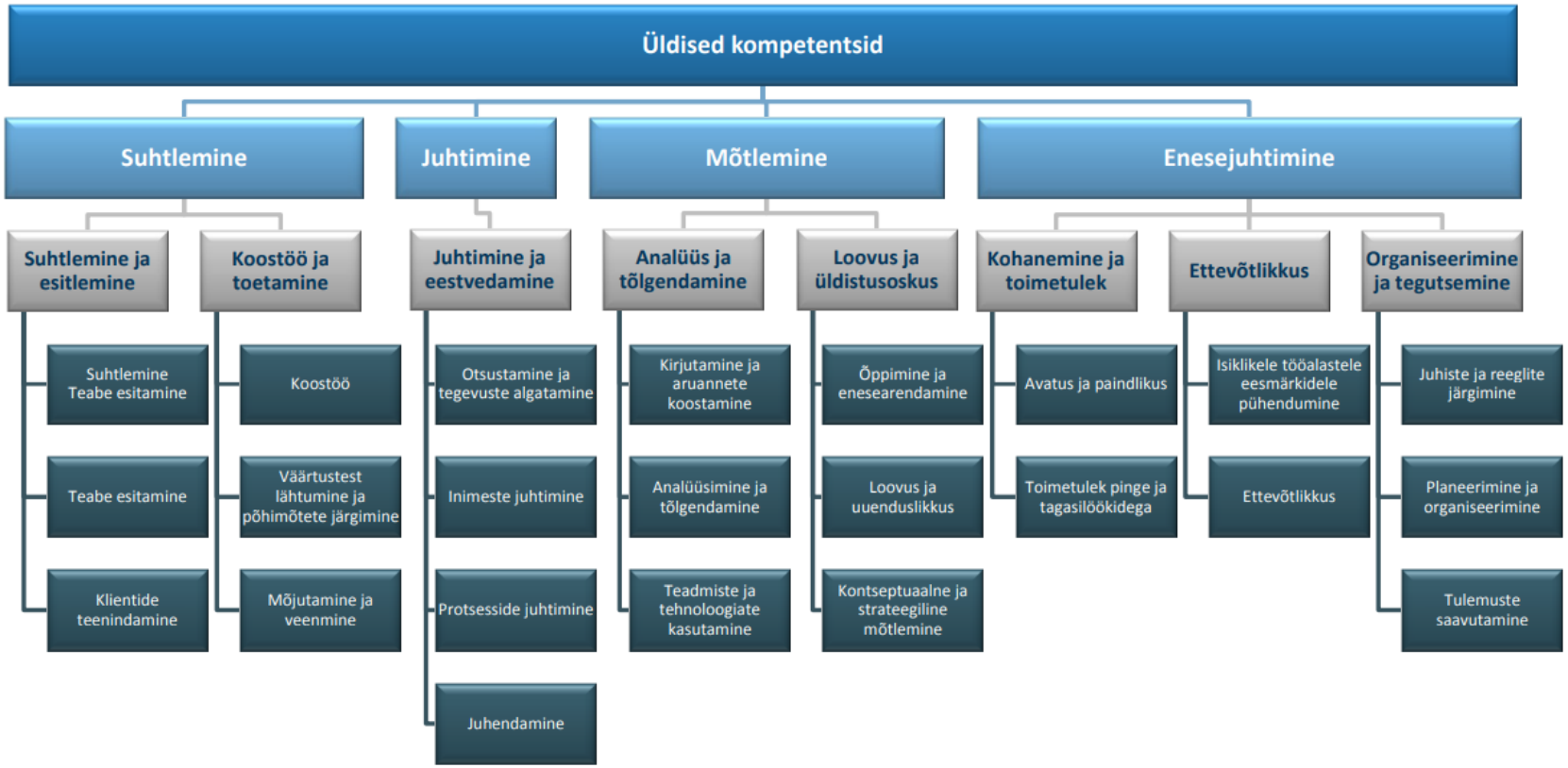
*Белкин, Р., 1987. *Криминалистика: проблемы, тенденции, перспективы. Общие и частные теории*. Москва: Юридическая литература.

TABELITE JA JOONISTE LOETELU

JOONISED

TABELID

Lisa 1. Üldkompetentside struktur



Joonis. Allikas: Üldkompetentside struktur (Haaristo, *et al*., 2015 ja Jamnes, *et al.*, 2013 põhjal, lk 29)

Lisa 2. Üld-digikompetentsid

1. Info haldamine – digitaalse info eesmärgipärane otsimine, sirvimine, hindamine, salvestamine ja taasesitamine.
2. Suhtlemine digikeskkondades – teadlik suhtlemine veebipõhistes keskkondades, info ja sisu jagamine, osalemine ühiskonnaelus ning koostöö digivahendite toel.
3. Sisuloome – digitaalse sisu loomine, olemasoleva digitaalse materjali muutmine ja lõimimine, loominguline eneseväljendus ja programmeerimine ning intellektuaalse omandi õiguste ja litsentside järgimine.
4. Turvalisus – identiteedi, tervise ning keskkonna kaitsmine; info- ja kommunikatsioonitehnoloogia turvaline ning kestlik kasutamine.
5. Probleemilahendus – vajaduste väljaselgitamine ja lahenduste leidmine sobivate digivahenditega, tehnoloogia loov kasutamine ning digipädevuse arendamine.

Tabel. Üld-digikompetentsid. Allikas: DigComp 2.0 (Vuorikari, *et al.*, 2016) raamistikus loetletud digioskuste sisu, mis on kasutatud kohtukriminalsitika eksperdi kutsestandardis, tase 8 (SA Kutsekoda, 2019)

Osaoskused	Osaoskuste kirjeldus
1. Info haldamine	**1.1. Info otsimine ja sirvimine** – määrab eesmärgi põhjal oma infovajaduse ning valib eesmärgiga sobivad meetodid digitaalse info otsimiseks ja sirvimiseks. **1.2. Info hindamine** – kogub ja töötleb digitaalset infot, eristab olulist infot ning analüüsib ja hindab seda kriitiliselt. **1.3. Info salvestamine ja taasesitamine** – salvestab digitaalset infot oma eesmärkidest lähtuvalt ning korrastab ja töötleb kogutud infot, et seda taasesitada.
2. Suhtlemine digitaalses keskkonnas	**2.1. Suhtlemine digivahenditega** **2.2. Info ja sisu jagamine** – jagab leitud info asukohta ja sisu teistega ning järgib intellektuaalse omandi kaitse häid tavasid. **2.3. Kodanikuaktiivsus veebis** – on kaasatud ning kaasab teisi ühiskonnaelu tegevustesse, kasutades IKT vahendeid ja võimalusi. **2.4. Koostöö digitehnoloogia toel** – kasutab digivahendeid meeskonnatööks ning ressursside, digitaalsete materjalide ja teadmiste koosloomeks. **2.5. Netikett** – praktiseerib digisuhtluses käitumisnorme ja häid tavasid ning arvestab suheldes kultuurilise eripära ja mitmekesisuse ilminguid. **2.6. Digitaalse identiteedi haldamine** – kujundab ja haldab oma digitaalset identiteeti ning jälgib oma digitaalset jalajälge.
3. Sisuloome	**3.1. Digitaalne sisuloome** – loob ise, muudab ja arendab eri formaatides enda ning teiste loodud digitaalset sisu. **3.2. Uue teadmise loomine** – muudab ja lõimib olemasolevat digitaalset materjali, et luua uut teadmist.

	3.3. Autoriõigus ja litsentsid – järgib digitaalses sisuloomes ning teiste loodud sisu kasutades intellektuaalomandi põhimõtteid.
4. Turvalisus	**4.1. Seadmete kaitsmine** – rakendab ohutus- ja turvameetmeid, et vältida füüsilisi ning virtuaalseid riske. **4.2. Isikuandmete kaitsmine** – arvestab digitegevustes teiste inimeste privaatsust ja ühiseid kasutustingimusi ning kaitseb oma isikuandmeid ja ennast veebipettuste, ohtude ning küberkiusamise eest. **4.3. Tervise kaitsmine** – väldib digitehnoloogia ja digitaalse info kasutamisest tulenevaid terviseriske. **4.4. Keskkonna kaitsmine** – teadvustab digitehnoloogia mõju keskkonnale.
5. Probleemilahendus	**5.1. Tehniliste probleemide lahendamine** – teeb veaotsinguga kindlaks tehnilised probleemid ning leiab võimalikud lahendused (veaotsingust kuni komplekssemate probleemideni). **5.2. Vajaduste väljaselgitamine ja neile tehnoloogiliste lahenduste leidmine** – valib ning hindab kriitiliselt enda vajaduste järgi sobivaid tehnoloogilisi võimalusi ja digilahendusi. **5.3. Innovatsioon ja tehnoloogia loov kasutamine** – rakendab tehnoloogiat loovalt eneseväljendamiseks ja probleemidele uudsete lahenduste leidmiseks. **5.4. Digipädevuse lünkade väljaselgitamine** – hoiab end kursis uute arengusuundadega digitehnoloogias, selgitab järjepidevalt oma digipädevuse puudujääke, arendab ennast ning toetab teisi digipädevuse arendamises

Lisa 3. CEPOL ECTEG-maatriksi digitaalsed pädevused

Tabel. CEPOL ECTEG-maatriksi digitaalsed pädevused. Allikas: European Cybercrime Training and Education Group, 2020 ref Beesley, 2021, pp. 14-15

Roll	Ülesannete kirjeldus	Kompetentsid
Küberkuritegevuse üksuse juht/rühma juht	Juhib küberuurijate ja – ekspertide tööd. Nad peaksid oskama tegema teadlikke otsuseid küberkuritegevuse juhtumite või muude keeruliste uurimiste puhul, mis hõlmavad küberkuritegevuse elemente.	➢ põhjalikud teadmised küberkuritegevuse ja küberkuritegude kohta ➢ täiustatud teadmised õigus- ja jurisdiktsiooni küsimustes ➢ teadmised rahvusvahelise koostöö institutsionaalsest raamistikust ➢ asjakohaste uurimismenetluste tundmine ➢ kõrgetasemelised teadmised uurimis- ja kohtuekspertiisi vahendite kohta ➢ teadmised koolitusvajadustest ja olemasolevatest ressurssidest ➢ personalijuhtimise oskused ➢ eelarve haldamise oskused ➢ projektide ja kavandite koostamise oskused ➢ suhete haldamine ja pehmed oskused ➢ suhtlemisoskus
Kübereksperdid	Sellesse kategooriasse kuuluvad spetsialistid, kes osalevad küberrünnakutes taktikaliste õiguskaitseorganite esindajatena; teevad koostööd teiste osalejatega (küberturbe amet, CSIRT, seotud IT-osakonnad ja juhtkond) sunniviisiliste tehniliste vastumeetmete algatamisel, samuti keeruliste (digitaalsete) jälgede ja elektrooniliste tõendite hankimisel, säilitamisel, analüüsimisel ja dokumenteerimisel.	➢ elektrooniliste tõendite tuvastamine ja konfiskeerimise head tavad ➢ täiustatud küberkuritegevuse alane teadlikkus ➢ täiustatud võrguekspertiis ➢ strateegiline ja operatiivne küberkuritegevuse analüüs ➢ analüütiliste ja visualiseerimisvahendite kasutamisoskus ➢ skriptide koostamine ➢ aruande koostamise ja tõendite esitamise oskused ➢ teadmised rahvusvahelisest õigusalasest koostööst küberkuritegevuse valdkonnas

Digitaalne kohtueekspert	Need spetsialistid teostavad üksikasjalikku kohtueekspertiisi arvutipõhiste digitaalsete tõendite kohta.	➢ täiustatud küberkuritegevuse alane teadlikkus ➢ täiustatud teadmised õigus- ja jurisdiktsiooni küsimustes ➢ digitaalsete tõendite töötlemine, säilitades samal ajal tõendite ahelat ➢ ekspertteadmised ühes või mitmes kohtuekspertiisi valdkonnas ➢ erinevate operatsioonisüsteemide ja rakenduste tundmine ➢ asjakohaste kommerts- ja avatud lähtekoodiga vahendite tundmine ➢ skriptide/programmeerimise ja andmebaasi päringute (SQL) tundmine. ➢ kohtuekspertiisi artefaktide ja andmete moonutamise mõistmine ➢ teadmised nii *post-mortem* kui ka reaalaja andmete kohtuekspertiisi kohta ➢ aruannete koostamise oskused ➢ tõendite esitamine
Küberkuritegevuse analüütik	Need spetsialistid keskenduvad kas strateegilisele analüüsile, uurides, analüüsides ja esitades viimaseid ohte ning andes ülevaateid olukorrast, või tegelevad rohkem operatiivanalüüsiga, et leida mustreid, suundumusi ja levialasid ning luua seoseid eluliste juhtumite vahel.	➢ strateegiline ja operatiivne kuritegevuse analüüs ➢ suurandmete haldamine ja analüüs ➢ täiustatud küberkuritegevuse alane teadlikkus ➢ analüütiliste ja visualiseerimisvahendite kasutamise oskus ➢ avatud lähtekoodiga uurimine ➢ sotsiaalsete võrgustike uurimine ➢ stsenaariumi koostamine/programmeerimine ➢ võrgueekspertiis ➢ aruannete koostamise oskused ➢ tõendite esitamine ➢ varjatud juurdluse põhialused
Veebiuurija	Ülesanneteks on jälgida digimaailma ja teha ettepanekuid uute teemade ja juhtumite uurimiseks; viia läbi või toetada uurimist.	➢ täiustatud küberkuritegevuse alane teadlikkus ➢ täiustatud teadmised õigus- ja jurisdiktsiooni küsimustes ➢ digitaalsete tõendite töötlemine, säilitades samal ajal tõendite ahelat ➢ täiustatud avatud lähtekoodiga uurimine ➢ sotsiaalsete võrgustike uurimine ➢ täiustatud võrgueekspertiis ➢ aruannete koostamise oskused ➢ varjatud uurimine (jälitustegevus)

		➢ stsenaariumi koostamine/programmeerimine ➢ intervjueerimisoskused (küsitlus- ja ülekuulamistehnikad)
Üldine kriminaaluurija	Peamised uurijad, kes puutuvad kokku interneti ja digitaalsete vahendite kasutamisega kurjategijate poolt.	➢ täiustatud küberkuritegevuse alane teadlikkus ➢ täiustatud teadmised õigus- ja jurisdiktsiooni küsimustes ➢ digitaalsete tõendite töötlemine, säilitades samal ajal tõendite ahelat ➢ täiustatud avatud lähtekoodiga uurimine ➢ sotsiaalsete võrgustike uurimine ➢ täiustatud võrguekspertiis ➢ aruannete koostamise oskused ➢ varjatud uurimine ➢ stsenaariumi koostamine/programmeerimine ➢ intervjueerimisoskused (küsitlus- ja ülekuulamistehnikad) ➢ tõendite esitamine
Esmareageerija	Puutuvad esimesena kokku võimalike elektrooniliste tõenditega. Patrullpolitseinikud, uurijad/jälitajad, piirivalvurid ja maksuametnikud võivad olla esmareageerija rollis.	➢ elektrooniliste tõendite tuvastamise ja konfiskeerimise standardid ja parimad tavad ➢ alusteadmised andmete kohtuekspertiisist ➢ alusteadmised digitaalsest kohtuekspertiisist (vahendid, tehnikad, meetodid ja parimad tavad), sealhulgas internetitehnoloogia, pime veeb ja krüptovaluutad. ➢ kuriteopaiga haldamine ➢ intervjueerimisoskused (küsitlus- ja ülekuulamistehnikad) ➢ üldine teadlikkus küberkuritegevusest

Lisa 4. Magistritöös välja töötatud kompetentsiraamistik

Kompetentsiraamistik digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks politseijaoskonna uurija tasandil (rollis)

Magistritöös lähtutakse teoreetilistes allikates kirjeldatud terrtitoriaalsuse põhimõttel politsei struktuuriüksustes töötavate uurijate rollist, kelle põhivaldkonnaks on teenindatava territooriumi elanike poolt toime pandud või nende vastu suunatud kuritegude uurimine ja juhtumite lahendamine. Töös kasutatakse mõistet „kohaliku tasandi (politseiüksuse) uurija“, mis on analoogne PPA politseijaoskonna uurija rollile. Kohaliku tasandi uurijatel tuleb koguda tõendeid ja lahendada kuritegusid, kus kurjategijad kasutavad digivahendeid kuritegude toime panemiseks. Raamistikus kajastatakse magistritöös teadusallikatele tuginedes ja praktilise suunitlusega allikatest sünteesitud kompetentse.

Kompetentsid on seotud töö sisuga (Marrelli, *et al*., 2005). Politseiuurija töö ja selle raames IKT kasutusala ühe võimalikest soovitusliku kirjelduse (European Commission, 2016, pp. 69-76) kohaselt seisneb politseiuurija töö keerulises teabepõhises tegevuses, mis nõuab mitmete andmeallikate integreerimist ning seda sageli lühikese aja jooksul. Politseiuurija (detektiivi) peamisteks tööülesanneteks on sündmuse uurimine ja selle kohta teabe kogumine, töötlemine ja analüüsimine ja tõenditel põhineva menetluskokkuvõtte koostamine.

Iga töö elemendi või ülesande täitmiseks kaardistatakse vajalikud teadmised, oskused, võimed ja isiksuseomadused. Kompetentsid võib jaotada tasanditeks, mille kaudu eristatakse tipptasemel ja alustasemel töötajale vajalikke kompetentse. Valmis kompetentsimudeli valideeritakse koostöös töövaldkonna asjatundjatega, kellel on ulatuslik kogemus sihttööga ja teadmised töö sisu kohta. Koostöös täpsustatakse definitsioonid, antakse hinnanguid kompetentsiraamistiku kohaldatavuse osas. Valmis kompetentsimudel (-raamistik) sisaldab kompetentside loetelu, mis on liigitatud tüübi järgi (nt põhikompetents, isiklik tõhusus, tehniline kompetents), koos iga kompetentsi määratluse ja mitme käitumisnäidisega kolmel või enamal kompetentsitasemel. (Marrelli, *et al*., 2005)

Kohaliku tasandi politseiuurija digitaalse komponendiga kuritegude uurimiseks ette nähtud komptentsuse taseme määratlemiseks kasutatkse Eesti kvalifikatsiooniraamistiku skaala (SA Kutsekoda, 2023) (vt: https://www.kutsekoda.ee/kvalifikatsiooniraamistiku-

tasemekirjeldused/). Magistritöö autori hinnangul politseijaoskonna uurija tasandi kompetentsid on piisavad, kui nad vastavad vähemalt Eesti kvalifikatsiooniraamistiku 3. taseme kirjeldusele. Väga head kompetentsid vastavad 5. tasemele.

Võtmekompetentside komplektid on olulised kõikidele sarnase tööga töötajatele. Neid täiendatakse kompetentsikategooriate kaudu, mis kehtivad konkreetsetele (siht)alarühmadele (Marrelli, *et al*., 2005).

Kohaliku tasandi uurija digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks vajalikud võtmekompetentsid on:

Üldkompetentsid on ülekantavad, need on vajalikud ja kasutatavad tööturu eri valdkondades. Magistritöös kasutatakse SA Kutsekoda (Jamnes, *et al*., 2013) taksonoomiat.

Üld-digikompetentsid on üldkompetentside osa, nad on samuti ülekantavad, vajalikud ja kasutatavad tööturu eri valdkondades. Raamistikus neid tuuakse eraldi välja, tuginedes DigComp 2,0 ja DigComp 2,1 (Carretero, *et al.,* 2017) raamistikele parema visualiseerimise eesmärgil.

Binkley, *et al.*, (2012) taksonoomia kohaselt üldkompetentse saab jaotada järgnevatesse oskuste gruppidesse:

- Mõtlemisviisidega seotud oskused (loovus ja innovatsioon; kriitiline mõtlemine, probleemide lahendamine ja otsuste tegemine; õppimine ja metakognitsioon),
- Tööviisidega seotud oskused (suhtlemine; koostöö ja meeskonnatöö),
- Töövahendite kasutamise oskused (infokirjaoskus; infotehnoloogia ja kommunikatsioonialane kirjaoskus)
- Üldised toimetuleku oskused (elu ja karjääri planeerimisoskus; isiklik ja sotsiaalne vastutus).

Van Laar, *et al*. (2017) aga nimetab üld- ja sealhulgas ülddigioskuseid 21. sajandi oskusteks ja jagab neid kahte gruppi, milleks on tehnilised oskused (infohaldus, kommunikatsioon, koostöö, loovus, kriitiline mõtlemine ja probleemide lahendamine) ja kontekstuaalsed oskused (eetilise teadlikkuse, kultuuriteadlikkus, paindlikkus, enesejuhtimine ja elukestev õpe).

Kutsespetsiifilised kompetentsid on politsei erialal töötamiseks ettenähtud kutseoskuste ja -teadmiste kogum. Neid tervikuna siin ei käsitleta, vaid keskendutakse konkreetsele kohaliku tasandi politseiuurija funktsioonile ja rollile (PPA politseijaoskonna uurija). Eeldatakse, et kohaliku tasandi politseiuurija roll erineb valdkonnaspetsiifilisest politseiuurija rollist, kes töötab funktsionaalüksuses ja tegeleb kitsalt spetsialiseeritud küberkuritegude uurimisega (nt organiseeritud kuritegevus, küberkuritegevus, laste vastu suunatud seksuaalkuriteod jms) või kelle tööülesanded on sügavalt spetsiifilised (nt küberekspert, veebiuurija, küberkuritegevuse analüütik) ja eeldavad eriettevalmistust. Vaadeldavaks tööfunktsiooniks on digitaalse komponendiga juhtumite käsitlemine ja kuritegude uurimine. Kohaliku tasandi politseiüksuse uurija on uurijate hierarhias esmane tasand, kelle ülesandeks on lahendada tööpiirkonna territoriaalsuse põhimõttest lähtuvalt erineva spektri kogukonnas kuriteotunnustega juhtumeid ja kuritegusid (enamasti traditsioonilisi), millel puudub spetsiifika (nt organiseeritud kuritegevuse tunnused, kõrgtehnoloogilise poole kuriteod (ehtsad küberkuriteod), majanduskuriteod jms. Digitaalse komponendiga kuritegude uurimiseks vajalikud oskused ja kompetentsid on sõnastatud erinevate valdkonna analüüside (CEPOL, Kanada) ja praktikate alusel (Kanada, USA). Nad kätkevad järgmisi aspekte:

- Õigusalased teadmised, menetlusreeglid (sh vajalikkus rahvusvahelise koostöö osas)
- Digitaalkriminalistika üldteadmised ja –rakendamisoskused menetlustoimingute vormistamisel
- Erialased digikompetentsid

Üldkompetentsid (4 kompetentsigruppi: 8 kompetentside kategooriat, 23 kompetentsi, mis mingil määral haakuvad ka digikompetentsidega)	**Tase** **3-5**	**Üld-digikompetentsid**	**Tase** **3-5**	**Kohaliku tasandi (politseiüksuste) uurijate kutsespetsiifilised kompetentsid digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks**	**Tase** **3-5**
➢ **Suhtlemine:** <u>suhtemine ja esitlemine</u> ● suhtlemine ● teabe esitamine ● klientide teenindamine <u>koostöö ja toetamine</u> ● koostöö ● Väärtustest lähtumine ja põhimõtete järgimine ● Mõjutamine ja veenmine ➢ **juhtimine** <u>juhtimine ja eestvedamine</u> ● Otsustamine ja tegevuste algatamine ● Inimeste juhtimine ● Protsesside juhtimine ● Juhendamine ➢ **Mõtlemine:** <u>analüüs ja tõlgendamine</u> ● Kirjutamine ja aruannete koostamine ● Analüüsimine ja tõlgendamine <u>loovus ja üldistusoskus</u> ● Teadmiste ja tehnoloogiate kasutamine ● Õppimine ja enesearendamine ● Loovus ja uuenduslikkus <u>Kontseptuaalne ja strateegiline mõtlemine</u> ➢ **Enesejuhtimine**		➢ **Info haldamine:** <u>Info otsimine ja sirvimine</u> – määrab eesmärgi põhjal oma infovajaduse ning valib eesmärgiga sobivad meetodid digitaalse info otsimiseks ja sirvimiseks. <u>Info hindamine</u> – kogub ja töötleb digitaalset infot, eristab olulist infot ning analüüsib ja hindab seda kriitiliselt. <u>Info salvestamine ja taasesitamine</u> – salvestab digitaalset infot oma eesmärkidest lähtuvalt ning korrastab ja töötleb kogutud infot, et seda taasesitada. ➢ **Suhtlemine digitaalses keskkonnas:** <u>Suhtlemine digivahenditega</u> <u>Info ja sisu jagamine</u> – jagab leitud info asukohta ja sisu teistega ning järgib intellektuaalse omandi kaitse häid tavasid. <u>Kodanikuaktiivsus veebis</u> – on kaasatud ning kaasab teisi ühiskonnaelu tegevustesse, kasutades IKT vahendeid ja võimalusi. <u>Koostöö digitehnoloogia toel</u> – kasutab digivahendeid meeskonnatööks ning ressursside, digitaalsete materjalide ja teadmiste koosloomeks. <u>Netikett</u> – praktiseerib digisuhtluses käitumisnorme ja häid tavasid ning arvestab suheldes kultuurilise eripära ja mitmekesisuse ilminguid. <u>Digitaalse identiteedi haldamine</u> – kujundab ja haldab oma digitaalset identiteeti ning jälgib oma digitaalset jalajälge.		➢ **Üldine teadlikkus küberkuritegevusest (küberkuritegude liigid: IKT kui ründeobjekt ja teo toimepanemise vahend) ja küberkriminoloogiast (kuritegude toimepanemise põhjused, kurjategijate profiilid)** ➢ **Teadmised digitaalse keskkonna toimeloogikast ja dimensioonidest (kihtidest), tumedast ja süvaveebist, krüptovaluutadest** ➢ **Põhiteadmised õigus- ja jurisdiktsiooni küsimustes, digitaalse keskkonnaga seotud õigusalased küsimused** ➢ **Üldine teadlikkus rahvusvahelisest õigusalasest koostööst küberkuritegevuse valdkonnas** ➢ **Teadmised elektrooniliste tõendite tuvastamisest ja konfiskeerimise headest tavadest, nende rakendamise oskus** ➢ **Kuriteopaiga (sündmuskoha) haldamise oskus digitaalse komponendiga juhtumis** ➢ **Digitaalsete tõendite töötlemise oskus, säilitades samal ajal tõendite ahelat;**	

kohanemine ja toimetulek ● Avatus ja paindlikkus ● Toimetulek pinge ja tagasilöökidega Ettevõtlikus ● Isiklikele tööalastele eesmärkidele pühendumine ● ettevõtlikkus organiseerimine ja tegutsemine ● Juhiste ja reeglite järgimine ● Planeerimine ja organiseerimine ● Tulemuste saavutamine (Jamnes, *et al.*, 2013) Kriitiline mõtlemine Elukestev õppe (Van Laar, et al., 2017)		➢ **Sisuloome:** Digitaalne sisuloome – loob ise, muudab ja arendab eri formaatides enda ning teiste loodud digitaalset sisu. Uue teadmise loomine – muudab ja lõimib olemasolevat digitaalset materjali, et luua uut teadmist. Autoriõigus ja litsentsid – järgib digitaalses sisuloomes ning teiste loodud sisu kasutades intellektuaalomandi põhimõtteid. ➢ **Turvalisus:** Seadmete kaitsmine – rakendab ohutus- ja turvameetmeid, et vältida füüsilisi ning virtuaalseid riske. Isikuandmete kaitsmine – arvestab digitegevustes teiste inimeste privaatsust ja ühiseid kasutustingimusi ning kaitseb oma isikuandmeid ja ennast veebipettuste, ohtude ning küberkiusamise eest. Tervise kaitsmine – väldib digitehnoloogia ja digitaalse info kasutamisest tulenevaid terviseriske. Keskkonna kaitsmine – teadvustab digitehnoloogia mõju keskkonnale. ➢ **Probleemilahendus:** Tehniliste probleemide lahendamine – teeb veaotsinguga kindlaks tehnilised probleemid ning leiab võimalikud lahendused (veaotsingust kuni komplekssemate probleemideni). Vajaduste väljaselgitamine ja neile tehnoloogiliste lahenduste leidmine – valib ning hindab kriitiliselt enda vajaduste järgi sobivaid tehnoloogilisi võimalusi ja digilahendusi. Innovatsioon ja tehnoloogia loov kasutamine – rakendab tehnoloogiat loovalt		**digitaalsete tõendite käsitlemise ja dokumenteerimise oskused** ➢ **Erineva sotsiaalse tausta isikute intervjueerimisoskused (küsitlus- ja ülekuulamistehnikad) digitaalse komponendiga juhtumite uurimisel** ➢ **Üldteadmised analüütilistest ja visualiseerimisvahenditest, nendest arusaamine ja kasutamise oskus** ➢ **Avatud allikaga luure (OSINT), tõendite kogumine ja analüüsi oskus** ➢ **Sotsiaalsete võrgustike toimeloogika tundmine ja nende uurimise oskus** ➢ **Põhiteadmised tööst geolokatsiooniliste andmete, seadmete ja platvormidega** ➢ **Põhiteadmised (e-posti) andmepüügist, Wi-Fi nuhkimisest** ➢ **Teadmised küberhügieeni ja küberturvalisusesest, digitaalselses keskkonnas turvalise käitumise ja digiseadmete turvalise kasutamise oskus** (CEPOL European Cybercrime Training and Education Group, 2020)	

		eneseväljendamiseks ja probleemidele uudsete lahenduste leidmiseks. Digipädevuse lünkade väljaselgitamine – hoiab end kursis uute arengusuundadega digitehnoloogias, selgitab järjepidevalt oma digipädevuse puudujääke, arendab ennast ning toetab teisi digipädevuse arendamises (Carretero, *et al.,* 2017; SA Kutsekoda, 2019)			

Koostas: Jevgenia Jakobson

06.03.2023

Kasutatud allikad:

Beesley, P., 2021. *Competency-based management framework for digital competencies in Canadian policing: A component of the Canadian Police Knowledge Network's Cybercrime Training and Digital Competency Development for Canadian Law Enforcement project*. Public Safety Canada [Võrgumaterjal] Leitav: https://www.cpkn.ca/wp-content/uploads/final_CBMF_Digital_Competencies_Report_June17_2021-1.pdf [Kasutatud 28.12.2022].

Binkley, M., Erstad, O., Herman, J., Raizen, S., Ripley, M., Miller-Ricci, M. & Rumble, M., 2012. Defining twenty-first century skills. In: P. Griffin, B. McGaw, & E. Care. eds. *Assessment and teaching of 21st century skills: Methods and approach*, Dordrecht: Springer, pp. 17–66.

Carretero, S., Vuorikari, R. & Punie, Y., 2017. *DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use*. Luxembourg: Publications Office of the European Union.

CEPOL European Cybercrime Training and Education Group, 2020. *Cybercrime Training Competency Framework: Cybercrime Training Competencies Framework Introduction*. [Võrgumaterjal] Leitav: https://www.ecteg.eu/tcf/co/TCG_OpaleModule_4.html [Kasutatud 15.02.2023].

European Commission, 2016. Police detective: The context: the use of ICT in police work. *The impact of ICT on job quality: evidence from 12 job profiles: An intermediate report from the study "ICT for work: Digital skills in the workplace – SMART 2014/0048*". INTERMEDIATE REPORT Prepared for the European Commission DG Communications Networks, Content & Technology, pp. 69–76.

Jamnes, P., Elenurm, T., Murre, S., Kerem, M.-K. & Randma, T., 2013. *Üldised kompetentsid: kvalifikatsiooniga seonduvad terminid Juhendmaterjal kutsestandardi koostajale, tasemeõppe ja täienduskoolituse õppekava koostajale ning karjäärinõustajale*. SA Kutsekoda: Iloprint. [Võrgumaterjal] Leitav: https://www.kutsekoda.ee/wp-content/uploads/2019/KS/Uldised-kompetentsid.pdf [Kasutatud 06.03.2023].

Marrelli, A. F., Tondora, J., & Hoge, M. A., 2005. Strategies for developing competency models. *Administration and Policy in Mental Health and Mental Health Services Research*, *32*(5), pp. 533–561.

SA Kutsekoda, 2023. Kvalifikatsiooniraamistiku tasemekirjeldused. [Võrgumaterjal] Leitav: https://www.kutsekoda.ee/kvalifikatsiooniraamistiku-tasemekirjeldused/ [Kasutatud 06.03.2023].

SA Kutsekoda, 2019. *Kutsestandardid: Kohtukriminalistikaekspert, tase 8.* [Võrgumaterjal] Leitav: https://www.kutseregister.ee/ctrl/et/Standardid/vaata/10723669 [Kasutatud 06.03.2023].

Van Laar, E., Van Deursen, A. J., Van Dijk, J. A., & De Haan, J., 2017. The relation between 21st-century skills and digital skills: A systematic literature review. *Computers in human behavior*, 72, pp. 577–588.

Lisa 5. Kompetentside tasemekirjeldused

SA Kutsekoda (2023) poolt välja töötatud hindamisskaala - Kvalifikatsiooniraamistiku tase **määratleb nõuded** koolihariduse õpitulemustele ja kutsesüsteemi erinevatele tasemetele.

Tabelis on näha, millised teadmised ja oskused mis kvalifikatsioonitasemele vastavad. Magistritöös välja töötatud kompetentsiraamistikus kasutatalse SA on määratletud, et kohaliku tasandi politseiuurija kompetentsid (oskused ja teadmised) peavad vastama tasemele 3-5.

	Teadmised **Eristatakse teoreetilisi teadmisi ja faktiteadmisi**	**Oskused** **Eristatakse kognitiivseid oskusi (nt loogilise, intuitiivse ja loova mõtlemise kasutamine) ning praktilisi oskusi (nt käelised oskused, meetodite, materjalide, tööriistade ja vahendite kasutamine)**	**Vastutuse ja iseseisva tegutsemise ulatus**
1. tase	Üldteadmised	Põhioskused lihtsamate (töö)ülesannete täitmiseks	Töötab või õpib otsesel juhendamisel piiritletud situatsioonis
2. tase	Põhilised tööalased või õppesuuna alased faktiteadmised	Põhilised kognitiivsed ja praktilised oskused vastava teabe kasutamiseks, et täita (töö)ülesandeid ning lahendada tavalisi probleeme, kasutades lihtsaid reegleid ja töövahendeid	Töötab ja õpib juhendamisel, kuid mõningase iseseisvusega
3. tase	**Teadmised tööalaste või õppesuunaalaste faktide, põhimõtete, protsesside ja üldiste mõistete kohta**	**Kognitiivsed ja praktilised oskused (töö)ülesannete täitmiseks ja probleemide lahendamiseks, valides ja rakendades põhimeetodeid, töövahendeid, materjale ja teavet**	**Vastutab töö- või õppeülesannete täitmise eest. Kohandab probleemide lahendamisel enda käitumist vastavalt olukorrale**
4. tase	**Tööalased või õppesuuna alased laiaulatuslikud fakti- ja teooriate teadmised**	**Tööalased või õppesuuna alased kognitiivsed ja praktilised oskused konkreetsetele probleemidele lahenduse leidmiseks**	**Juhib ise oma tööd ja õppimist vastavalt juhtnööridele situatsioonides, mida saab tavaliselt ette näha, kuid mis võivad muutuda. Juhendab kaaslaste tavatööd. Võtab mõningase vastutuse töö ja õppetöö hindamise ning edendamise eest**
5. tase	**Tööalased või õppesuunaalased põhjalikud, spetsialiseeritud, faktilised ja teoreetilised teadmised ning teadlikkus oma teadmiste piiridest**	**Igakülgsed kognitiivsed ja praktilised oskused abstraktsetele küsimustele loovate lahenduste leidmiseks**	**Juhib ja juhendab töö- ja õppesituatsioone, kus võivad juhtuda ettearvamatud muutused. Kontrollib ja arendab enda ja teiste tegevust**

6. tase	Tööalased või õppesuunaalased süvateadmised, sh kriitiline arusaam teooriatest ja printsiipidest	Meisterlikkust ja novaatorlikkust demonstreerivad arenenud oskused konkreetsete tööalaste või õppesuunaalaste keeruliste ja ettearvamatute probleemide lahendamiseks	Juhatab keerulisi tehnilisi või kutsealaseid tegevusi või projekte. Võtab vastutuse otsuste langetamise eest ettearvamatutes töö- või õppesituatsioonides. Vastutab üksikisikute ja rühmade kutsealase arendamise juhtimise eest
7. tase	Väga spetsialiseeritud, osaliselt tööalaste või õppesuuna alaste teadmiste esirinnas olevad teadmised, millel rajaneb originaalne mõtlemine. Kriitiline teadlikkus tööalastest või õppesuunaalastest ja eri valdkondade vahelistest probleemidest	Spetsialiseeritud probleemilahendamise oskused, mis on vajalikud teadus- ja/või innovatsioonitegevuses, selleks et luua uusi teadmisi ja protseduure ning siduda eri valdkondade teadmisi	Juhib ja muudab töö- või õppesituatsioone, mis on keerukad, ettearvamatud ja nõuavad uut strateegilist käsitlust. Võtab vastutuse kutseteadmistesse ja -tegevusse panuse andmise eest ja/või kontrollib meeskondade strateegilist tegutsemist
8. tase	Teadmised, mis on tööalaste või õppesuunaalaste ja valdkondadevaheliste teadmiste esirinnas	Eriti arenenud ja spetsialiseeritud oskused ja tehnikad, kaasa arvatud süntees ja hindamine, mis on vajalikud kriitiliste küsimuste lahendamiseks teadus- ja/või innovatsioonitegevuses ning olemasolevate teadmiste või kutseoskuste täiendamiseks ja uuesti määratlemiseks	Omab autoriteeti ja demonstreerib oma novaatorlikkust, iseseisvust, teadus- ja kutsealast meisterlikkust ning pidevat pühendumust uute ideede või protsesside arendamisel töö- või õppesituatsioonide, sh teadustöö, esirinnas

Allikas: SA Kutsekoda, 2023. Kvalifikatsiooniraamistiku tasemekirjeldused. [Võrgumaterjal] Leitav: https://www.kutsekoda.ee/kvalifikatsiooniraamistiku-tasemekirjeldused/ [Kasutatud 06.03.2023].

Lisa 6. Ekspertintervjuude küsimustikud

KÜSIMUSTIK A.

Küsimused PPA ekspertidele

Sissejuhatavad ja taustaküsimused:

- Mis valdkonda PPA-s Te esindate? Kas ja kuidas lubate kajastada magistritöös Teie andmeid ja tausta?
- Kuidas on Teie valdkond seotud PPA politseijaoskondade uurijate kompetentsuse teemadega?
- Kui kaua olete selle valdkonna ekspert ja milline on Teie üldine staaž politseiorganisatsioonis?
- Milline on teie haridustase ja valdkond?

Küsimused seoses digitaalse komponendiga juhtumite ja kuritegude ilmnemisega politseiuurijate töös ja nende mõjuga.

1) Kuidas on ühiskonna digitaliseerumine muutnud kohaliku tasandi politseiüksuse uurija (PPA politseijaoskonna menetlusüksuste uurija) töö iseloomu ja ülesandeid? Mis on selle juures positiivne ja mis negatiivne?

2) Mida Teile tähendab mõiste „digitaalne komponent“ uurija poolt lahendatava juhtumi või uuritava kuriteo juures? Palun tooge näiteid.

3) Milline on Teie arvates kõige parem digitaalse komponendiga juhtumi definitsioon? Kas ja mille poolest see eristub küberkuriteo definitsioonist? Miks? /küsimust täpsustati pärast esimese intervjuu läbiviimist – vt küsimustikku 2 ja 3/

4) Kus te näete kitsaskohti uurijate poolt digitaalse komponendiga juhtumite käsitlemises ja kuritegude uurimise nii oskusete omandamisel, kui ka kompetentsinõuete kaasajastamisel?

5) Kuidas võimalikke kitsaskohti maandatakse?

6) Millised tegurid võivad seada takistusi ja probleeme digitaalse komponendiga juhtumite käsitlemisel ja kuritegude uurimisel? (Sisemised vs välised tegurid) Millised on organisatsioonisisesed tegurid? Millised välised tegurid?

Küsimused PPA-s kohaliku tasandi politseiüksuse uurija rolli määratlemise kohta

7) Kuidas on määratletud politseijaoskonna tasand digitaalse komponendiga kuritegude menetluspädevuse jaotamisel politsei organisatsiooni vaates? Milliste kuritegude lahendamisega seal tegeletakse? Mille poolest erineb politseijaoskonna uurija roll funktsionaalüksuse uurija rollist? /tegelikult ja formaalselt/

8) Millest on seni lähtutud PPA-s politseijaoskonna uurija rolli ja töövälja määratlemisel? Palun kirjeldage neid põhimõtteid.

Küsimused on kompetentsuse kriteeriumide määratlemise kohta PPA-s. Huvitab, kuidas eksperdid näevad tänast PPA lähenemist digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks vajalike kompetentside kaardistamise protsessi võrreldes magistritöös välja töötatud raamistikuga.

9) Kuidas PPA-s toimub politseijaoskonna uurijale vajalike kompetentside kaardistamine? Millised komponendid moodustavad kompetentsust? Palun kirjeldage seda protsessi.

10) Kuidas on Teie arvates täna esindatud kompetentsiraamistiku osa, mis on vajalik politseijaoskondade uurijatele digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks?

11) Kuidas on kaardistatud politseijaoskonna uurijatetele ette nähtud koolitus- ja täiendusõppe vajadused? Millised tulevased koolitused on suunatud digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks vajalike kompetentside arendamiseks? Mis on riikliku tellimuse baaskompetentsid? Millised kompetentsid tuleb töötavatel uurijatel arendada/parendada täiendusõppe raames?

Küsimused kohaliku tasandi (politseiüksuse) uurijale digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks vajalikest võtmekompetentsidest ja nende täpsemast jaotusest üld- ja kutsespetsiifilisteks kompetentsideks.

12) Milline Teie hinnangul võiks olla politseijaoskondade uurijtele vajalik digitaalsete võtmekompetentside komplekt politseiorganisatsiooni vaates? Kas on erisusi võrreldes teiste üksuste (funktsionaalüksuste, eri liikide kuritegudele spetsiliseeritud) uurijatega? /Märkus: teaduskirjanduses on toodud, et digitaalse komponendiga kuriteod, st küberkuriteod, on erineva iseloomu ja raskusastmega,

ning küberkuritegevusele spetsialiseerunud üksuste uurijatele on nende teadmiste ja oskuste osas suuremad ootused./ Milline on olukord PPA-s?

13) Milline on üld- (sh digi-)kompetentside roll digikomponendiga juhtumite käsitlemiseks vajalike kompetentside seas? Kas ja miks tugevate üldkompetentside olemasolu on oluline?

14) Millised kutsespetsiifilised kompetentsid (sh digikompetentsid) on vajalikud politseijaoskonna uurija digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks?

15) Millised on Teie hinnangul kompetentsipõhise lähenemise (juhtimise) tugevused ja nõrkused, kui kaaluda selle kasutamist (nt personali ametijuhendite ja tööde kirjelduste koostamisel, koolitusvajaduste kaardistamisel jms)? Palun põhjendage.

16) Kas teie hinnangul magistritöö raames välja töötatud kompetentsiraamistik võiks olla kasulik uurija vajalike digikompetentside kaardistamisel/määramisel? Palun põhjendage.

17) Millised lahendused Teie arvates aitaksid veel politseijaoskondade uurijate digitaalse komponendiga juhtumite lahendamiseks ja kuritegude uurimiseks vajalike kompetentside määratlemiseks ning vastavusse viimiseks ja/või parendamiseks?

KÜSIMUSTIK B.

Küsimused Sisekaitseakadeemia politseieriala õppeprogrammide koostajale, arendajale, õppejõule, kelle õppeainetes digi-komponent sees on

Sissejuhatavad ja taustaküsimused:

- Mis valdkonda Sisekaitseakadeemias Te esindate? Kas ja kuidas lubate kajastada magistritöös Teie andmeid ja tausta?
- Kuidas on Teie valdkond seotud politseiuurijate kompetentsuse teemadega?
- Kui kaua olete selle valdkonna ekspert ja milline on Teie üldine staaž Sisekaitseakadeemias? Politseiorganisatsioonis?
- Milline on teie haridustase ja valdkond?

Küsimused seoses digitaalse komponendiga juhtumite ja kuritegude ilmnemisega politseiuurijate töös ja nende mõjuga.

1) Kuidas ühiskonna digitaliseerumine on muutnud kohaliku tasandi (politseiüksuse) uurija töö iseloomu ja ülesandeid? Mis on selle juures positiivne ja mis negatiivne?

2) Mida Teile tähendab mõiste „digitaalne komponent“ uurija poolt lahendatava juhtumi või uuritava kuriteo juures? Palun tooge näiteid.

3) Milline on Teie arvates kõige parem digitaalse komponendiga juhtumi definitsioon? Kas ja mille poolest see eristub küberkuriteo definitsioonist? Miks? Kui see on keeruline, siis kuidas Te iseloomustaksite digitaalse komponendiga juhtumit ja kas see erineb küberkuriteost? Tooge mõned näited.

4) Kus te näete kitsaskohti nii uurijate poolt digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks oskusete omandamisel kui ka kompetentsinõuete kaasajastamisel?

5) Millised on Teie arvates nende kitsaskohtade maandamise võimalused?

6) Millised tegurid võivad seada takistusi ja probleeme digitaalse komponendiga juhtumite käsitlemisel ja kuritegude uurimisel? (politseiorganisatsiooni sisemised vs välised tegurid) Millised on organisatsioonisisesed tegurid? Millised välised tegurid?

Küsimused kompetentsuse kriteeriumide määratlemise kohta politsei organisatsioonis. Huvitab, kuidas eksperdid näevad tänast politsei lähenemist digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks vajalike kompetentside kaardistamise protsessi võrreldes magistritöös välja töötatud raamistikuga.

7) Milline on politsei eriala digikompetentside spetsiifika kohaliku politseiüksuse uurija tasandil? Kas ja kuidas tuvastati Sisekaitseakadeemia poolt kohaliku tasandi (politseiüksuse) uurija vajadusi selles valdkonnas?

8) Millele tugineti politseiuurijate digikompetentse arendavate õppeprogrammide koostamisel ja õpiväljundite määratlemisel? Kas eristatakse erinevad kompetentsuse vajadused ja tasandid? Miks?

Küsimused kohaliku tasandi (politseiüksuse) uurijale digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks vajalikest kompetentsidest ja nende täpsemast jaotusest üld- ja kutsespetsiifilisteks kompetentsideks.

9) Milline võiks Teie hinnangul olla kohaliku tasandi (politseiüksuse) uurijtele vajalik digitaalsete võtmekompetentside komplekt politseiorganisatsiooni vaates? Kas on erisusi võrreldes teiste üksuste (funktsionaalüksuste, eri liikide kuritegudele spetsiliseeritud) uurijatega? /Märkus: teaduskirjanduses on toodud, et digitaalse komponendiga kuriteod, st küberkuriteod, on erineva iseloomu ja raskusastmega, ning küberkuritegevusele spetsialiseerunud üksuste uurijatele on nende teadmiste ja oskuste osas suuremad ootused. Kuidas Eestis sellega on?/

10) Milline on üldkompetentside roll digikomponendiga juhtumite käsitlemiseks vajalike kompetentside seas? Kas ja miks tugevate üldkompetentside olemasolu on oluline?

11) Millised kutsespetsiifilised kompetentsid (sh digikompetentsid) on vajalikud kohaliku tasandi (politseiüksuse) uurija digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks?

12) Millised on Teie hinnangul kompetentsipõhise lähenemise (juhtimise) tugevused ja nõrkused, kui kaaluda selle kasutamist (nt personali ametijuhendite ja tööde kirjelduste koostamisel, koolitusvajaduste kaardistamisel, õppeprogrammise koostamisel jms)? Palun põhjendage

13) Kas Teie hinnangul magistritöö raames välja töötatud kompetentsiraamistik võiks olla kasulik uurija vajalike digikompetentside kaardistamisel/määramisel? Mis osas? Palun põhjendage.

14) Millised lahendused Teie arvates aitaksid veel kohaliku tasandi (politseiüksuse) uurijate digitaalse komponendiga juhtumite lahendamiseks ja kuritegude uurimiseks vajalike kompetentside määratlemiseks ning vastavusse viimiseks ja/või parendamiseks?

KÜSIMUSTIK C.

Küsimused politsei välistele ekspertidele, kes erialaselt puutuvad kokku digikomponendi teemadega kriminaalmenetluses ja kohaliku politseiuurija tasandiga

Sissejuhatavad ja taustaküsimused:

- Mis valdkonda Te esindate? Kas ja kuidas lubate kajastada magistritöös Teie andmeid ja tausta?
- Kuidas on Teie valdkond seotud politseiuurijate ja/või nende kompetentsuse teemadega? Või milline on Teie kokkupuude politsei organisatsiooniga? Politseijaoskondade uurijatega?
- Kui kaua olete selle valdkonna ekspert olnud?
- Milline on teie haridustase ja valdkond?

Küsimused seoses digitaalse komponendiga juhtumite ja kuritegude ilmnemisega politseiuurijate töös ja nende mõjuga.

1) Kuidas ühiskonna digitaliseerumine on muutnud kohaliku tasandi (politseiüksuse) uurija töö iseloomu ja ülesandeid? Mis on selle juures positiivne ja mis negatiivne?

2) Mida Teile tähendab mõiste „digitaalne komponent“ uurija poolt lahendatava juhtumi või uuritava kuriteo juures? Palun tooge näiteid.

3) Milline on Teie arvates kõige parem digitaalse komponendiga juhtumi definitsioon? Kas ja mille poolest see eristub küberkuriteo definitsioonist? Miks? Kui see on keeruline, siis kuidas Te iseloomustaksite digitaalse komponendiga juhtumit ja kas see erineb küberkuriteost? Tooge mõned näited.

4) Kus te näete kitsaskohti nii uurijate poolt digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks oskusete omandamisel kui ka kompetentsinõuete kaasajastamisel?

5) Millised on Teie arvates nende kitsaskohtade maandamise võimalused?

6) Millised tegurid võivad seada takistusi ja probleeme digitaalse komponendiga juhtumite käsitlemisel ja kuritegude uurimisel? (politseiorganisatsiooni sisemised vs välised tegurid) Millised on organisatsioonisisesed tegurid? Millised välised tegurid?

Küsimused kompetentsuse kriteeriumite määratlemise kohta politsei organisatsioonis. Huvitab, kuidas eksperdid näevad tänast politsei lähenemist digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks vajalike kompetentside kaardistamise protsessi võrreldes magistritöös välja töötatud raamistikuga.

7) Millised on digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks kohaliku tasandi uurijale vajalike kompetentside kaardistamise võimalused?

8) Milline on politsei eriala digikompetentside spetsiifika kohaliku politseiüksuse uurija tasandil? Kuidas Teie seda näete?

Küsimused kohaliku tasandi (politseiüksuse) uurijale digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks vajalikest võtmekompetentsidest ja nende täpsemast jaotusest üld- ja kutsespetsiifilisteks kompetentsideks.

9) Milline Teie hinnangul võiks olla kohaliku tasandi (politseiüksuse) uurijtele vajalik digitaalsete võtmekompetentside komplekt politseiorganisatsiooni vaates? Kas on erisusi võrreldes teiste üksuste (funktsionaalüksuste, eri liikide kuritegudele spetsiliseeritud) uurijatega? /Märkus: teaduskirjanduses on toodud, et digitaalse komponendiga kuriteod, st küberkuriteod, on erineva iseloomu ja raskusastmega, ning küberkuritegevusele spetsialiseerunud üksuste uurijatele on nende teadmiste ja oskuste osas suuremad ootused/

10) Milline on üldkompetentside roll digikomponendiga juhtumite käsitlemiseks vajalike kompetentside seas? Kas ja miks tugevate üldkompetentside olemasolu on oluline?

11) Millised kutsespetsiifilised kompetentsid (sh digikompetentsid) on vajalikud kohaliku tasandi (politseiüksuse) uurija digitaalse komponendiga juhtumite käsitlemiseks ja kuritegude uurimiseks?

12) Millised on Teie hinnangul kompetentsipõhise lähenemise (juhtimise) tugevused ja nõrkused, kui kaaluda selle kasutamist (nt personali ametijuhendite ja tööde kirjelduste koostamisel, koolitusvajaduste kaardistamisel, õppeprogrammise koostamisel jms) politseis? Palun põhjendage

13) Kas Teie hinnangul magistritöö raames välja töötatud kompetentsiraamistik võiks olla kasulik uurija vajalike digikompetentside kaardistamisel/määramisel? Mis osas?

14) Millised lahendused Teie arvates aitaksid veel kohaliku tasandi (politseiüksuse) uurijate digitaalse komponendiga juhtumite lahendamise ja kuritegude uurimise kompetentside määratlemiseks ning vastavusse viimiseks ja/või parendamiseks?

Lisa 7. Ekspertide valim ja intervjuude läbiviimise ajakava

Intervjueeritava eksperdi tunnus	Eksperdi asutus	Tegevusvaldkond	Kogemus valdkonnas/ politseiorganisatsioonis/ kokkupuude politseiorganisatsiooniga	Haridus (tase/valdkond)	Intervjuu aeg ja koht/kanal	Intervjuu kestvus
Ekspert 1	PPA	Personali värbamis- ja koolitusteenus	7 aastat/ 16 aastat	Kõrgem, andragoogika	Skype rakenduse vahendusel	55 min
Ekspert 2	Sisekaitseakadeemia	Politsei eriala õppekava juht	5 aastat Sisekaitseakadeemias/ 1 aasta PPA arendusosakonnas / 5 aastat Siseministeeriumis politsei teemadega seonduvalt	Kõrgem, andragoogika (MA), sisejulgeolek (MA omandamisel)	Sisekaitseakadeemia	1 tund 14 min
Ekspert 3	PPA	Digikriminalistika keskuse juht	7 aastat küberkuritegude valdkonnas ja digikriminalistika keskuses	Kõrgem, IT	Skype rakenduse vahendusel	1 tund 29 min
Ekspert 4	PPA	Kokukonnasüütegude lahendamise teenuse omanik	4 aastat/ 27 aastat, sh 12 aastat kriminaalpolitseis	Kõrgem, sisejulgeolek	Skype rakenduse kaudu	1 tund 13 min
Ekspert 5	PPA	Kriminalistika teenuse omanik	5 aastat/ 15 aastat/ 12 aastat prokurörina	Kõrgem, juura	Skype rakenduse vahendusel	1 tund 3 min
Ekspert 6	Siseksitseakadeemia	Süüteomenetluse õppetool, õppejõud	7 kuud sisekaitseakadeemias/ 31 aastat (kriminaal-)politseis	Kõrgem, sisejulgeolek	Sisekaitseakadeemia	1 tund 36 min
Ekspert 7	Põhja Ringkonnaprokuratuur	abiprokurör	20 aastat prokurörina, neist 0,5 aastat küberkuritegude valdkonnas	Kõrgem, juura (MA)	Skype rakenduse vahendusel	50 min
Ekspert 8	Põhja Ringkonnaprokuratuur	abiprokurör	3,5 aastat prokurörina	Kõrgem, juura (MA)	Skype rakenduse vahendusel	55 min
Ekspert 9	Siseksitseakadeemia	Süüteomenetluse õppetool, õppejõud	4 aastat Sisekaitseakadeemias/ 15 aastat politseis (kuritegude uurimine)	Kõrgem, juura (MA)	Teams rakenduse vahendusel	1 tund 7 min
Ekspert 10	Põhja Ringkonnaprokuratuur	abiprokurör	15 aastat prokurörina	Kõrgem, juura (MA)	Skype rakenduse vahendusel	1 tund 7 min

Lisa 8. Uurimisküsimuste põhjal moodustatud ühine kategooriate ja koodide süsteem

Uurimisküsimus	Andmekogumismeetodiks on ekspertintervjuud A, B, C (vt lisa 6) ja dokumendianalüüsi valim (käesoleva töö lk 60)	Andmeanalüüsi kategooriad ja koodid
1) Millised on ühiskonna digitaliseerumisest tingitud aktuaalsed väljakutsed kohaliku tasandi uurijatele digitaalse komponendiga kuritegude uurimisel?	➢ Ekspertintervjuud, küsimused A1, A4, A6, B1, B4, B6, C1, C4, C6 ➢ Dokumendianalüüsi allikad D6, D7, D9	**1. Väljakutsed ja võimalused** 1.1 Politseiorganisatsiooni sisesed tegurid 1.2 Politeiorganisatsiooni välised tegurid 1.3 Takistuste ja kitsaskohtade ületamise võimalused 1.4 Digitaliseerumisega kaasnevad positiivsed muutused
2) Millised on digitaalse komponendiga kuriteod, mille lahendamisega tegelevad kohaliku tasandi politseiuurijad?	➢ Ekspertintervjuud, küsimused A2, A3, B2, B3, C2, C3	**2. Digikomponendiga juhtumid ja kuriteod** 2.1 Digikomponendi näited 2.2 Juhtumid ja kuriteod 2.3 Menetluspädevuse ja kompetentside ootuse erinevus kohalik tasand vs funktsionaalüksused)
3) Kuidas süstematiseerida kohaliku tasandi politseiuurijatele digitaalse komponendiga kuritegude uurimiseks vajalikke teadmisi ja oskusi?	➢ Ekspertintervjuud, küsimused A12, A13, A14, B9, B10, B11, C9, C10, C11 Dokumendianalüüsi allikad D1, D3, D4, D5, D6, D7, D8, D9, D10	**3a. Kompetentsiraamistiku välja töötamise meetod** 3.1a Tegelik olukord 3.2a Raamistiku korraldamise viis 3.3a Raamistiku koostamise etapid, elemendid
	➢ Ekspertintervjuud, küsimused A7, A8, A9, A1, A11, B7, B8, C7, C8 ➢ okumendianalüüsi allikad D2, D3, D4, D5, D6, D8, D9	**3b. Kohaliku tasandi uurija oodatavad kompetentsid** 3.1b Üldkompetentsid 3.2b Üld-digikompetentsid 3.3b Kutsespetsiifilised kompetentsid
4) Kuidas hindavad PPA, Sisekaitseakadeemia ja prokuratuuri esindajad magistritöös välja töötatud kompetentsiramistiku asjakohasust ja rakendusvõimalusi?	➢ kspertintervjuud, küsimused A5, A15, A16, A17, B5, B12, B13, B14, C5, C12, C13, C14	**4. Kompetentsiraamistiku rakendusvõimalused** 4.1 Kompetentsipõhise lähenemise tugevused 4.2 Kompetentsipõhise lähenemise nõrkused 4.3 Hinnangud ja arvamused magistritöös välja töötatud kompetentsiraamistiku kohta, rakendusvõimalused