

TARTU ÜLIKOOL

Sotsiaalteaduste valdkond

Ühiskonnateaduste instituut

Infokorralduse õppekava

Helena Velba

Ametnike ja nende lähedaste privaatsuse, eraelu ning identiteediga
seotud ohud avatud allikate luure (OSINT) ajastul: Politsei- ja
Piirivalveameti näitel

Lõputöö

Juhendaja: Maia Klaassen, MA

Kaasjuhendaja: Jaanika Merilo, MA

Tartu 2026

SISUKORD

SISSEJUHATUS	4
TERMINOLOOGIA.....	6
1. TEOREETILISED JA EMPIIRILISED LÄHTEKOHAD.....	7
1.1. Muutunud infokeskkond ja hübriidohud	7
1.1.1. Infooperatsioonid ja infosõda	8
1.2 OSINT mõiste ja rakendusvaldkonnad.....	10
1.2.1. OSINT mõiste.....	10
1.2.2. Rakendusvaldkonnad.....	11
1.2.3. OSINT praktikas, selle eelised ja puudused	12
1.2.4. Avatud allikate muutunud roll infokeskkonnas.....	13
1.3. Riskid avaliku sektori ametnikele	14
1.3.1. Ametnike nähtavus ja privaatsuse haavatavus.....	14
1.3.2. Seostamine ja tuvastatavus	15
1.3.3. Doxxing	17
2. METOODIKA	19
2.1. Uurimisviis ja valim	19
2.2. Andmekogumismeetod.....	20
2.3. Andmeanalüüs	20
2.4. Piirangud, eetika ja eneserefleksioon	21
3. TULEMUSED.....	23
3.1. OSINT-teadlikkus ning kasutuskogemus	23
3.1.1. Taust ja üldised erinevused riskitajus.....	23
3.1.2. OSINT mõiste tundmine, kasutusvaldkonnad ja olulisus.....	25
3.1.3. OSINT olulisus	26
3.2. OSINT riskid ja vastumeetmed	27
3.2.1. Riskitaju ametnike ja lähedaste suhtes	27
3.2.2. Peamised ohud ja kogemused juhtumitega.....	27
3.2.3. Riskide vähendamiseks kasutatavad vastumeetmed ja turvatunne.....	28

3.3. Asutuse roll ja OSINT-riskide käsitlemine strateegilisel tasandil.....	29
3.3.1. OSINT mõjutustegevuse kontekstis ja tajutus kasutus Eesti vastu	29
3.3.2. Asutuse roll ja OSINT-riskide käsitlemine strateegilisel tasandil.....	30
3.3.3. Juhised, koolitusvajadus ja ettepanekud.....	31
4. JÄRELDUSED JA EDASISED UURIMISSUUNAD	32
4.1. OSINT olemuse tajus	32
4.2. Riskid ja nende realiseerumine.....	33
4.3. Ametnike haavatavus ja asutuse roll OSINT käsitles	34
4.4. Järeldused ja edasised uurimissuunad	35
4.5. Ettepanekud	37
KOKKUVÕTE	39
SUMMARY	40
KASUTATUD KIRJANDUS	42
LISAD	49
Lisa 1. Saatekiri küsitluse läbiviimiseks	49
Lisa 2. Küsitluse vorm.....	50
Lisa 3. Kategoriseeritud vastuste näidis.	55

SISSEJUHATUS

Riigikaitse arengukava 2022–2031 toob hübriidohtude kasvu esile kui midagi, mis mõjutab Eesti julgeolekut (Riigikantselei, 2021: 30). Üha enam sõltub turvalisus sellest, mis toimub digitaalses infokeskkonnas ehk kuidas infot kogutakse, levitatakse ja kasutatakse. Ka Eesti küberturvalisuse strateegia rõhutab, et digiriigi kaitse eeldab head teadlikkust küberruumis toimuvast ning võimet mõista nii tehnoloogia arengut kui sellest tulenevaid uusi ohte (Majandus- ja Kommunikatsiooniministeerium, 2024: 11).

OSINT (*open source intelligence*) ehk avatud allikate luure tähendab avalikult kättesaadava teabe sihipärast kogumist, töötlemist ja analüüsimist eesmärgiga luua kasutatav teadmine või luureinfo (Merilo, 2025: 53). Kuigi avalikest allikatest info kogumine ei ole uus nähtus, on interneti ja digitehnoloogiate areng teinud selle varasemast oluliselt lihtsamaks, kiiremaks ja mahukamaks (Ünver, 2018: 4). Sellises raamistikus on OSINT muutunud vägagi praktiliseks töövahendiks. Antud lõputöö lähtekoht on, et just kogutud informatsiooni seostamise võimalus on määrav. Erinevatest keskkondadest kogutud infokillud saab kokku panna üheks tervikuks, mis muudab nii organisatsioonide kaardistamise kui isikute profileerimise oluliselt täpsemaks.

OSINT-i kasutatakse õiguskaitstes, julgeolekus, ajakirjanduses ja küberjulgeolekus ning sellel on oma väärtus. Samas võib see kasu ja võimekus muutuda riskiks. Avalikest allikatest kogutud infot saab kasutada sihtmärgistamiseks, mõjutamiseks, maine kahjustamiseks või tundliku info kogumiseks ja see pole kõik. Nagu rõhutab Ünver, võivad riigid ja organisatsioonid OSINT-ist saada sama palju kahju kui kasu, sest mõju sõltub kasutaja eesmärgist (Ünver, 2018: 6).

Avaliku sektori ametnike puhul on see küsimus kindlasti teravam. Demokraatia üks alustalasid ühiskonna koostöömiseks on läbipaistvus ning ametnikud tegutsevadki avalikes tingimustes ja peavad oma töö tõttu olema sageli nime, näo ja ametikohaga tuvastatavad. See loob olukorra, kus ametialast infot saab siduda eraelu tasandiga ehk isikuandmete, sotsiaalmeedia, registrite ja muude avalike allikatega. Selline seostamine võib paraku suurendada haavatavust lisaks ametnikule ka tema lähedasi.

Oluline on teadvustada, et ametnik ei tegutse oma ametis isiklikust huvist, vaid täidab asutuse ülesandeid ja talle pandud kohustusi. Seetõttu ei ole identiteedi-, privaatsuse- ja turvariskid ainult individuaalne mure, kuna nende mõju võib ulatuda asutuse toimimise, töötajate turvatunde ja julgeolekuni.

Kuigi OSINT-i kasutusvõimalusi käsitlev kirjandus on mahukas, on vähem uuritud, kuidas tajuvad OSINT-ist tulenevaid ohte ametnikud ise. Eriti vähe tähelepanu on pööratud sellele, kuidas digitaalne nähtavus ja avalike andmete seostatavus mõjutavad ametnike turvatunnet ning milliseid kaitsemeetmeid vajatakse organisatsiooni tasandil.

Lõputöö eesmärk on analüüsida OSINT-ist tulenevaid võimalikke ohte avaliku sektori ametnike identiteedile, privaatsusele ja turvalisusele ning kaardistada ametnike teadlikkust, riskitaju ja hinnanguid seniste kaitsemeetmete tõhususele. Töö põhineb Politsei- ja Piirivalveameti (PPA) ametnike seas läbi viidud ankeetküsitlusel (n = 90), mille tulemusi tõlgendatakse laiemas julgeoleku- ja infokeskkonna kontekstis.

Uurimisküsimused on järgmised:

1. Kui teadlikud on PPA ametnikud OSINT-i võimalustest ja ohtudest?
2. Milliseid riske võivad OSINT-ist tulenevad ohud põhjustada ametnike identiteedile, privaatsusele ja turvalisusele?
3. Milline võiks olla Eesti riigiasutuste roll OSINT-ist tulenevate identiteedi- ja privaatsusriskide ennetamisel?

Töö tulemused aitavad paremini mõista, kuidas muutunud infokeskkond mõjutab avaliku sektori ametnike turvalisust ning millist rolli võiksid riigiasutused täita ametnike identiteedi- ja privaatsusriskide ennetamisel.

TERMINOLOOGIA

Käesolevas töös on keskseks terminiks OSINT, mis tähendab avalikult kättesaadava teabe sihipärast kogumist ja kasutamist, et kujundada olukorrast või sihtmärgist kasutatav ülevaade. OSINT-i sisendiks võib olla nii ametlik avalik info kui ka igapäevaselt kasutatav allikas. Sellise tegevuse tagajärjel tekib digitaalne jalajälg, *st* tegevuse käigus teadlikult ja ka tahtmatult tekkivad andmed nagu postitused, metaandmed ja kontode seosed, mida saab koondada ja analüüsida (Eesti Keele Instituut, 2026). Tekkinud andmestiku põhjal kujuneb omakorda **digitaalne identiteet**, mis seob elektroonilises keskkonnas inimese tema füüsilise isikuga ja võimaldab temast koostada andmepõhise pildi ehk profiili (Eesti Keele Instituut, 2026).

Privaatsust mõistetakse siin eeskätt kui kontrollmehhanismi ehk kuidas inimese kohta käivat infot kogutakse ja kasutatakse, ning turvalisust kui kaitstust olukordades, kus OSINT teel saadud teave võib toetada mõjutamist, ähvardamist, ründe ettevalmistamist (Eesti Keele Instituut, 2026). Lõputöös kasutatakse mõistet **identiteedikaitse** rakenduslikus tähenduses, pidades silmas ametniku tuvastatavuse vähendamist ja privaatsuse ning turvalisuse kaitset OSINT-riskide vaates. *Sh* riskid võivad laieneda ka ametnike lähedastele, keda käsitletakse **pehmete sihtmärkidena** (*soft targets*), kuna nende kaudu on võimalik avaldada survet ametnikule (*Oxford Dictionaries*, 2014).

OSINT-ist tuletatud teavet kasutatakse tänapäeval aktiivselt ka infooperatsioonides, infosõjas ja hübriidohtude raamistikus, kus avalik info, desinformatsioon ja mõjutusvõtted teenivad strateegilisi eesmärke (Eesti Keele Instituut, 2026). Käesolevas töös mõistetakse **infooperatsioone** laiema, kui sihtrühmade mõjutamisele suunatud tegevusi. NATO (*North Atlantic Treaty Organization*) käsitluses on infooperatsioonid raamistik, mis aitab mõista infokeskkonda ja sihtrühmi ning kavandada tegevusi teatud mõju saavutamiseks, toetades samal ajal laiemat operatsioonide planeerimist (*North Atlantic Treaty Organization*, 2023: 67).

Tehisintellekt, tarkvara või süsteemi abil andmete ja algoritmide ülesannete täitmine (Eesti Keele Instituut, 2026) on lõputöös oluline, kuna see võib kiirendada andmete kogumist ja analüüsi ning lihtsustada manipuleeritud sisu loomist, mis omakorda mõjutab OSINT-ist sellest tulenevaid riske.

1. TEOREETILISED JA EMPIIRILISED LÄHTEKOHA

Käesolev peatükk avab lõputöö teoreetilise ja empiirilise lähtekoha ja selgitatakse töö keskset raamistikku, mille abil käsitletakse OSINT-ist tulenevaid riske ametnike identiteedile, privaatsusele ja turvalisusele. Peatükk algab infokeskkonna üldisest teadlikkusest ja liigub edasi hübriidohtude kirjeldusest OSINT-i riskimehhanismideni.

1.1. Muutunud infokeskkond ja hübriidohud

Infokeskkonna muutus ei ole ainult tehnoloogiline areng, vaid muudab ka seda, kuidas riske tajutakse ja kuidas neid praktikas kasutatakse. Seetõttu tuleb siduda infokeskkonnas toimuv hübriidohtude loogikaga ja mida see tähendab avaliku sektori ametnike jaoks. Fookus antud alapeatükis ei ole interneti olemusel, vaid sellel, kuidas avalik info ja selle andmete seostatavus muudavad sihtmärgistamise lihtsamaks, eriti avaliku sektori ametnike puhul, kes on antud töö keskmes.

Interneti areng on suurendanud avalikest allikatest pärineva teabe hulka ning muutnud info kättesaadavuse (Dokman ja Ivanjko, 2020: 192). Koos sellega on kujunenud võrguühiskond, kus info loomine ja levitamine ei ole enam tsentraliseeritud ning avalikult kättesaadav teave hõlmab lisaks ametlikele andmetele ka inimeste igapäevast tegevust, suhtlusmustreid ja käitumisharjumusi (Vihalemm jt, 2017: 279). Just sealt saab alguse selline infokeskkond, mis võimaldab OSINT-i abil siduda eri allikatest pärinevaid andmeid ning koostada detailseid profile, mis omakorda võib suurendada ametnike privaatsus- ja turvariske.

Infokeskkonna muutus tähendab ühtlasi, et avalikku teavet on lihtsam leida, koondada ja analüüsida, seega ka aina keerukam tuvastada infohäireid ja -manipulatsioone. Internet võimaldab teabele ligipääsu väheste piirangutega ning toetab info kiiret levikut ja kasutamist (Glassman ja Kang, 2012: 673). Samal ajal on digitaalse andmehalduse areng muutnud avaliku teabe mahu ja kättesaadavuse varasemast oluliselt suuremaks (Block, 2024: 95). Seetõttu on informatsioon ühtaegu ressurss ja potentsiaalne ohuallikas, andmetele on ligipääs sisuliselt igaühel.

Privaatsuse ja turvalisuse küsimused muutuvad sellises keskkonnas järjest olulisemaks. Tikk rõhutab, et infoühiskonnas on keskseks küsimuseks indiviidi informatsiooniline enesemääramine ja privaatsuse kaitse (Tikk, 2007: 2). Bambaueri järgi tähendab privaatsus soovitud kontrolli informatsiooni üle, turvalisus aga mehhanisme, millega seda kontrolli tagatakse (Bambauer, 2013:

669–676). Seetõttu võivad avalikest allikatest kogutud ja seostatud andmed kujutada riski nii üksikisikule kui ka organisatsioonile.

Avaliku sektori ja õiguskaitse vaates lisandub siia praktiline mõõde. OSINT võib pakkuda õiguskaitse- ja julgeolekuasutustele olulist võimekust avalikest allikatest pärineva info kogumiseks ja analüüsimiseks (Akhgar, 2017). Sarnaseid meetodeid saab kasutada ka ametnike vastu – näiteks mõjutamiseks, sihtmärgistamiseks või rünnete ettevalmistamiseks.

Eesti kontekstis on see eriti oluline, kuna Eesti on tuntud digiriik, kus teenused, registrid ja andmevahetus toimuvad suures osas digitaalselt (Majandus- ja Kommunikatsiooniministeerium, 2021: 6). Kuigi digitaalsed lahendused toetavad riigi toimimist ja haldussuutlikkust, võivad need samaaegselt suurendada võimalusi koguda ja seostada avalikest allikatest pärinevat teavet. Seda enam on oluline leida lahendus andmete kaitseks – digiriigi tugevuseks võiks olla ka isikuandmete kaitse ja nende põhjendatud mõõdukas avaldamine või piiramine.

Julgeolekukeskkonna muutumisega seoses on Eestis rõhutatud, et ohud ei avaldu üksnes sõjaliste rünnakutena, vaid võivad väljenduda ka küberrünnete, mõjutustegevuse ja muu mittesõjalise survena (Riigikantselei, 2021: 3). Digitaalse infokeskkonna avatus ja info laialdane kättesaadavus võivad selliseid tegevusi soodustada (Ünver, 2018: 7).

Tehisintellekti areng võimendab neid suundumusi veelgi. AI võib kiirendada haavatavuste leidmist, toetada sihitud ründeid ning muuta valeinfo loomise ja levitamise lihtsamaks, sealhulgas süvavõltsingute abil (Xu jt, 2023: 6). Samal ajal võimaldavad automatiseeritud OSINT-tööriistad koguda ja töödelda väga suuri andmemahtusid (Oerlemans ja Langenhuijzen, 2025: 582). See suurendab ka info väärkasutuse ja eksituste riski.

Seega ei käsitleta töös hübriidohte eraldiseisva nähtusena, vaid infokeskkonna loogilise jätkuna ehk mida rohkem on avalikku infot ja mida lihtsam on seda töödelda, seda suurem on võimalus seda kasutada ka pahatahtlikult. Avaliku sektori ametnike puhul lisandub siia rollipõhine nähtavus, mis teeb nad infokeskkonnas paremini kaardistatavaks ja seetõttu ka haavatavamaks. Järgmistes alapeatükkides avatakse OSINT-ist tulenevaid riske juba konkreetsemalt.

1.1.1. Infooperatsioonid ja infosõda

Hübriidohtudeks peetakse ohte, milles kombineeritakse konventsionaalseid, irregulaarseid ja küberruumi vahendeid strateegiliste eesmärkide saavutamiseks (Eesti Keele Instituut, 2026).

Praktikas võivad hübriidohud avalduda desinformatsiooni, küberrünnakute, luuretegevuse, majandusliku surve või muu koordineeritud mõjutustegevusena, mille eesmärk on mõjutada vastase otsuseid, vähendada usaldust institutsioonide vastu ning destabiliseerida ühiskonda (Sazonov jt, 2020: 11). Hübriidohtude levikut saadab edu, kuna digikeskkonnas levib info kiiresti, mis loobki soodsa pinnase sihipärasteks mõjutusoperatsioonideks (Ünver, 2018: 20).

Muutunud infokeskkonnas on infooperatsioonid ja infosõda kujunenud hübriidohtude oluliseks osaks, kus informatsiooni kasutatakse mõjutamiseks. Sellises raamistikus võib avalik teave muutuda strateegiliseks ressursiks ning avaliku sektori ametnikud võivad ametialase nähtavuse tõttu kujuneda mõjutustegevuse sihtmärkideks.

Autoritaarsete režiimide puhul kasutatakse infokeskkonna mõjutamist sageli sihipärase vahendina valitsemiseks. Eesmärk on kujundada avalikku arvamust, hoida kontrolli narratiivide üle ja mõjutada sihtrühmade käitumist. Van der Vet kirjeldab, et kaasaegsed autoritaarsed režiimid rakendavad infokontrolli, massjälgimist ja desinformatsiooni võimu hoidmiseks ning avaliku arvamuse suunamiseks (Van der Vet, 2021: 408). Gurkovi järgi kasutatakse Venemaal internetijärelevalvet ja infokontrolli poliitilise mõjuvõimu tugevdamiseks ning inforuumi kontrollimiseks (Gurkov, 2020: 96), mille eesmärk on kujundada avalikku arvamust nii riigisiselt kui ka rahvusvaheliselt (Bradshaw ja Howard, 2017; viidatud Van der Vet, 2021: 408).

Infooperatsioonides ongi keskseks ressursiks sageli avalik teave ja sellele antavad reaktsioonid. Avalikult kättesaadavad andmed, sotsiaalmeedia sisu ja inimeste tegevusmustrid internetis võimaldavad isikuid kaardistada, hinnata nende haavatavusi ning kujundada sihitud mõjutustegevust. Seetõttu võivad ametnikega seotud andmed ning nende lähedaste seostatavus muutuda mõjutusoperatsioonide tööriistaks.

Kaasaegsete konfliktide käsitluses rõhutatakse üha enam mittesõjaliste mõjutusvahendite tähtsust. Gerassimovi doktriini käsitluses peetakse informatsioonilist mõjutamist, küberoperatsioone ja muid mittesõjalisi meetodeid tänapäeva konfliktides vähemalt sama oluliseks, kui otsest sõjalist jõudu (Fridman, 2019: 106–107). See viitab, et konfliktid kanduvad üha enam infokeskkonda, kus mõjutatakse ühiskonna hoiakuid, usaldust ja otsustusprotsesse. Sellise loogika järgi võib sihtmärgiks kujuneda ka ametnike usaldusväärsus ja avalik kuvand, sest nende kaudu mõjutatakse laiemalt usaldust riigiasutuste vastu. Ukraina kogemus osutab, et infooperatsioonid võivad olla suunatud institutsioonide ja ametnike usaldusvääruse õõnestamisele, kus eesmärk ei ole ainult valeinfo levitamine, vaid usalduse vähendamine riigi ja selle esindajate vastu, et kujundada soodne pinnas edasiseks mõjutustegevuseks.

Mõjutustegevus ei ole üksnes teoreetiline risk, vaid tänapäeva reaalsus. Kaitsepolitseiameti aastaraamatus on kirjeldatud juhtumeid, kus infosõja ja mõjutustegevusega seotud tegevused on olnud suunatud Eesti avaliku ruumi ja institutsioonide mõjutamisele (Kaitsepolitsei aastaraamat, 2026: 8–9). Samuti näitab Svetlana Burceva kohtuasi, et mõjutustegevus võib toimuda ka näiliselt tavapärase info- ja meediategevuse kaudu (Siplane, 2025). Need näited illustreerivad, et avaliku info, narratiivide ja digitaalsete kanalite kasutamine võib kujuneda osaks laiemast mõjutus- ja julgeolekukeskkonnast.

Eesti julgeolekukeskkonna vaates tähendab see vajadust arvestada ja eeldada, et mõjutustegevuse sihtmärgiks võivad kujuneda ka riigiasutused ja ametnikud. Kui usaldust ametnike ja institutsioonide vastu vähendada, võib see mõjutada riigi toimimist laiemalt. Seetõttu ei kujuta ametnikega seotud avalikud andmed endast üksnes privaatsusrisiki, vaid võivad infooperatsioonide kontekstis muutuda julgeolekuküsimuseks, kui neid kasutatakse negatiivse mõjutamise eesmärgil.

Lõputöö kontekstis seostuvad infooperatsioonid otseselt OSINT-ist tulenevate riskidega. Mida rohkem on avalikku infot ja mida lihtsam on seda koguda, seostada ja analüüsida, seda suurem on võimalus kasutada seda pahatahtlikult. Avaliku sektori ametnike nähtavus muudab nad infokeskkonnas paremini haavatavamaks erinevatele mõjutamistele ja privaatsusrikkumistele.

1.2 OSINT mõiste ja rakendusvaldkonnad

Selles alapeatükis määratletakse avatud allikatel põhineva luure (OSINT) mõiste ning käsitletakse selle kasutusvaldkondi ja rolli tänapäevases julgeolekukeskkonnas. OSINT-i käsitletakse meetoodilise lähenemisena, mille keskmes on avalikest allikatest pärit teabe sihipärane otsimine, kogumine, seostamine ja analüüs. OSINT ei piirdu üksnes riikliku luure või sõjalise valdkonnaga, vaid on laialdaselt kasutusel ka teistes valdkondades. OSINT võib toetada nii turvalisuse tagamist kui ka pahatahtlikke eesmärke (Hwang jt, 2022: 2).

1.2.1. OSINT mõiste

Robert David Steele määratleb OSINT-i kui sihipäraselt avastatud, töödeldud ja levitatud informatsiooni kindlale sihtrühmale (Steele, 2006: 129). Antud töös lähtutakse sellest käsitlusest, et OSINT ei ole lihtsalt avalik teave, vaid protsess, mille käigus avalikest allikatest pärinev info muudetakse kasutatavaks teadmiseks. Seetõttu hõlmab OSINT lisaks andmete leidmisele ka nende kogumist, hindamist, seostamist ja analüüsi sarnaselt luuretsüklile.

Koops jt käsitlevad OSINT-i avatud allikatest pärinevate andmete kogumise, analüüsi ja kasutamisenä luure eesmärgidel ning rõhutavad, et andmete avalik kättesaadavus ei tähenda nende piiranguteta töötlemise lubatavust ehk OSINT-i kasutamisel võivad tekkida õiguslikud ja privaatsusega seotud küsimused (Koops jt, 2013: 677). See on oluline teadmine, sest avaliku info kasutamine puudutab ka vastutust ja reegleid.

Hwang jt kirjeldavad OSINT-i kui avatud allikatest pärineva teabe süstemaatilist otsimist, kogumist ja töötlemist, mille eesmärk on muuta killustatud info analüütiliselt kasutatavaks teadmiseks (Hwang jt, 2022: 1–3). Seetõttu annab OSINT andmetele uue tähenduse ja kasutusvõimalusi.

Tänapäevases infokeskkonnas on OSINT-i ulatus kindlasti laienenud. Traditsioonilise avaliku teabe kõrval kasutatakse üha enam ka kommertsallikaid, lekkinud andmeid ning digitaalseid jälgi (nt asukohaandmed ja sotsiaalmeedia tegevus), mis suurendab võimalusi inimeste tuvastamiseks ja profileerimiseks (Oerlemans ja Langenhuijzen, 2025: 581). Sellest vaatenurgast ei ole keskne ainult see, kas info on avalik, vaid kui lihtsaks on tehtud erinevate allikate kombineerimine.

Walkow ja Pöhn rõhutavad, et identiteediga seotud OSINT võimaldab süstemaatiliselt koguda ja analüüsida inimese kohta käivat infot, et tuvastada võimalikke haavatavusi ja ründevektoreid (Walkow ja Pöhn, 2024). Mida rohkem andmekilde on võimalik omavahel siduda, seda detailsemaks muutub isiku digitaalne profiil ning suureneb oht, et kogutud infot kasutatakse sotsiaalseks manipuleerimiseks, kontode seostamiseks või identiteedi kuritarvitamiseks. Kindlasti ei ole tegemist vaid teoorial baseeruvaga, vaid juba realselt aset leidnud juhtumitega.

Käesolevas töös käsitletakse OSINT-i seetõttu ühtaegu analüüsi- ja uurimisvahendi ning riskina. Avalik või killustatud teave võib seostamise kaudu muutuda praktiliseks ohuks.

1.2.2. Rakendusvaldkonnad

OSINT-i saab käsitleda luurepraktika osana, sest see toetab luureprotsessi põhietappe – info otsingut, kogumist, analüüsi ja levitamist. Phythiani järgi kasutatakse luuretsükli eri allikaid ja tehnoloogilisi vahendeid ning OSINT eristub teistest luurevormidest eelkõige seetõttu, et tugineb avalikult kättesaadavale teabele (Phythian, 2013: 17–18). Keeni käsitluses on luuretsükli keskmes info avastamine, tõlgendamine ja analüüs otsustamise toetamiseks (Keen, 1977: 317). Sellest vaatenurgast ei seisne OSINT-i väärtus üksnes info leidmises, vaid selles, kuidas avalikest allikatest kogutud andmed muudetakse otsuseid toetavaks teadmisteks.

Praktikas ei piirdu OSINT siiski luure- ja julgeolekuasutustega. Avalikest allikatest pärineva teabe kogumist ja analüüsi kasutatakse laialdaselt õiguskaitstes, ajakirjanduses, akadeemilises uurimistöös, ettevõtetes ja küberjulgeolekus (Hwang jt, 2022: 4–5). Nii toetab OSINT ajakirjanduses faktikontrolli ja uurivat tööd, õiguskaitstes kuritegude ennetamist ja isikute tuvastamist ning küberjulgeolekus ohtude ja haavatavuste avastamist (*OpenAI*, isiklik suhtlus, 20.04.2026). Ettevõtetes kasutatakse seda riskihindamiseks, konkurentsiolukorra mõistmiseks. Seega on OSINT pigem laiem meetod avaliku info süstematiseerimiseks ja analüüsiks, mitte kitsalt spionaaži tööriist.

Lõputöös on keskne just õiguskaitse ja riiklik julgeolek, sest selles valdkonnas puutuvad OSINT-i töövõtted otseselt kokku ametnike identiteedi, privaatsuse ja turvalisusega. OSINT võib küll aidata parandada olukorrateadlikkust, seostada isikuid ja võrgustikke ning ennetada ohte, kuid sama loogika töötab ka vastupidises suunas.

Õiguskaitse kontekstis nähakse OSINT-i olulise vahendina luurevõimekuse täiendamisel ja analüütilise sisendi loomisel (Akhgar, 2017). Samal ajal on püsiv probleem avalike allikate usaldusväärsus. Benes osutab, et OSINT-i piiranguks võivad olla vää- ja desinformatsioon (Benes, 2013: 24), seetõttu sõltub OSINT-i väärtus metoodikast, info kontrollimisest ja analüütilisest kompetentsist (Hulnick, 2002: 565; Van Puyvelde ja Rienzi, 2023: 533).

Laiemas plaanis peegeldab OSINT-i laialdane kasutus muutunud infokeskkonda. Avalik teave ei ole enam üksnes taustainfo, vaid ressurss, mida saab kiiresti koguda, seostada ja kasutada erinevatel eesmärkidel. Just seostamise võimekus on käesoleva töö seisukohalt määrav, sest see selgitab, miks näiliselt killustatud avalik info võib ametnike ja nende lähedaste puhul muutuda riskiks.

1.2.3. OSINT praktikas, selle eelised ja puudused

OSINT-i praktilist väärtust kinnitavad mitmed tuntud juhtumid. Bellingcat tuvastas 2014. aastal avatud allikate abil Vene üksuse, mis seostus MH17 lennuki allatulistamisega Ukrainas (Ünver, 2018: 15). Õiguskaitse kontekstis toob Rahman näite Bostoni maratoni pommirünnaku uurimisest, kus avalikest allikatest kogutud fotod, videod ja sotsiaalmeediapostitused aitasid kahtlustatavaid tuvastada ja liikumisteede rekonstrueerida (Rahman, 2025: 26). Sarnast loogikat kirjeldab ka *Molfar Intelligence Institute*, kus erinevate avalike andmete ja geolokatsiooniandmete ristkasutus võimaldas tuvastada Bucha rüüstamisega seotud isikud (*Molfar Intelligence Institute*, 2023).

Need näited toovad selgelt esile OSINT-i tuuma, kus killustatud andmete seostamine võimaldab rekonstrueerida sündmusi, luua seoseid ja tuvastada isikuid. Sama mehhanism on lõputöö kontekstis ühtlasi riskiallikas, sest pahatahtlikus kasutuses võib seostamine muutuda mõjutamise, jälgimise ja sihtmärgistamise vahendiks.

OSINT-i eelised tulenevad eelkõige avaliku info kättesaadavusest ja suurest andmemahust. Avalikest allikatest pärinev info toetab olukorrateadlikkust ja riskihindamist ka siis, kui muud allikad pole kättesaadavad (Hwang jt, 2022: 4). Samal ajal kaasnevad OSINT-iga olulised piirangud. Suure andmemahu tõttu võib olla keeruline eristada usaldusväärset infot ning ilma piisava kontekstita võivad järeldused osutuda ekslikuks (Hulnick, 2002: 565). Van Puyvelde ja Rienzi rõhutavad, et OSINT-i eristab juhuslikust info kogumisest just valideerimine, analüüs ja kontekstualiseerimine (Van Puyvelde ja Rienzi, 2023: 533) ehk oluline on hinnata ka informatsiooni usaldusväärsust ja allikaid.

Praktikas toetavad OSINT-i erinevad tööriistad ja tehnikad, mis aitavad avalikke andmeid koguda, korrastada ja seostada. Näiteks *Maltego* tööriist võimaldab visualiseerida isikute ja organisatsioonide seoseid, *Shodan* otsida internetiga ühendatud seadmeid ning *theHarvester* koguda avalikke e-posti aadresse ja domeeniandmeid (Chauhan ja Panda, 2015). Lisaks kasutatakse geolokatsiooni ja metaandmete analüüsi, et tuvastada isikute või objektide asukohti. See vaid kinnitab, et OSINT ei ole üksnes teoreetiline võimalus, vaid praktiline võimekus, mille mõju sõltub eesmärgist ja kasutusviisist.

1.2.4. Avatud allikate muutunud roll infokeskkonnas

Pärast Venemaa täiemahulise sissetungi algust Ukrainasse 2022. aastal on OSINT-i kasutamine märgatavalt kasvanud ning seda on rakendatud operatiivse info kogumiseks ja sündmuste dokumenteerimiseks ka olukordades, kuhu füüsiline ligipääs puudub (Formanchuk, 2025: 268). See näitab, et OSINT ei täida enam ainult taustainfo rolli, vaid võib kriiside ja konfliktide kontekstis toetada olukorrateadlikkust, tõendite kogumist ja sündmuste rekonstrueerimist.

Samas tekitab teaberohe ja kiiresti muutuv infokeskkond küsimuse, kuidas kogutud infot hinnata ja tõlgendada selliselt, et seda saaks usaldada. Seiler rõhutab, et infopädevus tähendab võimet infot kriitiliselt hinnata ja eetiliselt kasutada (Seiler, 2024: 46). Suur andmemahut muudab usaldusväärse analüüsi aina väljakutsuvamaks.

Küberjulgeoleku vaates võimaldab OSINT koguda ja analüüsida infot võimalike ohtude, pahatahtliku tegevuse ja ründeviiside kohta (Huang jt, 2021: 776–777). Risk ei teki sageli ühest

avalikust infokillust, vaid sellest, kui eri andmed omavahel seostatakse ja neist kujuneb terviklik pilt inimesest, organisatsioonist või tegevusest (Huang jt, 2021: 787). Sama loogika teeb OSINT-ist ühtaegu kasuliku töövahendi ja võimaliku haavatavuse allika. Hulnick rõhutab, et ilma laiemat konteksti mõistmata võib avalikest allikatest kogutud info tõlgendamine viia ekslike järeldusteni (Hulnick, 2002: 565).

Eesti kontekstis raamivad OSINT-i kasutamist lisaks tehnoloogiale ka õiguslikud ja institutsionaalsed tingimused. Avalikkuse ja läbipaistvuse põhimõtted tulenevad põhiseadusest ja avaliku teabe seadusest, samal ajal seavad isikuandmete kaitse ja riigi julgeolekuga seotud piirangud andmete kasutamisele piirid (Eesti Vabariigi põhiseadus, 2026; Avaliku teabe seadus, 2026; Isikuandmete kaitse seadus, 2026). Seetõttu võib ka õiguspäraselt avalikustatud teave koondamisel ja riskasutusel suurendada tuvastatavust ning võimendada privaatsus- ja julgeolekuriske.

Muutunud infokeskkonnas ei sõltu risk enam ainult sellest, millist infot avaldatakse, vaid ka sellest, kuidas avalikke andmeid seostatakse ja milline uus tähendus nende põhjal tekib. Seetõttu võib OSINT toimida “kahe teraga mõõgana”. See toetab küll turvalisust ja olukorrateadlikkust, kuid loob samal ajal võimalusi väärkasutuseks (Hwang jt, 2022: 2).

1.3. Riskid avaliku sektori ametnikele

Järgnevas peatükis keskendutakse täpsemalt OSINT-ist tulenevatele riskidele riigisektori ametnike vaatest, käsitledes nii nähtavuse, läbipaistvuse kui ka sihitud rünnakute ja *doxxingu* fenomeni. Samuti tuuakse esile OSINT-iga kaasnevad väljakutsed, sealhulgas operatiivtasandi turvalisuse küsimused.

1.3.1. Ametnike nähtavus ja privaatsuse haavatavus

Korrakaitseseaduse § 11 lg 1 kohaselt peab riikliku järelevalve meetmeid kohaldav ametiisik end selgelt tutvustama ning vajadusel tõendama oma pädevust (Korrakaitseseadus, 2026). See tähendab, et näiteks politseiametnikud peavad tööülesannete täitmisel olema avalikult tuvastatavad nime, näo ja ametikoha kaudu, et tagada õiguspärane ja läbipaistev tegevus.

Samas suurendab selline rollipõhine nähtavus vastuolusid ja haavatavust OSINT-keskkonnas. Digikeskkonnas tegutsevad samad inimesed, kelle käitumist mõjutavad emotsioonid, huvid ja motiivid, kuid internet muudab info kogumise, seostamise ja levitamise oluliselt lihtsamaks ning mõjusamaks (Kim jt, 2011: 676). Kuigi PPA struktuur ja isikkoosseis on Politsei ja piirivalve

seaduse kohaselt asutusesiseseks kasutamiseks mõeldud teave (Politsei ja piirivalve seadus, 2025), võib ametnik oma tööülesannete tõttu muutuda avalikult tuvastatavaks. Siin tekibki vastuolu, kus läbipaistvuse nõue on vajalik, kuid sama nähtavus võib suurendada ametniku privaatsus- ja turvariske.

OSINT võimaldab eri allikatest pärinevaid infokilde siduda ning luua detailseid profile inimese töö, eraelu, kontaktide ja harjumuste kohta. Nii võivad kasvada sotsiaalse manipuleerimise ja sihitud rünnakute riskid. Kim jt osutavad, et privaatsusohud ei pea väljenduma ainult nähtavas kahjus, vaid võivad avalduda ka vaimses surves ja psühholoogilises mõjus, mis tekib isikuandmete leviku või väärkasutuse tõttu (Kim jt, 2011: 676). Riskid ei piirdu seejuures alati ametnikuga, vaid võivad laieneda ka tema lähedastele.

Privaatsusriskide vähendamiseks kasutatakse infosüsteemides anonümiseerimist ja pseudonümiseerimist, mille eesmärk on takistada andmete otsest seostamist konkreetse isikuga (Rai jt, 2021: 1). Sama loogika aitab mõtestada ka ametnike nähtavust. Probleem ei ole ainult üksikus avalikus infos, vaid selles, et allikatest info koondamine võib muuta inimese tuvastatavaks ka siis, kui iga infokild eraldi tundub kahjutu.

Ametnike nähtavus ei tähenda siiski eraelu kaitse kadumist. Põhiseaduse § 26 kohaselt on igaühel õigus era- ja perekonnaelu puutumatusel (Eesti Vabariigi põhiseadus, 2026). Samal ajal põhineb avaliku sektori tegevus läbipaistvusel, mida rõhutab Euroopa Liidu toimimise lepingu artikkel 15 (Euroopa Liidu Teataja, 2016: 23). Praktikas tähendab see tasakaalustamise vajadust, et ühelt poolt on avalikkuse huvi ja kontroll, teiselt poolt aga on oluline ka ametnike privaatsus ja turvalisus.

Digitaalses infokeskkonnas on piir avaliku ja eraelu vahel muutunud hägusamaks. Harro-Loit märgib, et privaatsuse tähendus ning arusaam eraelu piiridest on ajas muutunud (Harro-Loit, 2010: 107–108). Seetõttu võib ka ametialaselt avalik info OSINT-i abil hakata toimima osana eraelu puudutavast profiilist. Probleem ei ole ainult selles, milline info on avalik, vaid selles, kuidas eri andmeid seostatakse ja milline uus tähendus nende põhjal tekib.

1.3.2. Seostamine ja tuvastatavus

OSINT-i võimalused ei piirdu avaliku info leidmisega nagu eelnevalt kirjeldatud. Keskne on see, kuidas eri allikatest pärit teave kokku viiakse ja milleks seda kasutatakse. Avalikult kättesaadavate andmete kombineerimine võimaldab luua detailseid profile nii asutuste kui ka üksikisikute kohta, sh tuvastada seoseid, liikumismustreid, tööga seotud rolle ja igapäevaharjumusi. Õiguskaitse- ja

julgeolekuasutuste töötajad tegutsevad seejuures samas digikeskkonnas, kus avalik teave võib olla korraga töövahend ja haavatavus (*OpenAI*, isiklik suhtlus, 07.05.2026).

OSINT-i kasutatakse õiguspäraselt uurimiste toetamisel, olukorrateadlikkuse parandamisel ja riskide hindamisel, kuid samu võtteid saavad kasutada ka pahatahtlikud osapooled. Kim jt rõhutavad, et isikuandmeid kogutakse sageli just avalikult kättesaadavaid profile, postitusi ja andmeid süstemaatiliselt koondades (Kim jt, 2011: 677–678). Seetõttu võib näiliselt ebaoluline info muutuda probleemiks siis, kui eri allikad seotakse üheks tervikpildiks.

Eesti kontekstis kinnitab selliste riskide reaalsust näiteks PPA poolt avaldatud juhtum, kus ametnikku ja tema perekonda ähvardati ametialase otsuse tõttu (Politsei- ja Piirivalveamet, 2022). See näitab, et sihtmärgiks ei pruugi kujuneda ainult ametnik, vaid ka tema lähedased, kelle kaudu saab avaldada survet või tekitada hirmu. Seega ei saa rääkida antud lõputöö kontekstis vaid teoreetiliselt juhtuda võivast, kuna sarnaseid juhtumeid on juba aset leidnud.

Seostamise ulatust illustreerivad ka rahvusvahelised näited. Ünver kirjeldab, kuidas spordirakenduse *Strava* kasutajate globaalsed GPS-andmed paljastasid tundlikku asukohateavet ning võimaldasid kaardistada liikumismustreid (Ünver, 2018: 16). Oerlemans ja Langenhuijzen rõhutavad, et asukohaandmed on eriti tundlikud, sest nende abil saab järeldada inimese igapäevaelu ja harjumusi (Oerlemans ja Langenhuijzen, 2025: 587). Sellised riskid ei puuduta ainult sõjalisi objekte või kõrge profiiliga isikuid, vaid võivad mõjutada ka riigisektori töötajaid, kelle ametialane nähtavus on suurem.

Lisaks sisulisele teabele sisaldavad digitaalsed failid metaandmeid, mis võivad anda infot faili loomise aja, asukoha, seadme või kasutaja kohta (Ünver, 2018: 13). Seetõttu ei pruugi risk tuleneda ainult teadlikult avaldatud sisust, vaid ka tehnilistest kõrvalandmetest, mida kasutaja ise ei märka. Avalike andmete riskasutus võib muuta ametniku töö- ja eraelu seostatavaks isegi siis, kui neid püütakse teadlikult lahus hoida.

Sellises keskkonnas muutub oluliseks OPSEC (*operational security*) ehk operatiivjulgeolek. Range jt määratlevad OPSEC-i protsessina, mille eesmärk on kaitsta asutuse ametnikke, nende pereliikmeid ja tuvastada tegevused ning indikaatorid, mida vastane võib jälgida ja analüüsida, rakendades seeläbi meetmeid nende haavatavuste vähendamiseks (*Defense Technical Information Center*, 2011: 1–2). Praktikas tähendab see, et risk ei teki ainult otsesest infolekkest, vaid ka nähtavusest ehk avalikest ja näiliselt tühistest detailidest, kuna nende kaudu võib saada toimiva pildi ette.

Õiguskaitseasutuste kontekstis võivad sellisteks indikaatoriteks olla näiteks ametniku sotsiaalmeedia kasutus, tööga seotud rutiinid, avalikud viited ametikohale, dokumendiregistrite lekked või korduvad liikumismustrid. OSINT-i abil on võimalik neid andmeid omavahel siduda ning teha järeldusi ametniku töövaldkonna, vastutusala või haavatavuste kohta. Seetõttu ei tähenda OPSEC ainult salastatud info kaitset, vaid ka teadlikku nähtavuse juhtimist, ametialase info piiritlemist ning töötajate teadlikkuse tõstmist. (*OpenAI*, isiklik suhtlus, 20.04.2026)

OSINT-ist tulenevad riskid haakuvad ka hübriidohtude ja infosõja käsitlusega. Tikk märgib, et tänapäevases infokeskkonnas hägustub piir riigi, ühiskonna ja üksikisiku vastu suunatud rünnete vahel (Tikk, 2007: 5–6). See tähendab, et sihtmärgiks ei pruugi olla ainult infosüsteemid või organisatsioonid, vaid ka konkreetsete ametnike identiteet, suhted ja digitaalne jalajälg. Seetõttu ei ole OSINT-i kontekstis määrav ainult see, millist infot avaldatakse, vaid ka see, milliseid uusi seoseid ja järeldusi avalikest andmetest saab tuletada. Nii tuleb OSINT-i käsitleda korraga nii väärtusliku tööriista kui ka riski mehhanismina, mille mõju sõltub kasutajast ja eesmärgist.

1.3.3. *Doxxing*

Risk ei teki sageli üksikust infokillust, vaid sellest, kuidas teabe kokku seotakse ja kasutusse võetakse. *Doxximine* on selle loogika üks konkreetsemaid väljendusviise ehk avaliku teabe süsteemne koondamine muutub surve- või ründevahendiks, kui infot kasutatakse konkreetse inimese sihtmärgistamiseks. Ünver märgib, et OSINT-i vahendusel üksikisikute ründamine võib laiemalt mõjutada ka valitsusasutuste toimimist ja usaldusväärsust (Ünver, 2018: 7). Avaliku sektori ametnike puhul lisandub siia ametialane seos asutusega, mis võib muuta surve ja ründe mõju ulatuslikumaks.

Mõiste *doxxing* pärineb 1990. aastate häkkerikultuuri väljendist „*dropping documents*“ ning tähistab isiku era-, konfidentsiaalse või tuvastatava teabe avaldamist internetis tema tahte vastaselt, enamasti pahatahtlikul eesmärgil (Douglas, 2016, viidatud Anderson ja Wood, 2021: 200). Praktikas kasutatakse *doxximist* hirmutamiseks, surveamiseks, maine kahjustamiseks või sihtmärgi häirimiseks. Politseiametnike puhul võib eesmärgiks olla ka politseitöö takistamine või avaliku korra õõnestamine (Huey jt, 2025).

Anderson ja Wood kirjeldavad *doxximist* kolme peamise muustrina: anonüümsust paljastava, sihistatud või legitiimsust õõnestava tegevusena (Anderson ja Wood, 2021: 206). Ühisosa on kõigil sama – inimese kohta kogutud ja seostatud info kasutatakse viisil, mis vähendab tema kontrolli oma nähtavuse üle ja suurendab haavatavust.

Doxximine ei piirdu ainult veebipõhise probleemi või ahistamisena. Kim jt rõhutavad, et internetikeskkonnast alguse saanud rünnakud võivad tekitada psühholoogilist survet, rikkuda privaatsust ning viia ka füüsiliste ohtudeni (Kim jt, 2011: 676). Douglas seob selle identiteedikontrolliga – kontroll oma nähtavuse üle aitab inimesel reguleerida sotsiaalset positsiooni ja turvatunnet ning selle kontrolli kaotus võib mõjutada mainet, töövõimet ja isiklikku turvalisust (Douglas, 2016: 202).

Avaliku sektori ametnike puhul võivad tagajärjed laieneda ka lähedastele. Tallinna Ringkonnakohtu 2025. aasta lahendis kirjeldatakse juhtumit, kus politseiametnikku ähvardati pärast tööalast kokkupuudet menetlusaluse isikuga ning ähvardused laienesid ka ametniku elukaaslasele ja lapsele (Tallinna Ringkonnakohus, 2025; Kruse, 2025). Kohtulahendist nähtub, et ametniku kodune aadress, töökohaandmed ja muud isikuga seotud viited olid sihipärase ähvardamise sisendiks. See illustreerib, kuidas ametialane nähtavus võib OSINT-keskkonnas kanduda üle era- ja perekondlikku sfääri.

Käesoleva töö vaates on oluline, et *doxximine* ei tähenda ainult andmete avalikustamist, vaid seostamise ja kasutamise viisi, tegemist on ründe vahendiga. Seetõttu on doksimine korraga nii privaatsusrisk kui ka turvalisusküsimus, eriti ametnike puhul, kelle rolli kaudu saab mõjutada ka usaldust institutsiooni vastu.

2. METOODIKA

Selles peatükis kirjeldatakse, kuidas uurimus läbi viidi, kuidas kujunes valim, milliseid uurimis- ja andmekogumismeetodeid kasutati ning kuidas andmeid analüüsiti. Peatüki lõpus käsitletakse ka metoodika piiranguid ning antakse eneserefleksioon uurimisprotsessi kohta.

2.1. Uurimisviis ja valim

Uuringu sihtrühmaks olid PPA ametnikud, keda käsitleti kõrgema riskiga sihtrühmana, kuna politseitöö eeldab rollipõhist nähtavust ja sagedat kokkupuudet konfliktsete olukordadega, mis suurendab riski saada sihtmärgiks. OSINT-keskkonnas võib ametialane info seostamise kaudu kanduda üle ka eraellu, kus sihtmärgiks ei pruugi olla üksnes ametnik, vaid ka tema lähedased.

Andmed koguti anonüümse veebiküsitlusega, mis avaldati PPA siseveebis. Osalemine oli vabatahtlik ning küsimustikule vastas 90 ametnikku ($n = 90$). Uurimus ei ole statistiliselt representatiivne kogu avaliku sektori suhtes ning uurimuse eesmärk ei olnud tulemuste üldistamine kogu populatsioonile, vaid OSINT-ist tulenevate riskide, hoiakute ja kogemuste kaardistamine kõrgema riskiga sihtrühmaga asutuses.

Uurimus on empiiriline ja kvantitatiivse suunitlusega. Andmete kogumiseks kasutati küsitlusuuringut, sest uuritavad nähtused (teadlikkus, riskitaju ja käitumispraktikad) on suures osas subjektiivsed ning otseselt mittevaadeldavad. Küsitlus võimaldas koguda standardiseeritud andmeid ning võrrelda vastajate hinnanguid ja kogemusi (Bryman, 2016: 10). Uurimisküsimused määrasid, millist infot koguda ja kuidas tulemusi tõlgendada (Bryman, 2016: 9).

Uurimisviisiks valiti küsitlusuuring, kuna käesoleva töö eesmärk ei olnud üksikute juhtumite detailne analüüs, vaid ülevaade ametnike teadlikkusest, riskitajust ja hinnangutest OSINT-ist tulenevatele ohtudele. Kuna teemat ei ole Eesti avaliku sektori kontekstis varasemalt ulatuslikumalt uuritud, oli oluline esmalt kaardistada probleemi olemasolu, nende tajumine ning võimalikud riskimustrid.

Valimi moodustamisel kasutati mittetõenäosuslikku sihipärast valimit. Sihipärane valik oli põhjendatud, kuna uurimus keskendus konkreetsele sihtrühmale, kelle tööülesanded ja nähtavus võivad OSINT-i riske võimendada. Kvantitatiivuuringutes sõltub valimi kujundamine uurimuse eesmärgist ning alati ei ole eesmärgiks statistiliselt üldistatava valimi saavutamine (Tartu Ülikool, i.a).

2.2. Andmekogumismeetod

Küsimustiku koostas töö autor, lähtudes uurimisküsimustest ning teoreetilisest raamistikust, mis käsitles OSINT-i, identiteedi ja privaatsuse haavatavust ning erinevaid riske (sh seostamine, tuvastatavus). Küsimuste eesmärk oli kaardistada vastajate OSINT-teadlikkust, riskitaju, võimalikku kokkupuudet juhtumitega ning hinnanguid kaitsemeetmetele ja organisatsioonilisele toele.

Küsimused sõnastati võimalikult selgelt ja neutraalselt, et vähendada tõlgendamis- ja mõõtmisvigu. Küsimustik sisaldas valikvastustega ja Likerti skaalal põhinevaid küsimusi, mis võimaldasid koguda võrreldavaid andmeid nii kategooriliste kui ka järjestustunnustega (Rootalu, 2014). Täiendavalt kasutati avatud vastuse võimalusi ning „muu” variandi juurde lisatud kommentaarivälju, et vastajad saaksid vajadusel oma seisukohti täpsustada (Bryman, 2016: 10–11). Küsitlusuuring võimaldas koguda standardiseeritud andmeid inimeste hoiakute, kogemuste ja hinnangute kohta ühtsete küsimuste abil (Fowler, 2017: 1–3).

Küsimustik jagati kolme sisulisse plokki, mis vastasid uurimisküsimuste loogikale: OSINT-i teadlikkus ja kasutus, OSINT-ist tulenevad ohud, riskitaju ja kaitsemeetmed ning OSINT-i roll mõjutustegevuse ja hübriidohtude kontekstis ning ootused organisatsioonilistele meetmetele. Lisaks koguti taustaandmeid vastajate soo, vanuse, tööstaaži, töö iseloomu ja tööüksuse kohta.

Andmed koguti anonüümse veebiküsitlusega, mis koostati *Google Forms*is (vt lisa 2). Enne küsitluse avaldamist taotleti PPA kooskõlastus ning pärast loa saamist avaldati küsitluse link PPA siseveebis. Küsimustik oli sihtrühmale avatud 10.04.2025–21.04.2025. Küsitlusele lisati saatekiri (vt lisa 1), milles selgitati uuringu eesmärki, OSINT-i tähendust, anonüümsuse põhimõtteid ning andmete kasutamist üksnes lõputöö eesmärgil. Samuti toodi välja küsitluse eeldatav kestus (u 15 minutit), küsimuste arv (31) ja osalemise vabatahtlikkus.

Osalemine oli vabatahtlik, vastajatel oli võimalus igal ajal katkestada ning teavitamisel käsitleti eesmärki, anonüümsuse tagamist, andmekasutust ja võimalikke riske (Eesti Teadusagentuuri töörühm, 2025: p 19–20; 23–24).

2.3. Andmeanalüüs

Andmeanalüüsi eesmärk oli enamat kui vastuste kirjeldamine. Tulemusi tõlgendati uurimisküsimuste ja teoreetilise raamistiku vaatest. Fookus oli muustritel ja korduvatel teemadel,

eriti sellel, kuidas vastajate hinnangud haakuvad OSINT-ist tulenevate riskimehhanismidega, mida käsitleti teooriaosas (nt seostamine ja tuvastatavus ning ametnike rollipõhine nähtavus).

Suletud küsimuste vastuseid analüüsiti kirjeldava statistika abil, kasutades esinemissagedusi ja protsentjaotusi. Tulemused esitati tekstina ning vajaduse korral tabelitena. Kirjeldav statistika võimaldab kvantitatiivuuringus tulemusi süstemaatiliselt koondada ja võrrelda (Tartu Ülikool, i.a).

Avatud vastuseid (*sh* „muu“ valikuga lisatud kommentaarid ja vabatekstilised ettepanekud) kasutati kvantitatiivsete tulemuste täiendamiseks ja täpsustamiseks. Avatud vastuste maht oli väiksem, kui suletud küsimuste puhul, mistõttu ei olnud eesmärk põhjalik kvalitatiivne sisuanalüüs, vaid korduvate seisukohtade ja ettepanekute koondamine temaatilisteks rühmadeks (Bryman, 2016: 11). Kategooriad kujunesid vastuste sisulise sarnasuse alusel ning hõlmasid näiteks teadlikkust ja koolitusi, tuvastatavuse vähendamist, sotsiaalmeediat ja küberhügieeni, tehnilisi OPSEC-meetmeid ning organisatsioonilist tuge.

Analüüs viidi läbi kombineeritult. Tekstiliste vastuste süstematiseerimisel kasutati MAXQDA tarkvara, mis toetab kodeerimist, temaatilist rühmitamist ning kvalitatiivse ja kvantitatiivse info sidumist (Masso jt, 2014). Kategoriseerimise koondtabel koostati *Microsoft Excelis*, kus iga avatud vastus seoti vastava teemaga ning tulemuste illustreerimiseks valiti representatiivseid tsitaate (vt lisa 3).

Analüüsi eesmärk ei olnud hüpoteeside testimine, vaid OSINT-riskide, riskitaju ja kaitsepraktikate kaardistamine ning peamiste probleemkohtade esiletõstmine uuritavas sihtrühmas. Tulemuste tõlgendamisel lähtuti põhimõttest, et andmeanalüüs hõlmab lisaks esitamisele ka sisulist mõtestamist uurimisküsimuste ja teoreetilise raamistiku kontekstis (Tartu Ülikool, i.a).

2.4. Piirangud, eetika ja eneserefleksioon

Uurimuse piiranguks on sihipärane mittetõenäosuslik valim, mis ei võimalda tulemusi statistiliselt üldistada kogu PPA ega avaliku sektori kohta või kogu populatsioonile. See on kooskõlas uurimuse eesmärgiga kaardistada OSINT-ist tulenevaid riske, kogemusi ja hoiakuid kõrgema riskiga sihtrühmas, mitte saavutada representatiivset tulemust (Bryman, 2016: 9–10). Tulemusi tuli seetõttu käsitleda eeskätt kui ülevaadet mustritest ja probleemkohtadest, mis selles sihtrühmas esile kerkivad.

Tulemuste tõlgendamisel tuli ka arvestada, et vastused põhinevad vastajate hinnangutel ja kogemustel. Riskitaju, teadlikkus ja turvatunne on subjektiivsed ning sõltuvad varasemast kogemusest, tööülesannetest ja teadmistest. Samuti on võimalik, et osa vastajatest vastas

ettevaatlikult või sotsiaalselt soovitaval viisil, eriti teemadel, mis puudutasid turvalisust, organisatsioonilisi praktikaid või isiklike kogemusi (Fowler, 2017: 10–12).

Uuringu läbiviimisel lähtuti teaduseetika üldpõhimõtetest ehk vabatahtlikkus, konfidentsiaalsus ja osalejate heaolu kaitse (Eesti Teadusagentuuri töörühm, 2025: p 10–11). Anonüümsuse tagamiseks välditi küsimusi, mis eeldanuks operatiivse või tundliku teabe avaldamist. Arvestati ka varasemas teooriaosas käsitletud seostamise loogikaga, et digikeskkonnas võivad ka kaudsed tunnused koondumisel suurendada tuvastatavust. Seetõttu esitati tulemused koondatud kujul ning avatud vastuste näidete valikul välditi detaile, mis võiksid vastajaid kaudselt tuvastatavaks muuta (Bos, 2020: 158–160). Kogutud andmeid kasutati üksnes teaduslikul eesmärgil ning vastajatel oli võimalik küsitlus igal ajal katkestada.

Uurimisprotsessis tuli autoril arvestada ka oma varasema kokkupuute ja teadmistega uuritavast valdkonnast. Töö teema valik oli osaliselt seotud autori ametialaste kogemustega avalikus sektoris, sh kokkupuutega olukordades, kus konfliktsete menetluste või vaidlustega seotud isikud on püüdnud koguda täiendavat teavet, luua kontakti või avaldada survet. Need kogemused aitasid mõista uuritava probleemi praktilist mõõdet ning kujundasid huvi teema vastu, kuid samal ajal tähendasid vajadust teadlikult hoida käsitlus neutraalne, allikakriitiline ja akadeemiline.

Uurimuse koostamisel püüdis autor toetuda eelkõige teaduskirjandusele, empiirilistele andmetele ja uurimistulemustele. Töö eesmärk ei olnud hirmu või ebakindluse võimendamine, vaid teadlikkuse tõstmine OSINT-ist tulenevatest riskidest, nende võimalikest mõjudest ning vajadusest ennetavate kaitsemeetmete ja teadlikkuse suurendamise järele.

Töö koostamisel kasutati tehisintellektil põhinevat tekstirobotit ChatGPT uurimisprotsessi toetava abivahendina. Tööriista kasutati keerukamate võõrkeelsete terminite ja keerukamate tehniliste lausete mõistmiseks, samuti mahukamate võõrkeelsete materjalide tõlkimisel. Lisaks kasutati ChatGPT-d võimalike allikasuundade leidmisel. Autor kontrollis kogu töö sisulise päritolu, allikad, viited iseseisvalt üle just rakendusest saadud informatsiooni usaldusväärsuse eesmärgil. Tekstiroboti kasutamisel lähtuti Tartu Ülikooli suunistest tekstirobotite kasutamiseks õppetöös. (Tartu Ülikool, 2023)

3. TULEMUSED

Tulemuste peatükk põhineb PPA ametnike seas läbiviidud struktureeritud ankeetküsitlusel. Küsimustik koosnes valdavalt suletud vastusevariantidega küsimustest, mis võimaldasid kirjeldada OSINT-teadlikkust, riskitaju ning identiteedikaitsega seotud hoiakuid ja käitumispraktikaid. Kvalitatiivset täiendust annavad avatud küsimused ning lisatud kommentaarid, mida kasutatakse tulemuste illustreerimiseks ja murekohtade täpsustamiseks. Tulemused on struktureeritud vastavalt uurimisküsimustele.

3.1. OSINT-teadlikkus ning kasutuskogemus

Käesolevas alapeatükis käsitletakse vastajate teadlikkust OSINT-i mõistest, selle kasutusvõimalustest ning kokkupuudetest OSINT-iga tööalases või igapäevases kontekstis. Lisaks vaadeldakse, kuidas vastajad mõtestavad OSINT-i rolli õiguskaitstes, julgeolekus ja mõjutustegevuses.

3.1.1. Taust ja üldised erinevused riskitajus

Tabel 1 annab ülevaate vastajate taustatunnustest. Valimis olid esindatud erineva vanuse, tööstaaži ja tööiseloomuga PPA ametnikud. Enim vastajaid kuulus vanuserühmadesse 25–34 ja 35–44 aastat ning suurima rühma moodustasid 2–5-aastase teenistusstaaziga ametnikud. Töö iseloomu järgi domineerisid sisetöoga seotud ametikohad, kuid esindatud olid ka kombineeritud ja välitöö rollis töötavad ametnikud. Ligikaudu kolmandiku vastajate andmed olid avalikult leitavad PPA ametlikul kodulehel, mis on käesoleva töö kontekstis oluline, kuna teooriaosas käsitleti ametialast nähtavust ja avalike andmete seostatavust võimaliku riski mehhanismina.

Tabel 1. Vastajate taustatunnused (N = 90).

Tunnus	n (%)
Sugu	
Mees	48 (53,3)
Naine	42 (46,7)
Vanus	
Alla 25 aasta	14 (15,6)
25–34 aastat	28 (31,1)
35–44 aastat	27 (30,0)

45–54 aastat	19 (21,1)
55+	2 (2,2)
Töö liik	
Sisetöö	45 (50,0)
Kombineeritud töö	30 (33,3)
Välitöö	15 (16,7)

Allikas: autori koostatud küsitluse põhjal.

Taustatunnuste võrdlusest ilmnes, et kõrgem riskitaju oli üldiselt seotud suurema nähtavuse kokkupuutega. Kõige selgem erinevus tuli esile vastajate puhul, kelle andmed olid avalikult leitavad PPA ametlikul kodulehel. Nendest vastajatest hindas 87,9% OSINT-i pahatahtlikku kasutamist kõrge ohuna, samas ka mitteavalike andmetega vastajate seas oli vastav näitaja 63,2% ehk siiski piisavalt kõrge. See viitab, et ametialane nähtavus ja avalike andmete seostatavus mõjutavad otseselt seda, kuidas hinnatakse võimalikke identiteedi- ja privaatsusriske.

Sarnane muster ilmnes töö iseloomu puhul. Välitööd tegevate ametnike seas hindas 86,7% vastajatest OSINT-ist tulenevaid ohte kõrgeks, samas kui sisetööd tegevate ametnike hinnangud olid mõnevõrra mõõdukamad. Seda võib seostada suurema kokkupuutega avalikkuse, konfliktsete olukordade ning võimalike sihtmärgistamise riskidega. Välitöös on ametnik sageli nähtavam ja otsesemalt seotud menetluste, sekkumiste ja kontrolltegevustega, mis võib suurendada ka haavatavust.

Vanuserühmade lõikes paistsid nooremad vastajad olevat OSINT-i mõiste ja selle võimalustega paremini kursis ning hindasid ka võimalikke riske kõrgemalt. Alla 25-aastastest vastajatest märkis 85,7%, et nad tunnevad OSINT-i mõistet ja rakendusi, ning sama suur osa hindas pahatahtlikku kasutamist kõrge riskina. Vanuserühmas 25–34 aastat oli vastav näitaja 78,6%. Nooremate vastajate kõrgemat riskitaju võib seostada tihedama kokkupuutega digikeskkonna ja sotsiaalmeediaga, kus avaliku info seostatavus ja digitaalne nähtavus on igapäevasemad.

Ka tööstaaži lõikes ilmnes erinevusi. Alla ühe aasta staažiga vastajatest hindasid kõik OSINT-i pahatahtlikku kasutamist kõrge ohuna. Pikema staažiga ametnike seas olid hinnangud mõnevõrra mõõdukamad. Lühema töökogemusega vastajad tõid sagedamini välja ka turvatunde puudumist teadmise tõttu, et nende kohta on võimalik avalikest allikatest infot koguda. See võib viidata, et uuemad ametnikud tunnetavad muutunud digikeskkonna mõju selgemalt või puutuvad tööväliselt rohkem kokku keskkondadega, kus digitaalne nähtavus ja info jagamine on tavapärasemad.

Soo löikes olid üldised hinnangud OSINT-i pahatahtliku kasutamise ohtlikkusele üsna sarnased. Kõrge ohuhinnangu andis 70,8% meestest ja 73,8% naistest. Erinevus ilmnis aga turvatunde küsimuses. 54,8% naistest märkis, et nad ei tunne end turvaliselt teadmiseiga, et nende kohta on võimalik OSINT-i abil infot koguda või neid tuvastada, samas kui meeste seas oli vastav näitaja 41,7%. Avatud vastustes rõhutasid naised sagedamini privaatsuse ja lähedaste kaitse teemat, meeste vastustes kerkis rohkem esile tehniline ja operatiivne vaade.

Kokkuvõttes viitavad tulemused sellele, et OSINT-ist tulenev riskitaju on seotud ametniku nähtavuse, tööiseloomu ja digitaalsete oskuste, teadmistega. Kõrgem riskitaju ilmnis eriti nende vastajate seas, kelle töö või avalik nähtavus suurendab nende tuvastatavust ja seostatavust avalikus infokeskkonnas.

3.1.2. OSINT mõiste tundmine, kasutusvaldkonnad ja olulisus

Vastajate teadlikkus OSINT-i mõistest oli üldjoontes olemas. Küsimusele, kas ollakse kursis terminiga OSINT, vastas 62,2% vastajatest, et nad on tuttavad nii mõiste kui ka selle rakendustega. Veel 22,2% märkis, et on terminist kuulnud, kuid ei tea täpselt selle sisu või kasutusvõimalusi. 15,6% vastajatest ei olnud OSINT-i terminiga kursis. See näitab, et kuigi suurel osal vastajatest oli OSINT-ist vähemalt üldine arusaam olemas, ei olnud teadmised kõikide ametnike seas ühtlased.

Teadlikkuse kõrval hinnati ka seda, kas vastajate arvates kasutatakse OSINT-i Eesti õiguskaitse- ja julgeolekuasutustes ametlikus töös. 80% vastajatest leidis, et kasutatakse, 18,9% ei osanud sellele küsimusele kindlat hinnangut anda ning vaid 1,1% leidis, et OSINT-i ametlikus töös ei kasutata. Tulemused viitavad, et OSINT-i nähakse valdavalt reaalse töövahendina, mitte ainult teoreetilise mõistena.

OSINT-i kasutusvaldkondade hindamisel seostati seda eeskätt julgeoleku- ja õiguskaitsevaldkonnaga. Kõige sagedamini nimetati riiklikku julgeolekut (80%), küberjulgeolekut (78,9%) ning ajakirjandust ja uurivat meediat (75,6%). Õiguskaitset märkis 69,9% vastajatest ning äri sektorit ja konkurentsianalüüsi 57,8%. Selline jaotus näitab, et OSINT-i ei tajuta ainult asutusesisese töövõttena, vaid laiemalt kasutatava võimekusena, mis ulatub erinevatesse valdkondadesse.

Avatud vastustes seostati OSINT-i selgelt ka mõjutus- ja julgeolekuohtudega. Mitmes vastuses toodi välja, et OSINT-i võivad kasutada vaenulikult meelestatud riikide eriteenistused, kurjategijad ja muud uudishimulikud isoonid. See näitab, et OSINT-i ei käsitleta neutraalse

infokogumisenä, vaid osana laiemast mõjutus- ja infosõja loogikast, kus avalik info võib olla ühtaegu nii ressurss kui ka ründevahend.

OSINT-i kasutuskogemus oli vastajate seas mitmekesine. 31,1% märkis, et OSINT on otsene osa nende tööülesannetest, 44,4% leidis, et see on tööülesannete täitmisel abiks, kuigi mitte kohustuslik, ning 42,2% oli kasutanud OSINT-i meetodeid või tööriistu isiklikust huvist. Samas 30% vastajatest märkis, et nad ei ole OSINT-i kasutanud. See viitab, et OSINT ei ole ainult kitsalt spetsialiseeritud ametikohtade tööriist, vaid osa laiemast digitaalsest töökeskkonnast ja infokasutusest.

Vastuste põhjal peeti OSINT-i õiguskaitse ja julgeoleku kontekstis väga oluliseks töövahendiks. Küsimusele, kui oluline on OSINT selles valdkonnas hindamisskaalal (1-5), andis 61,1% vastajatest hinnangu 5 („väga oluline“) ning 21,1% hinnangu 4. Madalaks hindas OSINT-i olulisust vaid 2,2% vastajatest.

Kokkuvõttes näitavad tulemused, et OSINT-i seostatakse eelkõige julgeoleku, õiguskaitse ja mõjutustegevusega ning paljudel vastajatel on ka praktiline kokkupuude selle kasutamisega. Samas ilmneb, et teadmised OSINT-i sisust, kasutuspraktikatest ja võimalustest ei ole kõikide ametnike seas ühesugused, mis võib mõjutada ka riskitaju ja arusaama identiteedi- ning privaatsuskaitse vajadusest.

3.1.3. OSINT olulisus

Vastuste põhjal peetakse OSINT-i õiguskaitse ja julgeoleku kontekstis väga oluliseks töövahendiks. Küsimusele, kui oluline on OSINT selles valdkonnas (skaala 1–5), andis 61,1% vastajatest hinnangu 5 („väga oluline“) ning 21,1% hinnangu 4. Neutraalse hinnangu (3) valis 15,6% vastajatest, hinnangut 2 ei valitud ning 2,2% hindas OSINT-i olulisust madalaks.

Hinnangute jaotus sobitub OSINT-i käsitlusega kui võimekusega, mis annab väärtuse siis, kui avalik info muudetakse süstemaatilise kogumise, seostamise ja tõlgendamise kaudu kasutatavaks teadmisteks. Teisisõnu ei paista OSINT vastajate jaoks olevat midagi kõrvalist, vaid osa sellest, kuidas infot otsitakse ja olukorda mõtestatakse.

Samas jääb sama tulemusteploki kõrvale see, et varasemates küsimustes ilmnes OSINT-i mõiste ja kasutuspraktikate tundmises ebaühtlus. Seetõttu võib kõrge olulisuse hinnang tähendada eri vastajate jaoks erinevat asja: ühel juhul konkreetset töövõtet, teisel juhul üldist arusaama, et avalik info on kasulik. Just selline erinev tõlgendus loob tausta, miks järgmises alapeatükis on mõistlik

vaadata eraldi riskitaju ametnike ja nende lähedaste suhtes ning seda, milliseid ohte OSINT-iga seostatakse.

3.2. OSINT riskid ja vastumeetmed

Selles alapeatükis keskendudes sellele, milliseid ohte ja riske seostavad vastajad OSINT-i pahatahtliku kasutamisega ning mil määral tajutakse ohtu ametnikele ja nende lähedastele. Lisaks kirjeldatakse, milliseid konkreetseid ohte peetakse OSINT-i kaudu kõige suuremaks ning kas vastajad on kokku puutunud juhtumitega, kus tundlik teave on avalikult levinud.

3.2.1. Riskitaju ametnike ja lähedaste suhtes

Vastuste põhjal tajutakse OSINT-i pahatahtlikku kasutamist selge ohuna. Küsimuses, kui ohtlik see võib olla (skaala 1–5), andis 42,2% vastajatest hinnangu 5 ja 30,0% hinnangu 4. Neutraalseks jäi 24,4% ning madalaks hindas riski 3,3%, hinnangut 1 ei valitud. Selline jaotus näitab, et OSINT-i ei käsitleta ainult neutraalse infokogumisena, vaid sellega seostatakse ka võimalikkue kahjusid.

Sarnane pilt ilmneb ametnike endi puhul. 41,1% leidis, et OSINT kujutab ametnikele suurt ohtu, ning 42,2% märkis, et oht on olemas mingil määral. Vähesed pidasid riski väikeseks või olematuks ning 10% ei osanud hinnangut anda. See viitab, et riskitaju on laialt levinud, kuid osa vastajatest ei seosta OSINT-i võimalusi otseselt oma tööpraktikaga või puudub neil kokkupuude juhtumitega, mis teeksid riski nende jaoks selgelt tajutavaks.

Lähedaste puhul peeti riski samuti oluliseks. 31,1% vastajatest pidas OSINT-ist tulenevat ohtu lähedastele väga tõenäoliseks ning 50,0% leidis, et oht on olemas mingil määral. See sobitub töö käsitleusega, et oht ei teki üksikust infokillust, vaid seostamisest. Ametniku nimi, ametikoht, kontaktid ja muud avalikud viited võivad eri allikatest kokku panduna anda piisava pildi, et avaldada survet kas otse ametnikule või tema lähedaste kaudu.

Sellest tulenevalt ei piirdu OSINT-i riskitaju ainult ametialase sfääriga, vaid puudutab ka eraelu ja turvatunnet. Järgmises alapeatükis vaadeldakse, milliseid konkreetseid ohte vastajad esile tõid ning millist kokkupuudet nad võimalike juhtumitega kirjeldasid.

3.2.2. Peamised ohud ja kogemused juhtumitega

OSINT-i kaudu peeti suurimateks ohtudeks isikuandmete lekitamist ja privaatsuse rikkumist (87,8%). *Doxximist* ning isiklikke ähvardusi nimetas ohuna mõlemal juhul 83,3% vastajatest.

Identiteedivargust märkis 78,9% ning desinformatsiooni levikut ja mainekahju 74,4% vastajatest. Vastusevarianti „ei näe ohtu” ei valinud ükski vastaja.

Need valikud koonduvad kaheks suuremaks mustriks. Ühes otsas on privaatsus- ja tuvastusriskid (andmelekked, privaatsuse rikkumine, *doxximine*, identiteedivargus), teises otsas mõjutus ja survega seotud riskid (ähvardused, mainekahju, desinformatsioon). Selline jaotus sobib kokku töö teoreetilise lähtekohaga ehk risk ei teki ainult avalikust infost, vaid sellest, et eri allikatest pärit killud saab kokku panna ning kasutada neid inimese tuvastamiseks ja tema mõjutamiseks.

Küsimused kogemuste kohta näitavad, et isiklik kokkupuude on pigem harvem. 67,8% vastajatest märkis, et nad ei ole tundliku info levikuga (nt lekkinud andmed, kodune aadress) isiklikult kokku puutunud. Samas 28,9% teadis kolleegidega seotud juhtumeid ning 6,7% oli sellist olukorda ise kogenud. See tähendab, et riskid ei ole vastajate jaoks ainult teoreetiline, kuna teadmine juhtumitest liigub organisatsioonis ka siis, kui kõigil ei ole isiklikku kogemust.

Sarnane pilt ilmneb negatiivse avaliku kuvandi küsimustes. 11,1% märkis, et nende kohta on levitatud negatiivset infot, 5,6% ütles, et nende isikuandmeid on avalikustatud, ning 13,3% tõi välja, et neid on filmitud või pildistatud ilma loata. Kõige sagedamini teati siiski kolleegidega seotud juhtumeid (44,4%). Need vastused viitavad, et nähtus on organisatsioonis tajutav pigem kollektiivse kogemuse kaudu. Otsene juhtum võib tabada väheseid, kuid selle mõju jõuab laiemale ringini.

Avatud vastustes kirjeldati ka ennetavat käitumist, näiteks seda, et kontrollitakse teadlikult võimalike andmeleketega seotud riske või jälgitakse, milline info enda kohta internetis kättesaadav on. See lisab siia tulemusteplokki olulise mõõtme. Osa vastajaid ei räägi ainult ohtudest, vaid näitab, et OSINT-i loogikat arvestatakse juba igapäevases enesekaitstes (oma digitaalse jalajälje jälgimine, avalikult kättesaadavad ja lekkinud info regulaarne kontroll).

3.2.3. Riskide vähendamiseks kasutatavad vastumeetmed ja turvatunne

Riskide vähendamiseks piirati kõige sagedamini isikuandmete ja fotode avalikku nähtavust (77,8%). Pseudonüüme või alternatiivseid kasutajanimi kasutas 54,4% ning anonüümseid sotsiaalmeediakontosid 48,9% vastajatest. Sotsiaalmeediakontosid ei kasutanud 13,3% vastajatest ja 4,4% märkis, et kuigi ohtudest ollakse teadlikud, konkreetseid meetmeid ei rakendata.

Nimetatud võtted koonduvad eelkõige loogika ümber, kus vähendatakse enda avalikku seostatavust. Kui enda nime, näo, kasutajanimede ja kontaktide jälg on väiksem, on keerulisem siduda erinevatest allikatest pärinevaid teabekilde ühe konkreetse inimesega. Mõned vastajad

kirjeldasid ka tehnilisemaid samme, näiteks VPN-i kasutamist, eraldi seadmete ja kontode loomist ning töölase ja isikliku digitaalse identiteedi teadlikku lahushoidmist. Sellest paistab, et nähtavust püütakse juhtida mitte ainult sisu tasandil, vaid ka tehniliste valikutega.

Turvatunde küsimuses jagunesid vastused peaaegu võrdselt. 48,9% vastajatest tundis end turvaliselt teadmisega, et OSINT-i abil on võimalik nende kohta infot leida, samas kui 47,8% ei tundnud end turvaliselt. See näitab, et sama teadmine OSINT-i võimalustest ei mõjuta kõiki ühtemoodi, osa võtab seda paratamatu taustana, osa tajub seda igapäevase riskina, mis vajab pidevat tähelepanu.

Need, kes ei tundnud end turvaliselt, tõid peamise põhjusena esile OSINT-i kaudu leitava info enda või lähedaste kohta (47,8%). Sageli mainiti ka vaenulikku suhtumist ametnike vastu sotsiaalmeedias (37,8%) ning *doxximist* või muu tundliku info leket (35,6%). Lisaks leidis 27,8% vastajatest, et asutuse kaitsemeetmed ei ole piisavad. Nendest vastustest joonistub välja, et mure ei ole ainult võimalikes ohtudes, vaid ka nähtavuses ja tähelepanus, mis võib olla vaenulik ning kanduda veebist väljapoole.

Avatud vastustes tuli korduvalt esile, et riskitaju mõjutab ka käitumist. Mainiti näiteks vajadust kohandada oma nähtavust suurema riskiga tööülesannete puhul ning kasutada eraldi kontosid, seadmeid ja kontaktandmeid. Samas ei ilmne vastustest ühtset mustrit, mis viitab, et ennetuspraktikad on pigem individuaalsed ja sõltuvad töörollist, kogemusest ning sellest, kui nähtavaks end peetakse.

3.3. Asutuse roll ja OSINT-riskide käsitlemine strateegilisel tasandil

Selles alapeatükis vastatakse uurimisküsimusele kolm, keskendudes ametnike hinnangutele ja ootustele riigiasutuste rollile OSINT-riskide ennetamisel ja ametnike privaatsuse, turvalisuse kaitsel. Esitatakse vastajate seisukohad OSINT-i seostamisest mõjutustegevusega ning hinnangud sellele, kas OSINT-riskide ennetamine peaks kuuluma riikliku küberturvalisuse strateegia alla.

3.3.1. OSINT mõjutustegevuse kontekstis ja tajutus kasutus Eesti vastu

OSINT-i kasutamist mõjutustegevuses Eestis pidas enamik vastajatest reaalselt olemasolevaks. Küsimusele, kas OSINT-i kasutatakse Eestis desinformatsiooni, narratiivide kujundamise või trollimise eesmärgil, vastas 91,1% jaatavalt ning 8,9% eitavalt. Samuti leidis 75,6% vastajatest, et OSINT-i kasutatakse Eesti riigiametnike ja riigiasutuste vastu, samas kui 24,4% ei pidanud seda tõenäoliseks.

Need vastused näitavad, et OSINT-i ei seostata ainult infokogumisega. Vastajate jaoks on OSINT pigem osa samast tööloogikast, mida kirjeldati infooperatsioonide peatükis, avalik teave on sisend, mille abil saab kujundada sõnumeid, profileerida sihtmärke ja suunata tähelepanu. Nii muutub oluliseks mitte ainult see, mida keegi avalikest allikatest leiab, vaid kuidas see info hiljem kommunikatsioonis ja mõjutamises tööle pannakse.

Ukraina sõja ja Venemaa mõjutustegevuse kontekstis seostati OSINT-i eriti selgelt infooperatsioonidega. 63,3% vastajatest leidis, et OSINT mängib sellistes tegevustes olulist rolli, ning 21,1% käsitles seda mõjutustehnikate osana. Väike osa hindas selle mõju piiratumaks. Siit paistab, et vastajate jaoks ei ole OSINT neutraalne taust, vaid midagi, mis võib toetada tervikpilti ja samal ajal ka sihitud narratiive.

Oluline on ka see, et OSINT-i võimalik kasutus riigiametnike ja riigiasutuste vastu on vastajate hinnangul realistlik. Siin tuleb tagasi töö keskne teema, ametnike nähtavus ja avaliku info seostatavus. Kui ametniku nimi, roll, kontaktid või harjumused on eri allikatest kokku pandavad, siis tajutakse seda mitte lihtsalt privaatsusprobleemina, vaid mõjutamise ja sihtmärgistamise võimalusena.

3.3.2. Asutuse roll ja OSINT-riskide käsitlemine strateegilisel tasandil

Valdav enamik vastajatest leidis, et riigiasutused peaksid pöörama rohkem tähelepanu ametnike kaitsele OSINT-ist tulenevate riskide kontekstis. Seda seisukohta toetas 94,4% vastajatest ning 5,6% ei pidanud seda vajalikuks.

Selline tulemus näitab, et identiteedi- ja privaatsuskaitset ei paigutata ainult ametniku isikliku ettevaatuse vastutusse. Vastajate vastustest jääb mulje, et üksikute nippide kõrval oodatakse organisatsioonilt selgemat raamistikku, mis annaks ühtsed põhimõtted, praktilised juhised ja toe olukordades, kus risk realiseerub. See sobitub töö varasema loogikaga, kus ametnike nähtavus ja avalike andmete seostatavus loovad haavatavuse, mida üks inimene ei suuda alati ise kontrollida.

Sarnane hoiak ilmnes ka küsimuses, kas OSINT-riskide ennetamine peaks kuuluma riikliku küberturvalisuse strateegia alla. Sellist lähenemist toetas 93,3% vastajatest ning 6,7% ei pidanud seda vajalikuks. Need vastused asetavad teema ametniku tasandilt laiemasse raamistikku. OSINT-i käsitletakse siin mitte ainult privaatsuse küsimusena, vaid osana riigi toimepidevusest ja usaldusest institutsioonide vastu.

3.3.3. Juhised, koolitusvajadus ja ettepanekud

OSINT-ist tulenevate ohtude käsitlemist ametnike koolitusprogrammides pidas vajalikuks 95,6% vastajatest. See tulemus on kooskõlas varasemate alapeatükkidega, kus riskitaju oli kõrge ja oht seostus sageli seostatavuse ning nähtavusega. Koolitusvajadus tuleb siin välja kui praktiline vastus küsimusele, kuidas sellises keskkonnas üldse toime tulla.

Olemasolevate juhiste ja koolituste kohta olid vastused ebaühtlasemad. 52,2% leidis, et asutus pakub ametnike privaatsuse ja turvalisusega seotud juhiseid või koolitusi, 28,9% ei osanud seda hinnata ning 14,4% arvas, et neid ei pakuta. Selline jaotus viitab, et isegi kui juhised on olemas, ei pruugi need jõuda kõigi töötajateni või ei seostata neid otseselt OSINT-ist tulenevate riskidega. Vastustest jäi eristusena kõlama ka see, et üldised andmekaitsealased juhised ei pruugi katta ametnike isiklikku tuvastatavust puudutavaid olukordi.

Avatud ettepanekutes kordus kolm põhilist suunda. Esiteks sooviti regulaarseid koolitusi ja lihtsaid, elulisi juhiseid, mis aitaksid paremini mõista OSINT-i võimalusi ja enda digitaalset jalajälge. Teiseks rõhutati tehniliste ja organisatsiooniliste meetmete tugevdamist, näiteks töö- ja eraelu selgemat eristamist ning turvalisemaid töövõtteid ja vahendeid. Kolmandaks tõsteti esile ametnike avaliku nähtavuse vähendamist avalike kontaktandmete ja nimepõhise seostatavuse puhul, samuti nime asemel identifikaatori või koodi kasutamine tööülesannete täitmisel.

Need ettepanekud näitavad, et teemat ei käsitleta ainult individuaalse ettevaatuse küsimusena. Pigem oodatakse, et identiteedi- ja privaatsuskaitse oleks osa asutuse igapäevastest praktikatest ja töökorraldusest, nii et ametnik ei jääks riskide maandamisel üksi.

4. JÄRELDUSED JA EDASISED UURIMISSUUNAD

Selles peatükis esitatakse uurimistöö peamised järeldused ja arutletakse tulemuste üle, lähtudes uurimisküsimustest. Analüüs põhineb varasemates peatükkides kirjeldatud teoreetilisel taustal ja empiirilistel tulemustel. Nii saab hinnata, kuivõrd kattuvad tulemused senise teaduskirjandusega ja milliseid uusi tõlgendusi need lisavad. Arutelu on jaotatud uurimisküsimuste järgi. Peatüki lõpus võetakse kokku peamised järeldused, tuuakse välja töö piirangud ning tehakse ettepanekud edasisteks uurimissuundadeks.

4.1. OSINT olemuse taju

Küsitluse põhjal tajuvad vastajad OSINT-i eelkõige osana igapäevasest töö- ja mõjutuskeskkonnast, mitte pelgalt kitsa luureterminina. OSINT seostub nende jaoks julgeoleku, küberjulgeoleku ja õiguskaitsega ning samal ajal arvestatakse, et sarnane võimekus on ka vastaste käes. Nii asetub OSINT vastajate mõtlemises laiemasse informuumi, kus avalik info võib mõjutada hoiakuid, usaldust ja otsuseid. See haakub Eesti julgeolekukäsitlusega, mis rõhutab informuumi kaitse vajadust riigikaitse raamistikus (Riigikantselei, 2021: 30). Mõjutustegevuse vaates on oluline ka Naritsa tähelepanek, et emotsionaalselt laetud sõnumid ja nendega seotud võtted võivad toetada usalduse õõnestamist (Narits, 2015: 68). Vastajate vastustest jääb mulje, et OSINT-i vaadatakse just sellise mõjutusloogika ühe praktilise sisendina, mitte üksnes info otsimisena.

Samas ei ole OSINT-i rakendus ja piirid organisatsiooni sees vastajate hinnangul ühtmoodi selged. Esile toodi juhiste ja koolituste ebaühtlus ning arusaam, et praktilised põhimõtted sõltuvad liiga palju üksusest või olukorrast. Mitmes ettepanekus küsiti sisuliselt sama asja – kuidas OSINT-i kasutada nii, et see toetaks tööd aga ei suurendaks tarbetult ametnike enda nähtavust ja riske. See näitab lõhet OSINT-i tajutud olulisuse ja ühtse kasutuspraktika vahel.

Teooria aitab seda lõhet seletada. OSINT-i tuum ei ole avalik info, vaid protsess, kus killustatud teave muudetakse eesmärgipäraseks teadmisteks. Steele määratleb OSINT-i sihipäraselt avastatud, töödeldud ja levitatud informatsioonina kindlale sihtrühmale (Steele, 2006: 129). Hwang jt rõhutavad, et OSINT tekib süsteemsest otsimisest, kogumisest ja analüütilisest töötlemisest (Hwang jt, 2022: 1–3). Kui seda metoodikat mõistetakse ebaühtlaselt, on loogiline, et ebaühtlaseks jääb ka riskide tajumine ja ohutu kasutuse piiride tunnetus. Just seostamise moment teeb OSINT-ist ühtaegu väga kasuliku ja samas haavatavusi avava võimekuse.

Vastajate riskitaju toetab ka arusaam, et OSINT ei piirdu enam klassikalise avaliku infoga. Oerlemans ja Langenhuijzen kirjeldavad, et praktikas võivad OSINT-i alla kuuluda ka kommertsandmed ja lekkinud andmed (Oerlemans & Langenhuijzen, 2025: 581–582), mis nihutab fookuse otsimiselt identiteedikildude seostamisele ehk kasutajanimed, kontaktid, asukohaviited ja muud killud võivad eri keskkondades kokku joosta ning anda detailsema pildi, kui üksik allikas eraldi. Sama loogikat kinnitas ka põgus OSINT-tööriistade ülevaade, kus osa keskkondi teeb sihitud otsingu ja seostamise tehniliselt väga lihtsaks.

OSINT-i ohutu kasutuse teema seostub otseselt operatiivjulgeolekuga, kus edukas riskijuhtimine peaks ennetama ohte asutusele, ametnikele ja nende lähedastele. Eesti julgeolekupraktika näited ostavad, et mõjutustegevus ei ole abstraktne mõiste. See võib avalduda konkreetsetes tekstides, levikanalites ja vastutuses. Kaitsepolitsei aastaraamatus kirjeldatud Sevastopoli ülikooli programm ning Burceva juhtum näitavad, et mõjutustegevust tehakse sihipäraselt ja see võib jõuda ka Eesti institutsioonide tasandile (Kaitsepolitsei aastaraamat, 2026: 8–9; Siplane, 2025). Sellest tulenevalt ei ole OSINT-i puhul keskne ainult oskus leida, vaid ka oskus mitte võimendada manipuleerivat materjali ning hoida omaenda tegevusviisid ja nähtavus kontrolli all. Kui OSINT on organisatsioonis päriselt kasutusel, vajab see selget metoodikat, ühtseid põhimõtteid ja praktilist juhendamist, et võimekus ei töötaks kasule vastu.

4.2. Riskid ja nende realiseerumine

OSINT osas tajutakse pahatahtlikku kasutamist selge riskina nii ametnikele kui ka nende lähedastele. Oluliseks peeti, et oht ei jää töörolli piiridesse. Pereliikmed võivad kujuneda sihtmärgiks, kelle kaudu on võimalik avaldada survet või mõjutada ametniku turvatunnet. See sobitub *doxximise* ja sihitud mõjutamise loogikaga, kus rünnak ei pea algama asutusest, vaid võib alata inimesest ja tema lähikonnast.

Kirjeldatud ohud koonduvad suuresti privaatsuse ja tuvastatavuse ümber. Esile tulid isikuandmete lekked ja avalikustamine, *doxximine*, ähvardused, identiteedivargus ning mainekahju. Kim jt rõhutavad, et privaatsusrikkumisel võib olla pikaajaline psühholoogiline mõju ning kahju ei pea avalduma ainult füüsilise ohuna (Kim jt, 2011: 676). Vastuste põhjal ei tajutud riske kitsalt andmekaitse probleemina, vaid koos nendega mainiti järjekindlalt ka surve ja mõjutamise elemente, näiteks ähvardusi ja mainekahju.

Williams ja Blum kirjeldavad, et andmete koondamine ja analüüs toob esile mustrid ja seosed, mille kaal on suurem kui üksikul infokillul (Williams ja Blum, 2018: 10). Sama mehhanism

selgitab, miks näiliselt tühine detail võib osutada oluliseks siis, kui see asetub teiste andmetega samasse pilti. Tehnoloogia võimendab seda protsessi, sest teeb info nähtavaks, leitavaks ja kombineeritavaks (Alkhudhayr jt, 2019). Pastor-Galindo jt osutavad, et ka eraldiseisvad infokillud võivad koondatuna muuta isiku tuvastatavaks, isegi juhul, kui üksikute andmete puhul kasutatakse kaitsemeetmeid (Pastor-Galindo jt, 2020: 10301). Seetõttu ei ole ohutu alati see, mis tundub üksikult vaadates tähtsusetu.

Küsitluses selgus ka, et risk ei ole ainult teoreetiline. Mitmed vastajad tõid esile kolleegidega seotud juhtumeid ning olukordi, kus tööga seotud konflikt kandus üle isiklikku sfääri. Selline kogemuslik taust on OSINT-riskide puhul tüüpiline, üksikud juhtumid mõjutavad turvatunnet laiemalt ja suurendavad ettevaatlikkust ka neil, kes pole ise otseselt sihitud olnud.

Eraldi väärivad tähelepanu asukohaandmed ja tehnilised kõrvalandmed. Asukohaandmete põhjal saab tuletada liikumismustreid ja igapäevaseid harjumusi ning see tõstab privaatsusrisiki märkimisväärselt. Praktikas lisandub sellele metaandmete kiht, mis võib anda vihjeid faili päritolu, loomise aja või kasutatud seadme kohta. Kui sellised kõrvalandmed seotakse ametniku nähtavuse ja muu avaliku infoga, võib kujuneda detailne pilt inimese tegevusest, seostest ja harjumustest. Uuringu vastustest jäi samasugune arusaam kõlama ka üldisemalt, avalikest allikatest peeti võimalikuks kokku panna üsna põhjalik profiil nii ametniku kui ka tema lähedaste kohta, eriti kui sotsiaalmeedia, registriandmed ja muu avalik info omavahel kokku viia.

Doxximise puhul muutub keskseks see, et delikaatne info tehakse nähtavaks ja kergesti leitavaks ning selle hilisem levik ei ole enam kontrollitav. Douglas kirjeldab *doxximist* küberjälitamise tööriistana, mille mõju võib olla pikaajaline, sest internetti jõudnud info võib jääda püsivalt kättesaadavaks ja nähtavuse üle kontrolli kaotamine mõjutab seetõttu nii identiteeti, mainet kui ka tegutsemisvabadust (Douglas, 2016: 199, 202).

Selle alapeatüki põhjal on OSINT-riskide keskmes seostamine ja sellest tekkiv tuvastatavus. Samad töövõtted, mis aitavad õiguspäraselt infot koguda ja analüüsida, võivad pahatahtlikus kasutuses muutuda surve, hirmutamise või maine kahjustamise vahendiks. Seetõttu ei piirdu riskide maandamine üksikute tehniliste nippidega, vaid eeldab läbimõeldud praktikaid ja kokkuleppeid, mis aitavad ametniku nähtavust juhtida ning reageerida siis, kui risk realiseerub.

4.3. Ametnike haavatavus ja asutuse roll OSINT käsitluses

Ametnike nähtavus digitaalses infokeskkonnas toimib kahel viisil. Ühelt poolt on see tööalane vajadus, sest avaliku sektori töö eeldab sageli nime, ametikoha või muu tööalase info avalikkust.

Teiselt poolt muudab sama nähtavus ametniku lihtsamini tuvastatavaks ja seostatavaks, eriti kui avalikud infokillud jooksevad kokku sotsiaalmeedia, registrite ja muu digijäljega. Nii ei jää OSINT-ist tulenev risk ainult inimese isiklikuks mureks, vaid puudutab ka asutuse toimimist ja usaldusväarsust.

Küsitluse vastustest paistis selgelt, et risk ei piirdu ametnikuga. Lähedasi kirjeldati *nn* pehmete sihtmärkidena, kelle kaudu on võimalik avaldada survet või tekitada hirmu, mis omakorda mõjutab ametniku turvatunnet ja töövõimet. Siin kandub töörollist tulenev nähtavus üle eraellu, sest rünnaku või surve lähtepunkt võib olla just inimese lähikond, mitte asutus tervikuna.

Turvatunde teemal oli vastustes palju ebakindlust. Turvatunde puudumist seostati eeskätt võimalusega, et enda või lähedaste kohta saab avalikest allikatest infot koguda ja seostada. Samuti mainiti vaenulikku suhtumist sotsiaalmeedias ning *doxximise* või muu tundliku info avalikustumise riski. Osades vastustes kerkis esile ka see, et kaitsemeetmed ja juhised ei ole piisavalt selged või ei jõua ühtlaselt kõigi töötajateni. See teeb riskidega toimetuleku pigem individuaalseks ning sõltuvaks sellest, kui palju keegi ise oskab ja viitsib enda nähtavust hallata.

OSINT tõstatab paratamatult ka küsimuse, kus lõpeb avaliku info õiguspärane kasutus ja algab privaatsust kahjustav tegevus. OSINT ise võib tugineda avalikele andmetele, kuid kui info süstemaatiliselt kokku koguda, seostada ja sellest profile koostada, muutub inimese identiteet, harjumused ja suhted detailselt kaardistatavaks. Hansen ja Nissenbaum osutavad, et küberohtude intensiivne julgeolekustamine võib tekitada pingeid teiste väärtustega ning suurendada *mh* privaatsuse piiramise riski (Hansen ja Nissenbaum, 2009: 1156–1160). See pinge on ametnike puhul eriti nähtav, sest läbipaistvus on töö osa, kuid samal ajal suureneb vajadus kaitsta inimese eraelu ja turvalisust.

Vastuste põhjal oodatakse, et OSINT-riskide maandamine ei jääks ainult isikliku ettevaatuse tasandile. Korduvalt rõhutati ühtsemaid põhimõtteid, regulaarset koolitamist, praktilisi juhiseid ja tuge siis, kui risk realiseerub. OPSEC-meetmed ja teadlik nähtavuse juhtimine ei ole siin “lisateema”, vaid osa sellest, kuidas ametnikke kaitsta keskkonnas, kus infokillud liiguvad kiiresti ja seostuvad kergesti. OSINT-ist tulenevad ohud seostuvad seega tehnoloogia kõrval ka töökorralduse, juhiste kättesaadavuse ja asutuse praktikatega.

4.4. Järeldused ja edasised uurimissuunad

OSINT on korraga nii võimekus kui oht. Digitaalset sisu saab manipuleerida ning allikate usaldusväarsust ei ole alati lihtne hinnata, mistõttu muutuvad kontrollimehhanismid üha

olulisemaks. Andmete avalikkus ja kättesaadavus ei tähenda automaatselt usaldusväarsust (Formanchuk, 2025: 269).

Lõputöö eesmärk oli selgitada välja, kuidas tajuvad PPA ametnikud OSINT-ist tulenevaid riske ning milliseid ohte nähakse ametnike ja nende lähedaste identiteedi, privaatsuse ja turvalisuse seisukohalt. Lisaks vaadeldi, kuidas hinnatakse olemasolevaid kaitsepraktikaid ja millist organisatsioonilist tuge peetakse vajalikuks riskide vähendamisel.

Tulemused osutavad, et OSINT ei ole vastajate jaoks abstraktne mõiste, vaid osa tänapäevasest töökeskkonnast. Risk ei seostu ainult sellega, et mingi info on kuskil olemas, vaid sellega, kuidas eri allikatest pärinevad infokillud kokku viiakse ja tõlgendatakse. Kui andmeid saab seostada, on võimalik koostada üsna detailne pilt inimese identiteedist, harjumustest ja seostest ning see omakorda avab ruumi nii privaatsusrikkumisteks kui ka sihitud mõjutamiseks.

Ametnike haavatavus OSINT-keskkonnas on osaliselt struktuurne. Avaliku sektori töö eeldab nähtavust ja tuvastatavust, kuid sama nähtavus võib kujuneda ründe lähtepunktiks. Uuringu üks selgemaid tähelepanekuid oli, et riskid ei piirdu ametnikuga. Lähedasi tajuti pehmete sihtmärkidena, kelle kaudu mõjutada seeläbi ametniku turvatunnet ja töövõimet.

Samuti tuli esile, et riskide maandamine ei saa jääda ainult individuaalse ettevaatuse tasandile. Vastajad rõhutasid ühtsemaid põhimõtteid, regulaarseid koolitusi, praktilisi juhiseid ja tuge olukordades, kus risk realiseerub. See näitab, et identiteedi- ja privaatsuskaitse on vastajate silmis korraga isiklik teema ja asutuse töökorralduse küsimus, mis mõjutab ka organisatsiooni usaldusväarsust ja toimepidevust.

Uurimuse piirangud tulenevad valimist ja meetodist. Kasutati mittetõenäosuslikku sihipärast valimit, mistõttu ei saa tulemusi statistiliselt üldistada kogu PPA-le ega avalikule sektorile. Küsitlus põhines hinnangutel, mida võivad mõjutada isiklikud kogemused, teadlikkus ja erinev arusaam OSINT-ist.

Edasistes uuringutes võiks võrrelda eri asutuste ametnike riskitaju ja kaitsepraktikaid ning analüüsida, millised organisatsioonilised lahendused töötavad kõige paremini. Samuti oleks väärtuslik uurida, kuidas asutused ise mõtestavad ametnike nähtavust ja privaatsust ning kus nad tõmbavad piiri individuaalse vastutuse ja organisatsioonilise toe vahel. Eraldi tähelepanu vajab tehisintellekti ja automatiseeritud andmekogumise mõju, sest see võib muuta profiilide koostamise kiiremaks ja odavamaks ning suurendada nii ründe- kui ka eksimisriske. *Sh* tasub uurida, millised

koolitus- ja teadlikkuse tõstmise viisid aitavad praktikas kõige paremini vähendada ametnike ja nende lähedaste haavatavust.

4.5. Ettepanekud

OSINT-i käsitlemine peaks lähtuma asutuse valdkonna eripärast. PPA ja teised riigiasutused tegutsevad valdkonnas, kus eesmärgiks on avaliku korra ning riigi ja ühiskonna toimimise tagamine. Sellisest vaatest ei ole ametniku nähtavus ainult isiklik teema, vaid osa riigi toimimisest. Kui ametnik tajub, et ta on digikeskkonnas kergesti kaardistatav ning asutus ei paku piisavat ennetust ega tuge, mõjutab see paratamatult turvatunnet ja valmisolekut, *sh* keerulisi ülesandeid täita. Individuaalsed kaitsemeetmed on vajalikud, kuid need ei saa olla ainus kaitseliin ega üksikvastutus. Ametnik tegutseb riigi esindajana, mitte isiklikust huvist ning rünnak ametniku või tema lähedaste vastu kandub kiiresti üle töömotivatsiooni, töö kvaliteedile ja usaldusele institutsiooni vastu. Seetõttu on OSINT-riskide ennetamine ja reageerimine mõistlik siduda asutuse tavapärase praktikate ja töökorraldusega, mitte jätta üksikisiku kanda.

Läbiviidud uurimuse tulemused kinnitasid, et OSINT-ist tulenevaid riske ei tajuta ainult ametniku isikliku ettevaatuse küsimusena. Vastajad ootasid selgemaid reegleid, paremat tuge ja ühtlasemat praktikat, sest nähtavus ja seostatavus ei ole täielikult inimese enda kontrolli all. Seetõttu tasub OSINT-riskide vähendamist käsitleda asutuse töökorralduse osana ning ühendada see teadlikkuse, juhiste ja tehniliste valikutega.

On mõistlik arendada regulaarseid OSINT-i, OPSEC-i ja küberhügieeni koolitusi. Koolitused peaksid jääma praktiliseks ning lähtuma igapäevastest olukordadest, näiteks sotsiaalmeedia kasutus, digitaalne jalajälg, metaandmed, asukohaandmed ja avaliku info seostamine. Kui ametnik näeb harjutuste kaudu, kuidas infokillud kokku jooksevad, muutub ka riskipilt selgemaks ning ennetus ei ole enam juhuslik, vaid teadlik valik.

Organisatsioonilised põhimõtted vajavad ühtlustamist. Tulemustest paistis, et juhised on kas ebaühtlased või ei jõua kõigini. Vajalik on lühike ja selge raamistik, mis ütleb, mida OSINT-i kontekstis arvestada, kuidas hoida töö- ja eraelu piire ning kuidas käituda siis, kui tekib kahtlus lekkele, *doxximisele* või sihitud rünnakule. Sama oluline on, et ametnik teaks, kuhu pöörduda ja milline on asutuse tugi, kui risk realiseerub.

Asutus roll on toetada töö- ja eraelu lahushoidmist. Praktikas tähendab see eraldi töö- ja erakontaktide kasutamist, võimalusel eraldi kontosid ja seadmeid ning selgemaid soovitusi, millist infot mitte siduda ametialase rolliga. Mõnes vastuses pakuti ka ametnike avaliku identifitseerimise

vähendamist, näiteks kasutada nime asemel identifikaatorit või koodi olukordades, kus see ei kahjusta tööülesannete täitmist. Selline lahendus ei kaota vastutust, kuid võib vähendada otsest seostatavust avalikus inforuumis.

Samuti tasub kriitiliselt üle vaadata avalik nähtavus seal, kus see ei ole tööks vältimatu nagu näiteks sotsiaalmeedias ametnike ja nende tegemiste kuvamine. Eesmärk ei ole läbipaistvuse vähendamine, vaid selle mõtestamine nii, et avalik kontakt ei muutuks automaatselt isikuandmete kogumispunktiks ja riskifaktoriks. Rollipõhised kontaktid ja üldkanalid aitavad siin sageli rohkem, kui isikupõhine avalik kommunikatsioon.

Sh tuleb arvestada, et automatiseeritud andmekogumine ja tehisintellekt muudavad OSINT-i kiiremaks ja massilisemaks. Seetõttu on vaja õpetada, kuidas hinnata automaatselt leitud info usaldusväärsust, kuidas märgata manipulatsiooni ja kuidas vähendada enda digitaalset haavatavust ka siis, kui otsing ja profileerimine on automatiseeritud.

Vastused peegeldasid, et inimfaktor on keskne element. Ametniku turvatunne ja valmisolek oma tööd teha sõltuvad sellest, kas ta tunneb, et asutus aitab riske ennetada ja vajadusel reageerida, kaitsta. Identiteedi- ja privaatsuskaitse ei jää siis üksikute inimeste enda *nn* targaks toimetamiseks, vaid muutub osaks asutuse tavapäraest praktikatest.

KOKKUVÕTE

Avalikult kättesaadava info hulk ning võimalused seda koguda, siduda ja analüüsida on viimastel aastatel märgatavalt arenenud. OSINT ei ole enam ainult luure- ja julgeolekuasutuste töövahend, vaid osa laiemast digitaalsest infokeskkonnast, kus eri allikatest pärinevaid andmeid kasutatakse ka pahatahtlikult. See teeb eriti oluliseks ametnike identiteedikaitse, privaatsuse ja turvalisuse küsimuse.

Töö eesmärk oli selgitada, kuidas tajuvad PPA ametnikud OSINT-ist tulenevaid riske ning milliseid ohte nähakse ametnike ja nende lähedaste identiteedi, privaatsuse ja turvalisuse seisukohalt. Samuti uuriti, milliseid kaitsemeetmeid peetakse vajalikuks ning kuidas hinnatakse olemasolevat organisatsioonilist tuge. Empiiriline osa põhines anonüümsel veebiküsitlusel, milles osales 90 PPA ametnikku.

Teoreetiline käsitus osutas, et riskid ei teki üksnes avaliku info olemasolust, vaid sellest, kuidas eri allikatest pärinevad infokillud kokku seotakse ja tõlgendatakse. Digikeskkonnas võib ka näiliselt tühine detail muutuda probleemiks, kui see asetub sobivasse konteksti või kombineeritakse muu teabega.

Küsitluse põhjal tajutakse suurimate riskidena isikuandmete leket, privaatsuse rikkumist, *doxximist*, identiteedivargust, ähvardusi ja mainekahju. Oluline on, et oht ei piirdu ametnikuga, kuna vastajate hinnangul võib see laieneda ka lähedastele ning seetõttu mõjutada inimese turvatunnet ja igapäevaelu.

Üheks keskseks järelduseks kujunes, et OSINT-ist tulenevaid riske ei saa käsitleda ainult individuaalse probleemina. Ametnikud täidavad avalikult ülesandeid ning nende sihtmärgistamine võib mõjutada lisaks üksikisikule ka asutuse töövõimet, usaldusväärsust ja laiemalt julgeolekut.

Läbiviidud küsitlus tõi esile vajaduse süsteemsemate organisatsiooniliste meetmete järele. Oluliseks peeti regulaarseid OSINT-i, OPSEC-i ja küberhügieeni koolitusi, praktilisi juhiseid ning ühtsemaid põhimõtteid ametnike identiteedi ja privaatsuse kaitseks. Vastajate hinnangul ei tohiks ametnike turvalisus jääda ainult nende endi kanda, vaid see peaks olema osa organisatsiooni julgeoleku- ja riskijuhtimisest.

Kokkuvõttes näitab töö, et OSINT-ist tulenevad riskid on reaalsed ja seotud nii digitaalse infokeskkonna kui ka asutuse praktikatega. Ametnik on lisaks tööülesannete täitjale ka inimene, kelle turvatunne ja valmisolek oma tööd teha mõjutavad otseselt asutuse toimepidevust.

SUMMARY

Open-Source Intelligence (OSINT) Threats to the Privacy, Private Life and Identity of Public Officials and Their Relatives: The Case of the Estonian Police and Border Guard Board

The amount of publicly available information, and the possibilities to collect, link and analyse it, have increased significantly in recent years. OSINT is no longer only a tool for intelligence and security agencies, but part of a broader digital information environment in which data from different sources can also be used maliciously. This makes the protection of officials' identities, privacy and security particularly important.

The aim of this thesis was to explain how officers of the Police and Border Guard Board (PBGB) perceive OSINT-related risks, and what threats they see to the identity, privacy and security of officials and their close ones. The study also examined which protective measures are considered necessary and how existing organisational support is assessed. The empirical part was based on an anonymous online survey in which 90 PBGB officers participated.

The theoretical discussion indicated that risks arise not merely from the existence of public information, but from how fragments of information from different sources are combined and interpreted. In a digital environment, even seemingly trivial details can become problematic when placed in the right context or combined with other data.

Based on the survey, the most significant risks were perceived as personal data leaks, violations of privacy, doxxing, identity theft, threats, and reputational harm. Importantly, the threat is not limited to the official: respondents considered that it may also extend to close ones, thereby affecting a person's sense of safety and everyday life.

A key conclusion was that OSINT-related risks cannot be treated as solely an individual problem. Officials perform public duties, and targeting them may affect not only the individual but also the organisation's capacity to function, its credibility, and security more broadly.

The survey highlighted the need for more systematic organisational measures. Respondents considered regular OSINT, OPSEC and cyber hygiene training, practical guidelines, and more consistent principles for protecting officials' identity and privacy to be important. In their view, officials' security should not rest only on the individual, but should be part of the organisation's security and risk management.

In summary, the study shows that OSINT-related risks are real and linked both to the digital information environment and to organisational practices. An official is not only a task performer, but also a person whose sense of safety and willingness to do the job directly affect the organisation's resilience.

KASUTATUD KIRJANDUS

Akhgar, B., Bayerl, P. S., & Sampson, F. (Eds.). (2017). Police use of open source intelligence: The longer arm of law. In *Open source intelligence investigation: From strategy to implementation* (pp. 21–31). Springer. https://link.springer.com/chapter/10.1007/978-3-319-47671-1_3

Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019, May). Information security: A review of information security issues and techniques. In *2019 2nd international conference on computer applications & information security (ICCAIS)* (pp. 1-6). IEEE. <https://ieeexplore.ieee.org/document/8769504>

Anderson, B., & Wood, M. A. (2021). Doxxing: A scoping review and typology. <https://www.emerald.com/books/oa-edited-volume/12133/chapter/82199087/Doxxing-A-Scoping-Review-and-Typology>

Avaliku teabe seadus. RT I, 06.03.2026, 3. (2026). <https://www.riigiteataja.ee/akt/122032011010?leiaKehtiv>

Bambauer, D. E. (2013). Privacy versus security. *J. Crim. L. & Criminology*, 103, 667. https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/jclc103&id=696&men_tab=srchresults

Benes, L. (2013). OSINT, new technologies, education: Expanding opportunities and threats. A new paradigm. *Journal of Strategic Security*, 6(3), 22-37. <https://www.jstor.org/stable/26485053>

Block, L. (2024). The long history of OSINT. *Journal of Intelligence History*, 23(2), 95-109. <https://www.tandfonline.com/doi/full/10.1080/16161262.2023.2224091>

Bos, J. (2020). *Research ethics for students in the social sciences* (p 287). Springer Nature. <https://link.springer.com/content/pdf/10.1007/978-3-030-48415-6.pdf>

Bryman, A. (2016). *Social research methods*. Oxford University Press.

Chauhan, S., & Panda, N. K. (2015). *Hacking web intelligence: Open source intelligence and web reconnaissance concepts and techniques*. Syngress. Web Intelligence.

Douglas, D. M. (2016). Doxing: A conceptual analysis. *Ethics and Information Technology*, 18(3), 199-210. <https://link.springer.com/article/10.1007/s10676-016-9406-0>

Eesti Keele Instituut. (2026). *Eesti keele instituudi veebileht*. <https://eki.ee>

Eesti Teadusagentuuri töörühm (2025). *Inimuuringute hea tava*.

Eesti Vabariigi põhiseadus. RT I, 11.04.2025, 3. (2025).
<https://www.riigiteataja.ee/akt/127042011002?leiaKehtiv>

Euroopa Liidu Teataja. (2016). *Euroopa Liidu toimimise lepingu ja EL toimimise lepingu konsolideeritud versioonid* (59. aastakäik, C 202). <https://www.pria.ee/sites/default/files/2021-08/EL%20toimimise%20lepingu%20ja%20EL%20toimimise%20lepingu%20konsolideeritud%20versioonid.pdf>

Formanchuk, A. (2025). OSINT as a tool for proving war crimes. In *Maritime security of the Baltic-Black Sea region: Challenges and threats* (pp. 267–270).
<http://baltijapublishing.lv/omp/index.php/bp/catalog/view/689/18358/39134-1>

Fowler, F. J. (2012). *Survey research methods*. Thousand Oaks: Sage.

Fridman, O. (2019). On the “Gerasimov Doctrine”. *Prism*, 8(2), 100-113.
<https://www.jstor.org/stable/26803233?seq=1>

Gurkov, A. (2020). Personal data protection in Russia. In *The Palgrave handbook of digital Russia studies* (pp. 95-113). Cham: Springer International Publishing.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, 53(4), 1155-1175. <https://doi.org/10.1111/j.1468-2478.2009.00572.x>

Huang, Y. T., Lin, C. Y., Guo, Y. R., Lo, K. C., Sun, Y. S., & Chen, M. C. (2021). Open source intelligence for malicious behavior discovery and interpretation. *IEEE Transactions on Dependable and Secure Computing*, 19(2), 776-789.
<https://ieeexplore.ieee.org/document/9566808>

Huey, L., Ferguson, L., & Towns, Z. (2025). “Cops Need Doxxed”: Releasing Personal Information of Police Officers as a Tool of Political Harassment. *Crime & Delinquency*, 71(3), 714-739. <https://doi.org/10.1177/00111287241271069>

Hulnick, A. S. (2002). The downside of open source intelligence. *International Journal of Intelligence and CounterIntelligence*, 15(4), 565-579.
<https://doi.org/10.1080/08850600290101767>

Hwang, Y. W., Lee, I. Y., Kim, H., Lee, H., & Kim, D. (2022). Current status and security trend of OSINT. *Wireless Communications and Mobile Computing*, 2022(1), 1290129.
<https://doi.org/10.1155/2022/1290129>

Isikuandmete kaitse seadus. RT I, 06.03.2026, 10. (2026).
<https://www.riigiteataja.ee/akt/104012019011?leiaKehtiv>

Ivanjko, T., & Dokman, T. (2019). Open source intelligence (OSINT): Issues and trends. In *7th International Conference The Future of Information Sciences, INFUTURE2019* (pp. 191-196). FF Press. DOI: 10.17234/INFUTURE.2019.23

Kaitsepolitseiamet. (2026). *Aastaraamat 2025–2026*.
https://kapo.ee/sites/default/files/content_page_attachments/aastaraamat-2025-2026.pdf
Kasutatud 03.03.2026

Keen, P. G. (1977, June). The intelligence cycle: A differentiated perspective on information processing. In *Proceedings of the June 13-16, 1977, national computer conference* (pp. 317-320).
<https://doi.org/10.1145/1499402.1499458>

Koops, B. J., Hoepman, J. H., & Leenes, R. (2013). Open-source intelligence and privacy by design. *Computer Law & Security Review*, 29(6), 676-688.
<https://doi.org/10.1016/j.clsr.2013.09.005>

Korrakaitseadus, RT I, 07.04.2026, 7. (2011).
<https://www.riigiteataja.ee/akt/105072025012?leiaKehtiv>

Kruse, K. (2025, 8.jaanuar). «Kui kirstu vajad, siis tean ühte head firmat soovitada.» Sarisüütaja Erkki Pärn peab politseiniku postkasti jõudnud kirjade tõttu kohtule aru andma. *Postimees*.
<https://elu24.postimees.ee/8167414/kui-kirstu-vajad-siis-tean-uh-te-head-firmat-soovitada-sarisuutaja-erkki-par-n-peab-politseiniku-postkasti-joudnud-kirjade-tottu-kohtule-ar-u-andma>
Kasutatud 17.03.2026

- Majandus- ja Kommunikatsiooniministeerium. (2021). *Eesti digiühiskond 2030*. <https://valitsus.ee/sites/default/files/documents/2021-12/Eesti%20digiühiskond%202030.pdf>
- Majandus- ja Kommunikatsiooniministeerium. (2024). *Küberturvalisuse strateegia 2024–2030*. https://www.mkm.ee/sites/default/files/documents/2024-07/Kyberturvalisuse%20strateegia%202024-2030_labivalt_IT_vaatlik_Eesti.pdf
- Masso, A., Salvet, S., Lepik, K., (2014). Kvalitatiivse analüüsi tarkvara. K. Rootalu, V. Kalmus, A.Masso, ja T. Vihalemm (toim.), *Sotsiaalse analüüsi meetodite ja metodoloogia õpibaas*. <https://samm.ut.ee/kvalitatiivse-analyysi-tarkvara/>
- Merilo, J. (2025). *Avalikel allikatel põhineva luureteabe kasutamine hübriidsõjas ning julgeoleku võimendamiseks Eestis*. <https://doi.org/10.15158/phc5-nj20>
- Molfar Intelligence Institute. (2023, 9.veebuar). Identification of Russian soldier looter from Bucha by stolen AirPods. <https://www.molfar.institute/en/russian-soldier-looter-bucha/> Kasutatud 03.03.2026
- Narits, T. (2015). *Psühholoogiline kaitse Eesti julgeolekupoliitika kujundajate käsitluses*. Magistritöö. Sisekaitseakadeemia, sisejulgeoleku instituut.
- North Atlantic Treaty Organization. (2023). *Allied joint publication AJP-10.1: Allied joint doctrine for information operations* (Edition A, Version 1, with UK national elements). NATO Standardization Office. https://assets.publishing.service.gov.uk/media/650c03bf52e73c000d9425bb/AJP_10_1_Info_Ops_UK_web.pdf
- Newman, E. (2001). Human security and constructivism. *International Studies Perspectives*, 2(3), 239-251. <https://doi.org/10.1111/1528-3577.00055>
- Oerlemans, J. J., & Langenhuijzen, S. (2025). Balancing national security and privacy: Examining the use of commercially available information in OSINT practices. *International Journal of Intelligence and CounterIntelligence*, 38(2), 579-597. <https://doi.org/10.1080/08850607.2024.2387850>
- OpenAI. (2026). *ChatGPT*, suur keelemudel (21.mai versioon), <https://chatgpt.com>

Oxford Dictionaries. (2014). *Soft target*.
https://web.archive.org/web/20140103144928/http://www.oxforddictionaries.com/us/definition/american_english/soft-target

Pai, Y., & Krishna Prasad, K. Open source intelligence and its applications in next generation cyber security-A. DOI: <https://doi.org/10.47992/IJAEML.2581.7000.0100>

Pastor-Galindo, J., Nespoli, P., Mármol, F. G., & Pérez, G. M. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Access*, 8, 10282-10304. DOI: <https://doi.org/10.1109/ACCESS.2020.2965257>

Phythian, M. (Ed.). (2013). *Understanding the intelligence cycle* (pp. 23-30). London: Routledge.

Politsei ja piirivalve seadus, RT I, 13.11.2024, 38. (2024).
<https://www.riigiteataja.ee/akt/131122024038>

Politsei- ja Piirivalveamet. (2022, 19.märts). Kohus võttis vahi alla mehe, kes ähvardas ametnikku vene propagandakanalite keelamise pärast. <https://www.politsei.ee/et/uudised/kohus-vottis-vahi-alla-mehe-kes-ahvardas-ametnikku-vene-propagandakanalite-keelamise-paerast-10422>

Kasutatud 03.03.2026

Rahman, M. S. (2025, June 4). The art of open source intelligence (OSINT): Addressing cybercrime, opportunities, and challenges. *SSRN*. <https://dx.doi.org/10.2139/ssrn.5281845>

Rai, B. K., Verma, R., & Tiwari, S. (2021). Using open source intelligence as a tool for reliable web searching. *SN Computer Science*, 2(5), 402. <https://link.springer.com/article/10.1007/s42979-021-00777-4>

Riigikantselei. (2021). *Riigikaitse arengukava 2022–2031*.
<https://riigikantselei.ee/sites/default/files/documents/2022-02/Riigikaitse%20arengukava%202022%20-%202031.pdf>

Riigisaladuse ja salastatud välisteabe seadus. RT I, 03.02.2026, 13. (2026).
<https://www.riigiteataja.ee/akt/107032023010?leiaKehtiv>

Rootalu, K. (2014). Tunnused ja nende tüübid. K. Rootalu, V. Kalmus, A.Masso, ja T. Vihalemm (toim), *Sotsiaalse analüüsi meetodite ja metodoloogia õpibaas*. <https://samm.ut.ee/tunnused-ja-nende-tyybid/>

Samad, M. Y., Ningtiyas, B. K., Rosny, F., & Permatasari, D. A. (2024). Anticipating cyber espionage: Open source intelligence (OSINT) investigation and cyber counterintelligence. *Journal of Students' Research in Computer Science*, 5(2), 167-184. <https://doi.org/10.31599/288ab341>

Sazonov, V., Koort, E., Heinsoo, P., & Paas, K. (2020). *Sisejulgeoleku hübriidohtude tutvustamine*. Uuringuraport. Sisekaitseakadeemia. <https://doi.org/10.15158/bw26-2y66>

Seiler, V. (2024). Infopädevus e-õppe teel. *Tartu Ülikooli Raamatukogu aastaraamat*, 13. <https://doi.org/10.15157/tyrtar.v13i1.24231>

Siplane, V. (2025, 11.juuni). Harju Maakohus karistas Svetlana Burcevat riigireetmise ja sanktsiooni rikkumise eest kuueaastase vangistusega. *Eesti Kohtud*. <https://www.kohus.ee/ajakirjanikule/uudised/harju-maakohus-karistas-svetlana-burcevat-riigireetmise-ja-sanktsiooni>

Tartu Ülikool. (2023). *Tartu Ülikooli suunis tekstiroboti kasutamiseks õppetöös* (versioon 1, 28. aprill). Tartu Ülikool.

Tartu Ülikool. (i.a). Valimi moodustamine kvantitatiivuuringus. *Teadustöö alused*. https://sisu.ut.ee/teadustoo_alused/valimi-moodustamine-kvantitatiivuuringus/ Kasutatud 07.05.2026

Tartu Ülikool. (i.a). Andmekogumine, andmeanalüüs ja tulemuste esitamine kvantitatiivuuringus. *Teadustöö alused*. https://sisu.ut.ee/teadustoo_alused/andmekogumine-andmeanaluus-ja-tulemuste-esitamine-kvantitatiivuuringus/ Kasutatud 07.05.2026

Tartu Ülikool. (i.a). Tulemuste tõlgendamine, järeldused ja diskussioon. *Teadustöö alused*. https://sisu.ut.ee/teadustoo_alused/tulemuste-tolgendamine-jareldused-ja-diskussioon/ Kasutatud 07.05.2026

Tikk, E. (2007). Informatsioon ja õigus. *Õiguskeel*, (4). <https://www.justdigi.ee/sites/default/files/documents/2021-07/Eneken%20Tikk.%20Informatsioon%20ja%20õigus.pdf>

Ünver, A. (2018). Digital open source intelligence and international security: A primer. *EDAM Research Reports, Cyber Governance and Digital Democracy*, 8. <https://ssrn.com/abstract=3331638>

U.S. Department of Defense. (2011). *Operations security (OPSEC) guide*. Defense Technical Information Center. <https://apps.dtic.mil/sti/html/tr/AD1038572/>

Vabariigi Valitsus. (2023). *Eesti julgeolekupoliitika alused 2023*. https://www.riigiteataja.ee/aktalisa/3280/2202/3001/julgeolekupoliitika_2023.pdf

Van der Vet, F. (2021). Spies, lies, trials, and trolls: Political lawyering against disinformation and state surveillance in Russia. *Law & Social Inquiry*, 46(2), 407-434. <https://doi.org/10.1017/lsi.2020.36>

Van Puyvelde, D., & Rienzi, F. T. (2023). The rise of open-source intelligence. *European Journal of International Security*, 1-15. <https://doi.org/10.1017/eis.2024.61>

Walkow, M., & Pöhn, D. (2024). Systematically searching for identity-related information in the internet with OSINT tools. <https://doi.org/10.5220/0011644200003405>

Williams, H. J., & Blum, I. (2018). Defining second generation open source intelligence (OSINT) for the defense enterprise. RAND Corporation. <https://apps.dtic.mil/sti/html/trecms/AD1053555/>
Kasutatud 12.12.2025

Xu, L., Qereshniku, E., Hazari, H., & Edwards, M. (2023). Understanding national security threats enabled by artificial intelligence: Implications for CSIS. *Artificial Intelligence*, 101(9). https://sppga.ubc.ca/wp-content/uploads/sites/5/2023/06/CSIS_Report_2023.pdf

LISAD

Lisa 1. Saatekiri küsitluse läbiviimiseks

Tere,

Olen Helena Velba, Tartu Ülikooli infokorralduse eriala kolmanda kursuse tudeng ning viin läbi uurimistööd, mille eesmärk on hinnata riigisektori ametnike teadlikkust avatud allikate luurest (**OSINT – Open Source Intelligence**) ning sellega seotud võimalustest ja riskidest.

OSINT tähendab avalikult kättesaadava teabe sihipärast kogumist ja analüüsimist ning seda kasutatakse laialdaselt nii avalikus, era- kui ka kolmandas sektoris. Samas kujutab OSINT endas ka ohte – näiteks volitamata isikuandmete avaldamist, desinformatsiooni levitamist või tekib olukordi, kus mõjutustegevuse kaudu jõutakse asutuse jaoks kriitilise teabeni.

Käesolev uurimus keskendub riigisektori ametnike teadlikkusele OSINT-ist ning analüüsib PPA ametnike teadlikkust tuues näiteid ja paralleele Venemaa Föderatsiooni-Ukraina konfliktist, kus OSINT-i on muuhulgas kasutatud isikute tuvastamiseks ja sihtmärkide valimiseks avalikest allikatest kogutud teabe põhjal.

Teie vastused aitavad paremini mõista, kuidas OSINT-i kasutatakse, millised on sellega seotud riskid ning kuidas see mõjutab ametnike turvalisust.

Uurimise läbiviimiseks on 07.04.2025 saadud luba nr 1.1-14/1-3 Politsei- ja Piirivalveameti uurimistööde koostööstamise komisjonilt.

Küsitlus on anonüümne, saadud andmeid kasutatakse üldistatud kujul ning vaid lõputöö uurimise eesmärgil.

Küsitlus võtab Teie ajast 15 minutit ning sisaldab 31 küsimust.

Küsimustik on avatud ajavahemikul: **10.04.2025 kuni 21.04.2025.**

Lisa 2. Küsitluse vorm.

I. OSINT teadlikkus ja selle rakendused

Esimeses osas uuritakse, kui hästi olete kursis OSINT-iga ning millised on Teie hinnangul selle kasutusvõimalused.

1. Kas Te olete kursis terminiga OSINT (*open source intelligence*)?
 - Jah, olen tuttav mõistega
 - Jah, olen kuulnud, kuid ei tea täpsemalt
 - Ei ole
2. Kas Teie arvates kasutavad Eesti õiguskaitse- ja julgeolekuasutused OSINT-i oma ametlikus töös (nt uurimises, analüüsides, riskihindamistes)?
 - Jah
 - Ei
 - Ei tea
3. Millistes valdkondades üleüldiselt teate, et OSINT-i kasutatakse? (võite valida mitu vastust)
 - Õiguskaitse
 - Riiklik julgeolek
 - Küberjulgeolek
 - Ajakirjandus ja uuriv meedia
 - Ärisektor (nr konkurentsianalüüs)
 - Ei tea
 - Muu
4. Kui olete OSINT-i meetodeid või tööriistu kasutanud (nt *Osint Handbook*, avalikud andmebaasid, pildiotsingud), siis millisel eesmärgil?
 - See on osa minu tööst
 - Tööülesannete raames on abiks aga ei ole kohustuslik
 - Isiklikust huvist olen kasutanud
 - Ei ole kasutanud
 - Muu
5. Milliseid vastumeetmeid rakendate OSINT-i võimalike riskide vähendamiseks? (võite valida mitu vastust)
 - Kasutan sotsiaalmeediakontosid, kuid hoian need anonüümsed
 - Kasutan pseudonüüme või alternatiivseid kasutajanimed veebikeskkondades
 - Piiran avalikku ligipääsu oma isikuandmetele ja fotodele (nt privaatsussätetega)
 - Ei kasuta sotsiaalmeediakontosid
 - Olen teadlik OSINT-i ohtudest, kuid ei rakenda ühtegi vastumeedet
 - Muu
6. Kui oluline on Teie arvates OSINT õiguskaitse ja julgeoleku kontekstis?
Ei ole oluline (1) – Väga oluline (5) (*Likerti skaala*)

II. OSINT-i ohud ja riskid

Teises osas keskendutakse sellele, milliseid riske ja ohte võib OSINT kaasa tuua Teie hinnangul.

7. Hinnake skaalal, kui ohtlik võib Teie arvates olla OSINT-i kasutamine pahatahtlikel eesmärkidel õiguskaitse ja julgeoleku kontekstis?

Ei ole ohtlik (1) – Väga ohtlik (5) (*Likerti skaala*)

8. Milisel määral Teie arvates kujutab OSINT ametnike identiteedile, nende lähedastele ja turvalisusele ohtu?

Ametnikele

- Jah, väga
- Mingil määral
- Vähesel määral
- Ei kujuta ohtu
- Ei ohtu

Lähedastele

- Jah, väga
- Mingil määral
- Vähesel määral
- Ei kujuta ohtu
- Ei ohtu

9. Milliseid ohte peate OSINT-i kaudu ametnikele kõige suuremaks? (võite valida mitu vastust)

Doxing, doxxing, doksimine - eraeluliste või delikaatsete andmete kogumine ja avalikustamine internetis, isiku/asutuse kahjustamise eesmärgil.

Desinformatsioon - eksitav või vale teave, mida levitatakse teadlikult kellegi huvides.

Identiteedivargus - isiku identiteedi volituseta kasutamine ehk teise isiku tähtsate isikuandmete (nt nimi, isikukood, pangakaart) andmete kuritarvitamine.

- Isikuandmete lekitamine (privaatsuse rikkumine)
- Doxxing (sihitud andmete kogumine ja avaldamine)
- Desinformatsiooni levik (nt mainekahju)
- Identiteedivargus (nt libakonto)
- Isiklikud ähvardused (nt ametniku isiklikule sotsiaalmeediakontole)
- Ei näe ohtu
- Muu

10. Kas olete kunagi isiklikult kogenud olukorda, kus Teie või Teie kolleegi kohta oleks avalikult levinud tundlikku teavet OSINT-i tulemusel (nt lekkinud andmed, avalikustatud kodune aadress, deepfake)? (võite valida mitu vastust)

Deepfake - võlts-video või -heli, kus kellegi nägu või hääl on asendatud teise inimese omaga, kasutades tehisintellekti.

- Jah, olen isiklikult kogenud
- Jah, tean juhtumeid kolleegide kohta
- Ei ole kogenud
- Muu

11. Kui tihti puutute oma töös kokku olukordadega, kus peate suhtlema või tegelema isikuga otse (nt kinnipidamine, küsitlemine)?

- Igapäevaselt
- 1-3 korda nädalas
- Rohkem, kui 3 korda nädalas
- Mõned korrad kuus
- Mitte kunagi
- Muu

12. Kui Te teate, et Teid on võimalik OSINT-i abil leida, siis kas tunnete end oma tööülesandeid täites turvaliselt?

- Jah
- Ei
- Muu

13. Kui tunnete end tööülesandeid täites ebaturvaliselt või ohustatuna, siis millised on peamised põhjused? (võite valida mitu vastust)

- OSINT-i kaudu leitav teave minu ja/või mu lähedaste kohta
- Sotsiaalmeedias leviv vaenulik suhtumine ametnike suhtes
- *Doxxing* või muu tundliku info lekitamine
- Ametiasutuse pakutavad kaitsemeetmed on ebapiisavad
- Ei kehti (kui vastasite eelmises küsimuses “ei tunne”)
- Muu

14. Kas Teie kohta on sotsiaalmeedias või muudes avalikes allikates levitatud ametiga seondult negatiivset teavet (nt isikuandmeid avalikustatud või ilma loata filmitud)? (võite valida mitu vastust)

15. Kui mõelda sellele, et teie kohta võib OSINT-i kaudu koguda infot (nt Facebooki postitused, avalikud registrid), siis kuidas hindate oma asutuse reegleid sellise teabe haldamise osas?

- Reeglid on selged ja neist peetakse kinni
- Reeglid on olemas, kuid vajavad täiendamist
- Ei ole piisavalt reguleeritud
- Ei oska öelda
- Muu

16. Kui turvaliseks hindate oma isikuandmete kaitstust avalikes allikates oma asutuse poolt?

Ei ole turvaline (1) – Väga turvaline (5) (*Likerti skaala*)

17. Kas Teie arvates peaks OSINT-i võimalusi ja ohte käsitlema osana ametnike koolitusprogrammist?

- Jah
- Ei

III. OSINT hübriid- ja infosõja kontekstis

Kolmandas osas uuritakse Teie hinnangut sellele, kuidas OSINT-i võidakse kasutada hübriid- ja infosõja kontekstis.

Hübriidsõda – erinevate mõjutusvahendite (nt küberrünnakud, propaganda) kombineeritud kasutamine eesmärgiga destabiliseerida riiki või ühiskonda.

Infosõda – sihipärane info levitamine, moonutamine või varjamine eesmärgiga mõjutada vastase seisukohti, otsuseid ja ühiskondlikku arvamust.

18. Kas Teie arvates kasutatakse OSINT-i Eestis mõjutustegevuseks (nt desinformatsioon, narratiivide levitamine, trollimine)?

Desinformatsioon - vale või eksitav info, mida levitatakse teadlikult kellegi huvides.

Narratiiv - sihilikult kujundatud vaatenurk mingi sündmuse või olukorra kohta, et mõjutada inimeste arusaama (nt "meie oleme ohvrid", "Lääs on allakäigul").

Trollimine - internetipõhistes suhtluskanalites provotseeriv ja viha külvav tegevus.

- Jah
- Ei

19. Kui tõhusalt Teie arvates kasutab Venemaa OSINT-i Ukraina vastu sõja- ja mõjutustegevuses?

Infooperatsioon - sihipärane tegevus info levitamise, moonutamise või varjamise kaudu, et mõjutada sihtgrupi arvamusi, tundeid või käitumist.

Mõjutustehnika - konkreetne võte või meetod, mida kasutatakse inimeste veenmiseks või suunamiseks (nt hirmutamine).

- OSINT mängib olulist rolli infooperatsioonides
- OSINT on osa mõjutustehnikatest
- OSINT-i roll on olemas, kuid mitte määrav
- OSINT-i kasutamine on piiratud mõjuga
- Ei oska öelda
- Muu

20. Kas Teie teadmiste kohaselt on OSINT-i kasutatud Eestis riigiametnike (nt poliitikud, ametnikud) ja -asutuste vastu?

- Jah
- Ei

21. Kas Teie arvates peaks Eesti riigiasutused rohkem keskenduma ametnike identiteedikaitsele OSINT-i riskide kontekstis?

Identiteedikaitse - meetmed, mille eesmärk on kaitsta inimese isikut puudutavat teavet (nt nimi, isikukood, töökoht, kontaktandmed)

- Jah
- Ei

22. Kas Teie arvates peaks OSINT-i riskide ennetamine kuuluma Eesti riikliku küberturvalisuse strateegia alla?

- Jah
- Ei
- Muu

23. Kas Teie asutus pakub juhiseid või koolitusi identiteedikaitse ning andmete privaatsuse kohta?

(nt kuidas kaitsta oma töölaseid andmeid, sotsiaalmeediakontot, vältida isikuandmete lekkeid või OSINT-i kaudu tuvastamist)?

- Jah
- Ei

- Ei oska öelda
- Muu

24. Milliseid meetmeid peaks Teie asutus rakendama OSINT-i ohtude vähendamiseks ametnike identiteedi ja eraelu kaitseks? (avatud küsimus)

25. Sugu:

- Mees
- Naine

26. Vanuserühm:

- Alla 25 aasta
- 25-34 aastat
- 35-44 aastat
- 45-54 aastat
- 55 aastat ja vanem

27. Töökoht:

Palun märki büroo ja üksus, kus töötad (nt Põhja prefektuuri kriminaalbüroo, Põhja prefektuuri Lääne-Harju politseijaoskond).

Avatud vastus

28. Töö kategooria:

- Välitöö
- Sisetöö
- Kombineeritud (sise- ja välitöö)

29. Kas Teie andmed (nt nimi, ametikoht, kontaktid) on Politsei- ja Piirivalveameti ametlikul kodulehel avalikud?

- Jah
- Ei

30. Tööstaaž asutuses:

- Alla 1 aasta
- 2-5 aastat
- 6-10 aastat
- 11-15 aastat
- 16-20 aastat
- Üle 20 aasta

31. Kas Teil on ettepanekuid või täiendavaid tähelepanekuid seoses OSINT-I, selle riskide ja võimalike kaitsemeetmetega Politsei- ja Piirivalveametis? (avatud vastus)

Lisa 3. Kategoriseeritud vastuste näidis.

KATEGOORIA	SISU	ETTEPANEKUD
Teadlikkus ja koolitusvajadus	Koolitused, juhised, elulised näited	„Kuigi hetkel tulenevalt tööst mingi briefing tehakse - kuidas oma andmeid kaitsta, kuidas OSINT tehnikaid rakendada selliselt, et mitte oma andmeid "välja anda" siis need on üsna korrapäratud, ei ole ühtset koolitust ning ilmselt ka ühtset põhimõtet, kuidas PPA-s neid meetodeid rakendada. Ma arvan isegi, et vastavate teadmiste edastamine võiks toimuda juba Sisekaitseakadeemias õppekava raames.”
Tuvastatavus	Nimesiltide asendamine numbriga/koodiga; ametnike nimede/kontaktide vähendamine avalikes kanalites	„Töötajate avalikult leitavad kontaktandmed kodulehel ei tohiks sisaldada andmeid isiklike sidevahendite, meilikontode ega sünniaja kohta. Hetkel on amet seda ka järginud.” „Tundliku teave eemaldamine võimalikest teabe allikatest; ametnike identiteedi ja eraelu puudutav teabe peaks olema kaitstud, ametnike identifitseerimine võiks olla vähendatud, nt. numbriga; Ametnike teadlikkuse suurendamine OSINT-i ohtudest ja riskidest; See nimekiri võib pikendada oluliselt.”
Küberhügieen	Sotsiaalmeedia privaatsusseadused, täisnime kasutuse piiramine, eraelulise info vähendamine; juhised sotsiaalmeedia kasutuseks	„Tuleb teadvustada ohte ametnikele ja ümber korraldada PPA enda suhtumist sotsiaalmeediasse. Näiteks - kas 1 septembril peaks olema üleval pildid vormis ja nimesiltidega ametnikest viimas oma lapsi kooli, nii et on näha nende laste näod ja koolid ning jutus kirjeldatud ka pere igapäevane rütm või marsruut? Mida sellise info avaldamine meile annab vs mis riske see võimaldab ja millist suhtumist see portreerib?” „1) Turvaline ühendus (VPN), 2) Anonüümsed seadmed (mitte seotud ametiga) OSINT töö läbiviimiseks, 3) Kasutatavate seadmete konfigureerimine selliselt, et oleks tagatud anonüümsus vähemalt soovitud tasemel, 4) Kasutakontode konfigureerimine selliselt, et need sobivalt sulanduksid.”

OPSEC-meetmed	Eraldi kontod/seadmed/SIM; VPN; seadmete ja kontode seadistamine ning digijälgede vähendamine OSINT-tegevuses.	„Andmekaitse seisukohalt on kindlasti see ala üsna reguleerimata - mis mõnes mõttes annab vabad käed, aga kui juhtumipõhiselt vaadata, milliseid andmeid on kuskil näiteks PPA ametnikud kasutanud juhtumite lahendamiseks või analüüsiks siis kindlasti võib tekkida küsimusi ja dilemmasid.” „Jälgimine ja analüüs: Asutused võiksid kasutada OSINT-tööriistu, et jälgida veebis leviva teabe ja ametnike tegevuste jälgi ning tuvastada võimalikke riske, kui tekib oht, et ametniku identiteet või tundlik teave on avalikustatud, tuleb viivitamatult rakendada turvameetmeid, nagu konto sulgemine ja teadlikkuse tõstmine.”
Organisatsiooniline tugi	Tugi intsidentide korral; seire; ühtsed põhimõtted ja ressursid (sh kriisihaldus).	„Isikliku ja ametialase info lahutamine; turvateadlikkuse parandamine; kriisihaldus ja tugi; OSINT-monitoringu meeskond: väike sisemine üksus, kes jälgib, kas tundlik info PPA ja ametnike kohta ilmub avatud allikatesse, ja reageerib kohe.” „Teadlikkuse tõstmine ja koolitused, tehnilised ja praktilised meetmed, seire ja ennetav tegevus, ametnike toetamine kriisiolukordades.”
Reeglid	Selged reeglid ja ühtne praktika (mida tohib avaldada/teha); AK ja tundliku teabe käsitlemine organisatsiooni lised põhimõtted.	„Võtma seisukoha, mis kaitseks ametnike identiteeti ja eraelu. Hetkel on olukord, kus tundub, et kodanike "uudishimu" kaalub üle ametniku heaolu. Näiteks uudiste artiklites avaldatud ametnike nimed, pildid jne. Samuti jäädakse PPA siseselt eriarvamusele selles osas, mida tähendab AK ehk asutusesisese kasutamiseks mõeldud ametikoht.” „Teema peaks olema osa laiemast ametnike kaitse paketist. Nii nagu õpetame ametnikke laskma, käsi väänama ja sundi rakendama ning anname kaitseks kuulivesti, kaitseprillid jne, võiks õpetada ohte internetis ja kuidas nende eest kaitsta. Eriti oluline on see ühiskonda raputavate löi löhestavate sündmuste puhul, kus alati on õiguskaitse vastaseid ja minnakse vägagi isiklikuks.”

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Helena Velba

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose

„Ametnike ja nende lähedaste privaatsuse, eraelu ning identiteediga seotud ohud avatud allikate luure (OSINT) ajastul: Politsei- ja Piirivalveameti näitel”, mille juhendajad on Maia Klaassen ja Jaanika Merilo

reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada Tartu Ülikooli digitaalarhiivi kuni autoriõiguse kehtivuse lõppemiseni;

2. annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi kaudu Creative Commons'i litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni;

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

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

Helena Velba

23.04.2026