TARTU ÜLIKOOL

Sotsiaalteaduste valdkond

Ühiskonnateaduste instituut

Infokorralduse õppekava

Hanna Oruaas

Sotsiaalteaduslik simulatsioon organisatsioonilise küberturbe mõõtmisel

Lõputöö

Juhendaja: Sten Torpan, PhD

Tartu 2026

SISUKORD

SISSEJUHATUS

Kriis toob ühiskonna haavatavused nähtavale (Tierney, 2019). Siiski ei ole neid võimalik täielikult ette näha ega ära hoida ning ka kõige põhjalikuma ettevalmistuse korral on võimalik eelkõige nende mõju leevendada, mitte tervikuna välistada. Sotsiaalteaduslikus käsitluses mõistetakse kriisi üldjuhul ootamatu ja suure mõjuga olukorrana, mida iseloomustavad oht, määramatus ja ajasurve ning mis seab ohtu organisatsiooni või kogukonna võime oma eesmärke saavutada (Schaedler et al., 2022; Koch et al., 2026). Kriisid võivad olla erineva vormi, ulatuse ja ühiskondliku mõjuga, kuid need ei eksisteeri sõltumatult inimesest, vaid kriisist teeb kriisi inimlik haavatavus (Tierney, 2019). Just nende mitmetahulisus, kõrge määramatus ja mõju ühiskonnale muudavad kriisid oluliseks uurimisobjektiks ka sotsiaalteadustes (Tierney, 2019).

Kriiside uurimise teeb keerukaks asjaolu, et nende kujunemist ei ole enamasti võimalik täpselt prognoosida. Seetõttu ei saa kriisi tavaliselt uurida selle toimumise hetkel, vaid uurijal tuleb tugineda tagantjärele tehtud analüüsile või spetsiaalselt loodud uurimiskeskkondadele (Walker et al., 2011). Sobiliku uurimiskeskkonna saab luua sotsiaalteadusliku simulatsiooniga, millega saab keerukaid sotsiaalseid olukordi modelleerida ja kontrollitud keskkonnas läbi mängida, et uurida inimeste käitumist, otsustusprotsesse ja omavahelisi vastastikmõjusid (Squazzoni et al., 2013). Simulatsioon loob võimaluse uurida nähtusi, mille käsitlemine reaalses kriisiolukorras oleks keeruline, eetiliselt problemaatiline või praktiliselt raskesti teostatav. Lisaks tekib võimalus mõõta osalejate tajutud olukorrateadlikkus ehk inimese subjektiivset hinnangut sellele, kui hästi ta kujunevat olukorda mõistab (Edgar et al., 2012). See mängib rolli eeskätt keerukates ja kiiresti muutuvates olukordades, kus otsuste kvaliteet sõltub suurel määral sellest, kui adekvaatselt suudavad osalejad olemasolevat infot mõtestada.

Üks valdkond, kus kriiside ennetamine ja nendeks valmistumine on keskse tähtsusega, on küberturve. Küberturbe valdkonnas kasutatakse kriiside uurimiseks ja nendeks valmisoleku hindamiseks laialdaselt erinevaid õppuseid, sealhulgas lauaõppuseid, mille eesmärk on harjutada osalejate oskusi, teadmisi ja võimekust olukorda lahendada (Angafor et al., 2020). Juba pikalt on küberturbes levinud mõtteviis, et selle tehnilise valdkonna nõrgim lüli on inimene ise, kuid üha enam nähakse inimestes ka potentsiaalset tugevat küberturbe vastupanu sammast eeldusel, et kasutusel on läbimõeldud sotsiotehniline lähenemine (Heartfield & Loukas, 2018; Zimmermann et al., 2024; Khadka & Ullah, 2025). Just sellest tekkis huvi, kas küberturbe kontekstis oleks võimalik kasutada ka sotsiaalteaduslikku simulatsiooni, et hinnata küberturbe

kriisidega tegelevate inimeste tajutud olukorrateadlikkust. Sellest lähtuvalt püstitasin kaks uurimisküsimust, millest esimene tuleneb sisulisest huvist ja teine metodoloogilisest huvist:

1. Kuidas mõjutab tajutud olukorrateadlikkus küberturbe kriisi haldamist?
2. Kuidas sobib sotsiaalteaduslik simulatsioon organisatsioonilise küberturbe matkimiseks?

Uurimisküsimustele vastamiseks korraldasin kriisisimulatsiooni, milles osalesid keskastme juhid Riigi Infosüsteemi Ametist. Simulatsioonis osalejad pidid hindama kriisistsenaariumi infosüstide tõesust ning seejärel määrama oma kindlustunde hinnangute täpsuse suhtes.

Töö esimeses pooles loon ülevaate relevantsetest mõistetest, tutvustan tajutud olukorrateadlikkuse olemust ja mõõtmisvõimalusi, küberturbe ja kriisihalduse konteksti ja sotsiaalteaduslikku simulatsiooni kui uurimismeetodit. Metoodika osas tutvustan simulatsiooniuuringu loomise protsessi, asutuse konteksti, valimi moodustamist ja andmeanalüüsimetoodikat. Kolmandas peatükis esitan simulatsiooniuuringu tulemused ja neljandas peatükis tulemuste arutelu.

1. TEOREETILINE TAUST

1.1. Olukorrateadlikkus

Olukorrateadlikkus (ingl *situation awareness*) tähendab kõige üldisemalt seda, et inimene tajub, mis tema ümber toimub, mõistab nähtud info tähendust ning suudab selle põhjal ette aimata, mis võib juhtuda järgmisena ning just seetõttu peetakse seda üheks keskseks eelduseks heale otsustamisele dünaamilistes ja keerukates olukordades (Endsley, 1995). Teaduslikus käsitluses kirjeldatakse olukorrateadlikkust sageli kolme omavahel seotud tasandina: olukorra elementide märkamine, nende tähenduse mõtestamine ja lähituleviku seisundi prognoosimine (Endsley, 1995). Ka uuem kirjandus kinnitab, et olukorrateadlikkus ei ole pelgalt „hea tunnetus", vaid oluline kognitiivne protsess, mis mõjutab otsuste kvaliteeti, koostööd ja sooritust väga erinevates valdkondades, sealhulgas tervishoius, kõrge riskiga meeskondades ja tehnoloogiliselt vahendatud tööolukordades (Weller et al., 2024).

See teeb olukorrateadlikkusest väärtusliku mõiste valdkondades, kus otsuseid tuleb teha kiiresti, ebakindlates tingimustes ja sageli puuduliku info põhjal, näiteks lennunduses, kriisijuhtimises, tervishoius või küberturbe kontekstis (Munir et al., 2022). Uuemad ülevaated osutavad, et olukorrateadlikkuse uurimine on liikunud üha enam üksikisiku tasandilt ka meeskondliku ja süsteemse toimimise suunas ehk oluline ei ole ainult see, mida üks inimene märkab, aga ka see, kuidas infot meeskonnas käsitletakse ja ühiseks arusaamaks kujundatakse (Weller et al., 2024).

Olukorrateadlikkust mõõdetakse teaduses mitmel viisil. Üks tuntumaid võtteid on SAGAT (*Situation Awareness Global Assessment Technique*), kus olukorra simulatsioon (tehislik läbimäng) peatatakse ning osalejalt küsitakse täpseid küsimusi selle kohta, mida ta olukorra kohta teab, see püüab hinnata olukorrateadlikkust võimalikult otseselt (Endsley, 2000; Munir et al., 2022). Teine levinud meetod on SART (*Situation Awareness Rating Technique*), kus inimene hindab pärast ülesannet ise oma teadlikkust ja tähelepanu olukorra suhtes, seda on lihtsam kasutada kuid tulemus on subjektiivsem (Munir et al., 2022). Samal ajal rõhutavad süstemaatilised ülevaated, et praktikas on olukorrateadlikkuse mõõtmine mitmekesine (Ghaderi et al., 2023; Cooper et al., 2013; Munir et al., 2022) ning sageli kasutatakse mitme meetodi kombinatsiooni, sest olukorrateadlikkus sisaldab nii vahetut teadmist, enesehinnangut kui ka käitumuslikke ja füsioloogilisi jälgi (Zhang et al., 2023). Kasutatakse ka vaatluslikke, soorituspõhiseid ja kombineeritud meetodeid, sest uurijad soovivad mõista, millise info najal tulemuseni jõuti (Zhang et al., 2023).

Olukorrateadlikkuse mõõtmise väärtus seisneb selles, et see aitab nähtavaks teha otsustamise "varjatud kognitiivse poole" ja kas probleem tekkis info vähesusest, valest tõlgendusest, suutmatuse tõttu olukorra arengut ette näha või hoopis sellest, et meeskond ei loonud ühist arusaama toimuvast. Uuemad uuringud rõhutavad, et selline teadmine on oluline koolituse, simulatsioonide, tööprotsesside, kasutajaliideste ja ohutussüsteemide arendajatele, sest olukorrateadlikkuse mõõtmine võimaldab hinnata mitte ainult seda, kas inimene või meeskond sai ülesandega hakkama, vaid ka miks see konkreetsel ajahetkel nii läks (Harper et al., 2023; Weller et al., 2024). Selle tõttu on olukorrateadlikkuse mõõtmine väärtuslik nii õppimise, hindamise kui ka teaduse seisukohalt. Küll aga on simulatsioonipõhiseid olukorrateadlikkuse mõõtmise tehnikaid ka kriitiliselt hinnatud, viidates just, et metoodika on veel "toores" ja vajab arendamist (Cooper et al., 2013; Ghaderi et al., 2023). Süsteemsed ülevaated näitavad, et eri meetoditel on erinevad tugevused ja nõrkused ning isegi kriitikud näevad metoodikas potentsiaali kui seda edasi arendada (Cooper et al., 2013; Ghaderi et al., 2023, Munir et al., 2022).

1.1.1. Tajutud olukorrateadlikkus

Kuna olukorrateadlikkust on keeruline objektiivselt hinnata, siis on teaduslikus lähenemises hakatud mõõtma ka tajutud olukorrateadlikkust. Tajutud olukorrateadlikkus (ingl *perceived situational awareness, PSA*) viitab sellele, kuidas inimene ise hindab oma arusaama toimuvast, samal ajal kui olukorrateadlikkus viitab tegelikule teadmisseisundile (Edgar et al., 2012; Thoelen et al., 2020).

Seega ei ole olukorrateadlikkus ja tajutud olukorrateadlikkus päris sama asi, sest esimene viitab tegelikule teadlikkuse tasemele, teine aga kirjeldab subjektiivset enesehinnangut ja enesekindlust oma olukorrateadlikkuses, mis ei pruugi olla tegeliku teadlikkusega kooskõlas (Edgar et al., 2012; Thoelen et al., 2020). Edgar et al. (2012) illustreerib selle olulisust näitega, kus 1994. aastal, Colorados hukkus õnnetuses 14 tuletõrjujat, sest päästemeeskonna juht hindas olukorda valesti ning oli oma hinnangus liigselt enesekindel – ehk madal olukorrateadlikkus on kõige ohtlikum siis, kui inimene seda ise madalana ei tunneta. Kui inimene on teadlik oma madalast olukorrateadlikkusest, siis on ta ettevaatlikum, teeb vähem riskantsemaid otsuseid ja kontrollib suurema tõenäosusega infot, mis talle antud on (Edgar et al., 2012). Seega on teaduses nende erinevus oluline, sest inimese hinnang oma teadlikkusele ei pruugi alati kattuda tema tegeliku suutlikkusega olukorda õigesti tõlgendada ehk objektiivsed ja subjektiivsed olukorrateadlikkuse mõõdikud võivad teineteisest märkimisväärselt lahkneda (Edgar et al., 2012; Thoelen et al., 2020). Näiteks on leitud, et automatiseeritud keskkondades võivad

inimesed hinnata oma olukorrateadlikkust kõrgeks isegi siis, kui nende ohtude äratundmine on aeglasem või ebatäpsem (Nasser et al., 2025). Teaduses mõõdetakse tajutud olukorrateadlikkust enamasti ülesande ajal või järel täidetavate küsimustikega, millest tuntumad on LETSSA (*Low-Event Subjective Situation Awareness*) ja QASA (*Quantitative Analysis of Situation Awareness*) (Moens et al., 2026; Edgar & Edgar, 2007). QASA-meetodi aluseks on eeldus, et hea olukorrateadlikkus väljendub suuresti selles, kuivõrd täpselt suudab inimene eristada tõest ja väära infot ning milline on tema kalduvus infot pigem tõese või väärana käsitleda (Edgar & Edgar, 2007). Meetod hõlmab tavaliselt osalejatele info esitlemist, mida nad hindavad tõeseks või vääraks ja seejärel peavad osalejad määrama enesekindluse oma hinnangule (Edgar & Edgar, 2007). Värskem koondülevaade rõhutab, et kõige usaldusväärsem pilt tekib siis, kui subjektiivseid ja objektiivseid mõõtmisviise kasutatakse koos, mitte eraldi (Moens et al., 2026; Zhang et al., 2023). Tajutud olukorrateadlikkuse mõõtmise väärtus seisneb selles, et see aitab uurida, kui kindlalt inimesed oma arusaamadesse suhtuvad ning kui hästi see enesehinnang vastab tegelikule sooritusele.

1.2. Küberturve kui sotsiotehniline protsess

Küberturve tähendab digitaalsete süsteemide ja andmete kaitsmist selliste rünnete, häirete ja kuritegevuse eest, mis võivad kahjustada andmete konfidentsiaalsust, terviklust või käideldavust (Admass et al., 2024). Lühidalt tähendab konfidentsiaalsus, et andmetele pääsevad ligi ainult selleks volitatud isikud, terviklus viitab, et andmeid ei ole volituseta muudetud ning käideldavuse eesmärk on tagada, et andmed on õigeaegselt kättesaadavad ja kasutatavad (Andmekaitse Inspektsioon, 2025). Kui aga andmete konfidentsiaalsus, terviklus või käideldavus saavad rikutud mistahes põhjusel, nimetatakse seda küberintsidendiks (RIA, 2025). Aastal 2024 kahekordistus Eestis registreeritud küberintsidentide arv võrreldes varasema aastaga ning 2025. aasta lõpuks oli arv kolmekordistunud (RIA, 2026a), mis viitab sellele, et intsidentide kasvav esinemissagedus muudab küberturbe teema ühiskonna jaoks järjest aktuaalsemaks. Tänapäevases teaduses ei käsitleta küberturvet enam üksnes tehnilise probleemina, vaid sotsiotehnilise nähtusena, kus turvalisus sõltub samaaegselt tehnoloogiast, inimkäitumisest, organisatsioonikultuurist ja juhtimisest (Khadka & Ullah, 2025; Pollini et al., 2022). Seetõttu võib küberturvalisus olla ka sotsiaalteaduses oluline, sest uurimisfookus võib olla tehnoloogiat kasutatavate inimeste otsustamisprotsess, usaldus, õppimine või isegi institutsioonide toimepidevus (Whitty et al., 2024; Khadka & Ullah, 2025).

Viimase viia aasta jooksul on küberturvalisuse olulisus maailmas kasvanud, sest ühiskonna digitaliseerumine on kiirenenud ning sellega koos on laienenud ka ründealad ja võimalike

kahjude ulatus (Admass et al., 2024). COVID-19 perioodil laialdaseks muutunud kaugtöö tõi eriti nähtavale, et küberrisk ei teki ainult serveriruumis, aga ka inimeste igapäevastes tööpraktikates, kodustes keskkondades ja harjumustes; see muutis "inimfaktori" küberturvalisuse keskseks küsimuseks (Whitty et al., 2024). Rõhutatakse, et organisatsioonid peavad liikuma üksikute tehniliste kaitsemeetmete juurest laiemale vastupanuvõime, ohuteabe kasutamise ja ennetava juhtimise mudelile (Saeed et al., 2023). Küberturvalisuse kasvavat tähtsust näitab ka see, et see on üha tugevamalt seotud elutähtsa taristu, avalike teenuste ja regulatsioonidega. Küberintsidente nähakse järjest enam ühiskondliku ja poliitilise, mitte pelgalt IT-riskina (Markopoulou & Papakonstantinou, 2021). Nii on küberturvalisusest saanud valdkond, mis on digitaalse ühiskonna kriitiline alustala.

1.2.1. Organisatsiooniline küberturve

Organisatsiooniline küberturve (ingl *organizational cybersecurity*) viitab küberturbe käsitlusele, mille keskmes on organisatsiooni inimesed, protsessid, vastutusjaotus ja otsustusloogika. Kui tehniline küberturve keskendub näiteks ligipääsukontrollile, seirele ja haavatavuste parandamisele, siis organisatsiooniline küberturve seob need tegevused laiemasse juhtimisloogikasse, kus keskmes on organisatsiooni eesmärgid (Handri et al., 2024; Liu et al., 2025). Neid on oluline eristada, sest teaduskirjandus on korduvalt osutanud, et tehnoloogiale liigne toetamine jätab tahaplaanile inimfaktorid ja organisatsioonikultuuri, kuigi just need mõjutavad tugevalt küberturbe tegelikku toimimist (Handri et al., 2024; Sutton & Tompson, 2025). Lisaks saab läbi organisatsioonilise küberturbe pöörata tähelepanu töötajate teadlikkusele, sisekommunikatsioonile, kriisiks valmisolekule ning varasematest juhtumistest õppimisele.

Organisatsiooniline küberturve tähendab seega küberturbe kujundamist organisatsioonilise protsessina, milles määratletakse rollid, hinnatakse riske, kehtestatakse reeglid, korraldatakse koolitusi ning luuakse mehhanismid intsidentidele reageerimiseks ja tegevuste ülevaatamiseks (Culot et al., 2021; Liu et al., 2025). See hõlmab ka seda, kuidas inimesed küberturvet mõistavad, infot tajuvad, vastutust tunnetavad ja ebakindlates olukordades otsuseid langetavad. Juhtimiskirjanduses eristatakse ka inimeste suunamist ja protsesside haldamist, mille kohaselt saab protsesse standardiseerida, mõõta ja korrigeerida, kuid inimeste puhul sõltub tulemus suurel määral juhtimisviisist, usaldusest ja tähendusloome võimalusest (Wang et al., 2022).

Küberturbe puhul tekib seetõttu pinge reeglite ja inimeste liigse kontrollimise vahel. Organisatsioonid käsitlevad töötajaid sageli "nõrgima lülina" ja või "inimriskina", mistõttu püütakse ka inimesi kontrollida, standardiseerida ja hallata (Zimmermann et al., 2024; Khadka

& Ullah, 2025). Liigne kontrollimine võib aga vähendada sisemist vastutustunnet, soodustada soodustada reeglitest möödahiilimist ning süvendada süüdistavat turvakultuuri (Sutton & Tompson, 2025; Panteli et al., 2025). Seetõttu peaks organisatsiooniline küberturve käsitlema inimesi küberturbe aktiivse osalisena, kelle tegutsemist toetavad juhtkonna eeskuju, kasutajasõbralikud reeglid ja psühholoogiliselt turvaline keskkond (Colabianchi et al., 2025; Tejay & Winkfield, 2025; Panteli et al., 2025). Nii tuleb fookusesse inimeste juhtimine ja suunamine, mitte nende kontrollimine.

1.3. Kriisihaldus

Kriisi käsitletakse juhtimis- ja kriisikirjanduses tavaliselt olukorrana, mis on osaliste jaoks ootamatu, suure mõjuga ning tekitab kõrget ebakindlust ja ohtu olulistele eesmärkidele. See on sündmus või sündmuste ahel, mis ületab tavapärase toimetuleku loogika ja nõuab kiiret otsustamist puuduliku info tingimustest (Schaedler et al., 2022; Koch et al., 2026). Kriisihaldust käsitletakse seega kui pidevat ja sihipärast tegevuste kogumit, mille eesmärk on ohtu märgata, selle tähendust hinnata, kahju piirata ning võimalusel kriisi mõju ennetada või vähendada (Vasickova, 2020). See tähendab, et kriisihaldus ei alga alles kriisi puhkemise hetkel, vaid hõlmab valmisoleku kujundamist, protsesside loomist, hoiatusmärkide jälgimist ja hilisemat õppimist, et järgmistes olukordades paremini toime tulla (Vasickova, 2020). Samas ei toimu kriisihaldus kunagi täielikult stabiilsetes tingimustes, isegi parima ettevalmistuse juures. Kriisidega kaasnevad tavaliselt ajasurve, ebakindlus, puudulik informatsioon ja erinevate eesmärkide vaheline pinge, mistõttu tuleb otsuseid teha keerulistes ja kiiresti muutuvates oludes (Carmine et al., 2021; Deverell & Ganic, 2024; Tierney, 2019). Selle tõttu sõltub kriiside lahendamine suurel määral sellest, kuidas inimesed olukorda mõistavad, millist infot nad usaldavad ja milliseid tegevusi selle põhjal kavandavad.

1.3.1. Küberturbe kriisid

Küberturbe kriis on selle üldise loogika erivorm, mis saab alguse küberturbe intsidendist. Intsident muutub kriisiks siis, kui tehniline intsident kasvab mõjult ja ulatuselt selliseks, et see hakkab ohustama organisatsiooni või ühiskonna põhifunktsioone, ületab tavapärast intsidendihalduse võimekust ning areneb kiiresti laiemaks juhtimis-, maine- või ühiskondlikuks kriisiks (Li & Liu, 2021; ENISA, 2024).

Küberründed ei toimu juhuslikult, nende ajendid ulatuvad rahalisest kasust ja andmete vargusest kuni kättemaksu, ideoloogilise vastandumise või poliitilise surve avaldamiseni, mistõttu peegeldavad küberintsidendid sageli nii kuritegelikke kui ka geopoliitilisi eesmärke

(Chng et al., 2022; Seebruck, 2015). Eesti näited illustreerivad seda hästi. Avalikus sektoris on poliitilise mõõtmega rünnaku näiteks 2007. aasta pronksiöö rünnakulaine, mis pani proovile Eesti riigi digitaalse toimepidevuse (ERR, 2017). Sarnane ideoloogiline muster ilmus 2022. aastal pärast Narva tanki teisaldamist, kui Eesti vastu suunati kõige ulatuslikumad ründed pärast pronksiööd (ERR, 2022). Erasektoris on sagedasem rahaline motiiv. RIA andmetel kaotasid Eesti ettevõtted 2022. aastal petuskeemide ja libaarvete tõttu kümneid tuhandeid eurosid, mis näitab, et küberintsidendi mõju võib avalduda otse finantskahjuna (RIA, 2023). Samuti proovitakse lisaks rahale kätte saada ka andmeid või ligipääse kriitilistele süsteemidele. Aastal 2024 tuli avalikuks Apotheka kliendiandmete leke, kus kurjategijad said kätte ligikaudu 700000 kliendi andmed, sealhulgas isikukoodid, kontaktandmed ja käsimüügi ostuajalugu (ERR, 2024). Juhtum näitab, et küberintsidendi eesmärk võib alternatiivselt otsesele rahalisele väljapressimisele olla ka suuremahulise tundliku andmehulga kätte saamine ja selle edasi müümine.

Teaduskirjandus rõhutab ka seda, et küberturbe kriisid on olemuselt sotsiotehnilised, mis tähendab, et kahju ei teki ainult infosüsteemides, vaid võib avalduda usalduskriisi, juhtimisraskuste ja ahelmõjudena teistes elutähtsates süsteemides (Backman, 2020; Prümmer et al., 2024).

1.3.2. Kriiside uurimine ja mõõtmine

Kriisihalduse efektiivsuse uurimisel ei keskenduta üksnes sellele, kas kriis lahendati edukalt, vaid ka sellele, kuidas organisatsioon või institutsioon kriisi jooksul tegutses. Uurijad on toonud välja, et efektiivsust saab hinnata näiteks selle järgi, kui kiiresti suudetakse olukorda mõtestada, olulisi osapooli teavitada, koostööd korraldada, ressursse suunata ning avalikkusele selget ja kontrollitud infot vahendada (Deverell & Ganic, 2024). Üha olulisemaks on muutunud arusaam, et kriishalduse edukus sõltub sellest, kuidas inimesed kriisiolukorras infot kätte saavad, seda mõistavad ja selle põhjal tegutsevad. Seetõttu uuritakse kriisihaldust ka haavatavuse vaatenurgast, pöörates tähelepanu kommunikatsioonitõketele, väärinfole ja erinevate sotsiaalsete rühmade ebavõrdsele toimetulekule (Hansson et al., 2020; Torpan, 2025). Sellest tulenevalt kasutatakse kriisihalduse uurimisel üha enam stsenaariumipõhiseid meetodeid ja simulatsioone, mis võimaldavad analüüsida nii institutsioonide valmisolekut kui ka erinevate sihtrühmade vajadusi võimalikes kriisiolukordades (Orru et al., 2025; Torpan, 2025). Niisugused lähenemised aitavad mõista, et efektiivne kriisihaldus tähendab ka võimet kohaneda, õppida ja teha põhjendatud otsuseid ebakindlates tingimustes (Deverell & Ganic, 2024; Vasickova, 2020).

1.3.3. Organisatsioonilise küberturbe haavatavuse elemendid

Sotsiaalsete ja organisatsiooniliste protsesside analüüsimisel on oluline vaadelda mitte ainult seda, milline info inimesteni jõuab, aga ka seda, kuidas nad infot otsivad, tõlgendavad, omavahel jagavad ja usaldavad. Nii ka küberturbe valdkonnas. Seetõttu on organisatsioonilise küberturbe haavatavuste mõistmisel olulised eelkõige infokäitumine, kommunikatsiooniga seotud haavatavused, info kvaliteet ja organisatsiooniline teadmus. Infokäitumine aitab selgitada, mida inimesed infoga teevad (Wilson, 1999; Robson & Robinson, 2013). Kommunikatsioonihaavatavus näitab, kuidas teabe kättesaadavus ja mõistmine võib tegutsemisvõimet mõjutada (Hansson et al., 2020). Info kvaliteedi segaja võib suunata tegutsemis- ja otsustustrajektoori valesse suunda (Shahbazi & Bunker, 2024). Organisatsiooniline teadmus seob protseduurid, rollid ja infoallikad institutsionaalse mäluga (Walsh & Ungson, 1991). Erinevad sotsiaalsed fenomenid aitavad selgitada, miks samas olukorras võivad mõned inimesed või organisatsioonid kujundada kiiresti toimiva arusaama, teised aga takerduda ebaselgusse, killustunud tõlgendustesse või valedesse järeldustesse (Wilson, 1999; Hansson et al., 2020; Shahbazi & Bunker, 2024).

Infokäitumine

Infokäitumine on neist nähtustest kõige üldisem, sest see kirjeldab viise, kuidas inimesed infot kontrollivad, otsivad, leiavad, väldivad, hindavad ja kasutavad (Wilson, 1999; Robson & Robinson, 2013). Wilsoni (1999) käsitluses on infokäitumise keskmes ebakindluse vähendamine, sest inimene ei otsi (ega jaga) infot juhuslikult, vaid püüab selle abil lahendada probleemi või kujundada olukorrast arusaama. Savolaineni (2007) järgi on infokäitumine ühtlasi katusmõiste, mis seob üksikud otsingutegevused laiema sotsiaalse ja praktilise tegevusega. Seega sõltub info kasutamine ka rollidest, harjumustest, kogemusest ja olukorra tajutud tähendusest. Organisatsioonilises kontekstis on see relevantne, sest infokäitumine määrab, millist infot peetakse asjakohaseks, millist allikat usaldatakse ja millist kontrollitakse ning millal tajutakse vajadust lisainfo järele. Seega kujuneb ühine arusaam olukorrast juba enne ametlikke otsuseid suurel määral inimeste infokäitumise kaudu (Wilson, 1999; Savolainen, 2007).

Kommunikatsioonihaavatavus

Kommunikatsioonihaavatavus (ingl *communication-related vulnerability*) osutab sellele, et haavatavus tuleneb kommunikatiivse keskkonna iseärasusest. Hansson et al. (2020) näitavad, et inimesed ja rühmad võivad muutuda haavatavaks siis, kui nad ei pääse infole ligi, ei mõista seda, ei suuda hinnata selle olulisust või ei saa seda kasutada enda olukorra parandamiseks.

Selline haavatavus võib tekkida näiteks siis, kui sõnumid on liiga keerulised, kanalid killustunud, info on vastuoluline või saaja kontekstiga pole arvestatud. Kommunikatsioonihaavatavus on vaheaste infokäitumise ja otsustamise vahel, sest see mõjutab, kas kogutud info muutub tegelikuks olukorramõistmiseks või jääb kasutamata (Hansson et al., 2020).

Info kvaliteedi segajad

Väärinfo (ingl *misinformation)* all mõistetakse eksitavat infot, mida ei pruugita levitada pahatahtlikult, kuid mis võib sellest hoolimata moonutada arusaamu ja suunata tegevust vales suunas (Wardle, 2018). Süstemaatiline kirjanduse ülevaade osutab, et väärinfo, desinformatsioon ja "fake news" on kujunenud interdistsiplinaarseks uurimisväljaks, kuna nende mõju ulatub individuaalsetest uskumustest kollektiivsete otsuste ja institutsionaalse usalduseni (Broda & Strömbäck, 2024). Kriitiliste intsidentide otsustusprotsesside ülevaates ilmneb, et keerulistes ja ajasurvelistes olukordades muutub relevantse ja irrelevantse info eristamine ise oluliseks väljakutseks (May et al., 2023). Infoüleküllus tekib siis, kui info maht, kiirus või keerukus ületab inimese või organisatsiooni töötlemisvõime ning selle tagajärgedeks võivad olla kognitiivne ülekoormus, raskem prioriseerimine ja halvenenud otsustamine (Shahrzadi et al., 2024). Nii võib probleem seisneda mitte info puuduses, aga hoopis selles, et oluline info mattub infomüra alla (Broda & Strömbäck, 2024; May et al., 2023; Shahrzadi et al., 2024).

Organisatsiooniline teadmus

Organisatsioonilise teadmuse alla kuuluvad nii teadmushaldus, organisatsiooniline mälu kui ka transaktiivne mälu. Walsh ja Ungsoni (1991) klassikalise käsitluse järgi talletub organisatsiooniline mälu erinevatesse "hoiukohtadesse", nagu üksikisikud, rollid, protseduurid, struktuurid ja kultuurilised praktikad. Wegneri (1987) transaktiivse mälu teooria peab oluliseks ka teadmist, kas mingit infot või ekspertiisi omab ja kuidas selleni jõuda. See tähendab, et organisatsioon "mäletab" lisaks dokumentidele ka tööviiside, tavade ja sisemiste või väliste ekspertiiside kaudu. Uuem teadmushalduse kirjandus rõhutab, et kriisides on teadmus operatiivne võimekus siduda hajutatud infot, muuta kogemus kasutatavaks teadmuseks ning toetada õppimist ka väga muutlikes oludes (Schiuma et al., 2021). Seetõttu aitab organisatsiooniline teadmus vähendada olukordi, kus iga uus häire mõjub enneolematu ja halvasti mõistetavana. Organisatsiooniline mälu väljendab võimet eristada, milliseid varasemaid kogemusi tasub uues olukorras rakendada ja milliseid mitte. Nii loob

teadmushaldus silla üksikute infokildude ja kollektiivse tegutsemisvõime vahel (Walsh & Ungson, 1991; Schiuma et al., 2021).

Kokkuvõttes moodustavad infokäitumine, kommunikatsioonihaavatavus, info kvaliteedi segajad ja organisatsiooniline teadmus ühtse analüütilise raamistiku, mille abil on võimalik mõista, kuidas keerulistes olukordades kujuneb või laguneb ühine arusaam tegelikkusest (Mayer et al., 1995; Shahbazi & Bunker, 2024). Neid nähtuseid on võimalik läbi mõeldud stsenaariumis infosüstidega esile kutsuda.

1.4. Sotsiaalteaduslik simulatsioon

Sotsiaalteaduslik simulatsioon on meetod, mis aitab mõista keerulisi olukordi nii, et uurija ei piirdu ainult nende kirjeldamisega, vaid saab neid teadlikult läbi mängida ja analüüsida (Squazzoni et al., 2013; Axelrod, 2006). Selle keskne väärtus seisneb selles, et simulatsioon loob kontrollitud, kuid sisuliselt realistliku keskkonna, kus on võimalik uurida, kuidas inimeste otsused, vastastikmõjud ja institutsionaalsed tingimused kujundavad sündmuste kulgu (Axelrod, 2006). Oma olemuselt sarnaneb simulatsioon lauaõppusega, mille eesmärk on harjutada või mõõta osalejate teadmisi, oskusi ja võimekust olukorda lahendada (Angafor et al., 2020). Sotsiaalteadusliku simulatsiooni põhiline erinevus lauaõppusega on just see, et fookuses on osalejate käitumine, otsuste langetamine, organisatsiooniline mõjutatus, info-käsitlus ja teadlikkus, mitte praktilised oskused ja teadmised (Axelrod, 2006; Squazzoni et al., 2013). Nii ei vaadelda üksnes seda, mis juhtus, vaid püütakse aru saada, miks ja milliste mehhanismide kaudu see juhtus (Axelrod, 2006; Squazzoni et al., 2013). Simulatsioon on iseseisev teaduslik lähenemine, mis aitab uurida keerukaid, raskesti vaadeldavaid või eetiliselt tundlikke nähtusi (Squazzoni et al., 2013).

Seetõttu peetakse simulatsiooni kasulikuks meetodiks olukordades, kus päriselu on liiga keerukas, kiire või ettearvamatu (nt kriisid), et seal toimivaid protsesse vahetult uurida (Axelrod, 2006; Asakura et al., 2021; Walker et al., 2011). Meetodi tugevus väljendub ka võimaluses siduda erineva tasandi protsesse, näiteks saab korraga vaadelda üksikosalejate otsustusprotsesse ja laiemat süsteemset infokäitumist (Squazzoni et al., 2013).

Sotsiaalteaduslikku simulatsiooni saab kasutada nii õppimismeetodina kui ka uurimis- ja hindamismeetodina. Õppimismeetodina võimaldab simulatsioon harjutada otsustamist, koostööd ja probleemilahendust turvalises, kuid pingelises olukorras, mis sarnaneb tegelikkusega rohkem kui tavapärane klassiruumiõpe (Chernikova et al., 2020). Uurimis- ja hindamismeetodina annab see võimaluse koguda süstemaatilist teavet selle kohta, kuidas

inimesed infot tõlgendavad, teadmisi rakendavad ja keerulistes olukordades tegutsevad (Asakura et al., 2021). Samas sõltub simulatsiooni teaduslik väärtus sellest, kui läbipaistev, põhjendatud ja valideeritud on selle ülesehitus ja mõõdikud (Rahmandad & Sterman, 2012; Wang, 2017).

Simulatsiooni kui uurimis- ja õppemeetodit kasutatakse sageli kriiside uurimisel, sest päriselulised kriisid on raskesti ette ennustatavad ning neid ei ole võimalik uurija jaoks kontrollitud tingimustes esile kutsuda. Seetõttu võimaldavad kriisisimulatsioonid luua osalejatele kogemuse olukordadest, mille tegelikku toimumist oleks raske või ebaeetiline uurimise eesmärgil oodata või korraldada (‘t Hart, 1997; Boin et al., 2004). Kriisi läbimäng aitab kujundada realistliku, kuid kontrollitud olukorra, kus saab jälgida otsustamist, info töötlemist, rollide ja vastutuse jaotumist ning koostööd olukorras, mida iseloomustavad ajasurve, ebakindlus ja puudulik informatsioon (‘t Hart, 1997; Boin et al., 2004). Lauaõppusi on kasutatud ka selleks, et tuvastada kriisiolukorras tekkivaid kommunikatsiooniga seotud haavatavusi, näiteks raskusi kriisiinfo kättesaamisel, mõistmisel või usaldamisel (Torpan et al., 2025). Küberturbe kontekstis on simulatsioonid samuti sobiv meetod, sest need võimaldavad stsenaariumipõhiselt läbi mängida organisatsiooni reageerimist, infovahetust ja otsustamist ilma tegelikku intsidenti esile kutsumata (Chowdhury & Gkioulos, 2023). Empiirilised uuringud näitavad, et kriisisimulatsioonid võivad parandada osalejate kriisijuhtimise kompetentse, kuid simulatsiooni mõjusus sõltub ka sellest, kuivõrd tõetruu, arusaadav ja kaasahaarav olukord osalejatele tundub (Wang, 2017).

Eestis on simulatsioone rakendatud näiteks Sisekaitseakadeemias (edaspidi SKA) päästetöö juhtide koolitamise käigus just olukorrateadlikkuse mõõtmiseks, kasutades selleks spetsiaalset virtuaalsimulatsiooni tarkvara (Polikarpus ja Danilas, 2021; Polikarpus ja Danilas, 2022). Tammik (2019), uurides SKA päästetöö juhtide õpimotivatsiooni tegureid, leidis, et simulatsiooni metoodika tekitas isegi eri põlvkondade juhtides kõrge kaasahaaratuse seisundi. See on märkimisväärne, sest kõrget kaasahaaratuse seisundit hinnatakse kui kriitiliselt olulist aspekti lisaks motivatsioonile õpiväljundite saavutamiseks (Skinner et al., 2008; Reeve, 2012). Tammiku (2019) kohaselt hindasid osalejad meetodit väga kõrgelt ja simulatsioonipõhine hindamisloogika võib sobida kõikidele asutustele, kellel on vaja arendada ajakriitilistes olukordades otsuse vastuvõtmise protsesse.

2. METOODIKA

2.1. Metoodika valik

Oma uurimuse metoodika valikul lähtusin töö kahest ala-eesmärgist ning uurimisküsimuste iseloomust. Esiteks oli töö eesmärk leida seoseid tajutud olukorrateadlikkuse ja küberturbe kriisi haldamise vahel. Teiseks soovisin hinnata simulatsiooni metodoloogilist sobivus organisatsioonilise küberturbe valdkonnas. Sellest tulenevalt tuli uurimus üles ehitada nii, et oleks võimalik samaaegselt hinnata simulatsiooni kasutatavust uurimismeetodina ning uurida kriisijuhtimisega seotud protsesse lihtsustatud ja kontrollitud keskkonnas.

Uurimuses kasutasin selleks sotsiaalteaduslikku simulatsiooni, mille käigus lõin kontrollitud kriisiolukorra osalejate tegevuse, infovahetuse, hinnangute ja otsustusprotsesside jälgimiseks. Simulatsiooni meetodi kasutamine oli esimese uurimisküsimuse vaates põhjendatud ka seetõttu, et uuritavad nähtused, nagu olukorrateadlikkus ja kriisijuhtimine, avalduvad kõige selgemini dünaamilises ja ajas arenevas olukorras ehk n-ö praktilise läbimängu käigus (Endsley, 1995; ‘t Hart, 1997).

Uurimise läbiviimiseks valisin Riigi Infosüsteemi Ameti ning simulatsiooni sisuliseks aluseks võtsin varasemad ID-kaardi kriisid. Selle valiku tingis ühelt poolt minu enda huvi teema vastu, kuid teisalt ka asjaolu, et ID-kaardi kriiside kohta leidus rohkelt avalikult kättesaadavat materjali, sealhulgas kirjeldavaid, analüüsivaid ja meediapõhiseid käsitlusi. See tegi võimalikuks realistliku ja sisuliselt põhjendatud simulatsioonistsenaariumi koostamise.

Oma lõputöös viisin läbi simulatsiooniuuringu küberturbe vastutusega avalikus asutuses. Andmed kogusin küberturvalisuse kriisisimulatsiooni käigus ning analüüsisin kombineeritud meetodil. Kvantitatiivsete ja kvalitatiivsete meetodite kombineerimisel analüüsisin, millised seosed esinevad tajutud olukorrateadlikkuse ja kavandatud tegevuste vahel küberturbe kriisi simulatsioonis ja kvalitatiivse analüüsiga hindasin simulatsiooni metodoloogilist väärtust.

2.2. Uuringu kontekst

Minu lõputöö temaatiliseks kontekstiks on Riigi Infosüsteemi Amet (edaspidi RIA), mis on Eesti riigi keskne IT- ja küberturvalisuse asutus. RIA tegutseb Justiits- ja Digiministeeriumi valitsemisalas, nende ülesanne on pakkuda digiriigi keskseid platvorme ja teenuseid ning korraldada riiklikku küberturvalisust (RIA, 2026b). Asutusel on seega oluline roll Eesti

digiühiskonna arendamisel ja kaitsmisel (RIA, 2026b). Seetõttu sobis RIA minu uurimuse läbiviimises hästi, kuna uuritav teema paikneb otseselt asutuse töövaldkonna keskmes.

RIA sobivus tulenes muu hulgas ka sellest, et Eesti digiriigi üks keskseid alustaristuid on elektrooniline identiteet ehk eID, mille olulisemaks kandjaks on ID-kaart. ID-kaart võeti Eestis kasutusele 2002. aastal ning sellest kujunes oluline vahend e-teenuste kasutamiseks, digiallkirjade andmiseks ja internetihääletamisel osalemiseks (Parsovs, 2021). Parsovs (2021) kirjeldab ID-kaarti Eesti digiriigi tehnoloogilise nurgakivina, mille turvalisus sõltub kaardikiibi krüptograafilisest funktsionaalsusest ja seda ümbritsevast ökosüsteemist.

Tehniliselt sisaldab ID-kaart kahte asümmeetrilist võtit koos X.509 avaliku võtme sertifikaatidega, millest autentimisvõtit kasutatakse e-teenustesse sisselogimiseks ja vajadusel krüpteeritud dokumentide avamiseks ning digiallkirja võtit õiguslikult siduvate allkirjade andmiseks (Parsovs, 2021). Avalik võti on seotud kasutaja identiteediga sertifikaadi kaudu, samal ajal kui privaatvõtme kaitstus on usaldusmudeli keskne eeldus (Parsovs, 2021). Kui privaatvõti muutub tuletatavaks või kontrollimatult kasutatavaks on ohus eID usaldusväärsus tervikuna.

Eesti ID-kaardi ajaloos on olnud mitu märkimisväärset turvajuhtumit, millest kahte võib käsitleda ID-kaardi kriisidena. Esimene neist puudutas 2011. Aastal väljastatud ID-kaarte, mille puhul avastati EstEID JavaCardi rakenduses tõsine turvanõrkus, mis mõjutas 120000 kaarti (Parsovs, 2021). Teine ja ulatuslikum kriis oli 2017. Aasta ROCA juhtum, mis tulenes Infineoni RSA võtmegenereerimise veast ja mõjutas enam kui 750000 kaarti (Parsovs, 2021).

Juhtumid näitavad, et tehniline turvarisk võib kiiresti muutuda laiemaks usaldus- ja kriisihalldusküsimuseks. Kuigi konkreetne viga ei pruugi olla RIA-st tulenev, siis avaliku sektori eID kompetentsikeskusena on RIA roll vea lahendamisel keskne (Parsovs, 2021).

Uuringu läbiviimine just sellises asutuses oli põhjendatud ka osalejate erialase tausta tõttu. Kuna valim moodustati RIA töötajatest, sai eeldada, et osalejad on küberturbe ja elektroonilise identiteedi teemadega kursis ning mõistavad valdkondlikku sõnavara. Samuti oli põhjendatud eeldus, et nad tunnevad vähemalt üldjoontes varasemaid ID-kaardi kriise. See võimaldas kasutada simulatsioonis vihjeid ja viiteid ilma, et neid oleks tulnud pikemalt selgitada. Selline erialane kontekst toetas realistlikuma simulatsiooni loomist ja sobis hästi minu uurimuse eesmärkidega.

2.3. Valim

Valim kujunes eesmärgipärase valiku alusel, hõlmates Riigi Infosüsteemi Ameti eID valdkonna töötajaid, kellel oleks võimaliku ID-kaardi kriisi korral roll selle lahendamises. Uurimuses osalemine oli vabatahtlik ning osalejate kaasamine toimus asutuse juhi vahendusel, kes tegi organisatsioonisiseselt sobivale sihtrühmale üleskutse uuringus osalemiseks. Lõplik valim kujunes nende isikute seast, kes avaldasid valmisolekut uuringus osaleda. Seega oli tegemist eesmärgipärase valimiga, mis kujunes vabatahtliku osalemise alusel.

Selline valimi moodustamise viis võimaldas kaasata uurimisküsimuste seisukohalt asjakohase teadmise ja kogemusega osalejad. Samas tuleb arvestada, et vabatahtlikkuse alusel kujunenud valim võib mõjutada tulemuste üldistatavust, kuna osalesid need sihtrühma kuuluvad isikud, kes olid valmis uuringus osalema. Seetõttu käsitlen saadud tulemusi eeskätt konkreetse uurimiskonteksti põhiselt.

Uuringus osales kokku seitse eelnevalt määratletud kriteeriumitele vastanud isikut. Arvestades uurimuse eesmärki ja sihtrühma spetsiifilisust, pidasin sellist osalejate arvu oma uuringu kontekstis piisavaks. Osalejate isikuandmeid ma ei kogunud ning asutuse soovil jätan ka osalejate ametinimetused ja osakondliku kuuluvuse konfidentsiaalsuse tagamiseks avaldamata.

2.4. Simulatsiooni koostamine

2.4.1. Stsenaariumi loomine

Simulatsiooni koostamine oli mulle täiesti esmakordne ja selle tõttu omaette väljakutse. Protsessi alustasin teemakohaste materjalide kogumisega. Esiteks oli vaja kokku koguda kõik avalikud materjalid ID-kaardi kriiside kohta. Otsisin RIA veebilehelt välja kõik ID-kaardi ja strateegia dokumendid, mille olemasolu teadsin ja seejärel tegin veel otsingumootorist järelkorje märksõnadega *site:ria.ee "põhimäärus" filetype:pdf.* Väärtuslikeks materjalideks osutusid ka teemakohased uurimistööd nagu Arnis Parsovsi 2021. aastal kaitstud doktoritöö teemal “Estonian Electronic Identity Card and its Security Challenges” ja TTÜ uurimismeeskonna poolt (eesotsas Ahto Buldase) loodud analüüsiv raport “ID-kaardi kaasuse õppetunnid”, milles arutleti üksikasjaliselt RIA poolt 2017. aastal teada saadud turvanõrkusele reageerimise ja lahendamise üle. Ülevaatlik materjal oli ka 2021 aasta novembris välja antud Pealtnägija episood, mis käsitles läbi aastate esinenud, kuid “maha vaikitud” ID-kaardi kriise. Aruannete, uurimuste ja avaldatud meediaväljaannete põhjal kaardistasin üldpildi erinevatest

ID-kaardi kriisidest, mis on senini toimunud ning hakkasin koostama hüpoteetilist kriisiolukorda, milles korduksid kombineeritult olulised elemendid varasematest juhtumitest.

Esialgu kirjutasin loomingulises vormis kriisiolukorra stsenaariumi ja seejärel hakkasin seda lahti harutama ja erinevateks infosüstideks eraldama. Protsessi käigus konsulteerisin otse Ahto Buldasega, kes stsenaariumi üle vaatas ja nõuandeid andis. Stsenaariumi kirjutamine ja infosüstide loomine toimus aasta 2025 kevadel/algas 2025 aasta veebruaris ja kestis kokkuvõtvalt umbes 4 kuud.

2.4.2. Stsenaariumi lühikirjeldus

Stsenaariumi kirjutasin kokku varasematest kriisidest ja intsidentidest inspireerituna, kombineerides erinevaid aspekte. Läbi selle tahtsin ka näha, milliseid aspekte osalejad ära tunnevad, mis annab vihjeid institutsionaalse mälu kohta. Viimane kriis oli rohkem kui viis aastat tagasi, mille jooksul võivad õpitud õppetunnid ununeda.

Stsenaarium algab välispoliitiliselt pingestatud ja tehniliselt haavatavas taustas. Eesti on sõlminud diplomaatilised suhted Taiwaniga, Hiina on reageerinud ähvardavalt, kahe nädala pärast toimuvad e-valimised ning samal ajal raskendab riisiasutuse tööd ulatuslik lumetorm. Keset sellist olukorda saab RIA teavituse Tsehhi teadlastelt, kes väidavad, et ID-kaardi kiibis esineb tõsine turvanõrkus. Teavituse põhielement seostub otseselt 2017. aasta eID kriisiga, kus RIA-t teavitati Infineoni turvakiipide haavatavusest, mis mõjutas ligikaudu 800000 Eesti dokumenti ning ohustas autentimist ja digiallkirjastamist (Tallinna Tehnikaülikool, 2018).

Järgneb kriisile iseloomulik järkjärguline selginemise loogika. Alguses on teada vaid risk, kuid mitte selle täpne olemus, ulatus ega lahenduskäik. Osalejad peavad hindama, kas ja millal teavitada PP-d, valitusust, partnereid ja avalikkust. See peegeldab samuti 2017. aasta juhtumi kronoloogiat, kus esmalt kinnitati riski mõju ja ulatus ning seejärel alles hakati osapooli kaasama (Tallinna Tehnikaülikool, 2018).

Oluline koht on ka kommunikatsiooniriskidel, meediasse ilmuvad kriitilised väited RIA varasema vaikimise kohta, e-valimiste usaldusväärsuse kahtluse alla seadvad arvamused ning hiljem ka infoleke, mille tõttu tekib ajasurve juhtum kiiresti avalikustada. Need motiivid põhinevad veel varasematel intsidentidel, kus meedia mängis suurt rolli otsuste tegemisel, nagu 2011. aastal väljastatud kaartide turvaprobleemi avastamise puhul (Parsovs, 2021).

Lisasin varasemate kriiside põhielementide kõrvale eksitavad ja kõrvalised infokihid, näiteks kvantarvutite läbimurde uudised, Smart-ID kohta käivad väited, CERT-EE ja RIA eraldiseisev

intsident. Nende kõrvalt on oluline eristada ID-kaardiga seotud infot kõrvalisest või väärast infost ning sai esile kutsuda info kvaliteedi segajad.

Stsenaarium lõppeb olukorraga, kus RIA, PPA ja minister teavitavad avalikkust ning algab pikem tehnilise ja organisatsioonilise lahenduse ettevalmistamine.

2.5. Andmekogumismeetod

2.5.1. Simulatsiooni läbiviimine

Simulatsiooni viisin läbi Riigi Infosüsteemi Ametis 22. mail 2025. Kui kõik osalejad olid kogunenud, tegin lühikese sissejuhatuse, milles tutvustasin ennast, oma uurimisteemat, uurimuse põhimõtteid ja kuidas simulatsiooni protokolli täita. Osalejate haldamiseks ja hõlpsamaks andmekogumiseks jagasin nad kahte gruppi, mis võimaldas ka tulemusi võrrelda ja tegevusmustreid kontrollida.

Simulatsiooni kestus oli suurusjärgus 60 minutit ja osalejad reageerisid selle aja jooksul 25-le infosüstile. Stsenaariumi arengu infokilde oli kokku 28. Iga infosüsti kohta hindasid osalejad info tõesust ja omaenda enesekindlust info tõesuse määramisel. Uuringus osalejate ülesanne oli kriisisimulatsioonis esitatavatud infosüstidele reageerida ja hinnata lihtsustatud skaalal enda olukorrateadlikkuse taju meeskonna tasemel. Rõhutasin ka, et simulatsiooni eesmärk ei olnud kriis edukalt lahendada ega jõuda parimale lõpptulemusele, vaid saada ülevaade inforuumi (sh väärinfo) tajumisest.

Andmed kogusin paberkandjal protokollidesse, mida kumbki meeskond simulatsiooni vältel täitis. Infosüstid edastasin osalejatele PowerPoint esitluse teel, lugedes iga uue infosüsti ka valjult ette. Simulatsiooni käigus vaatlesin osalejate käitumist ja omavahelist suhtlust.

2.5.2. Andmeanalüüsimetoodika

Uurimisküsimustele vastamiseks kogusin kõigepealt **kahte tüüpi andmeid** lähtudes Edgar & Edgar (2007) QASA-meetodi loogikast. Esimeseks andmetüübiks on osalejate hinnang saadud **info tõesusele ehk signaalile,** mida lasin osalejatel hinnata binaarsel skaalal: tõene või väär. Teiseks andmetüübiks on osalejate e**nesekindluse hinnang signaalile skaalal 1-5 ehk signaali tugevu**s, mis võimaldab mõõta osalejate taju oma teadmiste kindluse üle (Edgar ja Edgar, 2007). Edgar & Edgari (2007) alusel on enesekindlust võimalik mõõta nii binaarselt ehk “enesekindel” ja “mitte enesekindel”, kui ka skaala kujul, mida ka mina oma andmete kogumisel kasutasin. Enda uurimuses kasutasin andmete kogumisel skaala versiooni, sest tahtsin näha täpsemaid

seoseid signaali ja signaali tugevuste vahel ning tulemuste analüüsi käigus taandasin võrdlemiseks samuti binaarsele tasemele, sarnaselt kombineeritud tehnikale, mida kasutasid ka Edgar & Edgar (2007).

Kolmandaks andmetüübiks on vabas vormis lühivastused kolmele küsimusele iga infosüsti kohta, nendeks on "Mida teete?", "Mis info veel puudu on?" ja "Kust saate lisainfot?". Need lühivastused ei ole küll klassikalise QASA-meetodi põhiosa, kuid annavad kvalitatiivse selguse selle kohta, kuidas osaleja oma hinnangu kujundas.

Esimesele uurimisküsimusele vastamiseks koostasin signaali ja signaali tugevuse kohta kirjeldava statistika, millest tulenesid tajutud olukorrateadlikkuse tõlgendused ning kõrvutasin seda lühivastuste temaatilise sisuanalüüsi kaudu ilmnenud tegevuskoodidega.

Teisele uurimisküsimusele vastamiseks hindasin, kas simulatsiooni käigus kogutud andmetes ilmnesid need organisatsioonilise küberturbe haavatavuse fenomenid, mille esiletoomiseks infosüstid olid kavandatud.

2.6. Uurija reflektsioon

Uurijana olin seotud nii simulatsiooni ettevalmistamise, andmete kogumise kui ka tulemuste analüüsiga. See tähendab, et minu roll mõjutas uurimisprotsessi mitmes etapis, sh infosüstide valikul ja vastuste tõlgendamisel. Kuna uuritav teema on seotud küberturbega ja uuringu viisin läbi Riigi Infosüsteemi Ametis, tuleb arvestada minu valdkondlike eelteadmistega, mis võisid aidata stsenaariumit modelleerida ja vastuseid paremini konteksti asetada. Varasem kokkupuude asutusega võis mul aidata näha vastustes tähendusi, mis valdkonna-võõrale inimesele otseselt ei väljenduks.

Uurimisprotsessi käigus ilmnes ka terminoloogiline täpsustamise vajadus. Töö varasemas etapis oli kasutusel mõiste "halduslik küberturve", millega püüdsin tähistada küberturbe korralduslikku, protsessilist ja organisatsioonilist mõõdet. Mõiste osutus aga mitmetähenduslikuks tekitades ühest küljest seose küberturbe haldusega, haldusliku kui administratiivse tegevusega või isegi sellise küberturbega, mis puudutab ainult avalikku haldust. Kuigi võib väita, et küberturbe haldus on tegevus, mida inglisekeelses kirjanduses teatakse kui *cybersecurity management,* siis protsessi käigus selgus, et mõiste *management* tähendus pole eri teaduskondades üheselt kattuv. Sotsiaalteaduslikus kirjanduses mõeldakse selle all pigem juhtimist, samal ajal kui IT- ja küberturbe kontekstis on tihtipeale isegi rõhutud, et tegemist ei

ole juhtimisega, vaid just haldusega (AKIT, s.a.). Eesmärgiga vähendada mitmetähenduslikkust ja segadust leidsin, et minu uurimuse fookuse võtab paremini kokku mõiste "organisatsiooniline küberturve". See võimaldab rõhutada, et töö keskmes ei ole käsitletud küberturbe tehnilist poolt ega kitsas mõttes haldamist või juhtimist, vaid sellist küberturbe osa, milles ilmnevad organisatsioonilisel tasandil protsessid, rollid, teadmised, infokäitumine, infovajadused ja otsustamine. Sellega on fookuses just küberturbe kultuur ühe organisatsiooni siseselt ning mitte eraisiku küberturve või ühiskondlikul tasemel küberturbe teadlikkus. Organisatsiooniline küberturve vastab inglisekeelsele mõistele *organizational cybersecurity*, mis väljendub teaduslikus kirjanduses ka selliste väljendite kaudu nagu "*human factors in cybersecurity*" või "*cybersecurity culture*" või "*organizational aspects of cybersecurity*".

3. TULEMUSED

3.1. Tajutud olukorrateadlikkuse seosed kavandatud tegemistega küberturbe kriisis

3.1.1. Enesekindluse hinnangute tulemused

Esitatud väidetest 13 olid tõesed ja 12 väärad ning osalejad hindasid iga infosüsti kohta esmalt tõesust (tõene või väär) ja teisalt enda enesekindlust selle tõesuse määramisel viie palli skaalal. 1 tähendades kõige madalamat enesekindlust ehk ei olda üldse enesekindlad enda vastuses ja 5 tähendades kõige kõrgemat enesekindlust ehk ollakse enda vastuses täiesti kindel.

Tõeste väidete hindamisel oli kõige suurema intensiivsusega seda õigesti hinnatud ja enesekindlusega 4. Seda esines kahe grupi peale keskmiselt 26.9%. Väärade väidete hindamisel esines kõige rohkem (25%) madalat enesekindlust selle väite vääraks hindamisel ehk väärad väited tunti ära ja hinnati vääraks, kuid esines ebakindlust rohkem.

Kõikide väidete peale kokku hinnati nende tõesust õigesti keskmiselt 74% kordadest ja valesti keskmiselt 26% kordadest.

Tabel 1. Tõesuse ja enesekindluse hinnangute jagunemine nii tõeste kui ka väärade väidete lõikes

Tõesed väited										
	Õiged EK 5	*Õiged EK 4*	*Õiged EK 3*	*Õiged EK 2*	*Õiged EK 1*	*Valed EK 1*	*Valed EK 2*	*Valed EK 3*	*Valed EK 4*	*Valed EK 5*
Tõeste väidete vastuste arv G1	2	4	2	3	1	0	0	0	1	0
Tõeste väidete vastuste arv G2	2	3	3	1	2	1	1	0	0	0
Tõeste väidete vastuste arvu aritm. keskmine	2,0	3,5	2,5	2,0	1,5	0,5	0,5	0,0	0,5	0,0
Osakaal koguvalimist (tõeste väidete kõigist vastustest)	**15,4%**	**26,9%**	**19,2%**	**15,4%**	**11,5%**	**3,8%**	**3,8%**	**0,0%**	**3,8%**	**0,0%**
Väärad väited										

	Õiged EK 5	*Õiged EK 4*	*Õiged EK 3*	*Õiged EK 2*	*Õiged EK 1*	*Valed EK 1*	*Valed EK 2*	*Valed EK 3*	*Valed EK 4*	*Valed EK 5*
Väärade väidete vastuste arv G1	0	2	1	3	1	2	2	0	1	0
Väärade väidete vastuste arv G2	3	1	0	3	0	2	1	1	0	1
Väärade väidete vastuste arvu aritm. keskmine	1,5	1,5	0,5	3,0	0,5	2,0	1,5	0,5	0,5	0,5
Osakaal koguvalimist (väärade väidete kõigist vastustest)	**12,5%**	**12,5%**	**4,2%**	**25,0%**	**4,2%**	**16,7%**	**12,5%**	**4,2%**	**4,2%**	**4,2%**
Kõik väited kokku										
	Õiged EK 5	*Õiged EK 4*	*Õiged EK 3*	*Õiged EK 2*	*Õiged EK 1*	*Valed EK 1*	*Valed EK 2*	*Valed EK 3*	*Valed EK 4*	*Valed EK 5*
Vastuste arv G1	2	6	3	6	2	2	2	0	2	0
Vastuste arv G2	5	4	3	4	2	3	2	1	0	1
Vastuste arvu aritm. keskmine	3,5	5,0	3,0	5,0	2,0	2,5	2,0	0,5	1,0	0,5
Osakaal koguvalimist	**14,0%**	**20,0%**	**12,0%**	**20,0%**	**8,0%**	**10,0%**	**8,0%**	**2,0%**	**4,0%**	**2,0%**
	Õigesti vastatud					Valesti vastatud				
	74,0%					**26,0%**				

Allikas: koostatud autori kogutud andmete põhjal

3.1.2. Lühivastuste temaatiline sisuanalüüs

Simulatsiooni jooksul esitasin osalejatele 25 infosüsti ning iga infosüsti kohta oli protokollis 3 küsimust: “Mida teete?” (K1), “Mis info veel puudu on?” (K2) ja “Kust lisainfot saate?” (K3). Mõlema rühma kohta oli 75 võimalikku vastuseühikut. Kokku moodustas andmestik 150 vastuseühikut, millest 91 sisaldasid sisulist vastust, 58 olid tühjad ja üks vastus oli mitteloetav.

Tabel 2. Lühivastuste osakaalu jagunemine kahe grupi peale

Vastuse staatus	Grupp 1	Grupp 2	Kokku
Sisuline vastus	37	54	91
Tühi vastus	37	21	58
Mitteloetav vastus	1	0	1
Kokku	**75**	**75**	**150**

Allikas: koostatud autori kogutud andmete põhjal

Kõige rohkem sisulisi vastuseid anti küsimusele “Mida teete?”, millele vastati kokku 40 korral. Küsimusele “Mis info veel puudu on?” anti kokku 23 sisulist vastust ning küsimusele “Kust lisainfot saate?” anti 28 sisulist vastust.

Tabel 3. Lühivastuste jagunemine küsimusete lõikes

Küsimused	Grupp 1	Grupp 2	Kokku
K1: “Mida teete?”	15	25	**40**
K2: “Mis info veel puudu on?”	9	14	**23**
K3: “Kust lisainfot saate?”	13	15	**28**

Allikas: koostatud autori kogutud andmete põhjal

Avatud kodeerimise tulemusel koondasin vastustes esinenud koodid nelja põhiteema alla. Teemad ja nende alla kuuluvad koodid on esitatud tabelis 4.

Tabel 4. Lühivastuste kodeerimise tulemusel kujunenud tegevus- ja infovajaduskoodid

Teema	Teema alla kuuluvad koodid
Infokäitumine	*info kontrollimine, lisainfo otsimine, analüüsimine, testimine ja uurimine*
Kommunikatsioon	*kommunikatsiooniosakonnaga suhtlus, infovahetuse parandamine, ettevalmistumine*
Info kvaliteedi ja olukorra täpsustamise vajadus	*tehniline kinnitus, tõendid, allika usaldusväärsus, detailid*
Lisainfo allikad	*partnerasutused, avalikud allikad, algne infoallikas, välised eksperdid, asutusesisesed spetsialistid, infosüsteem*

Allikas: koostatud autori kogutud andmete põhjal

Kõige sagedasemani esinenud kood oli “info kontrollimine”, mis esines 13 korral. Grupp 1 vastustes esines see 3 korral ja Grupp 2 vastustes 10 korral. Kood “mõju hindamine” esines kokku 11 korral, sealhulgas Grupp 1 vastustes 3 ja Grupp 2 vastustes 8 korral. Lisainfo allikate seas esinesid sagedamini partnerasutused, avalikud allikad ja algne infoallikas.

Tabel 5. Tegevus- ja infovajaduskoodide esinemissagedus kahe grupi vaates

Teema	Teema alla kuuluvad avatud koodid	G1	G2	Kokku
Infokäitumine	*info kontrollimine*	3	10	**13**
	lisainfo otsimine	2	3	**5**
	analüüsimine, testimine, uurimine	2	1	**3**
	seoste kaardistamine	1	0	**1**
	lisainfo ootamine	0	1	**1**

	lisainfo küsimine	0	1	**1**
Kommunikatsioon	*infovahetuse parandamine*	1	1	**2**
	kommunikatsiooniosakonnaga suhtlus	2	2	**4**
	ettevalmistamine	1	3	**4**
	info edastamine	0	1	**1**
	asutusesisene suhtlemine	3	4	**7**
Info kvaliteedi ja olukorra täpsustamise vajadus	*relevantsuse hindamine*	3	1	**4**
	tõendid	4	3	**7**
	mõju hindamine	3	8	**11**
	allika usaldusväärsus	1	4	**5**
	tehniline kinnitus	3	4	**7**
	teadlikult mitte reageerimine	1	2	**3**
	detailid	4	1	**5**
Lisainfo allikad	*avalikud allikad*	3	6	**9**
	partnerasutused	6	4	**10**
	välised eksperdid	3	3	**6**
	algne infoallikas	4	5	**9**
	asutusesisesed spetsialistid	1	4	**5**
	register, infosüsteem	2	0	**2**

Allikas: koostatud autori kogutud andmete põhjal

Tabel 6. Üksikud näited vastustest

Teema	Näidis kood	Näide vastustest	Grupp
Infokäitumine	*info kontrollimine*	*"Kontrollin, millele tuginedes"*	G1
Kommunikatsioon	*ettevalmistamine*	*"valmistuda, et on avalik"*	G2
Info kvaliteet	*allika usaldusväärsus*	*"Kes on allikas?"*	G2
Infoallikad	*partnerasutused*	*"Elektrilevist"*	G1

Allikas: koostatud autori kogutud andmete põhjal

3.1.3. Tajutud olukorrateadlikkuse seos temaatiliste vastustega

Tabelist 7 ilmneb, et õige tõehinnangu korral varieerusid kavandatud tegevused vastavalt enesekindluse tasemele. Kõrge enesekindlusega korral kirjeldati konkreetseid tegevusi. Enesekindluse langemisel toetusid vastused üha enam info kontrollimisele, tõendite kogumisele ja ekspertidega suhtlemisele. Vale hinnangu korral aga ei olnud kõrge enesekindluse juures väga enesekindlat käitumist näha, vaid pigem oldi ettevaatlikud. Esines infot ja infoallikaid kontrollivad tegevused. Madalamate enesekindluse tasemetel muutusid vastused harvemaks (esines rohkem tühjasid lahtreid) ja passiivsemaks ehk ei väljendatud tegutsemisele viitavaid tegevusi.

Tabel 7. Tajutud olukorrateadlikkuse seos lühivastuste koodidega

Tajutus olukorrateadlikkuse hinnangu olukord	Lühivastustes esinevad koodid
Õige EK 5	Konkreetsed tegutsemisele viitavad vastused nagu “analüüsin”, “uurin”, “infovahetuse parandamine” või otsustavad vastused nagu “ei reageeri”.
Õige EK 4	Tehnilisele kinnitusele suunatud vastused nagu “tehnilised detailid” ja “infoallikaga suhtlus” ja “asutusesisene suhtlus”.
Õige EK 3	Ilmnesid vastused nagu “lisainfo otsimine”, “tehniline kinnitus” ja “info algallikas”, “dokumentidega tutvumine”, “allika usaldusväärsus”, “välised eksperdid”, “mõju hindamine” ja “info kontrollimine”.
Õige EK 2	Ilmnesid vastused, mis vihjavad info asjakohasuse kontrollimisele “relevantsuse hindamine”, “mõju hindamine” ja “seoste kaardistamine”.
Õige EK 1	Esines info kontrollimist, vajadust tõendite ja mõju ulatuse järele.
Vale EK 5	Pigem oldi ettevaatlikud. Infot ja infoallikat kontrollivad tegevused nagu “kontrollin infot”, “tõendid”, “tehniline kinnitus” ja “ekspertidega suhtlemine”.
Vale EK 4	Ei olnud tegevusi kirjeldatud, kui ainult mainitud, et soovivad tehnilist kinnitust.
Vale EK 3	Tegevustes esines info kontrollimist, vajadust tõendite järele ja infoallikana toodi välja avalikud allikad.
Vale EK 2	Vastustes esines info kontrollimist, tehnilise kinnituse vajadust ja väliste ekspertidega suhtlemist.
Vale EK 1	Esines info kontrollimist, vajadust tõendite ja mõju ulatuse järele ning allika usaldusväärsuse kinnitamist. Infoallikate seas toodi välja väliseid eksperte ja avalikke allikaid.

Allikas: koostatud autori kogutud andmete põhjal

3.2. Sotsiaalteadusliku simulatsiooni sobivus organisatsioonilise küberturbe mõõtmisel

3.2.1. Infokäitumine

Infokäitumise fenomeni esilekutsumiseks kavandatud infosüstide vastustes ilmnesid peamiselt info kontrollimise, lisainfo otsimise, allikate hindamise ja ekspertidega konsulteerimisega seotud tegevuskoodid. K1 vastuste tegevuskoodides kordus kõige sagedamini info kontrollimine, mis esines enamiku infokäitumise infosüstide juures. K2 vastuste infopuuduste koodides esines vajadust tehnilise kinnituse, tõendite, detailide ja mõju kohta käiva info järele, mis näitab ka, et infokäitumise infosüstid tõid esile ka infovajadusi. K3 vastuste infoallikate koodides kordusid kõige enam välised eksperdid, avalikud allikad ja info algallikas.

Tabel 8. Infokäitumise fenomeni esinemine vastustes

IS nr	Väljenduv fenomen	K1 vastustest ilmnenud tegevuskoodid	K2 vastustest ilmnenud infopuuduste koodid	K3 vastustest ilmnenud infoallikate koodid

1	Infokäitumine	*lisainfo otsimine*	*tehniline kinnitus, mõju detailid*	*info algallikas, avalikud allikad*
3	Infokäitumine	*info kontrollimine*	*tehniline kinnitus, mõju*	*info algallikas*
6	Infokäitumine	*info kontrollimine*	*tõendid*	*info algallikas, avalikud allikad*
8	Infokäitumine	*analüüsimine ja testimine, olukorra analüüs, mõju hindamine*	*detailid, mõju*	*välised eksperdid*
12	Infokäitumine	*lisainfo otsimine, info kontrollimine*	*tehniline kinnitus, allika usaldusväärsus*	*välised eksperdid*
13	Infokäitumine	*info kontrollimine*	*tõendid, tehniline kinnitus*	*avalikud allikad*
14	Infokäitumine	*info kontrollimine*	*tehniline kinnitus ja allika usaldusväärsus*	*välised eksperdid ja avalikud allikad*
16	Infokäitumine	*info kontrollimine*		
25	Infokäitumine	*dokumentidega tutvumine, info kontrollimine*	*allika usaldusväärsus*	*välised eksperdid*

Allikas: koostatud autori kogutud andmete põhjal

3.2.2. Kommunikatsioonihaavatavused

Kommunikatsioonihaavatavuse fenomeni esilekutsumiseks kavandatud infosüstide vastustes ilmnesid suhtlemise ja koordineerimisega seotud tegevuskoodid. Osalejad viitasid kommunikatsiooniosakonnaga suhtlemisele, asutusesisesele suhtlemisele, info kontrollimisele ja info relevantsuse hindamisele. Tulemused näitavad, et kommunikatsioonihaavatavuse infosüstide puhul seostusid vastused eelkõige tõendite kogumise, kommunikatsiooni ettevalmistamise ja osapoolte kaasamisega.

Tabel 9. Kommunikatsioonihaavatavuse fenomeni esinemine vastustes

IS nr	**Väljenduv fenomen**	**K1 vastustest ilmnenud tegevuskoodid**	**K2 vastustest ilmnenud infopuuduste koodid**	**K3 vastustest ilmnenud infoallikate koodid**
5	Kommunikatsiooni-haavatavus	*infoallikaga suhtlemine*	*allika usaldusväärsus*	*info algallikas*
7	Kommunikatsiooni-haavatavus	*info kontrollimine, ettevalmistamine*	*tõendid*	*avalikud allikad*

10	Kommunikatsiooni-haavatavus	*kommunikatsiooni-osakonnaga suhtlemine, ettevalmistamine*		
11	Kommunikatsiooni-haavatavus	*info edastamine, asutusesisene suhtlemine, relevantsuse hindamine*		
17	Kommunikatsiooni-haavatavus	*info kontrollimine, suhtlemine algallikaga*	*mõju*	*partnerasutused, asutusesisesed spetsialistid, teenuse omanik*
20	Kommunikatsiooni-haavatavus	*relevantsuse hindamine*	*lisainfo otsimine*	*asutusesisesed spetsialistid*
21	Kommunikatsiooni-haavatavus	*infovahetuse parandamine*		*asutusesisesed spetsialistid*
24	Kommunikatsiooni-haavatavus	*kommunikatsiooni-osakonnaga suhtlemine, ettevalmistamine*	*tõendid*	*algne infoallikas*

Allikas: koostatud autori kogutud andmete põhjal

3.2.3. Info kvaliteedi segajad

Info kvaliteedi segajate esilekutsumiseks kavandatud infosüstide vastustes ilmnesid peamiselt info kontrollimise, relevantsuse hindamise, mõju hindamise ja teadlikult reageerimata jätmisega seotud tegevuskoodid. Kõrvalise info puhul kordusid vastustes eelkõige relevantsuse hindamine ja väärinfo puhul kordus eelkõige info kontrollimine. Infopuudustes esines vajadust tõendite, mõju ja juhtumi põhjuse info järele. Infoallikate seas toodi välja partnerasutusi, avalike allikaid ja asutusesiseseid spetsialiste. Üldpildis seostusid info kvaliteedi segajatega seotud vastused peamiselt info asjakohasuse, tõendamise ja mõju hindamisega.

Tabel 10. Info kvaliteedi fenomeni esinemine vastustes

IS nr	**Väljenduv fenomen**	**K1 vastustest ilmnenud tegevuskoodid**	**K2 vastustest ilmnenud infopuuduste koodid**	**K3 vastustest ilmnenud infoallikate koodid**
2	Info kvaliteedi segajad: kõrvaline info	*relevantsuse hindamine, mõju hindamine, info kontrollimine*		*partnerasutused, avalikud allikad, partnerasutused*
6	Info kvaliteedi segajad: väärinfo	*Info kontrollimine*	*tõendid*	*avalikud allikad*
9	Info kvaliteedi segajad: kõrvaline info	*info kontrollimine, relevantsuse hindamine, mõju hindamine*	*tõendid, mõju*	*partnerasutused*

15	Info kvaliteedi segajad: kõrvaline info	*info kontrollimine, teadlikult mitte reageerimine*	*tõendid*	*avalikud allikad, infosüsteemid*
18	Info kvaliteedi segajad: väärinfo	*info kontrollimine*		*partnerasutused, teenuse omanik*
20	Info kvaliteedi segajad: väärinfo	*relevantsuse hindamine*	*põhjus*	*asutusesisesed spetsialistid*
22	Info kvaliteedi segajad: kõrvaline info	*teadlikult mitte reageerimine*		

Allikas: koostatud autori kogutud andmete põhjal

3.2.4 Organisatsiooniline teadmus

Organisatsioonilise teadmuse infosüstidele antud vastustes ilmnesid peamiselt lisainfo otsimise ja ootamise, asutusesisese ja infoallikaga suhtlemise tegevuskoodid. Infoallikate koodides kordusid vastused, mis viitasid algsele infoallikale, avalikele allikatele, spetsialistidele, välistele ekspertidele ning partnerasutustele. Vastustest tuleneb, et organisatsioonilise teadmuse infosüstide puhul otsiti täiendavat teadmist nii organisatsiooni seest kui ka organisatsiooni välistest allikatest.

Tabel 11. Organisatsioonilise teadmuse esinemine vastustes

IS nr	**Väljenduv fenomen**	**K1 vastustest ilmnenud tegevuskoodid**	**K2 vastustest ilmnenud infopuuduste koodid**	**K3 vastustest ilmnenud infoallikate koodid**
21	Organisatsiooniline teadmus	*infovahetuse parandamine*		*asutusesisesed spetsialistid*
19	Organisatsiooniline teadmus	*asutusesisene suhtlemine*		
5	Organisatsiooniline teadmus	*infoallikaga suhtlemine*	*allika usaldusväärsus*	*info algallikas*
1	Organisatsiooniline teadmus	*lisainfo otsimine*	*tehniline kinnitus, mõju, detailid*	*info algallikas, avalikud allikad*
4	Organisatsiooniline teadmus	*lisainfo ootamine*	*tehniline kinnitus, mõju*	*info algallikas, avalikud allikad, partnerasutused*
23	Organisatsiooniline teadmus	*tõendid, mõju hindamine*		*info algallikas*

13	Organisatsiooniline teadmus	*info kontrollimine*	*tõendid, tehniline kinnitus*	*avalikud allikad*
12	Organisatsiooniline teadmus	*info kontrollimine, lisainfo otsimine*	*tehniline kinnitus, allika usaldusväärsus*	*välised eksperdid*

Allikas: koostatud autori kogutud andmete põhjal

4. ARUTELU

Andmetele peale vaadates paistab kohe silma, et Grupp 2 andis märgatavalt rohkem sisulisis vastuseid kui Grupp 1, eriti veel tegevusreaktsiooni küsimuses, kus Grupp 2 andis vähemalt ühe sisulise vastuse kõigile infosüstidele. Grupp 1 puhul jäi osa vastuseid tühjaks, mistõttu teen Grupp 1 kohta sisulisi järeldusi mõnevõrra ettevaatlikumalt.

4.1. Tajutud olukorrateadlikkuse mõju küberturbe kriisi haldamisele

Simulatsiooni tulemused viitavad, et kõrgema enesekindluse ja õige tõesuse hinnangu korral oli osalejatel lihtsam liikuda olukorra mõtestamiselt kavandatud tegevuseni. Osalejad hindasid väidete tõesust korrektselt keskmiselt 74% kordadest. Sellisel juhul kirjeldati vastustes konkreetseid edasiviivaid tegemisi näiteks uurimist, analüüsimist ja infovahetuse parandamist. Ebavajaliku info äratundmise korral oli vastuse seas teadlikku mitte reageerimist, mis viitab sellele, et kriisiolukorras ei kulutata aega ebarelevantsetele teemadele. See seostub Endsley (1995) käsitlusega, mille järgi kõrgem olukorrateadlikkus toetab konkreetsemat otsustamist keerulistes olukordades. Kui osaleja hinnang info tõesusele oli õige ja sellega kaasnes suurem kindlustunne, oli ka tegevusreaktsioon selgem.

Samas ei olnud tulemuste põhjal tajutud olukorrateadlikkuse mõju ühesuunaline. Madalama enesekindluse korral ei asendunud tegevus alati valede otsustega, vaid suurenes vajadus infot kontrollida, otsida tõendeid, otsida tehnilist kinnitust või pöörduda ekspertide ja allikate poole. Tõlgendan seda positiivse ettevaatlikkusena. See näitab, et tajutud olukorrateadlikkus mõjutab kriisi haldamist infokäitumise kaudu ning mida ebakindlam on arusaam olukorrast, seda olulisemaks muutub info kontrollimine ja täiendavate allikate kasutamine. Samal ajal võib liigne ebakindlus viia ka passiivsemate või tühjemate vastusteni, mis viitab sellele, et ebakindlus ei pruugi alati käivitada sisukat infokäitumist.

Edgar et al. (2012) rõhutavad, et tajutud ja tegelik olukorrateadlikkus ei pruugi kattuda ning eriti riskantne on olukord siis, kui vale arusaam kaasneb kõrge enesekindlusega. Minu uuringu simulatsioonis ei ilmnenud vale hinnangu ja kõrge enesekindluse korral läbivalt riskantset tegutsemist. Pigem väljendati tungivalt info kontrollimise ja tõendite otsimise vajadust. Seega jätsid osalejad ruumi täiendavale kontrollile ega käsitlenud oma hinnangut alati lõpliku teadmisena. Seostan tulemust küberturbe valdkonna eripäraga, kus tehnilisi haavatavusi on tihtipeale võimalik kontrollida ning isegi ka kõige loogilisema ja tõenäolisema info saamise puhul on levinud tava saada ka tehniline kinnitus. Siin ilmnes huvitav vastuolu infokäitumise

teooriaga. Isegi kui Wilsoni (1999) järgi on infokäitumise keskmes sageli ebakindluse vähendamine, siis läbi viidud simulatsioonis väljendus infot kontrolliv infokäitumine isegi siis, kui enesekindlus oli väga kõrge.

Küberturbe kriisi kontekstis tuleb arvestada, et olukorrateadlikkus ei kujune ainult üksikisiku peas. Uuem olukorrateadlikkuse käsitlus liigub üha enam rohkem meeskondliku ja süsteemse toimimise suunas (Weller et al., 2024). See väljendub ka tulemustes, sest kavandatud tegevused olid sageli seotud teiste osapooltega. Olgu nendeks info algallikas, asutusesisesed spetsialistid, partnerasutused, välised eksperdid või avalikud allikad – osalejad ei kartnud laenata teadmisi ekspertidelt ja spetsialistidelt. Seostudes organisatsioonilise teadmuse käsitlusega, mille järgi on oluline osa organisatsiooni mälust see, kus asub vajalik ekspertiis ja kuidas selleni jõuda (Walsh & Ungson, 1991; Wegner, 1987).

Tulemused viitavad, et tajutud olukorrateadlikkuse mõjutab küberturbe kriisi haldamist eelkõige tegevusreaktsiooni konkreetsuse ja suuna kaudu. Õige teadmine ja kõrgem enesekindlus toetab konkreetsemat tegutsemist, samas kui madalam ja ebakindlam olukorrataju suunab osalejaid allikaid hindama ja täiendavat teadmist otsima. Vale hinnang olukorrale ja kõrge enesekindlus ei toonud endaga kaasa ohtlikku käitumist, nagu varasem teooria väidab, vaid viitas pigem ettevaatlikule ja kindlatele faktidele põhinevat reageerimist. Seega leiti kõigepealt, et vajalik on infot kontrollida ja saada tehniline kinnitus, seejärel alles tegutseda.

Kuigi simulatsioonis olid olemas kriisihalduse kesksed tunnused, nagu ajasurve ja puudulik info, siis muutus küberturbe kontekstis eriti oluliseks info tehniline kontrollitavus, allikate usaldusväärsus ja vajadus esitada tähenduslikku infot infomürast. See eristab küberturbe kriisi paljudest teistest füüsilistest või nähtavalt avalduvatest kriisidest, sest probleemi tegelik ulatus ei ole kohe tajutav. Kui näiteks pääste-või looduskatastroofi kontekstis võib olukorra oht olla osaliselt vahetult nähtav, siis küberturbe kriisis tuleb oht sageli tuletada kaudsetest märkidest, logidest, tehnilistest kinnitustest või ekspertide infost. See erinevus ilmnes ka tulemustes. Küberturbe puhul ei esine kiire reageerimine alati välises tegevuses, vaid võib väljenduda ka kiires kontrolli- ja tõlgendusportsessis. Teisisõnu võib “tegutsemine” olla esmapilgul passiivne, kuid sisuliselt aktiivne.

4.2. Simulatsiooni sobivus organisatsioonilise küberturbe matkimiseks

Tulemuste põhjal võib väita, et sotsiaalteaduslik simulatsioon sobib organisatsioonilise küberturbe uurimiseks eelkõige siis, kui uurimishuvi ei ole tehniliste kaitsemeetmete toimimises, vaid selles, kuidas inimesed kriisiolukorras tegutsevad. Simulatsioon matkis küberturbe kriisi sotsiotehnilise protsessina, kus otsustamine kujuneb tehnilise info, inimliku tõlgenduse, rollide, allikate ja kommunikatsioonipraktikate koostoimes.

Simulatsiooni tugevus avaldus kõige selgemalt infokäitumise nähtavaks tegemises. Nendele infosüstidele, millega proovisin esile kutsuda infokäitumisele viitavaid tegevusi, anti vastustes märku eelkõige kontrolliva ja täpsustava vormiga infokäitumisest. Seega võib väita, et infokäitumise fenomen väljendus. Samas ilmneb tulemuste põhjal ka meetodi piirang, sest vastused näitavad, et osalejad pidasid info kontrollimist oluliseks, kuid ei ava piisavalt detailselt, mille alusel info kontrollimine toimuks. Simulatsioon võimaldab kirjeldada infokäitumise üldisi mustreid, kuid mitte alati hinnata nende kvaliteeti või tulemuslikkust.

Kommunikatsioonihaavatavuste puhul oli meetodi sobivus mõnevõrra piiratum. Vastustest tulid esile asutusesisene suhtlus, ettevalmistamine ja info edastamine, mis näitab, et simulatsioon võimaldas tuvastada kommunikatsiooniga seotud otsustuskohti ehk kellele info suunata, kellega koostöös teha ja millal hakata väliskommunikatsiooniks valmistuma. Samas jäid vastused pigem üldiseks ja kavatsuste tasemele ega avanud piisavalt, kuid kommunikatsioon tegelikult toimiks. Hansson et al., (2020) käsitluses tekib kommunikatsioonihaavatavus siis, kui inimesed ei pääse infole ligi, ei mõista seda või ei saa seda oma olukorra parandamiseks kasutada. Läbi viidud simulatsioon tõi esile kommunikatsiooniga seotud vajadused, kuid mitte täiel määral kommunikatsiooni toimimise protsessi. Kuigi kommunikatsioonihaavatavusi väljakutsuvate infosüstide vastustes kõlasid kommunikatsiooniga seotud tegevused, siis leian, et saadud vastustest ei ole võimalik välja lugeda, kas kommunikatsioonihaavatavused tegelikult esinesid või mitte. Seetõttu sobib kirjalikel vastustel põhinev simulatsioon potentsiaalsete haavatavuste ja vajaduste kaardistamiseks, aga mitte süvitsi matkimiseks.

Info kvaliteedi aspektist oli simulatsioon kui meetod asjakohane, sest osalejad hindasid info relevantsust, otsisid tõendeid, hindasid mõju ning otsustasid teadlikult mitte reageerida infole, mis ei olnud olukorra suhtes asjakohane. See haakub teooriaga, mille järgi väärinfo, infomüra ja infoüleküllus võivad kriisiolukorras otsustamist moonutada ja raskendada olulise info eristamist ebaolulisest (Broda & Strömbäck, 2024; May et al., 2023; Shahrzadi et al., 2024). Meetodi väärtus seisnes siin selles, et see tõi nähtavaks, et osalejad ei käsitlenud kogu kriisiinfot

võrdselt tegutsemist nõudvana. Võib järeldada, et simulatsioon võimaldas esile tuua info kvaliteediga seonduvaid otsustuskohti. Küll aga ei ava vastused täpselt, milliste kriteeriumite alusel nad otsustaksid, kas info on kõrvaline, eksitav või oluline.

Organisatsioonilise teadmuse poolest tõi simulatsioon nähtavale, et kriisiolukorras ei toetu osalejad ainult isiklikule teadmisele, vaid otsivad kinnitust erinevatest allikatest, sh nii asutusesisesed kui ka asutusevälised. See toetab Walshi ja Ungsoni (1991) organisatsioonilise mälu käsitlust, mille järgi organisatsiooni teadmus paikneb inimestes, rollides, protseduurides ja struktuurides. Samuti kinnitab see Wegneri (1987) transaktiivse mälu teooriat, mille järgi on lisaks vastuse teadmisele võrdselt oluline teada, kellel vajalik teadmine olemas on. Simulatsioon sobis seega hästi selleks, et nähtavaks teha infoallikate võrgustik, millele osalejad kriisiolukorras toetuksid. Siiski ei olnud võimalik teada saada, kui täpselt osalejad teavad või valivad konkreetseid kontakte või mida tehakse siis, kui infoallikad ei oska väärtuslikku sisendit pakkuda.

4.3. Meetodi edasiarendus ja tuleviku vaated

Uuringu tulemusena võib öelda, et sotsiaalteaduslik simulatsioon sobib organisatsioonilise küberturbe matkimiseks osaliselt. Meetod võimaldas esile kutsuda sotsiotehnilisi nähtuseid, mida tehniline lauaõppus või tavapärane kriisi-läbimäng sama hästi ei näitaks. Paremini tulid esile infokäitumine ja info kvaliteedi segajad ning edasiarendusi vajaksid kommunikatsioonihaavatavuse ja organisatsioonilise teadmuse osad. Reflekteerides kogu uuringu protsessi kulgu ja vaadeldes tulemusi arvan, et organisatsioonilise küberturbe valdkonnas oleks väärtuslik katsetada sotsiaalteadusliku simulatsiooni meetodi ühendamist küberturbe intsidendi lauaõppusega. See aitaks sama aegselt läbi mängida näiteks info kontrollimise või ekspertidega suhtlemise protsesse, aga ka mõõta jooksvat tajutud olukorrateadlikkust, mis oleks väärtuslik sisend organisatsiooni juhtkonnale. Organisatsioonilise küberturbe vaatepunktist oleks väärtuslikum koostada selline stsenaarium, mille puhul õige või vale otsuse tegemine muudab tulemust. Sellisel juhul oleks potentsiaalselt võimalik näha millise olukorrateadlikkuse juures lahenduskäik suunda ja olemust muudab.

KOKKUVÕTE

Minu lõputöö eesmärk oli katsetada sotsiaalteaduslikku simulatsiooni kui uurimismeetodit küberturbe valdkonnas ning läbi selle välja selgitada, kuidas mõjutab tajutud olukorrateadlikkus küberturbe kriisi haldamist ning kuidas sobib selline meetod organisatsioonilise küberturbe matkimiseks. Töö lähtekohaks oli arusaam, et küberturve ei ole üksnes tehniline kaitsemeetmete kogum, vaid sõltub olulisel määral ka organisatsiooni inimestest, protsessidest, info liikumisest ja otsustusvõimest. Eriti kriisiolukorras muutub nähtavaks, kuidas organisatsioon ebakindlat ja vastuolulist infot tõlgendab, kontrollib, jagab ja selle põhjal tegutseb.

Töö teoreetilises osas käsitlesin organisatsioonilist küberturvet, kriisijuhtimist, olukorrateadlikkust. Tõin välja organisatsioonilise küberturbe haavatavuse elemendid ja tutvustasin simulatsiooni kui sotsiaalteaduslikku uurimis-, õppimis ja hindamismeetodit. Metoodika osas tutvustasin uuringu ja valimi konteksti, kuidas simulatsioonistsenaariumit koostasin ja kuidas andmeid analüüsisin. Uuringu läbiviimiseks korraldasin varasematest ID-kaardi kriisidest inspireeritud kriisisimulatsiooni, milles osalesid Riigi Infosüsteemi Ameti kesktaseme juhid, vabatahtliku osalemise alusel. Stsenaariumi jooksul hindasid osalejad iga infosüsti kohta selle tõesust, märkisid oma enesekindluse hinnangu andmisel ja vastasid täiendavatele küsimustele. Andmeid analüüsisin kombineeritult, kasutades nii kirjeldavat statistikat kui ka temaatilist sisuanalüüsi. Selline lähenemine võimaldas siduda kvantitatiivsed hinnangud kvalitatiivsete vastustega ning vaadelda, kuidas tajutud olukorrateadlikkus, info tõlgendamine ja kavandatud tegevused omavahel seostusid.

Tulemused näitasid, et tajutud olukorrateadlikkus ja kavandatud tegevused olid omavahel seotud eelkõige selle kaudu, kui selgelt suutsid osalejad olukorra tähendust ja olulisust mõtestada. Kõrgema enesekindlusega hinnangute puhul olid tegevused sagedamini konkreetsemad ja suunatud tegutsemise algatamisele. Madalama enesekindluse puhul väljendus vastustest rohkem passiivsust ja lisainfo otsimise motiive. Osalejad hindasid 74% korral info tõesust õigesti, kuid vale hinnangu puhul ei esinenud riskantseid käitumismustreid ning tugevamalt väljendusid info kontrollimise ja tehnilise kinnituse saamise vajalikkus.

Sotsiaalteaduslik simulatsioon aitab küberturbe valdkonnas teha nähtavaks selliseid haavatavusi, mis tavapärases tehnilises käsitluses võivad jääda tagaplaanile, kuid potentsiaalselt rohkem väärtust annaks tehnilise lauaõppuse ja sotsiaalteadusliku simulatsiooni ühendamine

uueks kombineeritud meetodiks. Simulatsiooni kaudu väljendusid kõige selgemini infokäitumine ja info kvaliteedi segajatele reageerimine. Lauaõppusega ühendamisel oleks potentsiaalselt võimalik paremini esile kutsuda täpsemaid infoallikate käsitlusi, organisatsioonilisi teadmusi ja kommunikatsioonihaavatavusi.

Minu lõputöö uuringu puhul oli tegemist eelkõige meetodi katsetusega. Kandvate järelduste tegemiseks tuleb sotsiaalteaduslikku simulatsiooni korduvalt läbi viia erinevates küberturbega tegelevates organisatsioonides. Tulevastes uuringutes oleks väärtuslik katsetada lauaõppuse ja sotsiaalteadusliku simulatsiooni kombineerimist.

SUMMARY

A Social Simulation for Measuring Organizational Cybersecurity

The aim of this thesis was to test social simulation as a research method in the field of cybersecurity and to examine how perceived situation awareness influences the management of a cybersecurity crisis.

Two research questions were set:

1) How does perceived situation awareness influence the management of a cybersecurity crisis?
2) How suitable is a social simulation for imitating organizational cybersecurity?

The study was based on a crisis simulation inspired by earlier Estonian ID-card crises. During the simulation, participants assessed the truthfulness of information injections, rated their confidence in each assessment and described their planned actions, missing information and possible information sources. The data were analysed by combining descriptive statistics and thematic content analysis.

The results showed that higher confidence was more often presented with more concrete actions and the initiation of response activities. Lower confidence was more often connected with the need to search for additional information and verify the situation before acting. Participants assessed the truthfulness of information correctly in 74% of cases. Incorrect assessments did not lead to clearly risky behavioural patterns, but instead the participants expressed the importance of information verification and technical confirmation.

The study also showed that a social simulation can help reveal organizational vulnerabilities that may remain less visible in a purely technical approach to cybersecurity. The method was especially suitable for observing information behaviour and responses to information quality disturbances. However, the discussion suggest that even greater value could come from combining social simulation with a technical tabletop exercise. Such a combined method would allow organizational, communicative and technical aspects of cybersecurity crisis management to be studied together.

As this study was primarily a methodological test, broader conclusions require repeated simulations in different cybersecurity-related organizations. Future research could further develop and test a combined approach that brings together the social simulation approach and tabletop cybersecurity exercises.

TÄNUSÕNAD

Soovin tänada oma juhendajat Sten Torpanit toetava juhendamise ja heade nõuannete eest kogu tööprotsessi vältel. Tema suunavad küsimused ja tähelepanekud aitasid mul uurimisteemat paremini mõtestada.

Tänan ka Riigi Infosüsteemi Ametit koostöö ja praktilise abi eest uuringu korraldamisel ning kõiki uuringus osalejaid, kes panustasid oma aega ja mõtteid simulatsiooni läbimängu.

Suur tänu kuulub ka Ahto Buldasele teemakohase nõustamise eest. Samuti tänan oma sõpru ja lähedasi toetuse, kannatlikkuse ja julgustavate sõnade eest kogu töö protsessi vältel.

KASUTATUD KIRJANDUS

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications, 2*, 100031. https://doi.org/10.1016/j.csa.2023.100031

AKIT. (s.a.). *management (1)*. Kasutatud 15. mai 2026 https://akit.cyber.ee/term/911-management-1

Andmekaitse Inspektsioon. (2025). *Andmeturve*. https://www.aki.ee/isikuandmed/andmetootlejale/andmeturve

Angafor, G. N., Yevseyeva, I., & He, Y. (2020). Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *Security and Privacy, 3*(6), e126. https://doi.org/10.1002/spy2.126

Asakura, K., Gheorghe, R. M., Borgen, S., Sewell, K., & MacDonald, H. (2021). Using simulation as an investigative methodology in researching competencies of clinical social work practice: A scoping review. *Clinical Social Work Journal, 49*(2), 231-243. https://doi.org/10.1007/s10615-020-00772-x

Axelrod, R. (2006). Advancing the art of simulation in the social sciences. In J.-P. Rennard (Ed.), *Handbook of Research on Nature-Inspired Computing for Economics and Management*. IGI Global Scientific Publishing.

Backman, S. (2020). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management, 29*(4), 429-438. https://doi.org/10.1111/1468-5973.12347

Boin, A., Kofman-Bos, C., & Overdijk, W. (2004). Crisis simulations: Exploring tomorrow's vulnerabilities and threats. *Simulation & Gaming, 35*(3), 378-393. https://doi.org/10.1177/1046878104266220

Broda, E., & Strömbäck, J. (2024). Misinformation, disinformation, and fake news: Lessons from an interdisciplinary, systematic literature review. *Annals of the International Communication Association, 48*(2), 139-166. https://doi.org/10.1080/23808985.2024.2323736

Carmine, S. (2021). A paradox approach to organisational tensions during the pandemic crisis. *Journal of Management Inquiry, 30*(2), 138-153. https://doi.org/10.1177/1056492620986863

Chernikova, O., Heitzmann, N., Stadler, M., Holzberger, D., Seidel, T., & Fischer, F. (2020). Simulation-based learning in higher education: A meta-analysis. *Review of Educational Research, 90*(4), 499-541. https://doi.org/10.3102/0034654320933544

Chng, S., Lu, H. Y., Kumar, A., & Yau, D. (2022). Hacker types, motivations and strategies: A comprehensive framework. *Computers in Human Behavior Reports, 5*, 100167. https://doi.org/10.1016/j.chbr.2022.100167

Chowdhury, N., & Gkioulos, V. (2023). A framework for developing tabletop cybersecurity exercises. In S. Katsikas, F. Cuppens, C. Kalloniatis, J. Mylopoulos, F. Pallas, J. Pohle, M. A. Sasse, H. Abie, S. Ranise, L. Verderame, E. Cambiaso, J. Maestre Vidal, M. A. Sotelo Monge, M. Albanese, B. Katt, S. Pirbhulal, & A. Shukla (Eds.), *Computer Security. ESORICS 2022 International Workshops* (Vol. 13785, pp. 116-133). Springer International Publishing. https://doi.org/10.1007/978-3-031-25460-4_7

Colabianchi, S., Costantino, F., Nonino, F., & Palombi, G. (2025). Transforming threats into opportunities: The role of human factors in enhancing cybersecurity. *Journal of Innovation & Knowledge, 10*(3), 100695. https://doi.org/10.1016/j.jik.2025.100695

Cooper, S., Porter, J., & Peach, L. (2013). Measuring situation awareness in emergency settings: A systematic review of tools and outcomes. *Open Access Emergency Medicine: OAEM, 6*, 1-7. https://doi.org/10.2147/OAEM.S53679

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. *The TQM Journal, 33*(7), 76-105. https://doi.org/10.1108/TQM-09-2020-0202

Deverell, E., & Ganic, A. (2024). Crisis and performance: A contingency approach to performance indicators. *International Journal of Disaster Risk Reduction, 105*, 104417. https://doi.org/10.1016/j.ijdrr.2024.104417

Edgar, G., & Edgar, H. E. (2007). Using signal detection theory to measure situation awareness: The technique, the tool (QUASA), the test, the way forward. In M. Cook,

J. Noyes, & Y. Masakowski (Eds.), *Decision making in complex environments* (pp. 373-385). Ashgate. https://doi.org/10.1201/9781315576138-34

Edgar, G. K., Catherwood, D. F., Sallis, G., Brookes, D., & Medley, A. (2012). "I always know what's going on." Assessing the relationship between perceived and actual situation awareness across different scenarios. *World Academy of Science, Engineering and Technology, 6*(11), 1433-1434.

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37*(1), 32-64. https://doi.org/10.1518/001872095779049543

Endsley, M. R., & Garland, D. J. (Eds.). (2000). *Situation awareness analysis and measurement*. Lawrence Erlbaum Associates.

ENISA. (2024). *Best practices for cyber crisis management*. ENISA.

ERR. (2017, 21. aprill). *Priisalu: Enne pronksiööd räägiti küberteemadel kuskil salaja*. ERR. https://www.err.ee/589355/priisalu-enne-pronksiood-raagiti-kuberteemadel-kuskil-salaja

ERR. (2022, 18. august). *Narva tanki teisaldamine tõi kaasa suurima küberrünnete laine pärast pronksiööd*. ERR. https://www.err.ee/1608688192/narva-tanki-teisaldamine-toi-kaasa-suurima-kuberrunnete-laine-parast-pronksiood

ERR. (2024, 3. aprill). *Cybercriminals steal data of around 700,000 Apotheka pharmacy customers*. ERR. https://news.err.ee/1609302096/cybercriminals-steal-data-of-around-700-000-apotheka-pharmacy-customers

Ghaderi, C., Esmaeili, R., Ebadi, A., & Amiri, M. (2023). Measuring situation awareness in health care providers: A systematic review of measurement properties using COSMIN methodology. *Systematic Reviews, 12*(1). https://doi.org/10.1186/s13643-023-02220-6

Handri, E. Y., Indra Sensuse, D., & Tarigan, A. (2024). Developing an agile cybersecurity framework with organizational culture approach using Q methodology. *IEEE Access, 12*, 108835-108850. https://doi.org/10.1109/ACCESS.2024.3432160

Hansson, S., Orru, K., Siibak, A., Bäck, A., Krüger, M., Gabel, F., & Morsut, C. (2020). Communication-related vulnerability to disasters: A heuristic framework. *International Journal of Disaster Risk Reduction, 51*, 101931. https://doi.org/10.1016/j.ijdrr.2020.101931

Harper, A., Mustafee, N., & Pitt, M. (2023). Increasing situation awareness in healthcare through real-time simulation. *Journal of the Operational Research Society, 74*(11), 2339-2349. https://doi.org/10.1080/01605682.2022.2147030

't Hart, P. (1997). Preparing policy makers for crisis management: The role of simulations. *Journal of Contingencies and Crisis Management, 5*(4), 207-215. https://doi.org/10.1111/1468-5973.00058

Heartfield, R., & Loukas, G. (2018). Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. *Computers & Security, 76*, 101-127. https://doi.org/10.1016/j.cose.2018.02.020

Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security, 24*(3), 119. https://doi.org/10.1007/s10207-025-01032-0

Koch, T., & Viererbl, B. (2026). What constitutes an organizational crisis? A scoping review and a conceptual model of crises as stakeholder perceptions (CASPER Model). *Public Relations Review, 52*(2), 102681. https://doi.org/10.1016/j.pubrev.2026.102681

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Liu, M., Shore, M., Yeoh, W., Jiang, F., & Zeadally, S. (2025). Toward effective cybersecurity management: A hierarchical process model with performance assessment. *Journal of Cybersecurity, 11*(1), tyaf020. https://doi.org/10.1093/cybsec/tyaf020

Markopoulou, D., & Papakonstantinou, V. (2021). The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. *Computer Law & Security Review, 41*, 105502. https://doi.org/10.1016/j.clsr.2020.105502

May, B., Milne, R., Shawyer, A., Meenaghan, A., Ribbers, E., & Dalton, G. (2023). Identifying challenges to critical incident decision-making through a macro-, meso-, and micro-lens: A systematic synthesis and holistic narrative analysis. *Frontiers in Psychology, 14*. https://doi.org/10.3389/fpsyg.2023.1100274

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review, 20*(3), 709-734. https://doi.org/10.2307/258792

Moens, L. L., Lydon, S., Cucurachi, S., O'Connor, P., Sauter, T. C., Töndury, G.-A., & Manser, T. (2026). Measuring situation awareness: A meta-review across domains. *Human Factors, 68*(5), 632-672. https://doi.org/10.1177/00187208251412110

Munir, A., Aved, A., & Blasch, E. (2022). Situational awareness: Techniques, challenges, and prospects. *AI, 3*(1), 55-77. https://doi.org/10.3390/ai3010005

Nasser, G., Morrison, B. W., Wiggins, M. W., & Hoang, A. (2025). The mismatch between perceived situation awareness and hazard recognition in automated driving. *Applied Ergonomics, 128*, 104562. https://doi.org/10.1016/j.apergo.2025.104562

Orru, K., Hansson, S., & Nero, K. (2025). Social vulnerability triage: A dynamic scenario-based system for disaster planning and response. *Journal of Risk Research, 28*(6), 549-570. https://doi.org/10.1080/13669877.2025.2522660

Panteli, N., Nthubu, B. R., & Mersinas, K. (2025). Being responsible in cybersecurity: A multi-layered perspective. *Information Systems Frontiers, 28*(1), 209-227. https://doi.org/10.1007/s10796-025-10588-0

Parsovs, A. (2021). *Estonian electronic identity card and its security challenges*. University of Tartu.

Polikarpus, S., & Danilas, K. (2021). Eesti päästemeeskonna juhtide visiõppepõhise hindamise rakendamine ja tulemused. *Turvalisuskompass, 1*(1), 31-54.

Polikarpus, S., & Danilas, K. (2022). Olukorrateadlikkuse, olukorramõistmise ja kallutatuse mõõtmine siseturvalisuse valdkonnas. *Turvalisuskompass, 2*(1), 89-107.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognitive Technology & Work, 24*(2), 371-390. https://doi.org/10.1007/s10111-021-00683-y

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security, 136*, 103585. https://doi.org/10.1016/j.cose.2023.103585

Rahmandad, H., & Sterman, J. (2012). Reporting guidelines for simulation-based research in social sciences. *System Dynamics Review, 28*(4). https://doi.org/10.1002/sdr.1481

Reeve, J. (2012). A self-determination theory perspective on student engagement. In S. L. Christenson, A. L. Reschly, & C. Wylie (Eds.), *Handbook of Research on Student Engagement* (pp. 149-172). Springer. https://doi.org/10.1007/978-1-4614-2018-7_7

RIA. (2023). *Küberturvalisuse aastaraamat 2023*. Riigi Infosüsteemi Amet.

RIA. (2025). *Teavita küberintsidendist*. Kasutatud 01. aprill 2026 https://www.ria.ee/kuberturvalisus/kuberintsidentide-kasitlemine-cert-ee/kuberintsidendist-teavitamine

RIA. (2026a). *Olukord küberruumis*. Kasutatud 01. aprill 2026 https://www.ria.ee/kuberturvalisus/kuberruumi-analuus-ja-ennetus/olukord-kuberruumis

RIA. (2026b). *RIA strateegia 2026-2030*. Kasutatud 13. veebruar 2026 https://www.ria.ee/amet-uudised-ja-kontakt/amet-ja-juhtkond/ria-strateegia

Robson, A., & Robinson, L. (2013). Building on models of information behaviour: Linking information seeking and communication. *Journal of Documentation, 69*(2), 169-193. https://doi.org/10.1108/00220411311300039

Saeed, S., Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaisen, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors, 23*(16), 7273. https://doi.org/10.3390/s23167273

Savolainen, R. (2007). Information behavior and information practice: Reviewing the "umbrella concepts" of information-seeking studies. *The Library Quarterly, 77*(2). https://www.journals.uchicago.edu/doi/10.1086/517840

Schaedler, L., Graf-Vlachy, L., & König, A. (2022). Strategic leadership in organizational crises: A review and research agenda. *Long Range Planning, 55*(2), 102156. https://doi.org/10.1016/j.lrp.2021.102156

Schiuma, G., Jackson, T., & Lönnqvist, A. (2021). Managing knowledge to navigate the coronavirus crisis. *Knowledge Management Research & Practice, 19*(4), 409-414. https://doi.org/10.1080/14778238.2021.1992711

Seebruck, R. (2015). A typology of hackers: Classifying cyber malfeasance using a weighted arc circumplex model. *Digital Investigation, 14*, 36-45. https://doi.org/10.1016/j.diin.2015.07.002

Shahbazi, M., & Bunker, D. (2024). Social media trust: Fighting misinformation in the time of crisis. *International Journal of Information Management, 77*, 102780. https://doi.org/10.1016/j.ijinfomgt.2024.102780

Shahrzadi, L., Mansouri, A., Mousa, A., & Shabani, A. (2024). Causes, consequences, and strategies to deal with information overload: A scoping review. *International Journal of Information Management Data Insights, 4*(2). https://doi.org/10.1016/j.jjimei.2024.100261

Skinner, E., Furrer, C., Marchand, G., & Kindermann, T. (2008). Engagement and disaffection in the classroom: Part of a larger motivational dynamic? *Journal of Educational Psychology, 100*, 765-781. https://doi.org/10.1037/a0012840

Squazzoni, F., Jager, W., & Edmonds, B. (2013). Social simulation in the social sciences: A brief overview. *Social Science Computer Review, 32*(3), 279-294. https://doi.org/10.1177/0894439313512975

Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review. *Computers & Security, 148*, 104110. https://doi.org/10.1016/j.cose.2024.104110

Tallinna Tehnikaülikool. (2018). *ID-kaardi kaasuse õppetunnid*. Tallinn: Tallinna Tehnikaülikool.

Tammik, A. (2019). *Õpimotivatsiooni ja kaasahaaratuse tegurite kaardistus päästetöö juhtide arendamisel ja hindamisel.* Magistritöö. Sisekaitseakadeemia. https://digiriiul.sisekaitse.ee/handle/123456789/2230

Tejay, G. P. S., & Winkfield, M. (2025). Does leadership approach matter? Examining behavioral influences of leaders on employees' information security compliance. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-025-10592-4

Thoelen, F., Vastmans, J., Andersen, N., Bøhm, M., Holm, L. O. C. N., Arendtsen, B., Polikarpus, S., Taukar, M., Kütt, T., Fikke, R. C., Geertsema, T., Hazebroek, J. C., Tonnaer, C., Weewer, R., Figueras, A., Fuste, R., Catherwood, D., Baker, S., Brookes, D., & Walker, S. (2020). FireFront: A new tool to support training in fireground

situation awareness, situation understanding and bias. *International Fire Professional: The Journal of the Institution of Fire Engineers, 34*, 34-39.

Tierney, K. (2019). *Disasters: A sociological approach*. John Wiley & Sons.

Torpan, S. (2025). *European disaster risk reduction institutions' practices in mitigating communication-related vulnerabilities in disasters.* Doktoritöö. Tartu Ülikool. Tartu Ülikooli Kirjastus. https://hdl.handle.net/10062/114441

Torpan, S., Orru, K., Hansson, S., & Klaos, M. (2025). Using a table-top exercise to identify communication-related vulnerability to disasters. *International Journal of Disaster Risk Reduction, 119*, 105264. https://doi.org/10.1016/j.ijdrr.2025.105264

Vasickova, V. (2020). Crisis management process: A literature review and a conceptual integration. *Acta Oeconomica Pragensia, 27*, 61-77. https://doi.org/10.18267/j.aop.628

Walker, W. E., Giddings, J., & Armstrong, S. (2011). Training and learning for crisis management using a virtual simulation/gaming environment. *Cognition, Technology & Work, 13*(3), 163-173. https://doi.org/10.1007/s10111-011-0176-5

Walsh, J. P., & Ungson, G. R. (1991). Organizational memory. *The Academy of Management Review, 16*(1), 57-91. https://doi.org/10.2307/258607

Wang, M. (2017). Using crisis simulation to enhance crisis management competencies: The role of presence. *Journal of Public Relations Education, 3*(2), 96-109. https://journalofpreducation.com/2017/12/29/using-crisis-simulation-to-enhance-crisis-management-competencies-the-role-of-presence/

Wang, Q., Hou, H., & Li, Z. (2022). Participative leadership: A literature review and prospects for future research. *Frontiers in Psychology, 13*. https://doi.org/10.3389/fpsyg.2022.924357

Wardle, C. (2018). *Information disorder: The essential glossary*. Harvard Kennedy School.

Wegner, D. M. (1987). Transactive memory: A contemporary analysis of the group mind. In B. Mullen & G. R. Goethals (Eds.), *Theories of group behavior* (pp. 185-208). Springer.

Weller, J. M., Mahajan, R., Fahey-Williams, K., & Webster, C. S. (2024). Teamwork matters: Team situation awareness to build high-performing healthcare teams, a narrative

review. *British Journal of Anaesthesia, 132*(4), 771-778. https://doi.org/10.1016/j.bja.2023.12.035

Whitty, M. T., Moustafa, N., & Grobler, M. (2024). Cybersecurity when working from home during COVID-19: Considering the human factors. *Journal of Cybersecurity, 10*(1), tyae001. https://doi.org/10.1093/cybsec/tyae001

Wilson, T. (1999). Exploring models of information behaviour: The 'uncertainty' project. *Information Processing & Management, 35*(6), 839-849. https://doi.org/10.1016/S0306-4573(99)00029-1

Zhang, T., Yang, J., Liang, N., Pitts, B. J., Prakah-Asante, K., Curry, R., Duerstock, B., Wachs, J. P., & Yu, D. (2023). Physiological measurements of situation awareness: A systematic review. *Human Factors, 65*(5), 737-758. https://doi.org/10.1177/0018720820969071

Zimmermann, V., Schöni, L., Schaltegger, T., Ambuehl, B., Knieps, M., & Ebert, N. (2024). Human-centered cybersecurity revisited: From enemies to partners. *Communications of the ACM, 67*(11), 72-81. https://doi.org/10.1145/3665665

LISAD

Lisa 1. Simulatsiooni sündmustik

	Stsenaariumi areng	**Infosüst**	**Infosüstiga väljenduv fenomen**
	Eestis möllab viimase 10 aasta tugevaim lumetorm.		
	Mõned nädalad tagasi sõlmis Eesti Vabariik Taiwaniga diplomaatilised suhted. Hiina reageerib meedias valuliselt.		
	Kahe nädala pärast on tulemas e-valimised.		
	Paljud RIA töötajad on võtnud kodukontori päeva, et vältida lume kätte jäämist.		
	Ootamatult kutsub direktor kokku erakorralise koosoleku.		
	Rühm Tsehhi teadlasi on saatnud RIA-le ametliku teavituse, et ID-kaardis esineb tõsine turvanõrkus.		
1		Turvanõrkus esineb ID-kaardi kiibis. (T)	Organisatsiooniline teadmus Infokäitumine
	RIA määrab spetsialistid turvanõrkust analüüsima.		
2		Lumetormi tõttu on elektrijaamade töö häiritud ja mitmed linnad on elektrita. (T)	Info kvaliteedi segajad
	RIA spetsialistid teevad kindlaks, et turvanõrkus esineb, kuid selle täielik olemus pole selge.		
3		Turvanõrkuse olemus ja lahenduskäik on teadmata. (T)	Infokäitumine
4		RIA peab teavitama PPA-d ja valitsust. E-valimised tuleb viivitamatult ära jätta. (F)	Organisatsiooniline teadmus
	Turvanõrkuse olemuse uurimine jätkub.		
	Stanfordi Ülikooli teadlased avaldavad artikli, milles väidavad, et neil õnnestus ID-kaardist rünnaku järel privaatvõti kätte saada.		

5		ID-kaardist privaatvõtme kätte saamine on igal juhul turvanõrkus, hoolimata meetodist. (F)	Organisatsiooniline teadmus Kommunikatsiooni-haavatavus
	RIA üldmeilile saabub kritiseeriv kiri arvamusliidrist kolkafilosoofilt, milles sõimatakse "*süvariiki" ja "ID-käkki".*		
6		On tõenäoline, et info turvanõrkusest, millest teatasid Tsehhi teadlased, on avaldunud. (F)	Infokäitumine Info kvaliteedi segajad
7		Kommunikatsiooniosakond ütleb, et kiri on kokkusattumuslik, ning muretsemiseks pole põhjust. (T)	Kommunikatsiooni-haavatavus
	RIA on teinud kindlaks turvanõrkuse olemuse.		
8		Oluline on teada ka turvanõrkuse ulatust. (T)	Infokäitumine
	RIA jätkab turvanõrkuse uurimist.		
9		Tallinna osades piirkondades on suuremahulised elektrikatkestused. (T)	Info kvaliteedi segajad
	RIA majas kaob lumetormi tõttu elekter. Lülitatakse sisse UPS.		
	VPN on maas. Järgmised 4 käiku ei saa teise tiimiga suhelda.		
10		Tartu Ülikooli professor ja anonüümne "asjatundja" avaldavad meediale: "RIA-l on siiani kombeks ID-kaardi kriise maha vaikida." (F)	Kommunikatsiooni-haavatavus
11		Meedias spekuleeritakse: "Anonüümne asjatundja on RIA-sisene vilepuhuja." (F)	Kommunikatsiooni-haavatavus
12		Hiina on teinud läbimurraku kvanttehnoloogias. Ilmub esilehe uudis: "Meil on saavutatud tuhande kvantbitiga kvantarvuti ja sellel on ka tulemusi, oleme selle abil teostanud juba väikeseid näidisründeid." (F)	Infokäitumine Organisatsiooniline teadmus
13		Tartu Ülikooli füüsikaspetsialisti hinnangul oleks vaja ID-kaardi	Infokäitumine

		algoritmi murdmiseks 600 kvantbitti.	Organisatsiooniline teadmus
	Räuskav ärimees teeb meedias kära ning süüdistab RIA-t ja ID-kaarti oma 30 miljoni euro kaotuses.		
14		Mainitud Hiina kvantarvuti omab potentsiaalset ohtu ID-kaardi turvalisusele. (F)	Infokäitumine
15		Ärimees esitas RIA kohtusse. (F)	Info kvaliteedi segajad
16		RIA on teinud kindlaks, et turvanõrkusest on mõjutatud ligi 600 000 ID-kaarti. (T)	Infokäitumine
	RIA teavitab PPA-d, kuid teema jäätakse hetkel veel avalikkuse eest varjule. Kutsutakse kokku töögrupid, et probleemile lahendus leida.		
	RIAs otsustatakse lülitada sisse generaator, kuid toide ei lähe peale.		
	Tallinnas taastub üldine elektriühendus. RIA majas aga katkeb elektriühendus.		
	VPN on maas. Järgmised 4 käiku ei saa teise tiimiga suhelda.		
	Meedias lööb laineid lugu intsidendist: Riigiasutuse süsteemi on sisse tungitud, kadunud on kriitilised andmed.		
17		Seoses juhtumi uurimisega tuleb välja, et süsteemi oli logitud sisse Smart-IDga. Süsteemijuht eitab, et see oleks olnud tema. (F)	Kommunikatsiooni-haavatavus
	Uudis: "Riigiasutuse süsteemijuht oli intsidendi ajal Hong Kongis puhkusel."		
18		Hiina kvantarvuti omab potentsiaalset ohtu Smart-ID turvalisusele. (F)	Info kvaliteedi segajad
	RIA majas taastub elektriühendus.		
19		Viga oli juhtimissüsteemis. (T)	Kommunikatsiooni-haavatavus
	CERT-EE nimeserverid on rünnaku tõttu maas.		

20		Rünnak võib olla seotud ID-kaardi turvanõrkusega. (F)	Info kvaliteedi segajad Kommunikatsiooni-haavatavus
21		Osad töögrupid avaldavad pahameelt ning väidavad, et nendeni ei jõua piisavalt värsket infot. (T)	Organisatsiooniline teadmus Kommunikatsiooni-haavatavus
22		Meedias on kära valimisvastaste poolt: "E-valimisted pole usaldusväärsed." (F)	Info kvaliteedi segajad
23		Intervjuu järel Stanfordi teadlastega selgub, et rünnaku toimimiseks kasutasid nad füüsilist kaarti koos pin-koodidega ja tegid selle vastu 30 000 pöördumist. (T)	Organisatsiooniline teadmus
	Spetsialisti hinnangul läheks Smart-ID lahti murdmiseks vaja vähemalt 10 000 kvantbitti.		
	Uudis: "Intsidendi hetkel oli süsteemijuht baaris ja hooples purjuspäi oma arvutioskustega. Hong Kongi politsei teatas tema töökohta ja tegi distsiplinaarmärkuse."		
24		Info ID-kaardi kriisist jõudnud ühe väljaandeni, kes soovib teemat võimalikult kiiresti avalikustada. (T)	Kommunikatsiooni-haavatavus
	RIA teavitab ID-kaardi turvanõrkusest Riigikogu kantseleid.		
25		Avaldub analüüsiv teadusartikkel Hiina kvantarvutite läbimurraku kohta: "Mainitud näidisründed on eksperimentaalsed ja ei kehti ID-kaartidele." (T)	Infokäitumine
	RIA, PPA ja ministeerium osalevad pikal koosolekul, arutades võimalusi.		
	RIA, PPA ja minister esinevad pressikonverentsil, teavitades kriisist avalikkust.		

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Hanna Oruaas,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „Sotsiaalteaduslik simulatsioon organisatsioonilise küberturbe mõõtmisel“, mille juhendaja on Sten Torpan, 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 Commonsi 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.

Hanna Oruaas

21.05.2026