Kohaliku omavalitsuse kriisikommunikatsiooni küpsusmudel

AINAR PRÄÄM
Rae valla arendus- ja haldusameti IT-osakonna juhataja

MATI MÕTTUS
Tallinna Ülikooli arvutitunnetuse lektor

PEETER NORMAK
Tallinna Ülikooli informaatika professor

KAUR KAASIK-AASLAV
Sisekaitseakadeemia projektijuht

CATLYN KIRNA
Tallinna Ülikooli sotsiaalteaduste lektor

Kohalike omavalitsuste kriisikommunikatsioon Eestis on ebaühtlane ja sageli ebapiisavalt läbi harjutatud. Lahendusena pakuvad autorid välja kriisikommunikatsiooni küpsusmudeli, mis aitab omavalitsustel oma valmisolekut hinnata, kitsaskohti märgata ja samm-sammult üles ehitada süsteem, mis toimib ka siis, kui digikanalid alt veavad.

Kuressaare 2023. aasta mai ja Tallinna 2025. aasta detsembri veekriisid näitasid, et elanikud ei olnud nendeks valmis ega teadnud kriisi tekkides, kuidas toimida. Need sündmused viitasid taas, et elanikkonna teavitamist ja juhendamist kriisiolukorras on vaja parandada. See on eriti oluline, kuna mitmed teenused, sh veega varustamine ja kanalisatsioon, on elutähtsad ning nende toimepidevuse tagamine on seadusega kohalikele omavalitsustele pandud ülesanne.

Elutähtsad teenused põhinevad suuresti info- ja kommunikatsioonitehnoloogia (IKT) lahendustel (Coombs, 2019; Seeger jt, 2003). Samas loob Eesti kõrge digiteerituse tase, mida kinnitab ÜRO e-valitsemise uuring (2022), paradoksaalse olukorra:

mida enam toetume digilahendustele, seda suurem on haavatavus nende mittetoimimise korral (Kitsing, 2011).

Artiklis käsitleme kriisi kui tavaolukorrast erinevat seisundit, mis raskendab või muudab võimatuks märkimisväärse hulga inimeste oluliste vajaduste rahuldamise.

Kriisi võivad põhjustada näiteks elektrikatkestus, joogivee või õhu reostus, üleujutus, pandeemia, lumetorm jmt. Sageli tekivad kriisid ootamatult, eeldavad inimestelt käitumist, mis pole tavapärane, ning võivad olla isegi eluohtlikud. Kriisist põhjustatud kahju ärahoidmisel on esmatähtis kriisikommunikatsioon – elanike ja teiste osapoolte olukorrast informeerimine ja juhendamine.

Vajadus kvaliteetse kriisikommunikatsiooni järele on ilmne ja omavalitsustele on seatud ka vastavad ülesanded, ent Siseministeeriumi tellitud uuring näitab, et olukord ses vallas on siiski murettekitav.

Kriisikommunikatsiooni (edaspidi KK) defineerime järgnevalt: KK on kriisihaldajate ja erinevate sihtrühmade vaheline strateegiline teabevahetus enne võimalikke kriise, nende ajal ja järel, eesmärgiga vähendada kriisist tulenevat kahju või selle tekkimise riski. Strateegiline teabe jagamine tähendab, et see tugineb selgetele, juba enne kriisi määratletud ja läbi harjutatud põhimõtetele, protseduuridele ning vastutuse jaotusele. Riskide määratlemiseks ja analüüsimiseks on koostatud vastav juhend (Riigikantselei, 2024).

Vajadus kvaliteetse kriisikommunikatsiooni järele on ilmne ja omavalitsustele on seatud ka vastavad ülesanded, ent Siseministeeriumi tellitud uuring näitab, et olukord ses vallas on siiski murettekitav (Siseministeerium, 2021).

Kriisikommunikatsiooni valdkonnas on Eestis tehtud vähe uuringuid ning olemasolevad käsitlused on keskendunud peamiselt tehnilistele küsimustele. Samuti puuduvad terviklikud analüüsid, mis käsitleks kriisikommunikatsiooni süsteemi ülesehitamist, toimimise tagamist ja selle tõhususe hindamist. Kohalike omavalitsuste tegevuse hindamise ja arendamise vahendina selles valdkonnas pakuvad autorid välja kriisikommunikatsiooni võimekuse küpsusmudeli (ingl *capability maturity model*). Selle teoreetiline alus tugineb võimekuse küpsusmudelite üldkäsitlusele, turvalisuskriitiliste süsteemide teooriale (Leveson, 1995), kasutatavuse inseneeriale (Nielsen, 1993) ning kaasdisaini metoodikale (Sanders & Stappers, 2008).

Käesolev uuring rakendab kvalitatiivset lähenemist, kombineerides dokumendianalüüsi, sekundaarandmete integreerimist ja ekspertintervjuud. Metodoloogiline lähenemine põhineb Mayringi (2014) kvalitatiivsel sisuanalüüsil ning Brauni ja Clarke'i (2006) temaatilisel analüüsil. Erinevalt kirjanduses domineerivast situatsioonikesksest KK teooriast (Coombs, 2016) ja kuvandi taastamise teooriast (Prasetio, 2025) lähtub käesolev uuring teenusekesksest käsitlusest, keskendudes süsteemide toimepidevusele ja kommunikatsiooni praktilisele rakendatavusele.

TEOREETILINE RAAMISTIK

Kriisikommunikatsioon on otseselt seotud elutähtsate teenuste tagamisega, mistõttu tuleb selle kavandamisel ja teostamisel lähtuda üldistest kriitiliste süsteemide toimepidevuse ja kättesaadavuse tagamise põhimõtetest. Nendeks on antud konteksti

arvestades valitud liiasuse, kasutatavuse ja turvalise toimimise põhimõtted. KK taseme hindamise vahendiks oleme valinud nn võimekuse küpsusmudelite lähenemise.

Kriisikommunikatsiooni liiasus

Reasoni (1990) Šveitsi juustu mudeli järgi tekib süsteemis tõrge siis, kui mitme kaitsekihi augud reastuvad. Siit tuleneb liiasuse (ingl *redundancy*) põhimõte: iga kriitilise info edastamiseks peab olema vähemalt kaks sõltumatut kanalit, millest üks toimib ka võrguühenduse puudumisel, n-ö *offline*-režiimis (Jung & Nag, 2019). KK kontekstis tähendab see hübriidset lähenemist, kus kriitilised funktsioonid – kontaktide nimekirjad, evakuatsiooni- ja kerksuskeskuste aadressid, põhilised protokollid jmt – on kättesaadavad ka võrguühenduseta. Praktikas tähendab tasakaalu saavutamine kolmeastmelist lähenemist: 1) tuvastada kriitilised kommunikatsioonifunktsioonid, mis peavad toimima igas olukorras, 2) tagada iga sellise funktsiooni jaoks vähemalt üks internetist sõltumatu lahendus ning 3) korraldada regulaarselt õppusi, et veenduda nende lahenduste toimivuses.

Olgu märgitud, et vajadus ohuteavituse lisakanalite kasutuselevõtuks tõusis esile ka 2022. aastal Siseministeeriumi läbiviidud ohuteavituse SMS-sõnumite märgatavuse ja arusaadavuse hindamise uuringus (Siseministeerium, 2022).

Kriisikommunikatsiooni lahenduste kasutatavus

Kuna kriisiolukorras on inimesed enda jaoks harjumatus olukorras ja sageli stressis, siis on kommunikatsioonivahendite kasutatavus, sh intuitiivsus ja lihtsus, eriti oluline. Kognitiivse koormuse teooria (Sweller, 1988) põhjal on stressis kasutajate infotöötlusvõimekus oluliselt piiratud – süsteemid, mis tavatingimustes on kasutatavad, võivad kriisis muutuda liiga keeruliseks. Kriisiolukorras võib ka kontekst olla ebastabiilne: kasutaja võib asuda tundmatus kohas, seadmed võivad olla kahjustatud, võrguühendus puududa ning kasutaja olla emotsionaalselt pinges (Dourish, 2004). Paraku traditsioonilised toimepidevuse mõõdikud RTO (Recovery Time Objective) ja RPO (Recovery Point Objective) kasutajakogemusega ei arvesta (Gibb & Buchanan, 2006). Kasutajakogemus on eriti oluline nn kaskaadiefekti korral, kus ühe süsteemi tõrge põhjustab häiringuid seotud süsteemides (Boin & McConnell, 2007). See esitab kommunikatsioonile erilised väljakutsed: mitme teemavaldkonna samal ajal kommunikeerimine, mitme osapoole vahel koordineerimine, piiratud ressursside tingimustes prioriteetide seadmine jne.

Eelöeldust tulenevalt pakume välja KK lisamõõdiku – RTU (Recovery Time to Usability), mis mõõdab aega süsteemi tehnilisest taastamisest kuni hetkeni, mil kasutajad suudavad teenust efektiivselt kasutada. Seejuures peame RTU mõiste all silmas kasutatavust laias mõttes, mis hõlmab nii süsteemi kasutatavuse kui ka funktsionaalsuse puudustest tulenevaid probleeme.

Tehnoloogia turvaline toimimine kui kriisikommunikatsiooni eeldus

Taristu olemasolu ja selle turvaline toimimine on tänapäeval mistahes teenuse vältimatu eeldus. Näiteks riiklikul tasandil tehtavat infovahetust võimaldab SITREP keskkond, kuid see eeldab internetiühendust; sisekommunikatsiooni võimaldavad Microsoft 365 pilveteenused eeldavad võrguühendust; autentimissüsteemid (mobiil-ID, Smart-ID), mida kasutab üle 90% elanikest (RIA, 2023), eeldavad mobiilsidevõrku jne. Kuigi efektiivseim on SMS-teavituse kasutamine, ei taga seegi sihtrühma täielikku kaetust (Siseministeerium, 2022). Lisaks KK lahenduste toimimisele on vaja tagada nende turvalisus, sh andmete konfidentsiaalsus, terviklus ja käideldavus. Teenuste äralangemisel on nende asendamiseks (nt SITREP asendamiseks e-postiga)

loodud nn *fallback*-protokollid, kuid nende kasutamine eeldab vastava kompetentsi ja kasutuskogemuse olemasolu (Woods jt, 2010).

Eeltoodut arvestades pakume välja hübriidse *offline-first*-lähenemise (Allsopp, 2014), mille kohaselt on kriitilised funktsioonid kättesaadavad ka võrguühenduseta, järgides liiasuse põhimõtet.

Peale selle soovitame kasutusele võtta kriisimeeskonnale eelnevalt väljastatud ühekordse kasutusega autentimisvahendid (OTP, *one-time password*), paberipõhise isikutuvastuse evakuatsioonikeskustes ning perspektiivis ka biomeetrilise tuvastamise (Naumann & Hobgen, 2009).

Eeltoodut arvestades pakume välja hübriidse* offline-first-*lähenemise, mille kohaselt on kriitilised funktsioonid kättesaadavad ka võrguühenduseta, järgides liiasuse põhimõtet.

Võimekuse küpsusmudel kui taseme hindamise ja tõstmise vahend

Standardid kui tavapärased kvaliteedi ja nõuetele vastavuse hindamise vahendid on kvaliteedi tõstmise seisukohalt üldjuhul väheefektiivsed, kuna hindamise skaala on sisuliselt vaid kahepunktiline – vastab / ei vasta standardile. Seetõttu on alates 1990. aastatest eri valdkondades välja töötatud üldjuhul viieastmelised institutsioonide tasemete hindamise vahendid, nn võimekuse küpsusmudelid. Tasemete nimetused võivad olla erinevad, kuid kõige üldisemalt on nende olemus järgmine:

1) Tegevus on reguleerimata ja kaootiline.

2) Tegevus on reguleeritud, kuid selle kvaliteet on konstantne (st mittekasvav).

3) Tegevus on süsteemne ning selle kvaliteet on kasvav.

4) Olemas on mõõdikud ning tegevuse tulemus on hinnatav.

5) Tegevus on optimeeritud. Iga tase on kirjeldatud mingite näitajate abil.

Allpool pakume välja KK võimekuse küpsusmudeli, lähtudes üldistest küpsusmudelite loomise praktikatest.

KRIISIKOMMUNIKATSIOONI KÜPSUSMUDEL

Võimekuse küpsusmudeliga seotud teemadest käsitleme siinkohal kahte: 1) kohaliku omavalitsuse kriisikommunikatsiooni võimekuse küpsusmudeli (edaspidi küpsusmudel) koostamist ning 2) loodud mudeli raames ühest küpsustasemest järgmisele liikumiseks vajalikke tegevusi. Loodud küpsusmudeli kasutamise osalist katsetamist on kirjeldatud peatükis, kus antakse ülevaade Rae vallas tehtud küsitlusest.

Küpsusmudeli tasemed

Lähtudes ülaltoodud KK definitsioonist, defineerime kohaliku omavalitsuse KK küpsuse kui dünaamilise mõiste, mis hindab kohaliku omavalitsuse võimet teavitada sihtrühma võimalikest kriisidest nende eel, ajal ja järel, et vähendada kriisist põhjustatud kahju või selle tekkimise riski. Küpsustasemete nimetamisel lähtume levinud terminoloogiast, mis on kohandatud kohalike omavalitsuste konteksti.

1) Algne – kriisikommunikatsiooni ei eristata tavapärasest kommunikatsioonist.

2) Kirjeldatud – kriisiolukorras toimuvad kommunikatsioonitegevused on kirjeldatud.

3) Süsteemne – loodud on KK tagamise toimiv süsteem.

4) Mõõdetav – loodud on KK mõõdikud ja hindamise süsteem.

5) Innovaatiline – KK valdkond on pideva arendamise objekt ning selles arvestatakse kodu- ja välismaist eesrindlikku kogemust.

Järgnevalt kirjeldame iga küpsustaset põhjalikumalt, arvestades teoreetilises raamistikus käsitletud aspekte ning üldisi haldustegevuse seisukohast olulisi valdkondi: riskide tuvastamine, planeerimine ja valmisolek, kommunikatsioon ja koordineerimine, koolitus ja teadlikkus, pidev parendamine ning tehnoloogia integreerimine. Samuti on lähtutud põhimõttest, et 5. tasemel kajastuks mh personaalse riigi määratluses toodud tunnused: inimesekesksus, laialdane ligipääs, proaktiivsus, usaldusväärsus ja läbipaistvus ning lisaväärtuse loomine.

Tase 1. Kriiside ajaks ei ole sätestatud lisajuhendeid, kommunikatsioonitegevusi, rakendatavaid kommunikatsioonikanaleid ega vastutust. Kommunikatsioon on üldjuhul ühesuunaline, ilma operatiivse tagasiside võimaluseta. Seniste kriiside ajal toimunud kommunikatsioonitegevused on dokumenteerimata ja õppetunnid kirjeldamata.

Tase 2. Sätestatud on kriiside ajal korraldatavad sihtrühmale suunatud kommunikatsioonitegevused, -kanalid ja vastutus. Samas ei ole tegevusi katsetatud. Juhul kui ongi koostatud mingid tegevuskavad või -plaanid, siis neid ei ole kas teostatud või on seda tehtud formaalselt. KK vallas ei korraldata omavalitsuse töötajatele õppusi.

Tase 3. Loodud on terviklik KK süsteem, mis hõlmab nii kriisieelseid (ennetavaid), kriisiaegseid kui ka -järgseid tegevusi. Võimalike kriiside jaoks on olemas konkreetsed tegevuskavad, mille toimimist on katsetatud. Regulaarselt hinnatakse kriiside toimumise riske, testitakse kommunikatsioonikanaleid ning tehakse õppusi ja simulatsioone.

Tase 4. Kehtestatud on KK efektiivsuse hindamise mõõdikud (osakaal sihtrühmast, kelleni teave jõuab; sihtrühma teavitamise keskmine kiirus; KK kahesuunalisuse määr jne) ja kasutusel on adekvaatne hindamissüsteem. Regulaarselt (vähemalt kord aastas) korraldatakse KK efektiivsuse hindamisi, tulemusi analüüsitakse ja arvestatakse KK süsteemi täiustamisel.

Küpsusmudelite väärtus seisneb selles, et need aitavad kavandada tegevusi, mis toetavad organisatsiooni küpsustaseme süsteemset tõstmist.

Tase 5. KK on kohaliku omavalitsuse strateegia lahutamatu osa. Tegutsemine on proaktiivne ja innovaatiline, kaasatakse sihtrühmi, kasutatakse uusi tehnoloogiaid ning arendatakse KK-alaseid strateegilisi partnerlussuhteid. Innotrepi (www.innotrepp.ee) mõistes on kultuuri ja inimeste ning innovatsiooniprotsesside ja praktikate osas saavutatud vähemalt kolmas tase.

Iga järgmine tase hõlmab eelnevaid. Seega on näiteks ka 4. taseme korral loodud 3. taseme kirjelduses sätestatud terviklik KK-süsteem, ilma et seda oleks 4. taseme kirjelduses eraldi välja toodud.

Üleminek järgmisele tasemele

Küpsusmudelite väärtus seisneb eelkõige selles, et neid saab kasutada selleks, et kavandada oma küpsustaseme tõstmisele suunatud tegevusi. Kuigi küpsusmudeli kirjeldusest on võimalik tuletada järgmisele tasemele jõudmise eeldused, toome

Tasand	Vastutaja	Peamised kanalid	Kriitiline aeg
Teenusepakkuja	Elutähtsa teenuse osutaja	Telefon, e-post, SITREP	< 15 min
Omavalitsus	Kriisimeeskond	Teams, e-post, raadiosaatjad	< 30 min
Elanik	Iga elanik individuaalselt	SMS, koduleht, raadio, Facebook	< 60 min

TABEL 1. Info liikumisahela omadused.

üleminekute olemuse ja vajalikud tegevused siin selgelt ja eraldi välja.

Tasemelt 1 tasemele 2: organisatsiooni loomine. Kohalik omavalitsus peab dokumenteerima kommunikatsioonikanalid ning nende kasutuse korra, info liikumise ahela allikast sihtrühmani, kaardistama rollid, vastutused ja volitused jne.

Info liigub teenusepakkujalt kriisimeeskonnale ja sealt elanikele, kusjuures iga lüli selles ahelas toob kaasa viivituse ja moonutuse riski.

Tasemelt 2 tasemele 3: kõikehõlmava süsteemi loomine. Dokumenteeritud protsessid integreeritakse igapäevastesse tegevustesse (sh omavalitsustöötajate koolitustegevusse), KK seotakse infoturbe juhtimissüsteemiga, luuakse mitme kanali koordineeritud kasutamise protseduurid, määratletakse harjutuste raamistik ning tagatakse vähemalt ühe internetist sõltumatu kanali olemasolu ja testimine.

Tasemelt 3 tasemele 4: mõõdetavuse tagamine. Kasutusele võetakse konkreetsed mõõdikud – teavituse kiirus, katvuse protsent, sõnumi arusaadavus – ning RTU mõõdik, mis täiendab tehnilisi näitajaid kasutajakeskse perspektiiviga. Regulaarne auditeerimine ja kasutajatestid tagavad andmepõhise parendamise.

Tasemelt 4 tasemele 5: strateegiline integratsioon. Kõrgeim tase eeldab proaktiivset lähenemist: elaniku vajaduste keskne käsitlus, lõppkasutajate kaasamine arendusprotsessi (kaasdisain), koostoimivuse arendamine riiklike süsteemidega ning iga kriitilise funktsiooni jaoks mitme sõltumatu kanali tagamine.

Kui tasemete kirjeldused on olukorda fikseerivad, siis järgmisele tasemele liikumine on kirjeldatud tegevustena, mistõttu on eelkõige tegevuse kavandamise instrumendiks.

KRIISIKOMMUNIKATSIOONI PROTSESSID RAE VALLAS

Rae vald valiti uuringuobjektiks kui Eesti kohaliku omavalitsuse esinduslik näide: vallal on nii linnalise kui maalise omavalitsuse tunnused, rakendatud on ISO/IEC 27001:2022 standard ning dokumenteeritud kriisihalduse süsteem.

Andmeid koguti kolmes etapis: põhidokumentide analüüs (HOLP, IKT valmidusplaan, ISMS), sekundaarandmete integreerimine (varasemad uuringud, riiklikud raportid, rahvusvahelised standardid) ning semistruktureeritud intervjuud ekspertidega.

Otsustusprotsessid ja vastutusahelad

Rae vald on üle 25 000 elanikuga Harjumaa omavalitsusüksus, mille tiheasustusega linnalähedased ja hõredama asustusega maa-alad loovad kriisikommunikatsioonile mitmekesised nõudmised. Info liigub teenusepakkujalt kriisimeeskonnale ja sealt elanikele, kusjuures iga lüli selles ahelas toob kaasa viivituse ja moonutuse riski

(Boin jt, 2017). HOLP-i kohaselt puudub standardiseeritud protokoll, mis tagaks info struktuuri ja täielikkuse.

Kriisiolukorra otsustusprotsessid põhinevad kolmel integreeritud dokumendil: HOLP (üldine raamistik), ISMS (infoturbe nõuded) ja IKT valmidusplaan (tehnilised protseduurid). HOLP määratleb kriisimeeskonna hierarhia: vallavanem (kriisijuht), abivallavanem (asetäitja), kriisikoordinaator (operatiivjuht), kommunikatsioonijuht, IT-juht ning valdkonnaspetsialistid. ISO/IEC 27001:2022 põhine ISMS integreerib infoturbe kriisihaldusega, eriti kontrollide A.5.29, A.5.23 ja A.8.27 kaudu (Von Solms & van Niekerk, 2013). IKT valmidusplaan määratleb taastamise prioriteedid RTO ja RPO väärtuste kaudu, kuid ei käsitle piisavalt kasutajakogemust.

MEETOD

Rae valla KK taseme hindamiseks kasutati poolstruktureeritud rühmaintervjuud, lähtudes küpsusmudeli tasemete kirjeldustest. Käsitleti järgmisi teemasid:

- kommunikatsiooni vorm,
- kommunikatsiooni sisu,
- kommunikatsioonikanalid,
- kommunikatsiooni osapooled,
- kommunikatsiooni taristu,
- kommunikatsioonijuhtimine.

90-minutisel intervjuul osales viis Rae valla kriisihaldusega seotud ametnikku. Kasutati kaasdisaini meetodit, luues ja analüüsides fiktiivseid stsenaariume. Selline meetod sobib eelkõige harvaesinevate ja vähetõenäoliste juhtude käsitlemiseks (Rosson & Carroll, 2002). Seejärel tehti suunatud sisuanalüüs (Mayring, 2014), et määratleda eespool loetletud teemade kaupa KK atribuudid (**tunnused**, **komponendid** ja nendega seotud **kontekst**).

Sisuanalüüsi tulemused

Sisuanalüüsi tulemusena määratleti 47 (kohati kattuvat) atribuuti, mis rühmitati 17 alateemaks (tabel 2).

Paar näidet stsenaariumitest: 1) teade kriisiolukorra tekkimisest saabus reede õhtul pärast tööpäeva lõppu tööalasele e-postile, mida loeti alles järgmise päeva hommikul; 2) info liikluskatkestuse kestuse kohta potentsiaalsele sihtrühmale, et suunata nad alternatiivsele marsruudile.

Kommunikatsioonikanalite all on atribuutidena loetletud Rae vallas praegu reaalselt kasutatavad kanalid. Kommunikatsiooni osapoolte all on elutähtsate teenuste osutajad paigutatud lausa kolme alamteema alla, sest mõne teenuse osutajad tegutsevad valla sees, teised aga väljaspool valda. Kommunikatsiooni taristu all leiti, et liiasuse tagamiseks on oluline arvestada vallasisese, Eesti-sisese ja Eesti-välise taristu (või kanalite) iseärasusi. Kommunikatsioonijuhtimise käsitlemisel ilmnes, et Rae vallas on kriisikommunikatsiooni arendamiseks kavandatud tulevikuplaane, sealhulgas vallasisese ja omavalitsustevahelise raadioside ning satelliitandmeside kasutuselevõttu. Samas tõstatati ka mure viimasega seotud kõrgete kulude pärast.

Küpsustaseme hinnang

Sisuanalüüsi tulemusena võib väita, et Rae valla kriisijuhtimine on tasemel 3 (süsteemne), suunaga taseme 4 poole: protsessid on dokumenteeritud, ISO/IEC 27001:2022 sertifitseerimine näitab süsteemset riskihaldust ning kommunikatsioonikanalid on kaardistatud. Esmaste arenguvajadustena toodi välja *offline*-stsenaariumide süstemaatilisem käsitlemine, kasutajakeskne testimine ja RTU mõõdikute rakendamine.

KOKKUVÕTE

Artiklis on nii küpsusmudel kui ka järgmisele tasemele üleminekud kirjeldatud suhteliselt üldsõnaliselt. Konkreetsed lahendused sõltuvad omavalitsuse spetsiifikast – suurusest, rahalistest võimalustest, kompetentsist, partnerite kaasamise võimalustest jne. Küll aga on oluline, et Eesti Linnade ja Valdade Liidu, Päästeameti (regionaalsete kriisikomisjonide kaasamisega) või mingi muu asjakohase institutsiooni koordineerimisel

loodaks kohalike omavalitsuste vahel toimiv KK-alase praktika ja kogemuse jagamise süsteem.

Teema põhjalikumaks käsitlemiseks on vaja jätku-uuringuid, et töötada välja terviklik kriisikommunikatsiooni süsteem, mis hõlmab nii erinevaid osapooli, nende rolle, vastutusalasid kui ka tegevusi. Kui käesolev uuring käsitles kriisikommunikatsiooni omavalitsuste aspektist, siis vaja on eraldi uuringut, mis lähtuks sihtrühma ehk elanike aspektist.

Peateemad	Alamteemad	Kommunikatsiooni atribuudid (kontekst, tunnused, komponendid)
Kommunikatsiooni vorm	kuivõrd toetavad info erinevad tüübid kommunikatsiooni?	▸ verbaalne (tekst, kõne) ▸ signaalid (kuuldavad ja nähtavad tähendusega märgid) ▸ meedia ja failid (kompleksne informatsioon)
Kommunikatsiooni sisu	kommunikatsioon kriisihalduse jaoks olulistes faasides	▸ esmane info (kriisi äratundmise info) ▸ kriisi ajaline püsivus, tähtajad
	andmevahetus	▸ pilvefailide lokaalne dubleeritus ▸ internetiteenuste *offline*-võimekus
	sisu üldised tunnused	▸ sisu arusaadavus, kommunikatsiooni täpsus
Kommunikatsioonikanalid	elektrooniline-virtuaalne teenus	▸ e-post ▸ SM grupid ▸ SITREP ▸ riigipilve teenused (kodanikeregister, sõidukiregistrid jm) ▸ Microsoft Teams (sisekommunikatsiooniks) ▸ mobiiltelefon (eelistatud vahend operatiivsideks) ▸ avalik meedia (riiklik, kommerts)
	reaalne-füüsiline teenus	▸ transport, virgatsid, teadetetahvlid külades ▸ kerksuskeskus valla/külade infovahetuskohaks ▸ avalik meedia, paberleht ▸ valjuhääldid
	kommunikatsiooni kiirus ja aeg	▸ kiiruse stabiilsus töövoos (nt töö- ja puhkeaeg) ▸ kasutatavuse taasteaeg (RTU) ▸ esmase info saamise kiirus ▸ kiiruse ja kanalite eelistused/seosed ▸ kiiruse sõltuvus kommunikatsiooni osapooltest
Kommunikatsiooni osapooled (sihtrühmad)	sisekommunikatsioon valla sees	▸ kriisi koordinaatorite vahel ▸ elutähtsate teenuste osutajad (vesi-kanalisatsioon, teehooldus)
	väliskommunikatsioon vallast välja	▸ päästeamet ▸ elutähtsate teenuste osutajad (elektrivarustaja, sideteenused)
	sissetuleva info allikad	▸ päästeamet ▸ üksikisikud (valla elanikud) ▸ elutähtsate teenuste osutajad ▸ KOV ametnike vaatlused
	väljamineva info saajad	▸ elanikkond, inimeste hulk ▸ tiheasustuse elanikkond ▸ hajaasustuse elanikkond ▸ üksikisikud ▸ avalikud asutused (koolid, lasteaiad, poed jm)

Peateemad	Alamteemad	Kommunikatsiooni atribuudid (kontekst, tunnused, komponendid)
Kommunikatsiooni taristud	kohalik taristu	▸ füüsiline sõnumiedastus (transport) ▸ FM raadiosaatjad külades (jahimehed, vaba FM-sagedus)
	üle-eestiline taristu	▸ RIA kaabel (e-kool, kodanikeregister, sõidukiregistrid jm) ▸ mobiilside ▸ kaabelandmeside
	Eesti-välised teenused	▸ SITREP serverid ▸ MS Teams ▸ SM-lahendused
Kommunikatsiooni juhtimine	planeerimine	▸ kriisiõppuste korraldamine (kuivõrd testitakse kommunikatsiooni) ▸ kommunikatsiooni standardite järgimine ▸ kommunikatsiooniprotseduuride dokumenteerimine, juurutamine ja järgimine, hädaolukordade lahendamise plaan, vastutus jm ▸ plaanide ja kavade regulaarne uuendamine/ ajakohastamine
	rahastusmeetmed	▸ kommunikatsioonile suunatud eelarve piisavus

TABEL 2. Kriisikommunikatsiooni atribuudid Rae valla näitel.

KASUTATUD ALLIKAD

ALLSOPP, J. (2014). Designing offline-first web apps. A List Apart.

BOIN, A. & McCONNELL, A. (2007). Preparing for critical infrastructure breakdowns: The limits of crisis management and the need for resilience. Journal of Contingencies and Crisis Management, 15(1), 50–59. – https://doi.org/10.1111/j.1468-5973.2007.00504.x.

BOIN, A., STERN, E. & SUNDELIUS, B. (2017). The politics of crisis management: Public leadership under pressure (2. trükk). Cambridge University Press.

BRAUN, V. & CLARKE, V. (2006). Using thematic analysis in psychology. Qualitative Research in Psychology, 3(2), 77–101. – https://doi.org/10.1191/1478088706qp063oa.

COOMBS, W. T. (03.03.2016). Reflections on a meta-analysis: Crystallizing thinking about SCCT. Journal of Public Relations Research. 28 (2): 120–122. – doi:10.1080/1062726X.2016.1167479. S2CID 147912618.

COOMBS, W. T. (2019). Ongoing crisis communication: Planning, managing and responding (5. trükk). SAGE Publications.

DOURISH, P. (2004). What we talk about when we talk about context. Personal and Ubiquitous Computing, 8(1), 19–30. – https://doi.org/10.1007/s00779-003-0253-8.

GIBB, F. & BUCHANAN, S. (2006). A framework for business continuity management. International Journal of Information Management, 26(2), 128–141. – https://doi.org/10.1016/j.ijinfomgt.2005.11.008.

ISO/IEC 27001: 2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements. International Organization for Standardization.

JUNG, J. & NAG, S. (2019). Effectiveness of redundant communications systems in maintaining operational control of small unmanned aircraft. NASA Ames Research Center.

KITSING, M. (2011). Success without strategy: E-government development in Estonia. Policy & Internet, 3(1), 1–21. – https://doi.org/10.2202/1944-2866.1095.

LEVESON, N. G. (1995). Safeware: System safety and computers. Addison-Wesley.

MAYRING, P. (2014). Qualitative content analysis: Theoretical foundation, basic procedures and software solution. Beltz.

NAUMANN, I. & HOBGEN, G. (2009). Privacy features of European eID card specifications. Network Security, 2009(8), 9–13. – https://doi.org/10.1016/S1353-4858(09)70092-4.

NIELSEN, J. (1993). Usability engineering. Morgan Kaufmann.

PRASETIO, B. (2025, detsember). Crisis Communication Strategies in the Digital Era: A Narrative Review of Contemporary Theories, Models, and Practices. Injurity: Interdisciplinary Journal and Humanity, 4, 12. – https://injurity.pusatpublikasi.id/index.php/inj/article/view/1502/468.

REASON, J. (1990). Human error. Cambridge University Press.

RIA (2023). Eesti infoühiskonna aastaraamat 2023. Riigi Infosüsteemi Amet.

RIIGIKANTSELEI (2024). Toimepidevuse riskianalüüsi ja plaani koostamise juhend. Elutähtsa teenuse osutajale. – https://kriis.ee/sites/default/files/documents/2024-12/TOIMEPIDEVUSE%20RISKIANAL%C3%9C%C3%9CSI%20JA%20PLAANI%20KOOSTAMISE%20JUHEND_uuendus%2017.06.2024.pdf.

ROSSON, M. B. & CARROLL, J. M. (2002). Scenario-Based Design. The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies and Emerging Applications (lk 1032–1050). Mahwah, NJ: Lawrence Erlbaum Associates.

SANDERS, E. B.-N. & STAPPERS, P. J. (2008). Co-creation and the new landscapes of design. CoDesign, 4(1), 5–18. – https://doi.org/10.1080/15710880701875068.

SEEGER, M. W., SELLNOW, T. L. & ULMER, R. R. (2003). Communication and organizational crisis. Praeger Publishers.

SISEMINISTEERIUM (2021). Riski- ja kriisikommunikatsiooni platvorm. Lõpparuanne. – https://www.siseministeerium.ee/sites/default/files/documents/2021-11/Risk%20%26%20Crisis%20Report%20ee_veebi%20üles.pdf.

SISEMINISTEERIUM (2022). Ohuteavituse SMS-i märgatavuse ja arusaadavuse hindamise uuring. – https://siseministeerium.ee/media/3268/download.

SWELLER, J. (1988). Cognitive load during problem solving: Effects on learning. Cognitive Science, 12(2), 257–285. – https://doi.org/10.1207/s15516709cog1202_4.

VON SOLMS, R. & VAN NIEKERK, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102. – https://doi.org/10.1016/j.cose.2013.04.004.

WOODS, D. D., DEKKER, S., COOK, R., JOHANNESEN, L. & SARTER, N. (2010). Behind human error (2. trükk). Ashgate Publishing.

ÜRO (2022). UN E-Government Survey 2022: The future of digital government. United Nations Department of Economic and Social Affairs.