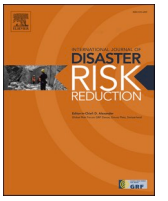
International Journal of Disaster Risk Reduction 80 (2022) 103173

Contents lists available at ScienceDirect

International Journal of Disaster Risk Reduction

journal homepage: www.elsevier.com/locate/ijdrr



Evaluation of emerging technological opportunities for improving risk awareness and resilience of vulnerable people in disasters

Juhani Latvakoski [b,*], Risto Öörni [a], Toni Lusikka [b], Jaana Keränen [c]

[a] VTT Technical Research Centre of Finland, B.O.Box 1000, 02044, VTT, Finland
[b] VTT Technical Research Centre of Finland, Kaitoväylä 1, FI-90571, Oulu, Finland
[c] VTT Technical Research Centre of Finland, P.O.Box 1300, FI-33101, Tampere, Finland

ARTICLE INFO

Keywords:
Risk awareness
Resilience
Vulnerable people
Location awareness
Social media
Emerging technologies and tools

ABSTRACT

The main contribution of this research is the evaluation of emerging technological opportunities for improving risk awareness and resilience of vulnerable people in disasters. The evaluation considered a survey, end-user evaluation, and co-creative workshops on technologies and was targeted to estimate the innovation potential, usefulness, importance, applicability, risks for vulnerable people, and ethical acceptability.

The capabilities of the Mobile Positioning Data tool (1) to increase risk awareness in rescue planning and emergency management in cyber-hazard situations and (2) to help in locating and evacuating tourists and other vulnerable people in disasters was evaluated. The capabilities of the Trasim tool to help in crisis communications training for improving preparedness and tackling mis/disinformation through simulated responses was evaluated. The evaluation indicated that there are a lot of innovation potential and useful technical enablers for improving disaster risk awareness and resilience, but there are also ethical challenges, and risks for misuse.

The digital divide between people in the unequal distribution of skills and access to technological means and tools remains an essential future challenge, especially with vulnerable people in a crisis. Issues of fairness and inclusivity need great attention in the application of these technologies in crises or disasters in order not to overlook such vulnerable people. The failure in critical infrastructures (e.g., energy and communications) seems to increase risks and exacerbate the situation of vulnerable people in crises. However, the potential of technological opportunities for improving operation in disasters is so essential that significant investment in research and development is recommended.

1. Introduction

The recent developments in technologies and tools have opened new emerging opportunities to improve risk awareness and resilience of vulnerable people in disasters. The weakest position in emergency situations is usually related to the vulnerability, which refers here to the characteristic of individuals, groups, and/or society of being susceptible to harm or loss, which manifests as situational inability (or situational weakness) to access adequate resources and means of protection to anticipate, cope with, recover, and learn from the impact of natural or man-made hazards [1,2]. It is essential to be aware of the risks of such vulnerabilities and estimate the required risk in preventing and mitigating actions, including risk-related data/information exchanging/sharing between official

* Corresponding author. VTT Technical Research Centre of Finland, Kaitoväylä 1, FI-90571, Oulu, Finland.
E-mail addresses: Juhani.Latvakoski@vtt.fi (J. Latvakoski), Risto.Oorni@vtt.fi (R. Öörni), Toni.Lusikka@vtt.fi (T. Lusikka), Jaana.Keranen@vtt.fi (J. Keränen).

https://doi.org/10.1016/j.ijdrr.2022.103173
Received 31 March 2022; Received in revised form 29 June 2022; Accepted 7 July 2022
Available online 2 August 2022

responders and non-governmental organizations. The resilience of such vulnerable people is seen to require specific proactive and reactive adaptation and changes in the face of risks, crises, and disasters, where serious disruption of the functioning of a community is caused by hazardous events, potentially leading to material, economic, and environmental losses and their impact. The main objective of this research has been to evaluate the emerging opportunities for improving risk awareness and resilience of vulnerable people in disasters.

The Sendai Framework [3] sets an applicable framework for the prevention of disaster risks, minimizing existing ones, and improving disaster preparedness for effective responses [4]. In this research, we focus on the points of view of vulnerable people on resilience to disaster risks (man-made or natural) and evaluate technologies and tools to increase awareness of risks, preparedness, and response to disasters. [5] argues that scrutinizing resilience models and the multiple variables they contain provides an opportunity to understand the complexity of resilience and identify and prioritize development targets to improve it. A framework for community stakeholders, such as residents, local government officers, and practitioners, assists in measuring resilience at the local level by offering a library of resilience indicators [6], which also highlights the diverse definitions of resilience. Social resilience can be studied on different levels (e.g., local, national, international) and perspectives (e.g., individuals, communities, emergency organizations). [7,8], and [9] have proposed frameworks of social resilience within communities that all identify essential social resilience indicators. In the BuildERS project, resilience is understood as "processes of proactive and/or reactive patterned adjustment, adaptation and change enacted in everyday life but, particularly, in the face of risks and crises." [2] Risk awareness is defined as "collective acknowledgment about a risk and potential risk prevention and mitigation actions," which is fostered by risk communication [2]. The key contribution of this research is related to the evaluation of emerging opportunities, which includes aspects of technological enablers, tools, and functions or services that are supporting improving risk awareness and resilience of vulnerable people in disasters. For example, the capability to detect the position (e.g., using a global positioning system (GPS)) and location of a person or physical device is a technical enabler. Some kind of a tool is needed to expose the position from a physical device (e.g., a smartphone) and transform it into a form that can be applied in the disaster management process. Such location-based services can support disaster management when finding vulnerable people in the disaster area. A critical analysis of the existing methods and technologies that are relevant to a disaster scenario, such as Wireless Sensing Network, remote sensing technique, artificial intelligence, Internet of Things (IoT), Unmanned Aerial Vehicle (UAV), and satellite imagery, to encounter the issues associated with disaster monitoring, detection, and management, has been carried out e.g. in Ref. [52]. The analysis of such technical enablers for disaster scenarios is essential, and actually, this research proceeds a step forward by focusing into evaluation of also tools and functions/services supporting improving risk awareness and resilience of the specific target group: vulnerable people in disasters.

The evaluation has been carried out in three phases: The first step was an analysis of existing emerging technologies and tools [10]. During that process, the importance and applicability of emerging technologies were evaluated first, and the set of tools was identified and categorized. In the second step, specific tools from step 1 were applied to the use cases of the BuildERS project and evaluated: a platform to simulate crisis communication developed for the training purposes (called the Trasim exercise platform) and a dashboard utilizing Mobile Positioning Data (MPD) [11]. These individual tools were evaluated using a questionnaire-based survey with end-users of the referred tools. In the third step, an evaluation of the emerging technologies was carried out through four international

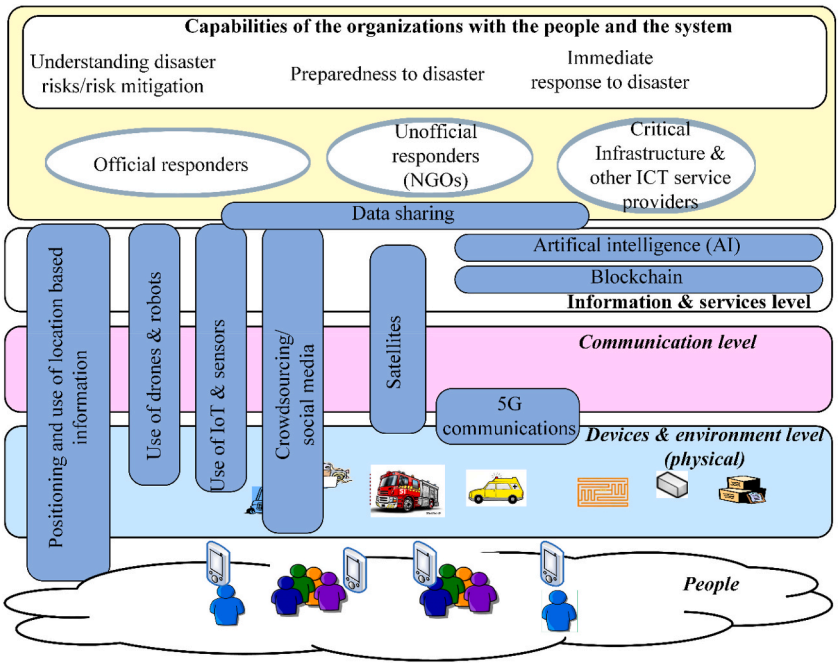


Fig. 1. Emerging technologies enable new ways to collect data in disaster situations [10,18].

and virtual co-creative workshops with the following themes: emerging technologies (satellite-based solutions, 5G, IoT, drones, artificial intelligence), location-based services, data sharing between authorities, and crowdsourcing for improving preparedness. Each workshop was targeted to evaluate the critical issues related to the innovation potential of these emerging technologies from such perspectives as desirability and usefulness of the new emerging technology, level of use (TRL level), importance (i.e., potential benefits for stakeholders), applicability (i.e., in which disaster life-cycle phases the technology can be applied), capabilities in pinpointing vulnerable people, risks and challenges, gaps (process, technological, financial, etc.), and ethical acceptability.

The rest of this paper is organized so that Chapter 2 clarifies the applied evaluation methods. Chapter 3 provides the results from the end-user evaluations. Chapter 4 explains the results from co-creative workshops. Chapter 5 discusses the results from the perspective of risk awareness and resilience. Finally, Chapter 6 provides the conclusions of this research.

2. Evaluation methods

The applied evaluation methods are described in this chapter, following the sequential order of the work proceedings. First, the analysis of emerging technological opportunities and tools are described to open the context and reasoning of the selections made in this research. Secondly, the methods applied in the end-user evaluations of specific tools are described. Finally, the methods used in the evaluations of emerging technological opportunities in co-creative workshops are provided.

2.1. Analysis of emerging technologies with reasoning for the selections for evaluation

In the first step of this research, technologies and tools developed within ~52 European research collaboration projects focused on disaster management aspects were analyzed [10]. The analysis revealed several technological opportunities that were estimated to be useful in disaster management and the potential for improving the *risk awareness* and *resilience* of vulnerable people in disasters. For example, emerging opportunities were identified, opportunities arising from positioning, location-based services, social media/-crowdsourcing, satellites, and IoT including sensors, drones/robots, artificial intelligence (AI), connectivity (5G), data sharing, and blockchains.

These emerging technologies enable new ways to collect, analyze, process, and share data in disaster situations (Fig. 1). The emergence of smartphones, mobile and satellite access infrastructures, and the Internet of Things (IoT) has created an essential basis for new opportunities for disaster management [12,13]. Smartphones can capture the geographic *location* of the user to help locate people affected by disasters. Furthermore, smartphones enable users to communicate in a richer way than basic mobile devices do, and *use* applications, such as *social media,* to rapidly exchange information during a crisis [14]. Thus, the role of smartphones in public safety warnings and emergency communications seems to be essential. However, the challenge is that these require smart actions from people.

The *IoT solutions* enable gathering information from different sensors attached to people, vehicles, buildings, infrastructures, environment, on the ground, etc. Such information streams can even be in real time, which could enable a totally new level of situational awareness in disasters. In addition to monitoring, new ways for enabling a control type of operation with cyber-physical systems (CPS), such as *unmanned robots* (e.g., drones) can enable increasing levels of detailed information that can be obtained from disaster areas [12,52]. For example, it is estimated to be possible to enrich *satellite images* by using images exposed from drone cameras. In addition to these physical assets, advancement in information sharing via heterogeneous communication channels and cloud computing, with storing of *big data* exposed from different sources, has led to possibilities for improving the situational awareness of authorities and also expanding it to NGOs, communities, and even ordinary people. The emergence of social media applications has opened possibilities for new ways of information exposure and sharing between communities of people and organizations. The recent advancement in *machine learning/artificial intelligence* is estimated to make it possible for decision-makers to get help in processing such a large information basis to improve their operation in disasters [15]. For example, increasing the smartness and combinations in processing satellite images is estimated to provide a new level in the granularity of information exposed from the raw image data. The importance of positioning, use of social media, satellite imaging, the Internet of Things, the use of drones [53–57], 5G [16], AI, and blockchain technologies [17] have a good potential to improve crisis management in the future. In addition, the emergency conditions increase the likelihood for disruptions in communication networks, and therefore the alternative networks can play a vital role in crisis management [52]. Therefore, the role of (wireless) communications as basic and critical enabler for the referred other technical enablers is highlighted.

The importance and applicability of these emerging technologies were prioritized in a preliminary way by the disaster management stakeholders of the BuildERS project. They estimated that information sharing via communications and the use of *location-based services* –related opportunities have the most essential meaning. The use of drones was estimated to enrich the information obtained from the disaster area, especially when it is challenging to get such information otherwise. The importance of AI, crowdsourcing, social media and 5G, IoT, sensors, and blockchain technologies was not yet seen to be so essential, even if they provide essential future potential. It seems that the cost of using satellite pictures hampers their application to help in disaster management. In addition, it seems that the information sharing and communications between local authorities and the not-officially accepted NGOs is a challenge in the crisis phases. Information sharing and communications between different organizations, information on the location of people and resources, and the analysis of satellite pictures are estimated to be essential in the mitigation phase. In preparedness, the applicability of crowdsourcing (people with smartphones/wearable electronics work as a kind of information-providing "sensors"), information sharing, and distributed data management, the location of people and resources for public warning systems, and data analysis for better situational awareness were estimated to be essential. In a crisis, it is important to find vulnerable people, share information for real-time situational awareness, locate people and resources, use drones for more detailed information from disaster

areas, and use all available trustworthy information in real time, even from physical assets in the response phase. In the recovery phase, information sharing and communications between organizations, location awareness, and combining information from different sources were estimated to be most applicable.

Based on these priorities, the evaluation of emerging technologies was grouped into four different categories: positioning and location-based services, crowdsourcing for improving preparedness, data sharing between authorities for crisis management, and emerging technologies for risk and vulnerability assessments (satellite-based solutions, connectivity referring to 5G and the Internet of Things, drones, and artificial intelligence). These four groups formed the basis for the division of emerging technologies into different co-creative workshops, established for a more detailed evaluation of emerging technologies.

2.2. Analysis of technological tools with explanations for the selections for evaluation

In the first step of this research, 118 technological tools were analyzed. The tools were classified, as shown in Table 1. The analysis showed that many tools can potentially be useful in disaster management for improving *risk awareness* and *resilience* of vulnerable people in disasters. In parallel to the analysis, the BuildERS project executed several use-case studies: managing a chemical spill emergency and mis/disinformation through simulated responses (UC1), vulnerability in post-disaster temporary housing (UC2), applying mobile positioning data for more precise rescue planning and emergency management under cyber hazard in Estonia (UC3), integration of public databases for identifying highly vulnerable people in need of relief prioritization by the Estonian Rescue Board (UC4), impacts of Elbe flooding disasters on socially underprivileged groups and lessons for resilience improvement (UC5), accessing strategies for improving hospital capacity for handling patients during a pandemic (UC6), and using mobile operators' data to locate, protect, and evacuate tourists and other vulnerable groups in disasters (UC7). Most of the cases were carried out without the help of any specific tools, but there were rather detailed statistical analyses of the data collected in light of the case-specific conditions and needs of the focused phase of the disaster life cycle. However, three of the cases applied technological tools: UC3 applied temporary population – a mobile position data (MPD) tool for precise rescue planning and emergency management under cyber hazards; UC7 applied the same tool with a different dashboard to locate, protect, and evacuate tourists and other vulnerable people; and UC1 applied the Trasim tool for training rescue staff for operating with mis/disinformation in a chemical spill emergency. These tools were also identified in the tool analysis and are indicated in bold font in Table 1. The analysis covered many other tools. However, a more detailed evaluation of them is not possible within the limits of this article. Therefore, the MPD and Trasim tools were selected for more detailed evaluation in this research. These are briefly described in the following sections.

Table 1
A snapshot of the classification of tools, with examples of tools.

Classes of tools	Number of tools analyzed	Examples of tools
Technologies & tools related to guidelines, methods, organizational development, training, and education	31	Resilience management guidelines, SMR [19] Multiplayer simulation environment, SimEnv [20] Game to develop empathy, Educen [21] **Messaging training simulator, Trasim** [22]
Technologies & tools related to risks related to natural disasters	26	Damage assessment, MDA [23] Weather- and climate-related, A4EU [24] Application of satellite images, Epos [25], CSW, EMS, Earthquake mapping, IREACT [26]
Technologies & tools related to the collaboration of multiple ecosystems, cyber-physical systems, and advanced IoT solutions in disaster management	12	Standardization roadmap, Resistand [27] Multisystem Information sharing, M2MGrids [28] UAV video delivery, ASA Location- and situation-aware views: Dynamic tagging [29], Swarm, Resisto [30], Hotosm [31]
Technologies & tools enabling more or less real-time operation during crisis or disaster events	53	Combining data from various sources: Heimdall [32], geolocation Collaborations and real-time training of responders: In-Prep [33], Trasim [34] Preparedness for attacks: Practise [35] Critical collaborations: Resisto [36], Cobra [37] Mobile apps and services for emergency situations: Nexes [38], eCall [39], ITAlert Situation-aware information for the public: Tilannehuone, Radiation today Situational awareness for responders: SaR-ESS, DMA, SITMAN, Blueware [40] **Smart positioning relying on past data: TemporaryPopulation**
COVID-19 -related tools	5	Tools representing the global epidemic situation: ESRI COVID-19 GIS hub Geographical location–aware services: ArcGIS Detecting people movements: DMA, Temporary population Tools following epidemic chains, ZoE Tools for tracing contacts using decentralized proximity logging: KoronaVilkku Use of digital QR codes with a smartphone application to control access of people away from home, taking a subway, going to work, entering cafes, restaurants, and shopping malls: WeChat mobile app by Alipay and Tencent

2.2.1. Temporary population, mobile positioning data (MPD) tool

The capability to define the location of potentially vulnerable people is essential for improving risk awareness. An example of a tool that relies on such technologies and provides location-aware services is the Temporary population tool – mobile positioning data (MPD) (Fig. 2). The tool can be used to analyze location data provided by mobile network operators (MNOs) relying on the positioning of people's smartphones. The data can reveal the number of people as a function of time in a certain municipality area and movements of people between such areas in some past time frame. It is estimated that the tool has the potential to improve preparedness for disasters by helping in risk awareness.

In the UC3, the MPD was applied to enable more precise rescue planning and emergency management in cyber hazards by creating spatial-temporal maps showing the positioning data of people [41]. Such maps will more precisely inform professional rescuers about the population distribution at different locations and times and will help to deliver better relief services according to need. The respective dashboard visually shows how many people are in different areas and what kind of people are there (people living in the area, people working in the area, people who regularly visit the area, domestic tourists, and foreign tourists) and also how many people in the area have a secondary home and its distance from the chosen special unit. The dashboard also shows the directions of movement and counts in different areas and secondary homes that are potentially useable as shelter in evacuations and accommodations. In addition, the dashboard can give daily, weekly, and seasonal volume changes and movement patterns using historical data for help.

The same tool has also been applied in the UC7 to locate, protect, and evacuate tourists and other vulnerable people in disasters [42, 48]. A separate dashboard has been built to support the case focusing on more real-time (24 h lag) positioning data for visually showing how many tourists are in different areas, where they are, and whether they are moving and where to. This is important to locate tourists who are especially vulnerable in a crisis such as volcano eruptions, earthquakes, tsunamis, and floods, in which they are not aware of local circumstances and have major challenges to act rationally, swiftly, and determinedly to protect themselves and avoid contributing to public chaos. The end users of the dashboard can see with almost real-time updates how many tourists are potentially affected and might need help and to follow where they are moving.

2.2.2. Trasim tool

The awareness and operation of responders with vulnerable people in disasters is an essential capability, which requires training. One example of a tool providing such training capability is Trasim (Fig. 3). Trasim is a simulation tool developed by Insta Digital Ltd., which can be used in preparedness and crisis management exercises [11]. The tool provides a platform for simulation-based collaborative real-time training of responders. It can be used to help in training real-time messaging of responders to a wider audience. The tool works so that simulated (mis/dis)information feeds of multiple social media sources and press can be sent to the responders. During training, the responders should act according to the simulated feeds (1) in public messaging space via Trasim and (2) at an operational level using other messaging channels. During the exercise, the operation of responders is followed, and feedback is given after the exercise to help in the learning process.

2.3. Methods for end-user evaluations of the selected tools

In the second step, Trasim and MPD, with two different dashboards, were evaluated in late 2020 and early 2021 [11,41,42]. End-user evaluations were carried out by demonstrating or presenting the referred technological tools to potential users at expert workshops and collecting information on participants' opinions and perceptions of the technology using an online questionnaire. The intended target groups of the workshops were public authorities in the countries covered by the case studies and other experts with knowledge about disaster management. The participants of the workshops were recruited using the contacts of the consortium members. This was necessary to ensure the participation of relevant stakeholders (e.g., public authorities). Three hybrid/online workshops were organized to demonstrate and present the technologies, one in each country: Finland, Estonia, and Indonesia. Each workshop had a different tool that was either tested by participants or presented and demonstrated to participants.

The Trasim tool was evaluated by the Finnish police and the Police University College, and it was applied in a series of crisis communication exercises. The workshop was divided into six sessions that involved different technology users from different police departments and regional rescue services. There were 60 participants in the sessions. Training exercises were organized by the Police University College, and the simulation was led by Insta Digital. Users from police departments and rescue services were the exercise participants. The tool was used to support the facilitation of tabletop exercises, so the participants were actively using the tool as part of the exercise.

MPD tools were evaluated in Estonia and used to analyze positioning data, which is automatically collected by the Estonian MNO. The Positium Data Mediator (PDM) of the tool cleans raw data, makes the needed calculations, and forms the aggregated data for building a dashboard that helps rescue organizations plan their human and material resources more accurately. In addition, it enables learning from past crisis scenarios and being able to base their decisions for future crises on this. The Estonian workshop took place in early 2021 and was held entirely online. There were 18 participants in the workshop, 14 technology users, and 4 organizers. The technology users were from different crisis management organizations: the Estonian Rescue Board, Police and Border Guard Board, Defense League, Ministry of Economic Affairs and Communication, city council, and Ambulance/First Aid. The workshop was organized by the University of Tartu and Positium Ltd. The technology and the dashboard were introduced and demonstrated to the users. Organizers first explained what MPD is and how it is used. Next, the dashboard was demonstrated via screen share. After the demonstration, participants were given temporary access to the dashboard, and they were able to practice using it. Finally, four different case scenarios were played through, and the technology users were able to use the dashboard to solve the tasks. The scenarios were: (1) people's behavior when storm warnings were given, (2) the number of people affected by a power outage, (3) how a power outage influenced the mobile connections, and (4) evacuation planning at large events (concerts, etc.).

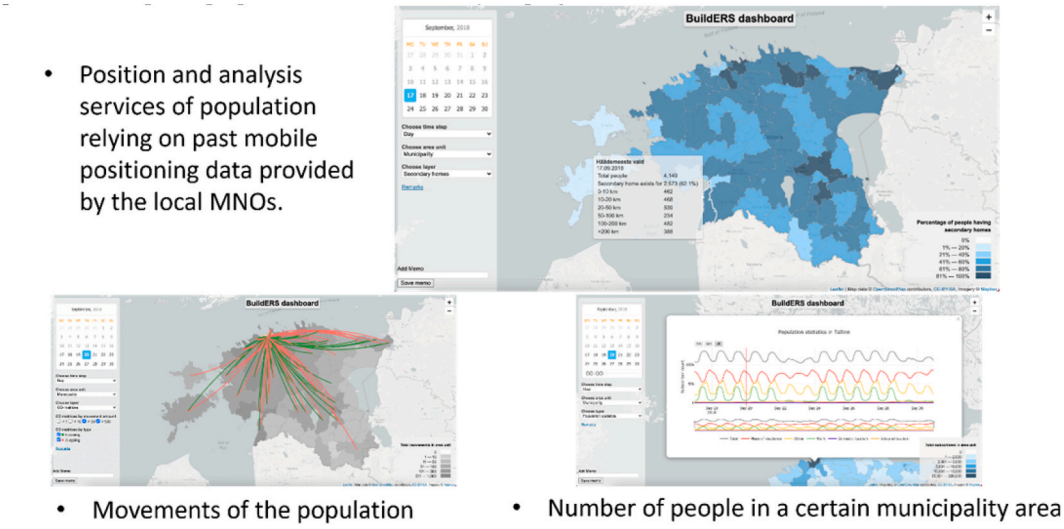


Fig. 2. Positioning and location-based services example: Temporary population tool, mobile positioning data (MPD) [41].

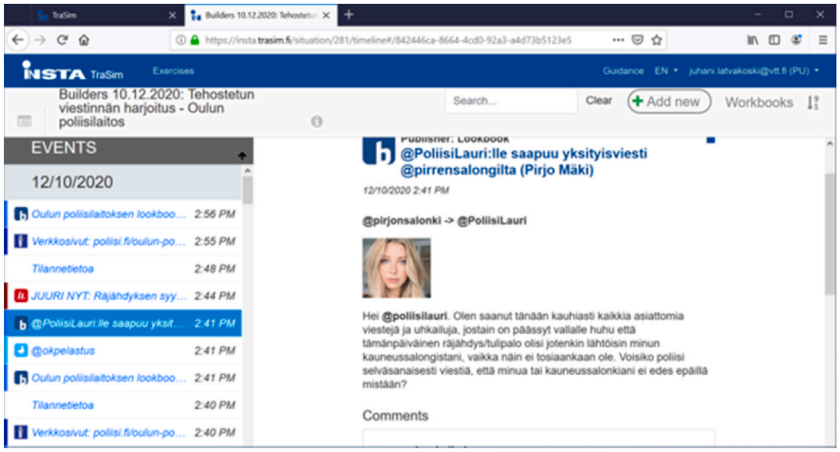


Fig. 3. Simulation-based collaborative real-time training of responders: Trasim.

The MPD technology was evaluated in Indonesia so that the applied dashboard was different than in the Estonian workshop. In this case, the dashboard was designed to be useful in crisis management in areas with a strong tourism presence. The purpose was to show (1) how many tourists were in the area when the crisis situation happened, where they are from, and (2) after/during the crisis situation, how many tourists are still in the area, where they are from, and if they are moving out of the area. The data used was simulated, but it was built and validated as if the data were real. The technology and the dashboard were demonstrated in an online workshop with 30 participants from various Indonesian government institutions (Indonesian Ministry of Foreign Affairs, Ministry of Tourism and Creative Economy, Ministry of Development Planning, National Disaster Management Agency (BNPB), National Statistical Office, Ministry of Social Affairs, and Provincial Government), non-government organizations, and civic-tech organizations. The workshop was organized by the University of Indonesia and Positium Ltd., while VTT was present as an observer. First, MPD and dashboard were introduced and demonstrated. Next, the participants were given the opportunity to ask questions and share their thoughts about the presentation. Following the discussion, case scenarios were presented to the participants: (1) information gathering in the usual process during and after disasters and (2) what information would be useful to be shown on the dashboard during a disaster, and how the information could help in the decision-making process at different times (1 day, 2 days, 3 days after the disaster). As the workshop was organized remotely, the users were not able to use the dashboard themselves, but they were able to ask organizers to show specific features and how they work.

After the technology in the UC7 had been presented or demonstrated, the participants of the event were requested to fill in an online

questionnaire, which was implemented using the Webropol tool. Participation in the questionnaire was voluntary, and responses were provided anonymously. Excluding small variations,[1] the content of the questionnaire was the same for all three case studies. The questionnaire was originally developed in English and translated and presented to respondents in the local languages of the countries covered by the case studies (Estonian, Finnish, and Indonesian).

Questionnaires were open for 1–4 weeks, and the participants were regularly reminded to answer the questionnaire. In the end, some of the participants had still not answered the questionnaire. Of the participants, 30% answered in UC1 (Finland), 80% in UC3 (Estonia), and 43% in UC7 (Indonesia). The questionnaire included six main parts. The first part of the questionnaire included questions on the stakeholder group of the respondent, the tool covered by the evaluation, and whether or not the respondent had used the tool or technology. The second part of the questionnaire focused on the respondents' general opinions of the technology, covering users' acceptance and perceived usability. The third part of the questionnaire included questions on the perceived risks related to the technology and perceived challenges for its deployment in practice. Ethical risks related to the technology were covered by the fourth part of the questionnaire. For each ethical risk, the respondents were asked to provide the expected severity of the risk for an individual or a group of people as well as its likelihood to be realized. The fifth part of the questionnaire included questions related to the technology and the BuildERS theoretical model [1]. In practice, the section included questions on the relevance of the tool in different phases of crisis management or emergency management, the scope of the technology in terms of protecting individuals, groups, or the whole society in crisis, and the ways the technology contributes to resilience-building in a crisis. The sixth part of the questionnaire included a question on the technical readiness and maturity of the tool, as well as an opportunity to express opinions and provide feedback as free text.

Except for a few free text fields, the questionnaire mostly included multiple choice questions. For most of the questions, respondents were asked to indicate on a five-step Likert scale (1–Strongly disagree, 2, 3, 4, 5–Strongly agree, or Do not know) whether they agree with the statements presented in the question or what their opinion is (parts 2, 3, questions on scope of the technology and contribution in building of resilience in part 5, and a question on technical readiness in part 6). In the case of ethical risks, an ordinal scale was used to measure the perceived likelihood that a risk will be realized as well as the perceived significance of the negative impact on individuals or groups (likelihood that risk will be realized: 1–Very unlikely, 2–Unlikely, 3– Likely, 4–Very likely, 5–Certain, Do not know; significance of negative impacts: 1–very minor, 2–minor, 3–moderate, 4–serious, 5–very serious, Do not know). For measuring the relevance of the technology in different phases of the crisis or emergency management, a five-step Likert scale was used (1–not relevant at all, 2, 3, 4, 5–highly relevant, Do not know).

The analysis of questionnaire results began by summarizing the distribution of responses to questions regarding users' acceptance and usability and the perceived ethical risks of the technologies. Basic statistical figures such as N (for numerical values 1–5), mean, and standard deviation were then calculated. The Wilcoxon signed-rank test for paired samples and binomial sign test were used to compare answers to different statements regarding users' acceptance and usability [43].

2.4. Methods for the evaluation of the emerging technologies in co-creative workshops

The evaluation of the emerging technologies was implemented through four international virtual co-creative workshops with the following themes: (1) Emerging technologies for risk and vulnerability assessments (satellite-based solutions, connectivity referring to 5G and the Internet of Things, drones, and artificial intelligence), (2) location-based services (and positioning technologies), (3) data sharing between authorities for crisis management, and (4) crowdsourcing for improving preparedness. The participants were end users, such as technology partners, first responders and service providers, officials of cities and local communities, supportive NGOs, and other stakeholders. They were chosen because they are potential actors in crisis management and would benefit from the use of different technologies, services, applications, and tools supporting crisis management activities. The technology partners were defined as technology developers and service providers who focus on solutions applicable in disaster management. First responders and service providers are typically agencies working in the first wave during an acute crisis. Officials of cities and local communities could be agencies of strategic or operational civil protection and crisis management. They could also be a contact point for risk assessment and/or preparedness planning or more communication-oriented agencies, such as communication specialists. Supportive NGOs typically act in the second wave of disasters, providing aid right after official rescue organizations. Other stakeholders could be actors focusing on education, consultancy services, or legal services. The participants of the co-creative workshops were recruited using the contacts of the consortium partners.

The evaluation started with an online kick-off event, where four technology themes and some technological solutions or applications of the theme were presented. The target of the kick-off event was to encourage participants to take part in the actual virtual co-creative evaluation workshops, which were opened just after the kick-off event. Workshops were organized using the Howspace platform and were open for eight weeks. Workshops included two parts—an informative part and an evaluation part. The informative part included written descriptions of each technology theme and some technological solutions or applications. These were written descriptions, figures, video recordings, and links to the material elsewhere, such as a link to the research project web page providing more information. In the evaluation part, participants gave their responses to the questions. There were both questions with answers on the Likert scale (ranging from 1 to 5) and open-ended questions.

Evaluation questions represented in the virtual workshops were formulated on the basis of the questionnaire-based survey. Evaluation themes were as follows: desirability and usefulness of the technology, importance and potential benefits for stakeholders, applicability, capabilities in pinpointing vulnerable people, risks and challenges, gaps (process, technological, financial, etc.),

[1] The Trasim questionnaire had one question more than in the other cases.

innovation potential, ethical acceptability, cost and benefit, and future perspectives.

The Howspace tool enables the possibility for free-form text answers to open questions as well as comments on other responses. If there is a response to an open question, other responders can see it and add their comments. This feature of the virtual tool further enables the co-creation of ideas. Features of the tool make it also possible to respond and write comments anonymously. The kick-off event and virtual workshops were held in English. However, it was possible to give responses to open-ended questions in a participant's native language, but none of the participants used this option.

The virtual workshop results were complemented by expert interviews. After the workshops, a series of interviews were organized. In these interviews, the same question format as in the online workshops was used. The interviewer read the questions out loud, one by one, and the interviewee gave the response, which the interviewer then wrote up. The interviews were carried out via online Teams meetings. At the beginning of the interview, the interviewer briefly described all four technological themes. After that, the interviewee chose one or two themes he/she wanted to answer.

The results of the virtual workshops and expert interviews were analyzed using qualitative content analysis. The analysis focused on what issues, themes, and concepts turned up from the workshop and interview information: what key themes and typical meanings were pointed out in the workshop participants' responses and what the interviewees had highlighted. The researcher-driven analysis was carried out without using any computer-aided tools.

3. Results from end-user evaluations

The results on users' acceptance and general opinions towards the tools under evaluation are presented in Tables 2–4 for the UC3 MPD tool (Estonia), UC1 Trasim tool (Finnish), and UC7 MPD/PDM tool (Indonesia). The tables include the distribution of responses and basic statistical figures (N for responses from 1 to 5, mean and standard deviation). In all three cases, most respondents had neutral or positive views on the perceived effectiveness and efficiency of the evaluated tools. This also applied to other statements related to users' acceptance, such as perceived ease of use and willingness to use the tools again, as well as their perceived suitability for civil protection, crisis management, and disaster risk management. This result is also indicated by the means of responses, which are close to 4 or 5 for all statements in all case studies, with only a few exceptions.

Due to the limited number of responses in the case studies, the results of the Wilcoxon signed-rank test for paired samples were calculated and analyzed only for the results of the Finnish case study, which had the largest number of respondents (N = 18) (Tables 5 and 6). For the differences between the responses to the different statements, the tables provide the Wilcoxon T, the z score calculated with the normal approximation of the Wilcoxon signed-rank test for paired samples, the number of pairs compared in the test (N) and the number of pairs to be compared after removing ties (Nr), and the exact two-sided p-value provided by the SPSS statistical package. Due to the low number of pairs in many of the comparisons, the exact p-value provided by SPSS was used instead of the asymptotic p-value based on the normal approximation.

For the Trasim tool (UC1 Finland), the Wilcoxon signed-rank test for paired data revealed only a few pairs of statements for which the median of the difference of answers was different from zero in a statistically significant manner (Tables 5 and 6). The perceived ease of use ("The technology is easy to use") had a statistically significant difference from most other statements. In addition, there was a statistically significant difference between the willingness to use the tool and willingness to have it adopted into regular use in the respondents own country (Finland). Finally, the suitability of the tool for disaster risk reduction had a statistically significant difference from several other statements. The differences identified with the Wilcoxon signed-rank test for paired data (measuring differences in median) were consistent with the differences in means of responses to different statements (Table 3).

Table 2
User's acceptance and general opinions of the MPD tool (UC3 Estonia) (N = 11).

Please indicate your opinions of the tool or technology regarding the following statements (from 1: strongly disagree to 5: strongly agree).	Distribution of responses						Statistical figures		
	1: Strongly disagree	2	3	4	5: Strongly agree	Do not know	N (1–5)	Mean	Standard deviation
The tool or technology is effective in achieving its purpose.				7	4		11	4.4	0.5
Regular use of the tool or technology would be an efficient use of resources (such as money or working time).			1	7	3		11	4.2	0.6
The tool or technology should be adopted into regular use in my country.			1	6	4		11	4.3	0.6
I would be willing to use the tool or technology again.				3	8		11	4.7	0.5
The technology or tool is easy to use			2	5	4		11	4.2	0.8
There are clear instructions on how to use the tool or technology.			1	6	3	1	10	4.2	0.6
The tool or technology is suitable for civil protection.			2	6	3		11	4.1	0.7
The tool or technology is suitable for crisis management.		2	2	5	2		11	3.6	1.0
The tool or technology is suitable for Disaster Risk Reduction (DRR).				7	4		11	4.4	0.5
The technology or tool is accessible.[a]		1	3	4	2		10	3.7	0.9

[a] Accessible means that websites and mobile applications and their contents are such that anyone could use them and understand what is meant in them.

Table 3
User's acceptance and general opinions of the Trasim tool (UC1 Finland) (N = 18).

Please indicate your opinions of the tool or technology in regard to the following statements (from 1: strongly disagree to 5: strongly agree).	Distribution of responses						Statistical figures		
	1: Strongly disagree	2	3	4	5: Strongly agree	Do not know	N (1–5)	Mean	Standard deviation
The tool or technology is effective in achieving its purpose.			1	14	3		18	4.1	0.47
Regular use of the tool or technology would be an efficient use of resources (such as money or working time).		2	4	7	3	2	16	3.7	0.95
The tool or technology should be adopted into regular use in my country.		2	6	5	3	2	16	3.6	0.96
I would be willing to use the tool or technology again.			3	9	6		18	4.2	0.71
The technology or tool is easy to use.			1	9	8		18	4.4	0.61
There are clear instructions on how to use the tool or technology.		2	4	6	4	2	16	3.8	1.00
The tool or technology is suitable for civil protection.		1	3	6	2	6	12	3.8	0.87
The tool or technology is suitable for crisis management.			5	8	1	4	14	3.7	0.61
The tool or technology is suitable for Disaster Risk Reduction (DRR.)		2	6	5		5	13	3.2	0.73
The technology or tool is accessible.[a]			7	3	2	6	12	3.6	0.79

[a] Accessible means that websites and mobile applications and their contents are such that anyone could use them and understand what is meant in them.

Table 4
User's acceptance and general opinions of the MPD/PDM tool (UC7 Indonesia) (N = 9).

Please indicate your opinions of the tool or technology in regard to the following statements (from 1: strongly disagree to 5: strongly agree).	Distribution of responses						Statistical figures		
	1: Strongly disagree	2	3	4	5: Strongly agree	Do not know	N (1–5)	Mean	Standard deviation
The tool or technology is effective in achieving its purpose.		1	2	3	3		9	3.9	1.05
Regular use of the tool or technology would be an efficient use of resources (such as money or working time).			2	3	4		9	4.2	0.83
The tool or technology should be adopted into regular use in my country.			1	5	3		9	4.2	0.67
I would be willing to use the tool or technology again.			2	4	3		9	4.1	0.78
The technology or tool is easy to use			2	3	4		9	4.2	0.83
There are clear instructions on how to use the tool or technology.			2	3	4		9	4.2	0.83
The tool or technology is suitable for civil protection.				4	5		9	4.6	0.53
The tool or technology is suitable for crisis management.				4	4	1	8	4.5	0.53
The tool or technology is suitable for Disaster Risk Reduction (DRR).			1	3	4	1	8	4.4	0.74
The technology or tool is accessible.[a]		1	2	3	3		9	3.9	1.05

[a] Accessible means that websites and mobile applications and their contents are such that anyone could use them and understand what is meant in them.

As part of the end-user evaluation, respondents were asked to evaluate the likelihood of different ethical risks being realized when the tools and technologies are used. The distributions of responses for the MPD tool (UC3 Estonia), Trasim tool (UC1 Finland), and MPD/PDM tool (UC7 Indonesia) are presented in Tables 7–9. The likelihood of risks being realized was measured using an ordinal scale (1: Very unlikely, 2: Unlikely, 3: Likely, 4: Very likely, and 5: Certain). For this reason, no means or standard deviations were calculated.

In the MPD tool (UC3 Estonia) and Trasim tool (UC1 Finland), most respondents considered the ethical risks to be very unlikely or unlikely to be realized. This applied to all the studied risks except the risk that accessibility requirements will not be met with the Trasim tool in UC1 and the MPD tool in UC3, and the risk of automatic profiling with the Trasim tool in UC1.

In the MPD/PDM tool UC7 (Indonesia), most respondents considered most of the ethical risks very unlikely or unlikely to be realized. Exceptions to this were infringement of privacy (which was considered as likely to be realized by most respondents) and compromise of personal data, collection of non-essential personal data, and automatic profiling (which were considered as likely or very likely to be realized by most respondents). In all three cases, the number of respondents was relatively low. This had to be considered when selecting analysis methods. It also must be considered when drawing conclusions from the results presented in Tables 2–9.

4. Evaluation results from co-creative workshops

A total of 76 responses were received in the virtual co-creative workshops, evaluating four emerging technology themes. Most of the responses (in total 31 responses, 41%) were regarding satellite-based solutions, connectivity (5G and IoT solutions), and location-

Table 5
Results of related-samples Wilcoxon signed-rank test for differences between respondents' answers to different statements regarding user acceptance and general opinions, Trasim tool (UC1 Finland).

Results of related-samples Wilcoxon signed-rank test for differences (A–B), Trasim tool (UC1 Finland)					
	A				
B	The tool or technology is effective in achieving its purpose	Regular use of the tool or technology would be an efficient use of resources (such as money or working time)	The tool or technology should be adopted into regular use in my country	I would be willing to use the tool or technology again	The technology or tool is easy to use
The tool or technology is effective in achieving its purpose.	-	T = 3 z = -1.933 N = 16 Nr = 7 p = 0.094	T = 9 z = -1.999 N = 16 Nr = 10 p = 0.072	T = 30 z = -0.302 N = 18 Nr = 11 p = 1.000	T = 10 z = -1.667 N = 18 Nr = 9 p = 0.180
Regular use of the tool or technology would be an efficient use of resources (such as money or working time).		-	T = 5 z = 0.000 N = 14 Nr = 4 p = 1.000	T = 2.50 z = -1.983 N = 16 Nr = 7 p = 0.78	T = 0 z = -2.807 N = 16 Nr = 9 p = 0.004 **
The tool or technology should be adopted into regular use in my country.			-	T = 0 z = -2.456 N = 16 Nr = 7 p = 0.016 *	T = 0 z = -2.970 N = 16 Nr = 10 p = 0.002 **
I would be willing to use the tool or technology again.				-	T = 3.5 z = -1.633 N = 18 Nr = 6 p = 0.219

based services. The least number of responses came from blockchain technology (3 responses, 4%). The majority of responses (30 responses, 39%) came from the public sector (e.g., from governments and other authorities), 26 responses (34%) came from the not-for-profit sector (e.g., from NGOs and faith-based organizations), and 17 responses (22%) were from the private sector (e.g., from businesses and self-employed). Three responses (4%) focused on the "other" option. Most of the responses came from the national level (36 responses, 47%) or global/EU level (23 responses, 30%). Of the responses, 11 (14%) were from the regional level, and six responses (8%) were from the local level.

4.1. Workshop results related to the arguments

The workshops had seven arguments to respond to on the Likert scale (1: strongly disagree, 2, 3, 4, 5: strongly agree). The results for these arguments are presented in Table 10 and Table. The number of responses varied between technological solutions and was between N = 1–11. Those average values that are presented in parentheses in Tables 10 and 11 included less than five responses. They are not included in the following comparison because the number of responses was low. Detailed results from the virtual co-creative workshops have been presented in the technical report of the BuildERS project [51].

The most substantial difference between responses occurred when evaluating the argument regarding the ethical issues of technologies. The satellite-based solutions appeared to have the fewest ethical issues (average value 1.8), while location-based solutions and artificial intelligence (average values 3.8 and 3.6, respectively) were thought to have the most ethical issues. However, the gap between the lowest- and highest-ranked technologies in terms of ethical issues was quite small, and none of the average values rose to agree or strongly agree (average value equal or more than 4) with technologies containing major ethical issues.

Table 6
Results of related-samples Wilcoxon signed-rank test for differences between respondents' answers to different statements regarding user acceptance and general opinions, Trasim tool (UC1 Finland) (Continued).

Results of related-samples Wilcoxon signed-rank test for differences (A–B), Trasim tool (UC1 Finland)					
	A				
B	There are clear instructions on how to use the tool or technology	The tool or technology is suitable for civil protection	The tool or technology is suitable for crisis management	The tool or technology is suitable for Disaster Risk Reduction (DRR)	The technology or tool is accessible*
The tool or technology is effective in achieving its purpose.	T = 10.50 z = -1.473 N = 16 Nr = 9 p = 0.176	T = 6 z = -1.000 N = 12 Nr = 6 p = 0.531	T = 10 z = -1.667 N = 14 Nr = 9 p = 0.180	T = 0 z = -2.762 N = 13 Nr = 9 p = 0.004 **	T = 3.5 z = -1.897 N = 12 Nr = 7 p = 0.109
Regular use of the tool or technology would be an efficient use of resources (such as money or working time).	T = 22.50 z = 0.000 N = 14 Nr = 9 p = 1.000	T = 1.5 z = -0.816 N = 11 Nr = 3 p = 0.750	T = 16 z = -0.302 N = 13 Nr = 8 p = 1.000	T = 3.50 z = -1.897 N = 12 Nr = 7 p = 0.109	T = 6 z = -0.447 N = 11 Nr = 5 p = 1.000
The tool or technology should be adopted into regular use in my country.	T = 37 z = -0.165 N = 15 Nr = 12 p = 0.996	T = 6 z = -1.000 N = 12 Nr = 6 p = 0.531	T = 25 z = -0.277 N = 14 Nr = 10 p = 1.000	T = 2.5 z = -1.730 N = 13 Nr = 6 p = 0.156	T = 6 z = -0.447 N = 10 Nr = 5 p = 0.655
I would be willing to use the tool or technology again.	T = 16 z = -1.563 N = 16 Nr = 11 p = 0.128	T = 7 z = -1.265 N = 12 Nr = 7 p = 0.359	T = 3 z = -1.933 N = 14 Nr = 7 p = 0.094	T = 0 z = -2.414 N = 13 Nr = 7 p = 0.016 *	T = 8 z = -1.508 N = 12 Nr = 8 p = 0.234
The technology or tool is easy to use.	T = 0 z = -2.598 N = 16 Nr = 8 p = 0.008 **	T = 0 z = -2.646 N = 12 Nr = 7 p = 0.016 *	T = 0 z = -2.887 N = 14 Nr = 9 p = 0.004 **	T = 0 z = -3.066 N = 13 Nr = 11 p = 0.001 **	T = 0 z = -3.000 N = 12 Nr = 9 p = 0.004 **
There are clear instructions on how to use the tool or technology.	-	T = 7.5 z = 0.000 N = 11 Nr = 5 p = 1.000	T = 20 z = -0.333 N = 13 Nr = 9 p = 1.000	T = 8 z = -1.508 N = 13 Nr = 8 p = 0.234	T = 2.5 z = -1.000 N = 10 Nr = 4 p = 0.625
The tool or technology is suitable for civil protection.		-	T = 3.5 z = -0.447 N = 11 Nr = 7 p = 1.000	T = 3.5 z = -1.897 N = 11 Nr = 7 p = 0.109	T = 7 z = -0.816 N = 10 Nr = 6 p = 0.688
The tool or technology is suitable for crisis management.			-	T = 0 z = -2.000 N = 12 Nr = 4 p = 0.125	T = 2 z = -0.577 N = 9 Nr = 3 p = 1.000
The tool or technology is suitable for Disaster Risk Reduction (DRR).				-	T = 0 z = -1.414 N = 9 Nr = 2 p = 0.500

Table 7
Ethical risks of the tools, likelihood of ethical risks being realized – MPD tool (UC3 Estonia).

Ethical acceptability of the tool or technology: How likely is it that the following risks will be realized when the tool or technology is used?	Very unlikely	Unlikely	Likely	Very likely	Certain	I do not know
Discrimination of individuals	7	4				
Deprivation of personal autonomy of an individual person	7	4				
Infringement of privacy	6	4	1			
Abuse of a relationship of trust	5	6				
Causing personal disadvantage for an individual person	6	5				
Stigmatization of individuals	8	3				
Inequality of individuals	6	5				
Inequality of different groups of people	4	5	2			
No freedom of choice to opt-out of the use of the tool or technology	4	4	1	1	1	
Restriction of individual's life	6	4	1			
Security of personal data is compromised	4	5		1		1
Collection of non-essential personal data	4	5		1		1
Automatic profiling	3	2	3	1		2
Accessibility requirements will not be met[a]	1	3	2	1		4

[a] Accessibility means that websites and mobile applications and their contents are such that anyone could use them and understand what is meant in them.

Table 8
Ethical risks of the tools, likelihood of ethical risks being realized – Trasim tool (UC1 Finland).

Ethical acceptability of the tool or technology: How likely is it that the following risks will be realized when the tool or technology is used?	Very unlikely	Unlikely	Likely	Very likely	Certain	I do not know
Discrimination of individuals	5	6	1			3
Deprivation of personal autonomy of an individual person	5	6	1			3
Infringement of privacy	4	6	2			3
Abuse of a relationship of trust	4	7	1			2
Causing personal disadvantage for an individual person	5	6	1			2
Stigmatization of individuals	4	6	2			2
Inequality of individuals	4	6	1			3
Inequality of different groups of people	4	6	1			3
No freedom of choice to opt-out of the use of the tool or technology	4	4	3			3
Restriction of individual's life	5	5	1			3
Security of personal data is compromised	4	5	1			4
Collection of non-essential personal data	4	6	2			2
Automatic profiling	4	6	1			3
Accessibility requirements will not be met[a]	4		1	2		7

[a] Accessibility means that websites and mobile applications and their contents are such that anyone could use them and understand what is meant in them.

Table 9
Ethical risks of the tools, likelihood of ethical risks being realized – MPD/PDM tool (UC7 Indonesia).

Ethical acceptability of the tool or technology: How likely is it that the following risks will be realized when the tool or technology is used?	Very unlikely	Unlikely	Likely	Very likely	Certain	I do not know
Discrimination of individuals	4	3	1	1		
Deprivation of personal autonomy of an individual person	2	4	2	1		
Infringement of privacy	2	1	5	1		
Abuse of a relationship of trust	2	5	1	1		
Causing personal disadvantage for an individual person	3	5		1		
Stigmatization of individuals	2	5	1	1		
Inequality of individuals	2	5	1	1		
Inequality of different groups of people	2	4	1	2		
No freedom of choice to opt-out of the use of the tool or technology	3	3		3		
Restriction of individual's life	2	6		1		
Security of personal data is compromised	1	2	4	2		
Collection of non-essential personal data	2	2	4	1		
Automatic profiling	1	2	4	2		
Accessibility requirements will not be met[a]		5		3		1

[a] Accessibility means that websites and mobile applications and their contents are such that anyone could use them and understand what is meant in them.

There was also greater variation regarding the argument for the use of technology in crisis management in the near future. Drones (average value 4.7), location-based services (average value 4.4), and crowdsourcing (average 4.0) were estimated to be widely used in crisis management in 5–10 years, while the connectivity opportunities through the Internet of Things and 5G technologies (average value 3.1) were estimated as the least-used technology.

Table 10
Workshop results related to the arguments.

Argument	Satellite-based solutions	Connectivity (IoT and 5G)	Drones	Artificial intelligence	Location-based services
This technology is very useful	4.1	3.9	4.5	**3.8**[a]	**4.9**
This technology has great innovation potential	4.3	3.9	**4.4**	**3.2**	**4.4**
This technology contains major ethical issues	**1.8**	3.3	2.8	3.6	**3.8**
This technology can increase or create risks for vulnerable people	**2.1**	2.6	2.4	3.0	2.9
This technology has great benefits with regards to its costs	3.9	3.5	**4.3**	**3.1**	4.0
This technology should be adopted into regular use in my country	4.0	**3.1**	**4.4**	3.3	4.3
This technology will be used widely in crisis management in 5–10 years	3.7	**3.1**	**4.7**	3.3	4.4

[a] The highest and the lowest averages of responses are shown in bold.

Table 11
Workshop results related to the arguments.

Argument	Data sharing	Blockchain technology	Data fusion from public datasets	crowdsourc-ing to produce new data	crowdsourc-ing to enhance data	Crowdsourc-ing to solve problems
This technology is very useful	4.5	(3.7)[a]	(4.3)	4.0	(4.0)	4.6
This technology has great innovation potential	(4.3)	(3.5)	(3.7)	(3.7)	(4.0)	4.0
This technology contains major ethical issues	(2.5)	(1.0)	(1.7)	(3.0)	(3.0)	3.4
This technology can increase or create risks for vulnerable people	(3.0)	(2.0)	(1.3)	(4.0)	(3.0)	**3.2**[b]
This technology has great benefits with regards to its costs	(3.8)	(2.5)	(3.7)	(2.7)	(3.0)	4.0
This technology should be adopted into regular use in my country	4.2	(2.5)	(3.7)	(2.7)	(3.0)	3.6
This technology will be used widely in crisis management in 5–10 years	(4.0)	(2.0)	(3.7)	(4.3)	(3.8)	4.0

[a] Those values included less than five responses are presented in parentheses.
[b] The highest and the lowest averages of responses are shown in bold.

Based on the results, the most useful technology was location-based services (average value 4.9). Crowdsourcing for improving preparedness (average value 4.6), data sharing solutions between authorities for crisis management (average value 4.5), drones (average value 4.5), and satellite-based solutions (average 4.1) were also estimated as very useful technologies. Artificial intelligence (average value 3.8) and IoT and 5G technologies (average 3.9) were evaluated to be less useful technologies in disaster management.

Drones (average value 4.4), location-based services (average value 4.4), satellite-based solutions (average value 4.3), and crowdsourcing (average value 4.0) were assessed to have great innovation potential. Artificial intelligence (average value 3.2) was evaluated to have the least innovation potential, but the average value also rose above 3, which refers to a more positive than negative opinion of the innovation potential.

Crowdsourcing (average value 3.2) and artificial intelligence (average value 3.0) were estimated to be able to increase or create risks for vulnerable people more than other technologies involved in the evaluation. Satellite-based solutions (average value 2.1) were estimated to increase or create risks for vulnerable people less than other technologies. The differences between average values in the assessment of potential risks for vulnerable people were moderate. It should also be noticed that none of the technologies were considered as creating risks to a great extent (average value less than 4 or 5).

Drones (average value 4.3), location-based services (average value 4.0), and crowdsourcing (average value 4.0) were estimated to have great cost benefits. Artificial intelligence (average value 3.1) was assessed to offer the least cost benefits. All average values were above 3, so the cost-benefit factor was seen as positive in all technologies.

The most important technologies to be adopted for regular use were drones (average value 4.4), location-based services (average value 4.3), and data sharing between authorities (average value 4.2). Connectivity opportunities through Internet of Things and 5G technologies (average value 3.1) were evaluated as less important to adopt for regular use. Again, all average values were above 3, so based on the results, all technologies were considered important to be adopted for regular use.

4.2. Workshop results from the open-ended questions

The workshops had nine open-ended questions. The questions clarified how technologies could be used and what kind of benefits they would offer for crisis management; how they could be used in identifying vulnerabilities not currently addressed or finding

vulnerable people in crisis; what kinds of risks, challenges, and gaps can be seen in using or adopting technologies; and what kind of future prospects there are regarding technologies.

It should be ensured that applications are inclusive, allowing for individuals who might face communication-related barriers to also use them. The most vulnerable people may not have the possibility to use mobile phones or other devices, or they do not find information on possible applications they could use to get help in a crisis. Regarding all evaluated technologies, it should be carefully defined as to who can use the information gathered from people. Data security, personal data protection, violation of privacy, and potential misuse of data were seen as big concerns. Who manages the data? Who can read, analyze, and use the data? Where is the data stored? And what kind of data is gathered? It should be ensured that data collected for a certain purpose is not used for any other purposes (such as commercial solutions) if not notified beforehand. There is also a risk of other misuse, such as weaponization of the data, which might increase people's vulnerabilities. Furthermore, privacy and personal data issues may be a reason that people are not willing to take technology into use. On the other hand, people might not fully understand what data (and what the data makes possible) they are providing to others when using the technology. Trust in authorities may also become a threshold for using technological services.

Another general view related to technologies was that, in the future, service platforms and communication systems will evolve, and they will be used more in everyday life. They can facilitate public actors to identify what kind of data society could produce. Data fusion from public datasets will improve understanding of vulnerability as a dynamic, rather than static, phenomenon. Better understanding could lead to the development of new methods and tools for crisis management. E-platforms will enable the building of new services. And with the help of sensor technology, personal sensors may monitor and transmit a wide range of data to other parties. A changing society will require public debate and agreement on common rules. Systems and technological solutions will likely become more complex and perhaps more susceptible to technical problems. Electrical dependence will increase, which will be a big concern for the resilience of society. The failure of the tools may put dependent services and service users at risk or exacerbate existing vulnerabilities, and the functionality of the surrounding technological structures has an impact on vulnerability in crisis [49].

4.3. Workshop results regarding the open-ended questions, satellite-based solutions, and drones

Due to the warming of the climate and extreme weather events, new areas are becoming at risk of disasters never faced before. In some areas, where crises have been rather minor, weather-related crises may be more hazardous and have more serious impacts on society in the future. These crises and their impacts could be examined more thoroughly by satellite-based solutions, which could offer new ways to identify vulnerabilities. For example, they could help identify people and areas that are threatened by ongoing disasters and where possible evacuation routes are blocked and alternative options must be considered. Drones could be used in areas where access is denied due to hazardous circumstances or where it is difficult to move. They can be used to look for people still caught in affected disasters and to locate people who need special assistance. Drones can also be used to collect visual information with infrared cameras to identify heat sources, like people who cannot be seen in the normal visual spectrum (e.g., in darkness).

On the other hand, satellite-based solutions may provide freely available pictures of private property that may pose a risk of misuse of information by, e.g., criminal parties. There might also raise the risks of violating privacy. The high costs of regarding launching and operating satellites may pose challenges. If the prices rise too high, disaster relief agencies may not be able to utilize satellite imagery. Problems may occur if the frequency and timeliness of satellite imagery are too low for real-time disaster detection and monitoring. On the other hand, the information relies heavily on a multilevel coordination plan. If such a plan is not implemented, the high cost of operations may not be justified. Drones can intrude into private spaces, they can threaten normal air traffic, or they can be easily weaponized. Drones may cause accidents and collisions with manned aircraft. They can be hacked and, therefore, led by someone whose intentions may be hostile. Existing regulations regarding drones were seen as insufficient. There is a need for clear regulation, stating who is allowed to fly drones, when, and in which conditions. General public acceptance was also seen as an issue that has to be considered when using drones and enacting legislation regarding them.

Some ethical issues arose. The very high-resolution imagery, which shows very detailed targets, can lead to a security risk of terrorism. It could also provide criminals with information about valuable targets for armed robberies or locate areas of chaos to exploit the chaos. State actors or private stalkers can use technology for spying on people. Aside from potential personal data and ethical issues and the potential weaponization of such information against migrant and refugee populations, homeless populations may also be at risk. This could increase the precarity of their situation. Similar concerns arose regarding the use of drones. Intrusion into privacy by very clear images of personal spaces and the potential use of weapons both concern major ethical problems.

Satellite-based solutions will increase knowledge about disasters' spatial extent that can be used both in real-time responses and for statistical purposes. To make better use of statistics in the future, service providers should provide easy-to-understand services and products so that all actors, such as first responders, government agencies, and care-providing organizations, have a clear and equal understanding of the data that can be used for evidence-based management. Still, the high price of the services can be an obstacle to large-scale exploitation. Drones are seen in routine use in crisis management in the future. They can replace costly manned aircraft, and they can access places with obstacles that hinder manned aircraft. Drones can be potentially used especially for remote positioning in areas at risk. However, current flight regulations still need improvement regarding remote flight and the use of drones.

4.4. Workshop results regarding the open-ended questions, location-based solutions

Location-based solutions can be used to identify vulnerabilities not currently addressed. Mobile applications can contact people in a certain area when a disaster occurs. If a person has a mobile phone and an appropriate application, it is possible to share two-way information, such as guidelines for evacuation from authorities or a for person in a disaster area to ask for help. With predownloaded applications, it is possible to store information on personal health problems or conditions that will make an individual

vulnerable in certain circumstances and what kind of help they would need from others. The technology could assess an individual's proximity or ability to access an evacuation route and/or their proximity to a center that could help in a crisis (i.e., earthquake or flood). The challenge is that when using personal data, such as health records, there are always ethical issues to be considered. However, data could illuminate the special needs of individuals and offer possibilities to be better prepared.

The technology could also enable multilingual communication in a crisis and send emergency warnings and evacuation guidance to phones located in a specific area or an operating range of a base station. An individual-level technology assistant could help disabled people in a crisis. Devices with the facial recognition feature can translate messages from different languages in order to reach crisis management personnel. This way, it is possible to tackle communication-related barriers in a crisis for populations like tourists (who may not have the same situational awareness as a local) or a migrant or refugee who may not speak the language of the host country.

There are also risks and challenges in using location-based technology. IoT solutions may cause privacy issues if a considerable aspect of everyday life is monitored. People also need to understand all the functions of the IoT devices they use so that they can decide what kind of information devices collect and share with other actors. There may be a risk that personal data will be shared with operators for purposes people may not want. For example, data can be exploited commercially, as commercial exploitation can be a prerequisite for the availability of technology. Authorities may use data for different purposes like invoicing services or taxation, or data can be used for criminal investigations. Careful definitions will be needed, in which the situations' authorities or other organizations can send mass messages to people. Processes and protocols should be properly defined and managed in order to avoid any misuse of power.

In some cases, vulnerable populations may not be as mobile as the others may be. For example, a homeless community may congregate in one particular area if it is known to be a safe area. If the positioning data is matched to their community, this information can potentially be weaponized against them. Aside from potential violations of privacy or security, location-based technology could further marginalize individuals who already face communication-related barriers. Populations like the homeless, refugees, and migrants may not have updated devices enabling connectivity technologies and may not be able to benefit from this technology.

Many actors are working to promote and improve the use of location-based data in various sectors in the future. However, there will be big challenges in locating persons, since ethical problems will exist. Significant added value from location-based services would be needed to accept extensive use of location-based applications for humans. Approval from the users related to technological applications and legislation are the key issues for promoting the technology on a wider scale.

4.5. Workshop results regarding the open-ended questions, artificial intelligence

Technological solutions such as artificial intelligence could be used to identify calls for help from social media platforms and to bring requirements to the attention of rescue organizations and other actors categorizing them according to urgency. AI could be used for identifying abnormal events and weak signals of undesirable phenomena from social media channels, so-called "red flags" that may indicate gradually evolving patterns. These might include vague or still hidden phenomena of vulnerabilities that should be better scrutinized, analyzed, understood, and considered in disaster management.

Artificial intelligence often has unknown or unrecognized biases based on the data used to train it. AI technology may be applied without fully understanding what it actually does. There might also be expectations that AI works in any case or case at hand if it has worked previously. On the other hand, AI itself was not seen as a risk as an analyzing tool, but the data AI analyzes might pose a risk. If AI analyzes data from social media or more personal data, it might raise issues and privacy concerns. On the other hand, if weather-based data is analyzed, no major risk for using AI was seen.

AI is a novel technology, and it might be very difficult to completely avoid mistakes. This might lead to ethical problems when data associated with people is processed. Due to the data used to train AI systems, they are often biased against population groups that are already discriminated against. Therefore, certain populations with no access to computers or mobile phones may be left out of the AI analysis, thus perpetuating normative conceptions. Technology, like technical platforms, was not seen as a problem for ethical issues as such. Ethical problems will be related to the content and data itself since information security and data protection issues may cause ethical problems. If vulnerable people are not covered by the data sources already collected, the vulnerability will not be identified when using this kind of tool. In that way, their visibility is further diminished.

In the future, AI will probably become much more widespread and an integral part of both everyday life and preparedness and disaster response efforts. However, it might be a subject for enormous discussions and controversies since it raises conflicting opinions, and many ethical aspects still need to be carefully scrutinized, evaluated, and decided.

4.6. Workshop results regarding the open-ended questions, crowdsourcing

Crowdsourcing can reveal new vulnerabilities that may not be visible in advance and give crisis management or care-providing organizations new insight into the realities of the populations they provide help for. The ability of this technology to find vulnerable people in a crisis may be limited, but if used in the same way as when mapping COVID-19 symptoms, for example, authorities or other organizations might have a better understanding of where certain populations may need help. However, crowdsourcing is limited to people who have access to mobile devices or other devices that may be connected to data networks.

Crowdsourcing largely relies on the use of mobile phones that can run newer applications. Certain individuals who may be a part of a population considered vulnerable may not have access to novel mobile phones. This may lead to them being excluded from the assessment when using technology. The involvement of citizens greatly depends on their capacity to participate. Language barriers or distrust in authorities could prevent some individuals from participating. If this happens, some populations will be left out of the co-creation problem-solving process, which may distort or at least adversely affect the results.

In crowdsourcing, people might deliver false information due to their own misunderstanding, they might have hostile intentions, or

they might even make jokes. Guidelines for collaboration in crowdsourcing will need to be defined in order to ensure suitability and aligned activities. Crowdsourcing could be most helpful in total catastrophes, floods, earthquakes, etc. However, in these situations, the mobile network does not always work. Too much reliance on digital communication networks and the applications they provide can become problematic if it fails due to a disaster, and there are no non-Internet-based backup systems.

5. A discussion on the evaluation results and risk awareness and resilience of vulnerable people in disasters

The user acceptance and general opinions of the systems, as well as the ethical risks, were studied using a questionnaire in three use cases (UC1, UC3, and UC7). In all three use cases, the number of responses to the questionnaire was limited. This had to be considered when selecting the analysis methods and drawing conclusions from the results presented in Tables 2–9 The end-user evaluation also had other limitations. First, the participants of the workshops were more or less self-selected and recruited by using the contacts of partners involved in the BuildERS consortium. This choice was necessary because it would have been difficult to use other means to engage with the stakeholders relevant to the study. The process of collecting responses with a questionnaire probably also contributed to the self-selection of respondents. In all three workshops, the response rate to the questionnaire was clearly less than 100%. It is probable that the participants of the end-user evaluation had more knowledge of the studied technologies than average members of the target group (expected users of the tools, including safety and security organizations and non-governmental organizations in the countries where the use cases were located). On the other hand, there is no reason to expect that the respondents were systematically more positive or more critical toward the evaluated technologies than the target groups in each of the countries covered by the end-user evaluation. The questionnaire was originally developed in English, but it was translated into Estonian, Finnish, and Indonesian before responses were collected. While efforts were made to ensure high-quality translation work, translating text to another language risks changing the meaning.

In general, participants of the end-user evaluation had positive or neutral perceptions of the three tools evaluated in the three use cases. This observation is based on the distributions of responses presented in Tables 2–4, without performing a detailed statistical analysis. In UC1, the Wilcoxon signed-rank test for paired data was used to identify differences in the medians of responses to different statements. A few observations can be made based on these results.

First, the results suggest that respondents of the UC1 were more willing to use Trasim again ($\mu = 4.2$, $\sigma = 0.71$, Table 3) than to recommend it for regular use in Finland ($\mu = 3.6$, $\sigma = 0.96$, Table 3), (Wilcoxon signed-rank test for paired data: $p = 0.016$, Table 5). The results of the questionnaire do not provide an obvious answer for why the respondents were more willing to use Trasim themselves than to recommend it for regular use in Finland. Respondents mostly considered Trasim effective in achieving its purpose ($\mu = 4.1$, $\sigma = 0.47$, Table 3) and considered it easy to use ($\mu = 4.4$, $\sigma = 0.61$, Table 3). However, respondents agreed slightly less with statements on Trasim's suitability for civil protection ($\mu = 3.8$, $\sigma = 0.87$, Table 3), crisis management ($\mu = 3.7$, $\sigma = 0.61$, Table 3), or disaster risk reduction ($\mu = 3.2$, $\sigma = 0.73$, Table 3), its accessibility ($\mu = 3.6$, $\sigma = 0.79$, Table 3), and perceived effectiveness in the use of resources when taken into regular use ($\mu = 4.1$, $\sigma = 0.47$, Table 3). Possible explanations include the relatively specialized scope of the Trasim tool and uncertainty about whether training sessions where Trasim is applicable should be regular activities or organized as one-off training events.

The analysis of differences between statements with the Wilcoxon signed-rank test was exploratory, as there were no prior assumptions on which of the statements regarding user acceptance and general opinions of the tools would rank highest when ordered according to their means or medians of differences. In other words, all pairwise comparisons between the variables describing user acceptance or general opinions of the tools were considered relevant when the analysis was planned. The analysis involved multiple comparisons between variables, and it can therefore be argued that the comparisons were unplanned, and a Bonferroni correction or other corresponding procedure needs to be applied to control the Type I error rate (null hypothesis is rejected incorrectly). On the other hand, the use of the Bonferroni correction in an analysis with 18 respondents and 40 comparisons with a null hypothesis would lead to a very conservative result and increase the Type II error rate, even though it would reduce the possibility of committing a Type I error. According to an earlier paper, the use of the Bonferroni correction is not recommended when the study results are used for creating hypotheses for further research or when a simple test (e.g., *t*-test) is used multiple times and the results of the individual tests are of interest [1]. For these reasons, the Bonferroni correction was not used to adjust the p-values. Instead, the possibility of Type I errors was considered when discussing the p-values obtained with the tests.

In total, the Wilcoxon signed-rank test for paired data identified 10 pairs of statements for which the median of differences in responses was unlikely to be zero ($p < 0.05$). Seven of these pairs of statements involved the statement on ease of use ("The tool or technology is easy to use"). This is consistent with the fact that the statement on ease of use also had the highest mean of responses ($\mu = 4.4$, Table 3). Although the number of responses was relatively low ($N = 18$), the high mean of responses regarding ease of use suggests that the participants of the training session were able to successfully interact with Trasim and obtain first-hand experience of the functionalities provided.

The end-user evaluation also covered the ethical risks of the tools studied in use cases UC1, UC3, and UC7. In the Estonian use case (UC3), most respondents considered the studied ethical risks very unlikely or unlikely to be realized, except for automatic profiling and the risk that the service will not meet accessibility requirements. In the Indonesian case, the technology to be evaluated was very similar to the Estonian case, but the results were different. In the Indonesian use case, the majority of the respondents classified more risks in the category of ethical risks as least likely to be realized or risks whose likelihood of being realized is unknown (Table 9, infringement of privacy, security of personal data is compromised, collection of non-essential personal data, and automatic profiling). Possible explanations for this include differences in the tools demonstrated to respondents and differences between countries in the perception of risks related to the processing of personal data.

When discussing more specifically about people who are vulnerable or with limited capability, an essential challenge arises from the fact that most of the tools and new technological opportunities (e.g., location-aware services) require the use of some physical asset device, such as a smartphone or any IoT device. When a vulnerable person is located somewhere in a disaster area without such a device or capability, then it is a real challenge to find him or her. The use of crowdsourcing, drones/robots, and imaging with artificial intelligence may provide some opportunities. However, the application of these technologies for finding such vulnerable people highlights the need for essential information collection and sharing-based actions in the preparedness phase. For example, the MPD tool applies the capability to collect historical data about locations and movements of people to be better prepared in a crisis. When vulnerable people have the required physical assets, then the use of location-aware services becomes easier, but then trust, security, privacy, and ethical issues bring challenges. In addition, using smartphones efficiently requires preceding actions related to application installation, configuration, and skills to use the referred applications.

The emergence of social media channels and applications has opened new ways of identifying and sharing information between people and organizations. Smartphones have enabled people to use various social media applications and contribute their own opinions and observations, as well as photos, videos, and audio clips in real time, even in mobile conditions. This technology utilizes information from the grassroots level that would be disseminated through collaborative networks. In this way, new vulnerabilities that had not previously been focused on could be illuminated. In order to ensure better opportunities to participate and share information, applications should be inclusive, allowing individuals who might face communication-related barriers to also use them. They should be widely available, cost-efficient, easy to use, and suitable for different devices, such as different types of mobile phones [50]. also emphasize factors related to the willingness of adoption such as perceived usefulness and perceived ease of use in the study of using information technology for disaster risk management. Developers of technology should also focus on how users can use technology to its maximum potential.

The digital divide between people that is related to the unequal distribution of skills and the access to technological means and tools remains an essential future challenge, especially with vulnerable people in crisis. For example, old people, children, homeless people, and people with limited financial resources can be such vulnerable people. Thus, issues of fairness and inclusivity need great attention in the application of these technologies in crises or disasters in order to avoid overlooking vulnerable people. It is essential that these issues are considered and included in the monitoring radar of emergency planners and responders. Furthermore, disruptions to vital infrastructure, like the electricity cut off during storms in recent years in Estonia and Sweden or the damage to the communication infrastructure (telecommunication masts) due to wildfires (Portugal, Sweden), indicate the fragility of the technological tools in a hazard situation. The failure of the tools may keep dependent services and service users at risk or exacerbate existing vulnerabilities. However, the potential of the discussed technical opportunities for improving operation in different disaster life-cycle phases is so essential that a significant investment in research and development actions is recommended. However, it is important to consider trust, security, privacy, and ethics-related challenges.

According to the results of the workshops, data security, personal data protection, violation of privacy, and potential misuse of data was seen as major concerns. It should be carefully defined as to who can use the data gathered from people and other sources. Data management procedures should be strictly defined and practices specified. Personal or sensitive data collected for a certain purpose should not be used for other purposes without careful consideration [44]. argues the same problem as a tendency to use information for purposes unrelated to the purposes the information was originally collected. There is also a growing need to share such data with other organizations, so solutions are needed for trusted data sharing. Organizations should be able to govern their data in order to uphold data protection, privacy, and security. Ethical aspects should also be taken into consideration when planning data gathering, sharing, and usage because breaches in data protection could potentially make people (more) vulnerable.

The results also showed that personal data and privacy issues may be a reason why people are not willing to use useful applications. This has also been seen in the public acceptance of COVID-19 contact tracing applications [45]. According to the results, distrust in authorities may also become an obstacle to introducing new technological tools and solutions since people expect that authorities will misuse the technology. Furthermore, people might not be aware of who or what organization is responsible for gathering sensitive information about them. For example, regarding cloud services, different technologies and services become intertwined and it is not always clear what people can expect concerning privacy [47]. Therefore, it can be said that the misuse and abuse of technologies might increase the vulnerability of people.

Service platforms and communication systems are evolving, and their use is becoming more commonplace. Electronic platforms enable the development of new services, and more common sensor technology allows for monitoring and transmitting a wide range of information to other parties. As a result, the understanding of what kind of data society could produce will grow. Combining data from public datasets improves the understanding of vulnerability as a dynamic phenomenon rather than a static one. A better understanding could lead to the development of new methods and tools for crisis management. The more sophisticated systems require common rules to be agreed in order to maintain data security and trust for public actors.

Crowdsourcing and artificial intelligence were estimated to be able to increase or create risks for vulnerable people more than other technologies involved in the evaluation. In crowdsourcing, this may happen because some part of the population does not have access to novel mobile phones, a sufficient data link, or a local mobile subscription, and thus they are excluded from the co-creation processes. They are not heard, and their opinions are not visible in the results. This may lead to decisions that do not consider the entire population but only those who speak the loudest. The risk of AI was related to the information being analyzed. If sensitive data (such as personal data) is used, there is a risk of violating privacy. AI can be easily misused (and mistrained), and there are serious risks to feed human rights violations [46]. If AI is used to analyze non-sensitive data and training data is well selected, benefits might become great. Predicting earthquakes, speeding up map creation, and image recognition of satellite photos are examples of developing applications giving hope to disaster actors. Satellite-based solutions were estimated to increase or create risks for vulnerable people less than other

technologies. However, satellite-based data can also be used for negative purposes, such as identifying vulnerable targets for hostile purposes.

The main differences between responses emerged when evaluating the argument on ethical issues of technologies. The least ethical challenges were estimated to be related to the satellite-based solutions, while location-based solutions and AI were estimated to have the most ethical challenges. It should be noted that none of the technologies evaluated in the workshops were estimated to include major ethical challenges.

Based on the results, technological solutions can be used in many ways to identify vulnerabilities that are not currently addressed or to find vulnerable people in disasters. Satellite-based solutions can identify people and areas threatened by ongoing disasters and find routes for evacuation. Drones can be used to collect visual information in areas where it is not possible to move and there is a need to locate people still needing help. Location-based services can be used to share information from rescue organizations to people in a disaster or vice versa. With technology, communication can be translated into other languages or shared in a way that individuals can receive and understand it. AI can be used for analyzing rising phenomena or weak signals from large amounts of data, such as social media channels. Individuals' first-hand information can be gathered by crowdsourcing, allowing them to share videos, pictures, etc., even in real time.

Location-based services can tailor information that authorities distribute to people in a disaster area. It is more personal, faster, and more seriously taken this way than writing on a news portal that there is a storm coming and the level of preparedness will be raised. People get the information faster, and this is essential during a crisis. People who read or listen to the news once or twice a week or don't consume social media that much are vulnerable, as they might not get the information fast enough. This technology would enable them to be less vulnerable.

There is already a lot of data and information available. The challenge is to identify and analyze existing data from the viewpoint of different actors. Silos and barriers between different actors prevent the sharing and effective use of information. Information sharing between authorities is prescribed by law, but there are exceptions regarding the confidentiality of the information. Other actors, such as non-profit care organizations and NGOs, are in an even more difficult situation with regard to access to information. The most impressive new functionalities may be found in the interfaces between actors who have not cooperated before. Vulnerability should be identified before a crisis happens in so-called "everyday life," which could enable fast responses when a crisis occurs and support comprehensive crisis management. A balance must be sought between the need to protect the privacy of personal data and the need to protect human lives in foreseeable disasters. This can be achieved by creating solutions for trusted data sharing and rules for data governance, assessing privacy impacts of novel technologies, researching how to minimize the impact of new technologies on privacy, and through public ethical discussion on the right balance between privacy and safety.

Systems and technological solutions will likely become more complex and may be more susceptible to technical problems. Dependency on electricity and communications is continuously increasing, which will be even bigger concern for the resilience of society in future. Non-technological tools and methods are still needed to support crisis management. These tools and methods should be used along with emerging technologies to improve technological solutions continuously. If technology and the number of remote services increase, personal contacts of vulnerable people with others will decrease, which in turn can have harmful consequences and increase the sense of being marginalized.

When assessing the ethics of the study carried out, the following issues should be specifically mentioned. The participants of the workshops or interviews participated voluntarily as a part of their duties. The participants registered as users of the Howspace tool (data collection and co-creation tool), but the personal information they provided in the registration phase was not linked to their responses and was not processed in the analysis of the results.

6. Conclusions

The key contribution of this research is related to the evaluation of technological tools and emerging technological capabilities for enabling new kinds of means to support disaster management. An example of such emerging technological capability is positioning—the capability to detect the position and location of a person or physical device—which can be used for help when finding vulnerable people in the disaster area. The evaluation has been carried out in three phases. The first step was an analysis of existing emerging technologies and tools. In the second step, specific tools were applied by the disaster management stakeholders in an organized manner in workshops and evaluated: a platform to simulate crisis communication developed for the training purposes called the Trasim exercise platform and a dashboard-utilizing Mobile Positioning Data (MPD). These individual tools were evaluated using a questionnaire-based survey with the end-users of the referred tools. In the third step, the evaluation of the emerging technologies was carried out through four international and virtual cooperative workshops with the following themes: emerging technologies (satellite-based solutions, 5G, Internet of Things, drones, artificial intelligence), location-based services, data sharing between authorities, and crowdsourcing for improving preparedness. Each workshop was targeted to evaluate the critical issues related to the innovation potential of these emerging technologies from such perspectives as desirability and usefulness of the new emerging technology, level of use (TRL level), importance (i.e., potential benefits for stakeholders), applicability (i.e., to which disaster life-cycle phases the technology can be applied, capabilities in pinpointing vulnerable people, risks and challenges, gaps (process, technological, financial, etc.)), and ethical acceptability.

The evaluated MPD tool is an example tool for applying positioning technologies for enabling location-based services. The evaluation highlighted the importance of collecting, sharing, and analysis of the data on the location and movements of people during preparedness phase. It could enable more precise rescue planning and emergency management, as well as locating, protecting, and evacuating tourists and other vulnerable groups in a crisis, such as volcano eruptions, earthquakes, tsunamis, and floods. The

application of location-aware services requires the use of a physical asset device, such as a smartphone or any IoT device, on which location data can be tracked. When a vulnerable person is located somewhere in a disaster area without such a device or capability, then it is a real challenge to find him or her. Therefore, collecting, sharing, and analysis of the data in the preparedness phase is important. However, trust, security, privacy, and ethical issues then introduce challenges. For example: Who can manage the data? Who can read, analyze, and use the data? Where is the data stored? What kind of data can be gathered? In the end-user evaluation (MPD tool in the Estonian case, UC3), most respondents considered the ethical risks to be very unlikely or unlikely to be realized, except for automatic profiling and the risk that the service will not meet accessibility requirements. In the Indonesian case (UC 7), the majority of the respondents classified more ethical risks as least likely to be realized. This could be due to differences in the MPD tool dashboards and differences between countries in the perception of risks related to the processing of personal data.

The evaluated Trasim tool is an example tool applying social media technologies for improving preparedness. In the Finnish case (UC1), it was used for training rescue people to act in a good way with vulnerable people in managing a chemical spill emergency and mis/disinformation situations. The evaluation highlighted the importance of social media, crowdsourcing, and artificial intelligence (AI). In crowdsourcing/social media systems, people can contribute their own opinions and observations, as well as photos, videos, and audio clips, even in mobile conditions in real time. Crowdsourcing and AI can be useful for getting data from vulnerable people rapidly; however, there is a high risk for mis/disinformation and illegal use of privacy-sensitive data. Therefore, their application also contains more ethical risks than the other technologies analyzed. In the end-user evaluation of the Trasim tool, the respondents were willing to use the tool again and mostly considered the tool achieved its purpose, but slightly fewer agreed with statements on Trasim's suitability for civil protection, crisis management, or disaster risk reduction. This may be because of the relatively specialized scope of the Trasim tool and uncertainty over whether training sessions where Trasim is applicable should be regular activities or organized as one-off training events.

The evaluation of the emerging technologies in collaborative workshops showed substantial differences regarding ethical issues. The satellite-based solutions appeared to have the fewest ethical issues, while location-based solutions and artificial intelligence were thought to have the most ethical issues but no major ones. Drones, location-based services, and crowdsourcing were estimated to be widely used in crisis management in 5–10 years, while the connectivity opportunities through the Internet of Things and 5G technologies were estimated as being not so much used. Based on the results, the most useful technology was location-based services. Crowdsourcing for improving preparedness, data sharing solutions between authorities for crisis management, drones, and satellite-based solutions were also estimated as very useful technologies. Artificial intelligence, IoT, and 5G technologies were evaluated to be less useful technologies in disaster management. Drones, location-based services, satellite-based solutions, and crowdsourcing were assessed to have great innovation potential. Crowdsourcing and artificial intelligence were estimated to be able to increase or create risks for vulnerable people more than other technologies included in the evaluation. Drones, location-based services, and crowdsourcing were estimated to have great benefits in cost. The most important technologies to be adopted for regular use were estimated to be drones, location-based services, and data sharing between authorities.

The evaluation of the emerging technologies via open questions and discussions raises several important aspects related to vulnerable people. Vulnerable people may not have the possibility to use mobile phones or other devices, or they do not find information about possible applications they could use to get help in a crisis. When information is collected, data security, personal data protection, violation of privacy, and potential misuse of data were seen as big concerns. It should be ensured that data collected for a certain purpose is not used for any other purpose (such as commercial solutions) without agreeing on it beforehand. Challenges with privacy and lack of trust towards authorities/service providers may prevent people from using the technology.

The satellite-based solutions and drones could offer new ways to identify vulnerabilities in environmental disasters. For example, they could help identify people and areas that are threatened by ongoing disasters, where possible evacuation routes are blocked, and alternative options must be considered. Drones could be used in areas where access is denied due to hazardous circumstances or where it is difficult to move to search for people affected by the disaster and locate people who need special assistance. Drones could also be used to collect visual information with infrared cameras to identify heat sources, like people who cannot be seen in the normal visual spectrum, e.g., darkness. On the other hand, satellite-based pictures may bring the risk of misuse, e.g., violating privacy for criminal purposes. In addition, the high operational cost and low frequency and slow image data processing may prevent the application of satellite images in disaster management. Drones can be misused to detect private spaces, even for hostile purposes, and they may cause accidents because regulations are considered insufficient. Very high-resolution imagery may lead to spying on people and the risk of terrorism. Satellite-based solutions have a high potential to increase knowledge about a disaster's spatial environment, which may be used statistically in preparedness and real-time responses. However, enabling benefits would require support for understanding and analyzing data for crisis management stakeholders.

Location-based solutions can be used to locate vulnerable people, identify them and their vulnerabilities, and contact them in the disaster area. For example, guidelines for evacuation from authorities can be provided (e.g., a route to the nearest assistance center) or a person in a disaster area can ask for help from authorities. The vulnerable person can apply a mobile application to store information on personal health problems or vulnerability conditions and clarify the needed help. The challenge is that when using personal data, such as health records, there are always ethical issues to be considered. The technology could also enable translations to the native language of the person traveling abroad. Location-based services with IoT solutions may collect privacy-sensitive data related to individual persons, which can cause privacy issues. There is a risk that such personal data is used for commercial purposes without permission, illegal purposes by criminals, but also useful purposes like invoicing or taxation by authorities. For example, vulnerable homeless people may be located in a certain area in a city, and this information can be used against them in a hostile or illegal way. Location-based services can be very useful, but they have serious ethical and privacy problems because of the possibility to locate individual persons.

Artificial intelligence could help rescue organizations detect urgent help requests from social media platforms. AI could also be used to identify abnormal events and weak signals of undesirable phenomena from social media channels, which may indicate gradually evolving patterns. These might include vague or still hidden phenomena of vulnerabilities that could train AI engines to enable better understanding and take them into account in disaster management. The results of such AI-enhanced analysis of data may raise ethical and privacy issues and thus risk information misuse. It is seen that AI will probably become much more widespread and become an integral part of both everyday life and preparedness and disaster response efforts in the future.

Crowdsourcing can reveal new vulnerabilities for crisis management and care-providing organizations related to the realities and viewpoints of people so that the people themselves reveal their own or their neighbors' conditions. It may help authorities to have a better understanding of where people may need help. Crowdsourcing largely relies on the use of smartphones and the capability of people to use social media/crowdsourcing tools, which may exclude some vulnerable groups of people living without such smartphones. Another challenge arises from wrong or misleading information, which may have hostile intentions. Crowdsourcing could be most helpful in total catastrophes, floods, earthquakes, etc., but the problem can be the stability of mobile networks in such conditions.

Summarizing the results from co-creative workshops, data security, data sharing, personal data protection, violation of privacy, and potential misuse of data were seen as a considerable concern in most of the analyzed emerging technological opportunities. There is already a lot of data and information available, but the challenge arises from the barriers between different actors to share and use the information. Sharing the information may be limited even by law so that the official responders cannot share information with non-governmental organizations (NGOs). Combining data from different sources can improve the situational awareness of authorities in crisis. However, the challenge arises from the heterogeneity, interoperability, governance, and access to such information. The governance of the data according to the needs of the owners as well as data protection, privacy, and security needs to be seriously considered when storing and sharing the data for other stakeholders. Ethical aspects should also be taken into consideration when planning data gathering, sharing, and usage as breaches in data protection could potentially make people (more) vulnerable. Distrust for the stakeholders hosting the data may prevent the adoption of new technology in use by people. It is estimated that new technological solutions are needed, e.g., for creating solutions for trusted data sharing and rules for data governance, assessing privacy impacts, and through public ethical discussion on the right balance between privacy and safety. However, such new solutions may increase risks and concerns related to the resilience of the society, and therefore non-technological tools and methods are still needed to support crisis management. These are especially needed for considering vulnerable people properly in a crisis. The digital divide between people related to the unequal distribution of skills and the access to technological means and tools remains an essential future challenge, especially with vulnerable people in a crisis. Older people, children, homeless people, and people with limited economic resources can be considered vulnerable people. There are (marginalized) people that at this point in history have a higher (or very high) risk of becoming vulnerable in crisis due to inequalities, not being considered or supported, etc. Issues of fairness and inclusivity need great attention in the application of these technologies in crises or disasters in order not to oversee such vulnerable people. It is very essential that these issues are considered and included in the monitoring radar of the emergency planners and responders. Furthermore, disruptions in vital infrastructures, such as electricity cutoff during storms (recent years in Estonia, Sweden) or the damage of communication infrastructure (telecommunication masts) due to wildfires (Portugal, Sweden), indicates the fragility of the technological tools in a hazard situation. The failure of the tools may retain dependent services and service users at risk or exacerbate the existing vulnerabilities, and the functionality of the surrounding technological structures has an impact on vulnerability in crises. However, the potential of the discussed technical opportunities for improving operation in different disaster life-cycle phases is so essential that significant investment in research and development actions is recommended.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The raw data collected and used during the research can be discussed separately with the authors.

Acknowledgments

The authors would like to thank their BuildERS colleagues for fruitful collaborations during the project. This paper has benefited from funding provided by the European Union's Horizon 2020 Research and Innovation Program under grant agreement No. 833496 (BuildERS).

References

[1] C. Morsut, et al., BuildERS D1.2 Final Report of the Unified Theoretical Framework on the Concepts of Risk Awareness, Social Capital, Vulnerability, Resilience and Their Interdependencies, 2020.
[2] C. Morsut, C. Kuran, B.I. Kruke, K. Orru, S. Hansson, Linking resilience, vulnerability, social capital and risk awareness for crisis and disaster research, J. Contingencies Crisis Manag. (2021) 1–11, https://doi.org/10.1111/1468-5973.12375.
[3] UNISDR (United Nations International Strategy for Disaster Reduction), Sendai Framework for Disaster Risk Reduction 2015-203, UNISDR, Geneva, 2015.
[4] T.K. Roy, S. Siddika, M.A. Sresto, Assessment of urban resiliency concerning disaster risk: a review on multi-dimensional approaches, J. Eng. Sci. 12 (3) (2021) 111–125, https://doi.org/10.3329/jes.v12i3.57484.
[5] S. Moradi, V. Vasandani, A. Nejat, A review of resilience variables in the context of disasters, J. Emergency Manag. 17 (5) (2019) 403–432.

[6] H. Tariq, C. Pathirage, T. Fernando, Measuring community disaster resilience at local levels: an adaptable resilience framework, Int. J. Disaster Risk Reduc. 62 (2021), 102358, https://doi.org/10.1016/j.ijdrr.2021.102358.
[7] S. Khalili, M. Harre, P. Morley, A temporal framework of social resilience indicators of communities to flood, case studies: Wagga wagga and Kempsey, NSW, Australia, Int. J. Disaster Risk Reduc. 13 (2015) 248–254, https://doi.org/10.1016/j.ijdrr.2015.06.009.
[8] A.H. Kwok, E.E.H. Doyle, J. Becker, D. Johnston, D. Paton, What is 'social resilience'? Perspectives of disaster researchers, emergency management practitioners, and policymakers in New Zealand, Int. J. Disaster Risk Reduc. 19 (2016) 197–211, https://doi.org/10.1016/j.ijdrr.2016.08.013.
[9] A.M.A. Saja, M. Teo, A. Goonetilleke, A.M. Ziyath, An inclusive and adaptive framework for measuring social resilience to disasters, Int. J. Disaster Risk Reduc. 28 (2018) 862–873, https://doi.org/10.1016/j.ijdrr.2018.02.004.
[10] J. Latvakoski, A. Bäck, E. Parmes, R. Öörni, Ö. Ceylan, A. Tominga, K. Orru, E. Siim, M. Klaos, A. Galvagni, A. Schieffelers, M. Myllylä, P. Jukarainen, M. A. Berawi, M. Max, BuildERS D2.4 Catalogue of Tools, Technologies and Media Opportunities for Disaster Management, BuildERS project, 2020.
[11] P. Jukarainen, M. Myllylä, C. Kattelus, R. Mäkelä, S.-T. Ames, J. Argillander, A. Bäck, T. Lusikka, Managing Chemical Spill Emergency and Mis-/disinformation through Simulated Responses, BuildERS project, 2021.
[12] Minges M., Disruptive Technologies and Their Use in Disaster Risk Reduction and Management 2019. ITUGET 2019 background document. 60p..
[13] D. INFSO, Networked Enterprise & RFID INFSO G. 2 Micro & Nanosystems, in Co-operation with the Working Group RFID of the ETP EPOSS, Internet of Things in 2020, Roadmap for the Future[R], Information Society and Media, Tech. Rep, 2008.
[14] M. Poblet, E. García-Cuesta, P. Casanovas, Crowdsourcing roles, methods and tools for data-intensive disaster management, Inf. Syst. Front 20 (6) (2018) 1363–1379, https://doi.org/10.1007/s10796-017-9734-6.
[15] J. Qadir, A. Ali, R. ur Rasool, A. Zwitter, A. Sathiaseelan, J. Crowcroft, Crisis analytics: big data-driven crisis response, J. Int. Humanitarian Action 1 (1) (2016) 12, https://doi.org/10.1186/s41018-016-0013-9. Available online. (Accessed 5 May 2020). accessed.
[16] Astilleros P. 5G Technology in Emergency Services. Version 1.0. 19.09.2019. EENA European Emergency Number Association. 22p.
[17] J. Rohr, Blockchain for Disaster Relief: Creating Trust where it Matters Most, 14 November, SAP News, 2017. Available online, https://news.sap.com/2017/11/blockchain-disaster-relief. (Accessed 5 May 2020). accessed.
[18] J. Latvakoski, M.B. Alaya, H. Ganem, B. Jubeh, A. Iivari, J. Leguay, J.M. Bosch, N. Granqvist, Towards horizontal architecture for autonomic M2M service networks, Future Internet 6 (2014) 261–301. http://www.mdpi.com/journal/futureinternet.
[19] Smart Mature Resilience, CORDIS EU research results, 2022. https://cordis.europa.eu/project/id/653569. (Accessed 16 March 2022). accessed.
[20] DARWIN, Project Deliverables, 2022. https://h2020darwin.eu/wp-content/uploads/2017/12/DARWIN_D3.3_ResilienceManagementGuidelinesToolkit_v1.0.pdf. (Accessed 16 March 2022). accessed.
[21] EDUCEN, CORDIS EU Research Results, 2022. https://cordis.europa.eu/project/id/653874. (Accessed 16 March 2022). accessed.
[22] Preparedness and Crisis Management Exercises, Insta website, 2022. https://www.insta.fi/en/services/national-security/exercise-activities. (Accessed 16 March 2022). accessed.
[23] SMARTeST, CORDIS EU Research Results, 2022. https://cordis.europa.eu/docs/results/244/244102/final1-final-report-section-4-1.pdf. (Accessed 16 March 2022). accessed.
[24] ANYWHERE, Catalogue Products, 2022. http://anywhere-h2020.eu/our-vision/catalogue-products. (Accessed 16 March 2022). accessed.
[25] EPOS Implementation Phase, CORDIS EU Research Results, 2022. https://cordis.europa.eu/project/id/676564/results. (Accessed 16 March 2022). accessed.
[26] I.- REACT, CORDIS EU Research Results, 2022. https://cordis.europa.eu/project/id/700256. (Accessed 16 March 2022). accessed.
[27] ResiStand, CORDIS EU Research Results, 2022. https://cordis.europa.eu/project/id/700389. (Accessed 16 March 2022). accessed.
[28] M2MGrids, Project Overview, 2022. https://itea4.org/project/m2mgrids.html. (Accessed 16 March 2022). accessed.
[29] BRIDGE, CORDIS EU Research Results, 2022. https://cordis.europa.eu/project/id/261817. (Accessed 16 March 2022). accessed.
[30] RESISTO, CORDIS EU research results, https://cordis.europa.eu/project/id/786409, (accessed 16 march 2022).
[31] Humanitarian OpenStreetMap Team, 2022. https://www.hotosm.org/. (Accessed 16 March 2022). accessed.
[32] HEIMDALL, Project Website, 2022. http://heimdall-h2020.eu/public-deliverables/. (Accessed 16 March 2022). accessed.
[33] IN-PREP, CORDIS EU research results, https://cordis.europa.eu/project/id/740627, (accessed 16 march 2022).
[34] Preparedness and Crisis Management Exercises, Insta website, 2022. https://www.insta.fi/en/services/national-security/exercise-activities. (Accessed 16 March 2022). accessed.
[35] PRACTICE, CORDIS EU Research Results, 2022. https://cordis.europa.eu/project/id/261728. (Accessed 16 March 2022). accessed.
[36] RESISTO, CORDIS EU Research Results, 2022. https://cordis.europa.eu/project/id/786409. (Accessed 16 March 2022). accessed.
[37] Cobra, CORDIS EU Research Results, 2022. https://cordis.europa.eu/project/id/875568. (Accessed 22 March 2022). accessed.
[38] NEXES, CORDIS EU Research Results, 2022. https://cordis.europa.eu/project/id/653337. (Accessed 16 March 2022). accessed.
[39] Mobility and Transform, European Commission, 2022, https://doi.org/10.1109/MCOM.2017.1600289CM. https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en, see also. (Accessed 16 March 2022). accessed.
[40] Blue Aware Tool, 2022. https://www.insta.fi/palvelut/johtaminen-ja-tilannetietoisuus/insta-blue-aware. (Accessed 23 March 2022). accessed.
[41] E.-J. Võik, A. Tominga, M. Klaos, S. Silm, K. Orru, T. Lusikka, BUILDERS D4.3 Practice & Product Innovation "Applying Mobile Positioning Data for More Precise Rescue Planning and Emergency Management under Cyber-Hazard in Estonia, BuildERS project, 2021.
[42] E.-J. Voik, M. Sari, A.V. Salim, M.A. Berawi, BuildERS D4.7 Indonesian Case: Using Mobile Operators' Data to Locate, Protect, and Evacuate Tourists and Other Vulnerable Groups in Disasters, 2021.
[43] D.J. Sheskin, Handbook of Parametric and Nonparametric Statistical Procedures, CRCPress, Boca Raton, Florida, United States, 2011, ISBN 978-1-4398-5801-1.
[44] B.-J. Koops, The concept of function creep, Law, Innovat. Technol. 13 (1) (2021) 29–56.
[45] M.V. Zetterholm, Y. Lin, P. Jokela, Digital contact tracing applications during COVID-19: a scoping review about public acceptance, Informatics 8 (3) (2021) 1–24.
[46] United Nations, Urgent Action Needed over Artificial Intelligence Risks to Human Rights, 2021. Available online, https://news.un.org/en/story/2021/09/1099972.
[47] J. Timmermans, B. Stahl, V. Ikonen, E. Bozdag, The ethics of cloud computing: a conceptual review, in: Proceedings - 2nd IEEE International Conference on Cloud Computing Technology and Science, CloudCom 2010, 2010, pp. 614–620, https://doi.org/10.1109/CloudCom.2010.59.
[48] M.A. Berawi, P. Leviäkangas, S.A.O. Siahaan, A. Hafidza, M. Sari, P. Miraj, R. Harwahyu, G. Saroji, Increasing disaster victim survival rate: SaveMyLife mobile application development, Int. J. Disaster Risk Reduc. 60 (2021), 102290, https://doi.org/10.1016/j.ijdrr.2021.102290.
[49] K. Orru, S. Hansson, F. Gabel, P. Tammpuu, M. Krüger, L. Savadori, S.F. Meyer, S. Torpan, P. Jukarainen, A. Schieffelers, G. Lovasz, M. Rhinard, Approaches to "Vulnerability" in Eight European Disaster Management Systems, Disasters, 2021, https://doi.org/10.1111/disa.12481 accepted article.
[50] K. Meechang, N. Leelawat, J. Tang, A. Kodaka, C. Chintanapakdee, The acceptance of using information technology for disaster risk management: a systematic review, Eng. J. 24 (2020), https://doi.org/10.4186/ej.2020.24.4.111. Issue 4.
[51] A. Bäck, et al., BuildERS D6.4 End-User Assessment of the New Tools and Technologies for Disaster Management, 2021.
[52] A. Khan, S. Gupta, S.K. Gupta, Multi-hazard disaster studies: monitoring, detection, recovery, and management, based on emerging technologies and optimal techniques, Int. J. Disaster Risk Reduc. 47 (2020), 101642, https://doi.org/10.1016/j.ijdrr.2020.101642. ISSN 2212-4209.
[53] A. Khan, S. Gupta, S.K. Gupta, Unmanned aerial vehicle-enabled layered architecture based solution for disaster management, Trans. Emerg. Telecommun. Technol. 32 (Dec 2021), https://doi.org/10.1002/ett.4370. Issue, 12.
[54] A. Khan, S. Gupta, S.K. Gupta, Emerging UAV technology for disaster detection, mitigation, response and preparedness, J. Field Robot. (14th Apr 2022), https://doi.org/10.1002/rob.22075. Available online (accessed 7th Jun 2022).

[55] A. Rashid, D. Sharma, T.A. Lone, S. Gupta, S.K. Gupta, Secure communication in UAV assisted HetNets: a proposed model, in: G. Wang, J. Feng, M. Bhuiyan, R. Lu (Eds.), Security, Privacy, and Anonymity in Computation, Communication, and Storage. SpaCCS 2019. Lecture Notes in Computer Science, 11611, Springer, Cham, 2019, https://doi.org/10.1007/978-3-030-24907-6_32.

[56] D. Sharma, S.K. Gupta, A. Rashid, S. Gupta, M. Rashid, A. Srivastava, A novel approach for securing data against intrusion attacks in unmanned aerial vehicles integrated heterogeneous network usiung functional encryption technique, Trans. Emerg. Telecommun. Technol. 32 (7) (1 sep 2020), https://doi.org/10.1002/ett.4114.

[57] A. Gupta, S.K. Gupta, M. Rashid, A. Khan, M. Manjul, Unmanned aerial vehicles integrated HetNet for smart dense urban area, Trans. Emerg. Telecommun. Technol. (17 Sep 2020), https://doi.org/10.1002/ett.4123.