Table 5. Test Results of the Security and Privacy of the Information Sharing Tools

	Security				Privacy				Non-repudiation
TOOLS	**Secure communication**	**Password requirements**	**2-factor authentication**	**Available at time of testing**	**Privacy policy statement**	**Configurable privacy**	**Privacy as default**	**Asking unneeded personal info**	**Modify/delete after reporting**
Social Media									
Twitter	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes (delete)
Facebook	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes (marked)
Google+	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
YouTube	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes (delete)
Wiki-based Tools									
Wiki for professionals	No	No[1)]	No	Yes	No[2)]	No	No	No	Yes (log)
Emergency 2.0 Wiki	?[3)]	?	?	Yes	Yes[4)]	?	?	?	?
Mobile App									
FEMA App	?[5)]	No	No	No[6)]	Yes	No	Yes	No	No (moderated)
Emergency+	N/A[7)]	N/A	N/A	No[8)]	No	No	No	N/A	No
Community Mapping									
Ushahidi deployments[9,10)]	Optional[11)]	N/A	N/A	Yes[12)]	Yes[13)]	Yes[14)]	Yes	Optional[15)]	No
Google Crisis Response	Yes	Yes	Yes	No[16)]	Yes[17)]	No	No	No	Yes
Facebook safety check	Yes	Yes	Yes	No[18)]	Yes	Yes	No	Yes	N/A
Instant Messaging									
Skype	Yes[19)]	Yes	No	Yes	Yes	Yes	No	Yes	Yes (marked)

Table notes: 1) Allows e.g. "123" which is a very weak password.; 2) Link present, but no text.; 3) Test user activation pending; 4) Activated LinkedIn group membership; 4) Via Terms of Use; 5) No information if photo upload is secure; 6) No personal identifiable information (PII) sent; 6) Only available in USA.; 7) Only for making phone calls; 8) Only available in Australia; 9) https://beinglgbtinasia.crowdmap.com;10)Deployment in Sweden http://www.diskrimineringskartan.se; 11) Depends on deployment. No PII sent by default.; 12) Deployed when needed; 13) Depends on deployment; 14) For deployment managers, not for end-users; 15) Anonymous allowed; 16) Deployed as needed; 17) Basic warning info only. 18) Activated when/where needed; 19) Call from skype to phone is not encrypted across the phone network.

an account, as opposed to most of the other tools. Google crisis response consists of several tools, we have chosen to evaluate the person finder. As no fully operational person finder was available at time of testing, we base our results on a test setup. In the same way, Facebook safety check is only made available in particular large-scale emergencies, and only for people in the affected regions, so it is not possible to test. Therefore, these results are based on information gathered from documentation and other relevant sources

5. DISCUSSION, SOLUTIONS, AND IMPLICATION FOR RESILIENCE

In this section, we will answer RQ3: In what way can security and privacy concerns strengthen or weaken the disaster resilience? We analyse the willingness of different groups (whistle-blowers, social

media users and active helpers) to share information during a crisis based on each group's preference on required security and privacy strength. A city is used as exemplary case in our analysis. Our discussion will focus on three points: 1) Situations that will strengthen or weaken the resilience, based on user group perspectives; 2) The predicted preferable tools of each group; and 3) The information flow model based on the tested tools linked to the predicted need for security and privacy, and user group categories that are suited for each information flow model.

Table 6 depicts the proposed framework to analyse the willingness to share information given different privacy and security strength in the engagement tools. The rows represent the user groups. The columns capture the strength categories of security and privacy embedded in the sharing tools i.e. "No privacy/ security", "Average privacy/ security" and "Strong privacy/ security/ anonymity". *The light grey* area on the right side represents the optimal smooth information flow to the city stakeholders, when the preferable privacy of users matches the provided information sharing tools. The dark grey colour area in the middle, shows the information flow to the city when the security and privacy level of the tools is average. While the black area in the left side is a situation where only people who do not bother so much about privacy, motivated by altruistic spirit and would just help facilitating the communications. In this situation, we may lose the potential information from two other groups, i.e. Whistle-blowers and social media users.

Table 6 implies that active citizen engagement for sharing disaster related information only occur if the stakeholders can provide tools that incorporate different groups' requirement for security and privacy. The grey area in Table 6 represents the information flow from different user groups that may be weakened or blocked.

Strong privacy could also include anonymity, which will encourage Whistle-Blowers, since they can submit reports without risk of repercussions. If we consider our analysis in Section 4, the Whistle Blower will tend to use e.g. Ushahidi-type tools where reporters can provide information without being identified or required to login. However, Ushahidi, of course, is very much dependent upon the preference and deployment configuration of the system owners if they would like to encourage submission of information from Whistle-Blowers or only from Active Helpers.

Why do we care about Whistle-Blowers in this information sharing context? Because Whistle-Blowers who want their privacy to be particularly protected, could be the group that possess unique and important information that may require rapid handling and mitigation. Therefore, they have a clear reason and need to be protected as informants. Wikileaks is an extreme example of framework that fits the Whistle-Blowers, where people feel secure to share information anonymously without fear of being identified as a reporter, apart from the controversy surrounding this case. In the disaster case, the example could be any extreme hazards such as industrial disaster hazards e.g. chemical leaks, radiation leaks to the water system or other critical infrastructure services that is vital for the city life and the citizens. In such case, the most knowledgeable person knowing the detail of the case may be reluctant to openly share the information because of many different reasons such as loss of reputation, job or even being taken to court for leaking confidential information.

The Active Helpers may not care about strong or weak security because the motivation is to help, share information and contribute as much as possible to mitigate the disaster impact. Thus, too much

Table 6. Willingness to share information

Users	Tools		
	No privacy/ security	Average privacy/ security	Strong privacy/ security/ anonymity
Whistle-blower			X
Social media users		X	X
Active helpers	X	X	X?

security may just hinder or slow them down to actively share information, which eventually may weaken the resilience. Thus, the X sign with a question mark in the right bottom corner in the Table 5 represents the double-edged sword issue that may arise, when the extra effort to ensure security becomes too much, while this group could in fact be the most active one.

By having a good framework for understanding the willingness to share in the different groups of users as shown in Table 6, we can then predict the preferred tools for each type of user group. The whistle blower prefers tools allowing anonymous submission or sharing. Social media users prefer Facebook, Twitter, YouTube or other channels. While active helpers will use social media, mobile apps, sharing tools (any available tools), but preferably simple tools. Note that this preferred tool example does not necessarily indicate that it should be exactly this one in reality. The security and privacy features are what matters in the indicated choices of our example. Figure 1 proposes five information flow models that link the user groups with predicted security requirements.

In Model 1, the information flows via sharing tool from citizen to citizen (C to C) is moderated. The intended communication of this type of users is to provide an alert about threats or dangers that if not reported, would have been unknown to other citizens. This type of information needs moderation for quality and truth validation. The tool needs to be supported by strong security and privacy. This model is likely to fit whistle-blowers.

Model 2 is unmoderated C to C information flow which typically intended for informing the circle of friends and family. The social media users belong to this second model, who are likely to be satisfied with medium security/privacy requirements. In this case, moderation is unnecessary.

Model 3 is moderated information flow from Special group to special group (SG to SG). The aim of the communication in this model is to voluntarily gather necessary disaster-related information as quickly as possible and share it to other voluntary groups. The ultimate goal is to help people affected by crisis with extra useful information. To a certain degree, it may help disaster responders. Moderation in this communication model is necessary. Predicted users are "active helper" groups, who can work with minimum security or privacy.

Model 4 is the moderated information flow from citizen to city (CSG to City). The intended communication of this type of users is twofold. For SG is to inform about the resources available, critical situations that need to be tackled, or other issues that are thought necessary for the stakeholders in crisis. For **C**, the communication goal is the same as Model 1, i.e. to give an alert. The information flow in this Model 4 does not need to be known by all people. The expectation is quick actions taken based on shared information. The active helpers and whistle-blowers belong to this fourth model. Thus, flexible security and privacy are highly important. In this case, moderation is necessary.

Figure 1. Information flow model, privacy-security requirement

No	Information flow model	Predicted Privacy/ Security Requirement	User Group
1	Citizen → Moderator → Citizen	Anonymity or strong security and privacy	Whistle Blower
2	Citizen → No Moderator → Citizen	Medium to strong security and privacy	Social media users
3	Special Group → Moderator → Special Group	Minimum is enough	Active helper
4	Citizen-Special Group → Moderator → City	Anonymity or strong security and privacy	Whistle Blower
		Minimum is enough	Active helper
5	Citizen → No Moderator → City	Minimum is enough	Active helper

Model 5 is unmoderated Citizen to City information flow. The intended communication is to notify stakeholders their availability or their volunteer efforts in responding to disasters. This type of communication does not need moderation.

6. CONCLUSION

In this article, we have proposed security and privacy metrics, and intuitive-based user group classifications with respect to the information and communication engagement tools. We conclude that the requirement for privacy and/or anonymity depends on the intended communication target, and this varies between the different user groups, and on the potential risk associated with a breach of privacy. The insights from the discussion in this paper is that we should mitigate reluctances of the whistle-blower to use any types of community engagement and information sharing. For a whistle-blower that sometimes carry urgent information, the risk is very high that he will be in major trouble if his privacy is violated. We also should not slow down the active helpers by making the tool too complex - e.g. through excessive security, although for an active helper, that risk is more like a minor annoyance. Both these groups usually want to spread the information as wide as needed to reach the proper authorities. On the other hand, social media users tend to target friends and family and may for example either want to tell that they are safe, or inform about local risks. This information may still be of use to the crisis handlers if it is available to the public, but reasonable privacy settings may also prevent this to happen.

Thus, the policy makers or local authority in the city should be willing to consider all relevant types of user groups in the society based on their preferred privacy and security requirements, and allow different user groups to participate through different tools, including representative tools from those classes of tools mentioned in Table 6. Leaving out whistle-blowers or slowing down and annoying active helpers would impair citizen engagement and ultimately resilience. To be able to get a complete picture from information shared by citizens, we suggest that both a specialised tool with simple verified-user messages as well as opening for moderated anonymous messages - and relevant social networks, should be utilized.

Finally, we also need to cover some limitations of our work: 1) We assume that evaluators of the security and privacy level of the engagement tools have a limited expertise on security but should know the minimum requirements to determine whether or not such criteria are fulfilled or covered. 2) The methods for evaluating security and privacy of the engagement tools are not from the insider perspective but from what information has been made available for public or is externally observable. 3) The suggested metrics are only an initial proposal. The security and privacy metrics that are relevant for city stakeholders can be elaborated further in different stages of the resilience cycle: preparedness, response, recovery and mitigation. Likewise, the matrix for the user groups can be elaborated further to include e.g. engagement tools for helping individuals that are affected by the disasters, where the security and privacy will be extremely important. For example, the engagement tools will include counselling for trauma, shocks or other psychological or psychosocial problems, or other issues that are not identified here. 4) To be aware that the strong privacy or anonymity that allows whistle-blowers to feel comfortable enough to submit their information, can also be used for actors with bad intentions, for misleading of even attempting to trap rescue personnel, or for submitting bomb threats and other criminal messages. 5) Our experiment, especially the evaluation of the availability metric is based on limited observation time, and not e.g. through monitoring over longer period, where then we could claim e.g. “uptime of 99%”.

There are many directions that could be investigated further based on this study, but it should still be able to stand on its own as a set of guidelines for the security and privacy aspects of selecting tools for engaging citizens in creating a resilient society.

REFERENCES

Aedo, I., Díaz, P., Carroll, J. M., Convertino, G., & Rosson, M. B. (2010). End-user oriented strategies to facilitate multi-organizational adoption of emergency management information systems. *Information Processing & Management*, *46*(1), 11–21. doi:10.1016/j.ipm.2009.07.002

Aldunce, P., Beilin, R., Handmer, J., & Howden, M. (2014). Framing disaster resilience: The implications of the diverse conceptualisations of "bouncing back". *Disaster Prevention and Management: An International Journal, 23*(3), 252-270. doi:10.1108/DPM-07-2013-0130

Assel, M., Wesner, S., & Kipp, A. (2009). A security framework for dynamic collaborative working environments. *Identity in the Information Society*, *2*(2), 171–187. doi:10.1007/s12394-009-0027-1

Avižienis, A., Laprie, J.-C., Randell, B., & Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, *1*(1), 11–33. doi:10.1109/TDSC.2004.2

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information system. *Management Information Systems Quarterly*, *35*(4), 1017–A1036. doi:10.2307/41409971

Bhamra, R., Dani, S., & Burnard, K. (2011). Resilience: The concept, a literature review and future directions. *International Journal of Production Research*, *49*(18), 5375–5393. doi:10.1080/00207543.2011.563826

Bharosa, N., Janssen, M., & Tan, Y.-H. (2011). A research agenda for information quality assurance in public safety networks: Information orchestration as the middle ground between hierarchical and netcentric approaches. *Cognition Technology and Work*, *13*(3), 203–216. doi:10.1007/s10111-011-0172-9

Bharosa, N., Lee, J., & Janssen, M. (2010). Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: Propositions from field exercises. *Information Systems Frontiers*, *12*(1), 49–65. doi:10.1007/s10796-009-9174-z

Birkland, T. A. (2009). Disasters, catastrophes, and policy failure in the homeland security era1. *The Review of Policy Research*, *26*(4), 423–438. doi:10.1111/j.1541-1338.2009.00393.x

Camenisch, J., Groß, T., & Heydt-Benjamin, T. S. (2009). Accountable privacy supporting services. *Identity in the Information Society*, *2*(3), 241–267. doi:10.1007/s12394-009-0023-5

Carpenter, S., Walker, B., Anderies, J. M., & Abel, N. (2001). From metaphor to measurement: Resilience of what to what? *Ecosystems*, *4*(8), 765–781. doi:10.1007/s10021-001-0045-9

Cavoukian, A. (2006). Privacy by design: The 7 foundational principles. Implementation and mapping of fair information practices. *Privacy Association*. Retrieved from https://www.privacyassociation.org/media/presentations/11Summit/RealitiesHO1.pdf

Cavoukian, A., Taylor, S., & Abrams, M. (2010). Privacy by design: Essential for organizational accountability and strong business practices. *Identity in the Information Society, 3*(2), 405-413. doi:10.1007/s12394-010-0053-z

Cha, J. (2014). Usage of video sharing websites: Drivers and barriers. *Telematics and Informatics*, *31*(1), 16–26. doi:10.1016/j.tele.2012.01.003

Chik, W. B. (2013). The Singapore personal data protection act and an assessment of future trends in data privacy reform. *Computer Law & Security Review*, *29*(5), 554–575. doi:10.1016/j.clsr.2013.07.010

Coles, E., & Buckle, P. (2004). Developing community resilience as a foundation for effective disaster recovery. *Australian Journal of Emergency Management*, *19*(4), 6.

Cottrill, C. D., & "Vonu" Thakuriah, P. (2015). Location privacy preferences: A survey-based analysis of consumer awareness, trade-off and decision-making. *Transportation Research Part C, Emerging Technologies*, *56*, 132–148. doi:10.1016/j.trc.2015.04.005

CrisisCommunication.fi. (2014). Crisis communication wiki for professionals. Retrieved from http://www.crisiscommunication.fi/wiki/Main_Page

DFID. (2011). *Defining disaster resilience: A dfid approach paper. Department of international development*. Retrieved from http://www.fsnnetwork.org/sites/default/files/dfid_defining_disaster_resilience.pdf

Dufty, N. (2012). Using social media to build community disaster resilience. *Australian Journal of Emergency Management*, *27*(1), 40.

Emergency2.0 Wiki Editors. (2011). Emergency 2.0 wiki. Retrieved from http://emergency20wiki.org/wiki/index.php/Main_Page

FEMA. (2017). Fema mobile app. Retrieved from https://www.fema.gov/mobile-app

Fernandez, E. B. (2004). A methodology for secure software design. *Paper presented at the Conference on Software Engineering Research and Practice (SERP'04)*, Las Vegas, NV.

Galiero, G., & Giammatteo, G. (2009). Trusting third-party storage providers for holding personal information. A context-based approach to protect identity-related data in untrusted domains. *Identity in the Information Society*, *2*(2), 99–114. doi:10.1007/s12394-009-0033-3

Gil-Garcia, J. R., Zhang, J., & Puron-Cid, G. (2016). Conceptualizing smartness in government: An integrative and multi-dimensional view. *Government Information Quarterly*, *33*(3), 524–534. doi:10.1016/j.giq.2016.03.002

Google. (2018). Google person finder. Retrieved from https://google.org/personfinder

Haworth, B. (2016). Emergency management perspectives on volunteered geographic information: Opportunities, challenges and change. *Computers, Environment and Urban Systems*, *57*, 189–198. doi:10.1016/j.compenvurbsys.2016.02.009

Hildebrandt, M. (2013). Balance or trade-off? Online security technologies and fundamental rights. *Philosophy & Technology*, *26*(4), 357–379. doi:10.1007/s13347-013-0104-0

Hong, J. I., & Landay, J. A. (2004). An architecture for privacy-sensitive ubiquitous computing. *Paper presented at the 2nd international conference on Mobile systems, applications, and services*.

Hull, G., Lipford, H. R., & Latulipe, C. (2011). Contextual gaps: Privacy issues on Facebook. *Ethics and Information Technology*, *13*(4), 289–302. doi:10.1007/s10676-010-9224-8

Jackson, S. (2013). Resilience principles for the ICT sector. *Critical Information Infrastructure Protection and Resilience in the ICT Sector*, 36.

Lederer, S., Hong, J. I., Dey, A. K., & Landay, J. A. (2004). Personal privacy through understanding and action: Five pitfalls for designers. *Personal and Ubiquitous Computing*, *8*(6), 440–454. doi:10.1007/s00779-004-0304-9

Lee, J., Bharosa, N., Yang, J., Janssen, M., & Rao, H. R. (2011). Group value and intention to use — a study of multi-agency disaster management information systems for public safety. *Decision Support Systems*, *50*(2), 404–414. doi:10.1016/j.dss.2010.10.002

Lindsay, B. R. (2011). *Social media and disasters: Current uses, future options, and policy considerations*. Retrieved from https://www.nisconsortium.org/portal/resources/bin/Social_Media_and_Dis_1423591240.pdf

Liu, P., & Chetal, A. (2005). Trust-based secure information sharing between federal government agencies. *Journal of the American Society for Information Science and Technology, 56*(3), 283-298. doi:10.1002/asi.20117

Liu, S. B. (2014). Crisis crowdsourcing framework: Designing strategic configurations of crowdsourcing for the emergency management domain. *Comput. Supported Coop. Work, 23*(4-6), 389-443. doi:10.1007/s10606-014-9204-3

Liza, P. (2011). Sociotechnical uses of social web tools during disasters. In C. Elayne (Ed.), *Knowledge development and social change through technology: Emerging studies* (pp. 97–108). Hershey, PA: IGI Global.

Manyena, S. B. (2006). The concept of resilience revisited. *Disasters, 30*(4), 434-450. doi:10.1111/j.0361-3666.2006.00331.x

Martin, R. (2012). Earthquake buddy app sends your location to friends when an earthquake hits. *Techinasia*. Retrieved from https://www.techinasia.com/earthquake-buddy-alert-location

Norris, F. H., Stevens, S. P., Pfefferbaum, B., Wyche, K. F., & Pfefferbaum, R. L. (2008). Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness. *American Journal of Community Psychology, 41*(1-2), 127-150. doi:10.1007/s10464-007-9156-6

NSW. (2018). Nsw rural fire service. Retrieved from http://www.rfs.nsw.gov.au/about-us/our-districts/mia/fire-information/fires-near-me

Oh, O., Agrawal, M., & Rao, H. R. (2013). Community intelligence and social media services: A rumor theoretic analysis of tweets during social crises. *MIS Quarterly: Management Information Systems*, *37*(2), 407–426. doi:10.25300/MISQ/2013/37.2.05

Palen, L., Anderson, K. M., Mark, G., Martin, J., Sicker, D., Palmer, M., & Grunwald, D. (2010). A vision for technology-mediated support for public participation & assistance in mass emergencies & disasters. *Paper presented at the 2010 ACM-BCS visions of computer science conference*.

Parrish, J. L. (2010). Papa knows best: Principles for the ethical sharing of information on social networking sites. *Ethics and Information Technology*, *12*(2), 187–193. doi:10.1007/s10676-010-9219-5

PDC. (2018). Disaster alert. Retrieved from http://www.pdc.org/solutions/tools/disaster-alert-app/

Pekárek, M., & Pötzsch, S. (2009). A comparison of privacy issues in collaborative workspaces and social networks. *Identity in the Information Society*, *2*(1), 81–93. doi:10.1007/s12394-009-0016-4

PEP. (2016). Public empowerment policies for crisis management. Retrieved from https://agoracenter.jyu.fi/projects/pep

Pfleeger, S. L. (2012). Security measurement steps, missteps, and next steps. *IEEE Security and Privacy, 10*(4), 5-9. doi:10.1109/MSP.2012.106

Pipek, V., Liu, S. B., & Kerne, A. (2014). Crisis informatics and collaboration: A brief introduction. *Comput. Supported Coop. Work, 23*(4-6), 339-345. doi:10.1007/s10606-014-9211-4

Plough, A., Fielding, J. E., Chandra, A., Williams, M., Eisenman, D., Wells, K. B., . . . Magaña, A. (2013). Building community disaster resilience: Perspectives from a large urban county department of public health. *American Journal of Public Health, 103*(7), 1190-1197. doi:10.2105/AJPH.2013.301268

Quakewatch. (2018). Earthquake prediction center. Retrieved from http://quakewatch.net

Rogers, P. (2013). Rethinking resilience: Articulating community and the UK riots. *Politics, 33*(4), 322-333. doi:10.1111/1467-9256.12033

Schwartz, P. M., & Solove, D. J. (2011). Pii problem: Privacy and a new concept of personally identifiable information, the. *NYUL Rev.*, *86*, 1814.

Solove, D. J. (2012). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*, 1880.

Stolfo, S., Bellovin, S. M., & Evans, D. (2011). Measuring security. *IEEE Security and Privacy*, *9*(3), 60–65. doi:10.1109/MSP.2011.56

Tapia, A. H., & Moore, K. (2014). Good enough is good enough: Overcoming disaster response organizations' slow social media data adoption. *Comput. Supported Coop. Work, 23*(4-6), 483-512. doi:10.1007/s10606-014-9206-1

Trnka, J., & Johansson, B. J. E. (2011). Resilient emergency response: Supporting flexibility and improvisation in collaborative command and control. In E. J. Murray (Ed.), *Crisis response and management and emerging information systems: Critical applications* (pp. 112–138). Hershey, PA: IGI Global. doi:10.4018/978-1-60960-609-1.ch009

Turner, M., Kitchenham, B., Brereton, P., Charters, S., & Budgen, D. (2010). Does the technology acceptance model predict actual use? A systematic literature review. *Information and Software Technology*, *52*(5), 463–479. doi:10.1016/j.infsof.2009.11.005

Twitter. (2016). Best practices for using twitter in times of crisis. Retrieved from https://about.twitter.com/products/alerts/helpful-assets

UN. (2014). World's population increasingly urban. Retrieved from http://www.un.org/en/development/desa/news/population/world-urbanization-prospects-2014.html

UNISDR. (2004). *Living with risk: A global review of disaster reduction initiatives: 2004 version - volume ii annexes*. Retrieved from http://www.unisdr.org/files/657_lwr21.pdf

UNISDR. (2005, January 18-22). Hyogo framework for action 2005-2015: Building the resilience of nations and communities to disasters. *Paper presented at the World Conference on Disaster Reduction*, Kobe, Hyogo, Japan.

Ushahidi Editors. (2018). Ushahidi. Retrieved from https://www.ushahidi.com/

Wells, K. B., Tang, J., Lizaola, E., Jones, F., Brown, A., Stayton, A., . . . Plough, A. (2013). Applying community engagement to disaster planning: Developing the vision and design for the Los Angeles County community disaster resilience initiative. *American Journal of Public Health, 103*(7), 1172-1180. doi:10.2105/AJPH.2013.301407

WikiLeaks. (2015). Wikileaks. Retrieved from http://www.wikileaks.com

Yang, T.-M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, *28*(2), 164–175. doi:10.1016/j.giq.2010.06.008

Jaziar Radianti received her PhD in System Dynamics applied for an information security area from University of Bergen, Norway. Dr. Radianti is a researcher for CIEM (Centre for Integrated Emergency Management) at Department of ICT, University of Agder, Norway. She has served as a reviewer for numerous international conferences and has published more than 60 scientific papers. Her research interests include the application of simulation approaches, especially system dynamics, fire dynamics, and Bayesian network modeling for disaster and crisis management. She has extensive research experience after completing her PhD education, as she has been working on the following research areas: cyber-security, fire emergencies, smartphone sensing, disaster resilience and serious game. Currently, Dr. Radianti is a head of CIEMlab and experimental operation centre, a situation room research infrastructure for crisis management, at the University of Agder (Since 2015 to date). She is also leading the KriseSIM project, a research on virtual training tool for a control room (2017-2019), and a senior researcher I H2020 project Smart-Mature Resilience on disaster resilience (2015-2018).

Terje Gjøsæter is an associate professor in universal design of ICT at Oslo Metropolitan University, Norway. He completed his PhD at the Department of ICT at University of Agder in 2015, in computer language theory with a focus on design principles and usability of meta-modelling tools. His research interests include such diverse topics as universal design, accessibility, security of critical infrastructure, usable security, privacy, emergency management, computer language theory and metamodelling, usability of domain-specific languages, and eHealth. He has published more than 30 peer-reviewed articles and conference papers and has experience from several EU projects. He participated in the FP6 EIAO IST project from 2004 to 2007, performing research and development related to large-scale automatic assessment of web accessibility. From 2012 to 2014, he joined the FP7 PRECYSE project, doing research related to establishing a methodology for assessing and enforcing security of critical infrastructures. From 2014 to 2016, he took part in the FP7 SEMIAH project on design and development a scalable, secure and privacy-preserving energy management infrastructure for aggregation of households in the smart grid.