Trust in Computer-Supported crisis management information sharing

Béatrice Linot

Linot Béatrice (2018): Trust in Computer-Supported crisis management information sharing. In: Proceedings of 16th European Conference on Computer-Supported Cooperative Work – Doctoral Colloquium papers, Reports of the European Society for Socially Embedded Technologies (ISSN 2510-2591), DOI: 10.18420/ecscw2018_dc07

Trust in Computer-Supported crisis management information sharing

Béatrice Linot
Psychology and Neurosciences Lab (2LPN-EA7489), Coast Team, University of Lorraine/INRIA (France)
Beatrice.linot@loria.fr; beatrice.linot@univ-lorraine.fr

Abstract. My Doctoral research aims to identify the psychological and social factors that influence trust and determine the information sharing behavior of professional participants in the crisis response system. Building on the idea that the computer disrupts these factors, our aim is to design tools that restore the conditions of trust in a framework of collaborative information sharing. I combine theory and methods used in psychology and human factors, with computer science to determine how and why trust is degraded in relation to civil security operations. I propose to (1) identify the multi-level factors influencing trust during collaborative activities supported by computers (e.g., contextual factors, organizational factors, individual factors,); and (2) identify data-based design guidelines for digital devices that promote the sharing of information related to civil security and thereby develop and maintain shared situational awareness during collaborative activities.

Related Work

France has experienced several disasters in the last decade: Floods (Var, Alpes Maritimes (2015), Seine basin & Loire (2016); Storms Lothar, Martin (1999), Klaus (2009), Xynthia (2010); Terrorist attacks, Charlie hebdo and Bataclan (2015), Nice (2016); the Germanwings crash (2015), explosion of AZF plan in Toulouse (2001). The resulting disorganization and puts a premium on communication between different specialties (e.g. Police, firefighters, medical technicians etc.). Communication between specialties is essential (Quarantelli, 1985). Lagadec (1995) and Dautun (2007) agree with this emphasis on communication, but enrich our understanding of the problem. Because crisis events are unexpected and stress local resources, they often require cooperation among team members who do not know each other and bring different technical expertise, experiences, culture, and organizations.

Groupware systems aim to provide participants with common awareness, i.e., information about the presence, activities, and availability of the other participants in the same system (Bente et al., 2008; Dunaway, Murphy, Venkatasubramanian, Palen & Lopresti, 2017; Xiu, Tredan & Datta, 2014). Yet empirical studies in several domains (e.g., e-banking, civil security, healthcare, military, industries, etc.) reveal low participant confidence in these systems. Additionally, low confidence generates inappropriate behavior (e.g., altering and degrading performance of users technology) reducing use, thereby affecting efficiency. The French tool CRISORSEC is intended to support information sharing among crisis actors. Yet, users question its utility, its form, its uses, its limits and its possible perverse effects. Laurence Créton-Cazanave (a sociologist-geographer), studied CRISORSEC difficulties in French metropolitan areas. Créton-Cazanave, reinforces the link between trust and communication (Cazanave, 2017). Rapport GéNéPi, (2015) echoes the same problems: the technical and tools issues, the communication issues and the organizational issues during crisis situation management. One of the limitations of these studies is the absence of performance data either with or without the assistance of communication tools. I suggest that understanding performance in these different situations informs design requirements.

My pilot data (including 4 visits, 4 observations and 18 interviews) revealed several issues in crisis management collaboration. In particular, several different tools complement CRISORSEC. This strongly suggests that CRISORSEC does not support communication as intended, potentially breaking the link between the source and recipient of information that is maintained in the chosen tools. Identifying (and compensating for) the cause of this drift will improve the design of next generation communication tools. Across the visits, observations and interviews) I noted incidents and malfunctions related to the notion of trust:
- To the tools due mainly to technical malfunctions (18), usability (11) and security (1).
- The data due to characteristics such as credibility and relevance (7), and recency (9).
- The person due to the skills (credibility, experience) of the person you trust (4), and the nature of the relationships, the well-being, and the previous experiences with the other (4).
Technical malfunctions and usability issues will yield to more rigorous engineering. However, the other categories suggest more subtle issues of design and functionality.

Research questions

A psychological model of communication, including trust, is key to the design of computer-supported crisis management communication tools. My research questions are:

1) Does mediation by computer for information sharing tools break the adaptive link in communication and thus reduce trust? The use of alternative communication tools such as e-mail and telephone aims potentially recreates a missing adaptive link in existing tools such as CRISORSEC. In conventional, unmediated communication, the sender shapes the message, taking into account the specific needs of recipient with respect to his tasks in a global plan. Participants trust other participants to provide important information. If observers omit detail, recipients are justified in assuming that the omitted detail is not relevant. The sender may specify schedule, data characteristics, and situation that determine the activity of the recipient. I will examine the use of alternative means of communication (phone calls, sms, secure email, etc.) despite tool availability:

- Presence, number and objectives of parallel exchanges (e.g., verification, cross-referencing, questions of relevance, recency, reliability of information, interpretation);
- The lack of use of information (Not taken into account and retention of information);
- The lack of sharing (on the sharing tool) of known information (sharing or not information, validation of information by the hierarchy);
- Development and use of a parallel tool in lieu of the common tool of sharing.

2) What is the role of context in establishing trust? During crisis response trust is a building process, depends mostly on contextual than individual and organizational factors. To support this claim, I must examine all three potential influences:
- Individual (propensity to trust, experience, domain expertise, perceived risk, task goals).
- Local context (the seriousness of the situation, the level of risk, distributed and mediated work? update and relevance data, context situation, etc).
- Organizational context (formal responsibilities, management structure, existing communication tools and practices).

Methods

The goals is to obtain performance data concerning the factors that influence the decision to accept or distribute information. I seek convergent, ideally quantifiable evidence to address the above research questions. Psychology and ergonomics provides three general methods to gather data while minimizing experimenter bias: observation, interviews/surveys and experimental tasks. The study participants staff Crisis intervention, in crisis cells triggered for a given event (e.g., from CODIS, CORGN, CRRA, prefecture, CIC, COZ and COGIC); and includes professionals such as (fire-brigade, civil security associations, staff of the SAMU, gendarmerie, police, prefecture, military, and other partners). The proposed work will be conducted in two phases: Phase 1 largely concerns realistic crisis response activities, including observation and interviews. Phase 2 concerns largely experimentally contrived tasks, which provide both quantitative and qualitative data.

Phase 1-step 1: "Crisis exercises" Observation: Observations will be conducted in simulated crisis response in the French territory. Data collection includes participant written responses, video/audio recording, photographs and/or experimenter notes. In contrast to a traditional ethnographic exercise, I seek evidence regarding the ebb and flow of trust.

Phase 1 Step 2: Self-confrontation interviews (post-observation): Purely observational data may not reveal the intentionality considerations behind the observed information sharing. The goal of follow-up interviews is to obtain explanation concerning the factors that influence the decision to accept or distribute information. *Phase 1 Step 3: Critical Incident interviews:* One of the problems with observational study is that the conclusions are dependent upon the particular sample observed. In complex domains, this sample is highly likely to be biased. The critical incident technique is designed to facilitate the study of unobserved events, incidents or processes that the subject has previously experienced as significant, to clarify how they have been managed and the resulting effects.

Phase 2 Step 1: Incident Sorting: One of the limitations of Phase 1 activity is the confounding of data with particular participants and the absence of a domain analysis that integrates the data. Card sorting allows participants to group incidents according to an abstraction hierarchy of similarity. Phase 2 will use Phase 1 data develop a systematic set of

scenarios concerning the sharing of information. Analysis identifies the terms, concepts, key words and actions inherent in the characteristics that distinguish those situations that foster trust in the sharing and exchange of data between different civil security services.

Phase 2 Step 2: Situational Judgment test (survey): My final method provides the best opportunity to obtain large scale evidence regarding a standardized set of operational conditions. A variety of Situational judgement tests concerning information sharing scenarios, informed by all of the above resources, will be distributed in the form of a questionnaire to professional civilian security on a larger scale. Of particular interest is the consistency or variability in response.

Expected contributions

- Examine the extent to which trust issues pervade current communication tools.
- Establish the main factors that build trust in the information sharing activity.
- Specify the essential contextual factors that favor conditions of trust and more particularly for the design of collaborative sharing tools.

Understanding mediated and unmediated communication will contribute design requirements for the next generation of crisis communication tools and more generally groupware systems.

References

Bente, G., Rüggenberg, S., Krämer, N. C., & Eschenburg, F. (2008) : Avatar-mediated networking: Increasing social presence and interpersonal trust in net-based collaborations. *Human Communication Research*, *34*(2), 287-318. DOI: 10.1111/j.1468-2958.2008.00322.x

Créton-Cazanave, L. (2017) : L'application *Crisorsec*, un dispositif numérique au coeur des enjeux de la gestion des crises en milieu métropolitain. *Sociologies pratiques*, 34,(1), 83-92. doi:10.3917/sopr.034.0083.

Dautun, C., (2007) : Contribution à l'étude des crises de grande ampleur : connaissance et aide à la décision pour la Sécurité Civile. Thèse pour obtenir le grade de docteur de l'Ecole Nationale Supérieure des Mines de Saint-Etienne.

Dolidon, H., Renou, T. (2015) : Granularité des niveaux de pilotage. Cahier des charges, SP1 : Cas d'utilisation, besoins et recueil de connaissance. *Agence Nationale de Recherche*.

Dunaway, M., Murphy, R., Venkatasubramanian, N., Palen, L., & Lopresti, D. (2017): Research Agenda in Intelligent Infrastructure to Enhance Disaster Management, Community Resilience and Public Safety*,* arXiv:1705.01985.

Lagadec P. (1995) : « Cellules de crise », les conditions d'une conduite efficace.

Quarantelli, E. L. (1985): Research Findings on Organizational Behavior in Disasters and implications for disaster planning. Preliminary Paper 107. Disaster Research Center (Report Series 18), University of Delaware, Newark, Delaware.

Xiu, L., Tredan, G. & Datta, A. (2014) :A Generic Trust Framework for Large-Scale Open Systems using Machine Learning". *Computational Intelligence 30*(4), 700–721.