ICT and Artificial Intelligence for Crisis and Emergency Management

Julie Dugdale
University Grenoble-Alps, CNRS
Grenoble Informatics Lab (LIG)
Julie.Dugdale@imag.fr

Elsa Negre
Paris-Dauphine University, PSL Research University, CNRS UMR 7243, LAMSADE, Paris.
elsa.negre@dauphine.fr

Murray Turoff
Information Systems Department
New Jersey Institute of Technology
murray.turoff@gmail.com

Technologies for crisis response and management have come a very long way over the years. The state of the art in crisis communications in the early to mid 1850s was the telegraph using a simple key to send Morse code. In 1906 the devastating 7.8 magnitude San Francisco earthquake destroyed 80% of the city. Communications with the outside world were cut off for 3 hours before Harry Jeffs, wire chief of the Western Union Telegraph Company, perched on a thirty-foot pole gave the US capital the first story of the disaster (SF Museum, n.d.). Telegraph, radiotelephony, and harmonic telegraphy (more commonly known to us nowadays as the telephone) then formed the backbone of modern crisis communications.

Today, a wealth of technologies is available to crisis managers and first-responders. We are living in an era where drones, sensors and robots can provide accurate information in real time about damaged buildings and landscapes, thus making rescue efforts safer and less time consuming. Augmented and virtual reality technologies are used to enhance training with more realistic environments (Sebillo et al. 2016). Serious games are used to increase awareness of roles and responsibilities all stakeholders participating in crisis management (Di Loreto et al. 2012). Computer simulation can provide decision makers with predictive tools for evacuations that realistically model human behaviours (Bangate et al. 2018)

Wearables for first responders are a huge growth area. Firefighters helmets can be equipped with gas sensors, optical and thermal cameras, indoor positioning technology, personal/local area network, and augmented reality abilities. Sensors can monitor vital signs such as temperature, heart rate and oxygen levels, as well as detect environmental pollutants and smoke. Tracking brackets can be used to pinpoint the position of responders. Decision support is becoming more advanced and situation awareness is increased due to the data from sensors and drones supported by artificial intelligence techniques, such as big data analytics and machine learning.

We are therefore moving away from our traditional notion of first responders towards a future of "digital responders". However, is this bright new future of digital crisis management realizable given the enormous challenges that we face? A sample of these challenges are listed here: Legal and regulatory issues must be addressed, for example most countries do not yet have legal frameworks for the use of UAVs meaning that their use needs to be cleared on an ad-hoc basis with local authorities. Privacy issues haunt the use of many technologies with potentially sensitive data streaming in from sensor technologies. How, and for how long, will this data be stored, and with whom will it be shared are major concerns. Many of the poorest countries in the world cannot afford to buy these new technologies, nor pay for the service of using them. New technologies also bring the burden of additional training for those who are expected to use them. Crisis management, command and control is largely governed by strict procedures and protocols; so how will these new technologies fit into existing work practices?

Martec's law tells us that technology changes exponentially, whereas organisations change logarithmically. Technology in crisis management is changing very rapidly, and those changes seem to be accelerating. Whereas changing an organization, how it thinks and behaves is still hard and slow. This was shown clearly with the use of social media in crisis situations. This technology had the power to revolutionalise information sharing and situation awareness, yet crisis managers are still struggling with the practicalities of how to incorporate this in their usual procedures and in their management structures. The reality is that technology and tools are advancing faster than the abilities of people trying to use them.

Despite the huge potential of new technologies there is still a chasm between what is possible and what is used on the ground. This gap needs to be bridged.

The notion of teamwork needs to be readdressed. It is said that a team is not a group of people who work together but a team is a group of people that trust each other (Sinek, 2012). The teams that we have now are socio-technical teams; teams where people and technology work together. For these teams to work we need trust, however trusting technology takes time. Is the black box of technology acceptable in crisis management, do we need explicable behaviours and clear explanations of the basics of how the technology works? Should we encourage practitioners to be more involved in

defining requirements and following the development of the tools in order to encourage a sense of ownership and engender trust?

We are facing a new era where the potential of new technologies for crisis management can be realized, but first we need to address the challenges that these technologies bring.

The series of papers, presented at the mini-track on AI and ICT for crisis management at HICSS 2019, explores new technological opportunities, the science behind them, and the challenges that we face.

6 papers have been selected. The first paper in the session is by Ahmed Abdeltawab Abdelgawad, Tor-Edin Farstad and Jose J. Gonzalez who look at the relatively new phenomenon of cyber-attack. Their paper is titled "Vulnerability Analysis of Independent Critical Infrastructures upon a Cyber-attack". Although the probability of such attacks could be low, their impact could be devastating. Considerable expertise and resources may be needed to perform such attacks. However, the authors argue that a smart attacker could exploit existing knowledge on cascading impacts with low resources with the result that critical infrastructures could be seriously disrupted. Based on some previous work the authors develop a systems dynamics model, which is applied to various scenarios, to show that this is possible.

The second paper, by Diana Fischer, Johannes Putzke-Hattori and Kai Fischbach concerns "Crisis Warning Apps: Investigating the Factors Influencing Usage and Compliace with Recoomendations for Action". This paper looks at people's usage intention of a warning app and the intention to comply with recommendations for action transmitted via the app. Whilst most research works in this area deal with the benefits and developments of warning apps, this paper goes further and looks at what factors affect their usage. The authors find that risk perception, trust and subjective norm positively influence both the use of a warning app and compliance intention, whereas concerns about data security have negative effects. This is an important result since it is often assumed that people will automatically want to use such apps and will follow the advice given. This paper shows that the promoters of such apps need to pay more attention to the intentions behind the use of warning apps if their uptake is to be more successful.

The third paper by Maude Arru, Elsa Negre and Camille Rosenthal-Sabroux continues the theme of warning apps. The paper "To alert or not to alert? That is the question" provides a method of data analysis that helps decision makers of crisis cells to assess whether they should alert the population or not. Like the previous paper, the work focuses on the users and analyses the population's behaviour during a crisis. The work describes a four-step decision support process, involving the use of decision trees, which will help to provide decision makers with an indication of the likely behaviour of a population in response to an alert. Armed with this information they can then decide whether to trigger an alert or not.

Artificial intelligence is behind many of the recent advances in technologies for crisis response and management. The fourth paper in the series looks at how deep learning may be applied to evacuation situations. The paper by Ricardo Buettner and Hermann Baumgarti concerns "A Highly Effective Deep Learning Based Escape Route Recognition Module for Autonomous Robots in Crisis and Emergency Situations". The underlying rationale for the work comes from merging situation awareness and socially relevant agent-based systems (Mancheva and Dugdale, 2016). The paper shows how artificial agents can precisely recognise escape signs, doors and stairs for evacuation route planning. In this case a convolutional neural network is used for image recognition in emergency situations. A particularly interesting result is high recognition accuracy, which outperforms current methods

The fifth paper by Carole Adam, Julie Dugdale and Catherine Garbay, aims to unpack the complex notion of social cohesion. The paper titled a "Multi-Factor Model and Simulation of Social Cohesion and its Effect on Evacuation" looks at how emotions, social norms, and mutual knowledge each play a role in social cohesion. Rather than just exploring this theme from a theoretical perspective the authors go further and develop an agent-based simulator to experiment with the dynamics of the three components of social cohesion. They show how cohesion may emerge and how positive emotions, with behaviours driven towards to welfare of others, have a cementing role. Conversely, unfair situations, with behaviours driven towards the obedience to shared norms, create the emergence of exclusive forms of cohesion, relying on discrimination.

The final paper is by Henry Muccini, Claudio Arbib, Paul Davidsson and Mahyar, Tourchi Moghaddam and concerns "An IOT Software Architecture for an Evacuable Building Architecture". Building evacuation is a frequent research topic in emergency management. However this work starts from a different point of view; rather than concentrating on evacuation in an existing building, we should think about the design phase of buildings. Here the idea is to build software, using a network flow model that supports building architects. In addition to its building design focus, the approach can also plan the best evacuation paths in real time for an IOT based environment (i.e. after the building has been constructed).

From this selection of papers the current concerns and advances in ICT for crisis

management are clear. New problems are being addressed (paper 1). A more human centred approach is needed if crisis-warning apps are to be used effectively and with a good response from the population (papers 2 and 3). Artificial intelligence has an important role to play in crisis technologies (paper 4). Human behaviour and in particular social cohesion plays a critical role in managing crisis situations (paper 5). Evacuation should not only be studied in currently operational buildings, but software is for architects in the design phase.

References

Bangate, J., Dugdale, J., Beck, E., & Adam, C. A Multi-agent System Approach in Evaluating Human Spatio-temporal Vulnerability to Seismic Risk using Social Attachment. In Risk Analysis XI. WIT Transactions on Engineering Sciences. WIT Press. Vol. 121, 2018. Eds. C.A. Brebbia and A. Fabbri. (In Press).

Di Loreto, I., Mora, S., & Divitini, M. (2012, June). Collaborative serious games for crisis management: an overview. In *Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), 2012 IEEE 21st International Workshop on* (pp. 352-357). IEEE.

Mancheva, L., & Dugdale, J. (2016, January). Understanding communications in medical emergency situations. In *System Sciences (HICSS), 2016 49th Hawaii International Conference on* (pp. 198-206). IEEE.

Sebillo, M., Vitiello, G., Paolino, L., & Ginige, A. (2016). Training emergency responders through augmented reality mobile interfaces. *Multimedia Tools and Applications*, *75*(16), 9609-9622.

Sinek, Simon (2012). http://businesscentral.net/7-simon-sinek-quotes-that-will-change-your-thinking-on-leadership-and-business. Retrieved 12th October 2018.

SF Museum, n.d. Telegraph Office Perched on Pole. How the Western Union built a New Plant in Four Days. San Francisco Chronicle. April 30, 1906. http://www.sfmuseum.org/conflag/wu.html Retrieved 12th October 2018.