Guest Editorial Preface

Special Issue on IT-Support for Critical Infrastructure Protection

Jens Pottebaum, Heinz Nixdorf Institute (HNI), Paderborn University, Paderborn, Germany

Christian Reuter, Science and Technology for Peace and Security (PEASEC), Technische Universität Darmstadt, Darmstadt, Germany

1. INTRODUCTION

The power outage in Turkey 2015 (50 million affected people), the electricity outage in Bangladesh 2014 (150 million people affected), the power failures in India 2012 (670 million affected people), in Brazil and Paraguay 2009 (87 million affected people), in Europe 2006 (10 million affected people) and in the USA and Canada 2003 (55 million affected people) show that major unintended interruptions of the electrical power supply can still happen everywhere on the planet, even today (Reuter, 2014). Using the example of an intense breakdown of the power supply, the German parliament (Deutscher Bundestag, 2011) analyzed the hazards for modern societies. The study revealed that the consequences of a breakdown can add up to an outstanding critical situation. Main driver for this criticality is the interfusion of electronic and smart devices in living and work environments (Deutscher Bundestag, 2011).

Besides failures of power supply, there is a range of additional possible reasons for incidents like breakdowns – for example hurricane Kyrill in Europe 2007; tsunami and earthquake disaster in Japan 2011; hurricane Sandy in the USA 2012; and even events which seem less harmful. Some studies indicated that the frequency and intensity of natural disasters increased over the last decades (Berz, 1999). The consequences can be such intensive that the security of the citizens is not only concerned in their private but even in their work environment, for example regarding the restraint of the continuous economic practice of enterprises. This can lead to problems in business processes and cause additional extensive damage (Reuter, 2015).

The special issue is focused on critical infrastructure protection and broader views of crisis management. It received several submissions. After two rounds of peer review the resulting articles were selected and divided into two editions. The second set of articles is outlined in the following.

2. SMART GRID TOPOLOGIES TOWARDS URBAN RESILIENT CONTINUITY MANAGEMENT

The first article *Smart Grid Topologies paving the Way for an urban resilient Continuity Management* is written by Sadeeb Simon Ottenburger and Thomas Münzberg (Karlsruhe Institute of Technology, Germany). This work opens up a kind of new branch in energy security research by presenting a promising technological approach to handle power shortage scenarios in the sense of Continuity Management with respect to Critical Infrastructures including enterprises and households. This approach is based on a dynamic criticality framework adapted to a smart power system, consisting of Distributed Energy Resources (DERs) and applying an Advanced Metering Infrastructure (AMI).

Furthermore, this work proposes a rationale for a 2-stage operationalization of the proposed criticality framework and thus contributes to concepts of a smart urban Continuity Management; the 2-stage operationalization refers to the Smart Grid planning phase and its operation mode. Additionally, a simulation framework is described that can be applied to assess Smart Grid topologies and power distribution strategies or algorithms resp. The outcomes of simulation studies, conducted for specific urban systems, are useful for planning Smart Grids and for embedding control mechanisms that determine urban resilient power flows in times of power scarcity.

3. EXPECTATIONS OF DISASTER INFORMATION PROVIDED BY CRITICAL INFRASTRUCTURE OPERATORS

The second article *European expectations of disaster information provided by critical infrastructure operators: Lessons learned from Portugal, France, Norway and Sweden* is written by Laura Petersen, Laure Fallou, Paul Reilly and Elisa Serafinelli (European-Mediterranean Seismological Centre/EMSC, France and University of Sheffield, UK). The knowledge gap that this article tries to address is the lack of research on social media use in crisis times in regard to critical infrastructure (CI) operators. This article examines public expectations of crisis communication on social media by CI operators via an online survey in four countries: France, Sweden, Norway and Portugal. Key findings include that even to the public, social media is meant to compliment traditional media, not replace it, and that the public do not appear to expect CI operators to use social media for two-way communication. Further, nationality is found to heavily influence crisis communication expectations. It then examines if CI operators currently meet these stated expectations via in-person, group, semi-structured interviews with IMPROVER project Living Lab operators. The article concludes that expectations for digital communication are not currently being met by operators, and proposes via a literature review ways in which CI operators could effectively use social media as a crisis communication channel. Thus, it helps to close the existing knowledge gap and proposes ways forward for further study.

4. SENSE-MAKING BARRIERS AND STRATEGIES ON SOCIAL MEDIA DURING CRISES

The article *Understanding Sense-Making on Social Media during Crises: A Categorization of Sense-Making Barriers and Strategies* by Stefan Stieglitz, Milad Mirbabaie and Jennifer Fromm deals with the public's use of social media for sense-making in man-made crisis situations. The authors interviewed 18 German social media users and identified their perceived sense-making barriers and applied sense-making strategies on different social media platforms such as Facebook, Twitter, YouTube, Reddit, Instagram, 4chan, Wikipedia, LiveLeak and Tumblr. Based on these results, the authors propose how emergency agencies as well as developers of social media platforms could support the public in bridging their knowledge gaps in times of crisis. Emergency agencies, for example, could contribute to successful sense-making by publishing situational updates more frequently.

Jens Pottebaum
Christian Reuter
Guest Editors
IJISCRAM

REFERENCES

Berz, G. (1999). Naturkatastrophen an der Wende zum nächsten Jahrhundert – Trends, Schadenpotentiale und Handlungsoptionen der Versicherungswirtschaft. *Zeitschrift Für Die Gesamte Versicherungswissenschaft*, *88*(2–3), 427–442. doi:10.1007/BF03188065

Bundestag, D. (2011). *Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung*. (T. Petermann, H. Bradke, A. Lüllmann, M. Poetzsch, & U. Riehm, Eds.). Retrieved from dip21.bundestag.de/dip21/btd/17/056/1705672.pdf

Reuter, C. (2014). Communication between power blackout and mobile network overload. *International Journal of Information Systems for Crisis Response and Management*, *6*(2), 38–53. doi:10.4018/ijiscram.2014040103

Reuter, C. (2015). Towards efficient security: business continuity management in small and medium enterprises. *International Journal of Information Systems for Crisis Response and Management*, *7*(3), 69–79. doi:10.4018/IJISCRAM.2015070105

Jens Pottebaum, DrIng, is senior researcher and lecturer at Paderborn University, Germany, in the Heinz Nixdorf Institute, department for Mechanical Engineering (research group 'Product Creation'). His research focuses on multi- and interdisciplinary approaches on applicability and application of information technology to solve challenges in (product) data management and virtual engineering as well as complex situations in public safety and security.

Christian Reuter, PhD, is Professor for "Science and Technology for Peace and Security" (PEASEC) at Technische Universität Darmstadt and supervisor of the BMBF research group KontiKat at the University of Siegen, Germany. His research focuses on interactive and collaborative technologies such as social media in safety-critical environments, conflicts, crises and emergencies.