Crisis management systems in Germany – A status report about the current functions and developments of private and public crisis management systems in Germany

Christian Neuhaus
University of Siegen – Institute for Media Research
neuhaus@ifm.uni-siegen.de

Daniela Giebel
University of Siegen – Institute for Media Research
giebel@ifm.uni-siegen.de

Mario Hannappel
University of Siegen – Institute for Media Research
hannappel@ifm.uni-siegen.de

Sabine Färfers
University of Siegen – Institute for Media Research
faerfers@ifm.uni-siegen.de

ABSTRACT

Crisis management systems play a critical role in supporting responders and decision makers in their crisis and emergency management functions. Even though these systems and solutions have been broadly adopted in private and public organizations, very few quantitative studies can be found on their functions, user groups, targeted stakeholders, their technological requirements and their scope of services. The present study gives an outline of our ongoing project and an insight in the first results of a three-year study of crisis management systems in Germany. The study will outline the methods of our analysis and will present some results from an analysis of over more than 170 systems from over 70 vendor/developers. It will then give a conclusion of the results and outline open and future questions.

Keywords

Crisis Management Systems (CMS), Command, Control & Communication (C3) Systems, Crisis Communication, Crisis Management, Interoperability, Emergency Management, Integrated Crisis Communication (ICC)

INTRODUCTION

Crisis management system (CMS) play a vital role in today's crisis management. Similar to the adoption of computer systems in our daily routines, pen and paper in crisis management have been more and more replaced by technology in the digital age. Such solutions are widespread and can be found in many organizations in the private and public sector in Germany and all over the world. CMS supports responders and decision makers in their work and are used for information, communication and command & control functions in all areas of emergency management. Even though the main application area of these systems can be found in the response and recovery phases of emergency management, their range of use also spans from training, preparing and documentation functions to daily operational functions of the affected organizations. Even though these systems are used in many organizations on a local, state and federal level, as well as in many large companies – especially providers of critical infrastructures and industrial companies – not many quantitative studies about these systems as a whole can be found. Most of the publications in crisis management only present single solutions, analyze the requirements or outline their technological applications for crisis management (see for example Turoff, M, White, C.M. Hiltz, C.M., 2010; Adler et al., 2011; etc.). Conclusive studies about the dissemination of such systems, their application areas, their functions, their user and their stakeholder groups, as well as an analysis of the changes in the CMS market are rare. One of the earliest analysis about the use and possibilities of computer-systems for emergency management in Germany and the United States is Wolf R. Dombrowsky's study for the German Civil Defense Ministry from 1991 (Dombrowsky, 1991).

Proceedings of the 9th International ISCRAM Conference – Vancouver, Canada, April 2012
L. Rothkrantz, J. Ristvej and Z. Franco, eds.

1

His analysis at that time consisted of 67 systems, of which only about 22 can be classified as an emergency management system from today's viewpoint . The majority of these systems were information systems for firefighters (with a focus on dangerous goods), other were used as simulation/ training solutions for chemical wastes accidents. Only a few were used for command and control functions and had a military background. Dombrowsky also included an analysis of the general use of computers in fire brigades in the federal state of Hessen, a province in the middle of Germany. His analysis showed that these systems had no command and control functions but were mainly used for administrative or office works (e.g. word processing, etc.). Even though this analysis is 20 years old, many of Dombrowsky's predictions became true. Due to the implementation of computer systems, processes and operations in emergency management had to be reorganized (p. 19), These changes have resulted into a growing complexity challenge due to inter-organizational interdependencies (p. 20 ff.), which could further on lead to life-line collapses and possible domino effects. Dombrowsky also pointed out, that with the implementation of computerized CMS there is also a future threat of new forms of crisis, due to the implications these systems have on society and emergency management organizations (p. 25).

A more recent noteworthy study from the United States is the Crisis Information Management Software (CIMS) Feature Comparison Report conducted by the Institute for Security Technology Study at the Dartmouth College, which was published in 2002 for the US Department of Justice (Department of Justice, 2002) and updated in 2004 by the Institute as a status report for interoperability for the Department of Homeland Security (Department of Homeland Security, 2004). Even though these reports focused on information management systems for emergency and crisis management and only analyzed a small number of systems – 10 for the CIMS Comparison report (Justice (Department of Justice, 2002, p. 8) and 19 for the CIMS Interoperability report Security (Department of Homeland Security, 2004, p. 8) – they are the first conclusive studies on CIMS on a larger scale. These studies not only give a first insight into these systems but also offering a detailed report about CIMS functions (Department of Homeland Security, 2004, p. 20 ff.), definitions and terminologies (Department of Homeland Security, 2004, p. 10ff.).

BACKGROUND

The terrorist attacks of 9/11 (2001), Madrid (2004) and London (2005) and large scale emergencies such the Indian Ocean Tsunami (2004) or Hurricane Katrina (2005) and severe weather/ phenomena such as thunder-storms, hurricanes and floods have led to an increased need for technological solutions and funding in security technology in the public and private sector. The Department of Homeland Security for example had a total funding of over 526.874.100 $ for its State Homeland Security Program (SHSP) in 2011 (Department of Homeland Security, 2012), which is aimed to fund projects on a state and local level , which help to prevent, protect, respond to and recover from terror attacks and catastrophic events. The German Federal Ministry of Education and Research (Bundesministerium für Bildung und Forschung, BMBF) has put a similar security research program into action, which is currently funding over 50 different research projects with a budget of over 116 Mio € (Bundesministerium für Bildung und Forschung, 2012). This program is aimed to increase the civil security and consists of two program lines: The first one is a scenario based security research which is user/stakeholder oriented and includes the natural sciences, humanities, social sciences, as well as technological disciplines. Its aim is to provide feasible security solutions and applications. The second program is aimed at the research within the framework of interoperable technology networks, which are needed in many scenarios, and includes e.g. the identification of hazardous materials, pattern recognition and the development of innovative security technologies. Yet, as the examples above have shown, there are not many conclusive studies or analysis about CMS and no general accepted definition or terminology for these systems as a whole exists. Our research about CMS started in 2006, while carrying out a research project for one of Germany's largest energy provider (see also Neuhaus, 2010; Müller and Pipek 2009). As part of that analysis, we conducted a small benchmark study of crisis management systems in the United States and Germany in order to establish a status quo of functions and requirements for CMS. This internal study gave us a first insight into these systems, but it also showed the lack of categories, definitions and terminology. In 2009, the German Federal Ministry of Education and Research granted a special research project aimed at analyzing aspects of crisis communication to the Institute for Media Research (IFM) at the University of Siegen. The project 'SiKomm - Emergency Communication for security: Preventive, proactive and reactive strategies for communications support in security and rescue operations' is an independent research project that is aimed at analyzing the different roles of communication in crisis management. As part of our work, we do not only try to answer questions of time and space relation in crisis communication of emergency relief workers by using GPS and cameras, or take a in depth look at ethical and educational questions of communication in emergency management. We also wanted to took a closer look at CMS in order study the role of CMS for crisis communication. By providing a detailed analysis, we hope to give a status report about CMS today and their importance for crisis communication. The

Proceedings of the 9th International ISCRAM Conference – Vancouver, Canada, April 2012
L. Rothkrantz, J. Ristvej and Z. Franco, eds.

2

results of our findings will be used for developing a guide or manual for private and public institutions, which are interested in purchasing or developing such systems.

Method of Analysis

In October 2009, we started with the ongoing collection and research of private and public crisis management solutions. In order to limit our findings, we chose to include only systems, which are computer systems, software or web based and support responders and decision makers in their crisis management work. We limited these to systems with information, communication and command & control functions in emergency and crisis management. Furthermore they had to be categorized as information and communications technology (ICT) system, which must consist of more than one component. We excluded all those solutions which are single build solutions, like for example fire extinguisher, smoke detectors, sensors, etc. We therefore defined crisis management solutions as: systems or programs that are either computer systems, software or web based and support responders and decision makers in their work and are used for information, communication and command & control functions in emergency and crisis management. These included solutions such as Emergency Operations Center's (EOC), alerting systems, multi-channel communication systems, communication/command and control (C2/C3) systems, information systems, training and simulation systems, etc. Based on the results of our experiences in conducting the preliminary benchmark study, we chose a multiple approach for collecting as many crisis management solutions as possible. In the time from October 2009 up until now, we used 5 different ways of looking for systems for crisis management: literature review, conferences, vendor meetings/ fairs, interviews with practitioners and developers and an extensive internet research.

One of our first steps was to conduct a comprehensive literature review and analysis of previous research in the area of crisis management systems in Germany. Overall, we found little studies on crisis management systems as a whole, but many detailed studies on single crisis management systems from the private and public domain. Most of these publications were either in the context of the security research of the BMBF, the Federal Ministry of the Interior (BMI), the Federal Office of Civil Protection and Disaster Assistance (BBK), as well as related conferences and meetings like the European Congress on Civil Protection and Disaster Management (http://www.civil-protection.com), the Research Forum on Public Safety and Security (http://www.sicherheit-forschung.de/en/index.html), etc. We also attended relevant vendor meetings and fairs, like the Security World Forum for Security and Fire Prevention in Essen (http://www.security-messe.de/en/security/index.html), the Cebit (http://www.cebit.de), the International Exhibition for rescue, fire prevention, disaster relief, safety and security – Interschutz (http://www.interschutz.de/homepage_e), the German Forum and Exhibition for emergency medical and rescue aids AKUT (http://www.messen.de/de/11178/in/Bremen/ Akut%2 0Bremen/ info.html) or the branch meeting for professional mobile radio and Command & control centers PMR Expo (http://www.pmrexpo.com), e.g. We conducted several interviews with practitioners and developers alike. Of all the methods we used, the internet research proved to be the most effective way of finding the relevant systems for our analysis. We used over 100 different words and word combinations, which were relevant to our research question, and we applied the Google Search Engine (www.google.com) for testing them for their relevance and accuracy. We only collected the solutions being developed and sold from German companies and being used in Germany. After 'finding' the systems, we approached the vendor and used the information provided in order to classify the systems with regard to its functions, its range of services and applications, system user, target group, technology or system requirements and references of where they are used. We collected the data from marketing brochures, white papers, homepages, case studies and interviews.

FINDINGS

Even though our study is not yet finished and still a work in progress, we have managed to analyze over 170 different systems and solutions from over 70 different companies, as well as 31 research projects, which are currently trying to develop crisis management systems. We tried to classify these systems in respect to their functions, i.e. we looked at what kind of functions were dominating. We therefore divided these functions in: communication, alerting, information and training or simulation functions first. Even though the alerting and communication function often use the same technologies, we made a distinction between them by dividing them in one- and two-way communication, because alerting and communication should be seen as different functions in crisis management. Information functions were identified by the existence of databanks for resources, personnel, geographical information systems (GIS), etc. Because some solutions have no dominating function, we also added the category of C2/C3 hybrid systems, this is to say systems which have two or more functions and are mostly used for coordinating functions in crisis. After dividing the systems into different functions, we also took a closer look at different combinations of functions in systems.

Even though we cannot publish the final results of our research yet – they will be published in the summer of 2012 – we can already give some early insights in the field of crisis management systems as a hole and the

Proceedings of the 9th International ISCRAM Conference – Vancouver, Canada, April 2012
L. Rothkrantz, J. Ristvej and Z. Franco, eds.

3

current trends and shifts. Most interestingly, there seem to be no dominating crisis management functions in the analyzed systems. Since most of the systems are designed to actively manage emergency situations, it was obvious for us that information, alerting und communication functions would be present, but we were surprised how evenly these functions were nearly equally divided (see Figure 1).
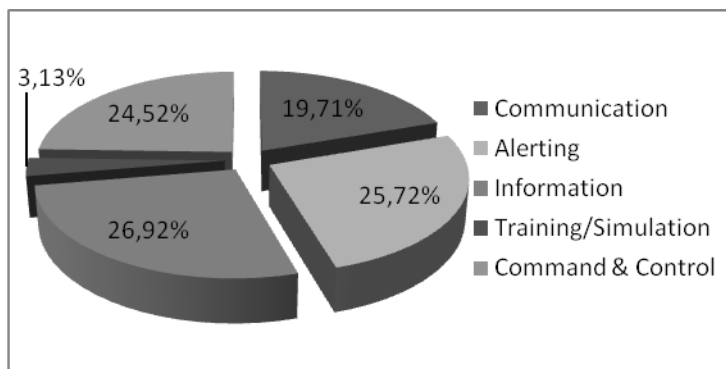

Figure1. Segmentation of Crisis management systems according to its functions

Based on our preliminary research and the literature review, we had assumed that we would find a majority of information systems. As you can see in Figure 1 information systems with 26,9 %, are closely followed by alerting systems with 25,7 % and command &control systems with 24,5%. With only 3 %, the training and simulation functions seem to play a minor role in existing systems. In our interviews with companies and user-groups, as well as with the developers, we found out that this function was often neglected due to financial restrictions or because the exercise drills were designed to integrate the real life systems into the simulation. Only a few systems, like e.g. the federal Information and communication systems Denis II [plus,] which is used on federal and state level, have with Denis II [Plus] ÜSA a full developed training simulation for the nationwide inter-ministerial and interstate crises management exercise LÜKEX (Länder Übergreifende Krisenmanagement-Übung/ Exercise). But that kind of training solutions is rare. Another surprise was that with 19,7% communication systems seem to play only a minor part for these solutions. Yet, when looking at the command & control systems or hybrid systems we quickly realized that communication plays an important part in coordinating crisis management efforts and the dissemination of information and therefore also this result has to be seen in a broader context.

Due to the work in progress, we cannot go into too much detail about our analysis, but we can point out some of the shifts and trends that we detected in the observation period. First of all, we detected a shift from single solution systems to hybrid systems. A considerable number of systems changed from offering only one single function, to adding more features and functions, which transformed these systems into a hybrid solution, which can fulfill more than one task or function in crisis management. We also detected that many vendors also provide a web- or mobile solution or service, which is based on their hard- or software solution. Due to the technological propagation of mobile devices such as smart phones, net books or tablet pc's, as well as increasing capacities of the mobile communication networks, we expect that more and more solutions will offer such services and integrate more and more features like location based services, apps and social network related solutions.

CONCLUSION AND FUTURE QUESTIONS/DISCUSSIONS

Since we are just finishing our analysis, we could only give a glimpse into our results. The database that we have constructed holds detailed information about each system, its application areas which can be differentiated into operation or tactical applications, their current application areas, and what kind of stakeholders can be targeted with this solution. It can also apply the same criteria to the user group already using the solution and if you need amateur or expert computer skills for working with the system. We are currently dividing the solutions according to their different functions, the combinations of functions and services. We also classified the systems to their different types (like e.g. software, hardware or web-solutions), their detailed functions, and their technological requirements and references. Several filters can be applied according to the criteria and therefore produce for example all available tactical systems for police forces. As we stated before, there is a lack of training and simulation solutions in CMS. Training and exercise functions – especially when it comes to communication (Giebel 2009, 2012, Reuter, Pipek, Müller, 2009) – play a vital role and should be taken into consideration when developing or purchasing a CMS.

Even though our results are only limited to Germany, many of our findings should also be applicable to the US or other countries. Questions of interoperability between systems can often not be answered, because there are

Proceedings of the 9th International ISCRAM Conference – Vancouver, Canada, April 2012
L. Rothkrantz, J. Ristvej and Z. Franco, eds.

4

no laws or recommended practices or state enforced norms by the German government, which would help to connect the different systems in order to improve the inter-organizational communication between different systems (Neuhaus, 2010). Many of the vendors we spoke to stated, that their system can be connected to other systems as well, but that therefore ports or interfaces had to be individually developed. It is our understanding that most of the CMS – especially from an inter-organization viewpoint – would perform more effectively, if there was a common protocol for these interfaces, like for example the Common Alerting Protocol (CAP), which is an XML-based data format for exchanging public warnings and emergencies between different alerting technologies. Yet projects like 'InfoStrom' (see also Balduin et al, 2010), which try to solve that problem by establishing an arena based platform as an integration solution, may give an answer to the challenge of integrated crisis communication and the exchange of information in the inter-organizational context. From our viewpoint, it is of vital importance to further analyze these systems not as single systems but to see them in comparison to other systems. Studies like the one presented here can give the private and public representatives the possibility to choose the correct solution for their needs or could help them to develop a systems according to their needs. We also believe, that studies such as ours should be conducted on a regular base in order to keep track with the fast developments of today's technology and therefore give us an insight on possible future developments – like Dombrowsky did 20 years ago.

ACKNOWLEDGMENTS

REFERENCES

1. Adler, C.; Krüsmann, M.; Greiner-Mai, T., Donner, A., Chavez, J.M., Estrem, A. (2010) IT-Supported Management of Mass Casualty Incidents: The e-Triage Project In: Proceeding of the 8th International ISCRAM Conference, Lisbon, Portugal.

2. Balduin, N., Becker, G., Brand, J., Görgen, M., Hannappel, M., Hasenfuß, P., Ley, B., Pipek, V., Probst, F., Reuter, C., Rose, T., Rusch, G., Wiedenhöfer, T. and Zinnen, A. (2010) InfoStrom: Learning information infrastructures for crisis management in case of medium to large electrical power breakdowns. In Future Security - Proceedings of the 5th Security Research Conference, Fraunhofer VVS, Berlin.

3. Bundesministerium für Bildung und Forschung (2012) URL: http://www.bmbf.de/en/11770.php, 2-08-2012.

4. Department of Homeland Security (2004) Crisis Information Management Software (CIMS) Feature Comparison Report, URL: http://www.ists.dartmouth.edu/library/213.pdf /, 2-08-2012.

5. Department of Justice (2002) Crisis Information Management Software (CIMS) Interoperability – A Status Report, URL: https://www.ncjrs.gov/pdffiles1/nij/197065.pdf, 2-08-2012.

6. Dombrowsky, W. (1991) Computereinsatz im Zilvil- und Katastrophenschutz. Möglichkeiten und Grenzen. Bundesamt für Zivilschutz, Bonn.

7. Neuhaus, C. (2010) Integrated Crisis Communication as a new approach in Crisis Management. In: Proceedings of the 7th ISCRAM Conference, Seattle, USA.

8. Giebel, Daniela (2009) Education in security communication (Firefighters, German Red Cross, German Federal Agency for Technical Relief), Working Papers No. 2, 3, 4, available online <http://www.uni-siegen.de/ifm/projekte/sikomm/downloads/ausbildung_sicherheitskommunikation.html?lang=de> (01/13/12).

9. Giebel, Daniela (2012) Sicherheitskultur - Resilienz durch Sicherheitskommunikation. In: Lange, Hans Jürgen, Endreß, Christian, Wendekamm, Michaela, Sicherheitskultur- Interdisziplinäre Betrachtung einer mehrdimensionalen Begrifflichkeit, VS, Wiesbaden [forthcoming].

10. Müller, C and Pipek, V. (2009) Socio-spatial implications of converging physical and digital infrastructures for crisis management. In: J. Landgren and S. Jul (Ed.): Proceeding of the 6th International ISCRAM Conference, Gothenburg, Sweden.

11. Reuter, C., Pipek, V., Müller, C. (2009) Avoiding crisis in communication: a computer-supported training approach for emergency management. *International Journal Of Emergency Management*, 6, 3/4, 356-368.

12. Turoff, M., White, C.M., Hiltz, S.R. (2010) A real time decision system, Version 2.0: Crisis Management Support during extreme events. In: Proceedings of the 7th ISCRAM Conference, Seattle, USA.

Proceedings of the 9th International ISCRAM Conference – Vancouver, Canada, April 2012
L. Rothkrantz, J. Ristvej and Z. Franco, eds.

5