TECHNICAL SCIENCES
Abbrev.: Techn. Sc., No 15(1), Y 2012

INFORMATION AND COMMUNICATION TECHNOLOGY AND CRISIS MANAGEMENT

***Wojciech Wojciechowicz*[1,2], *Jan Zych*[2], *Witold Hołubowicz*[2,3]**

[1] Institute of Computing Science, Poznań University of Technology
[2] ITTI sp. z o.o.
[3] Adam Mickiewicz University of Poznań

Key words: crisis management, ICT, communication.

Abstract

In the present article selected telecommunication aspects in the area of crisis management are exposed. In particular, the focus is put on the response phase, since there are new challenges at the junction of organisational and technical layers, incl. interoperability, new functionalities and models. Those aspects have not been exhaustively tested in real situations; thus such issues still require multiple testing, verification and validation. In this article the communication problems are collated with new solutions, such as the use of cloud computing, social media and additional functionalities to increase the security level. The main aim of this article is to introduce challenges, as well as new opportunities provided by the implementation of new Information and Communication Technologies in the area of crisis management.

ZAGADNIENIA TELEINFORMATYCZNE A ZARZĄDZANIE KRYZYSOWE

***Wojciech Wojciechowicz*[1,2], *Jan Zych*[2], *Witold Hołubowicz*[2,3]**

[1] Instytut Informatyki, Politechnika Poznańska
[2] ITTI sp. z o.o.
[3] Uniwersytet im. Adama Mickiewicza w Poznaniu

Słowa kluczowe: zarządzanie kryzysowe, ICT, łączność.

Abstrakt

W artykule opisano wybrane problemy telekomunikacyjne, które identyfikuje się w obszarze zarządzania kryzysowego. Szczególny nacisk położono na fazę reagowania. Na styku warstwy organizacyjnej i technicznej pojawiają się nowe problemy, np. z interoperacyjnością, nowymi funkcjonalnościami technicznymi, które nie zostały jeszcze dostatecznie sprawdzone w praktyce, a to wymaga wielowątkowych badań. Autorzy diagnozują problemy z obszaru łączności, uwzględniając takie zagadnienia, jak: zastosowanie chmury obliczeniowej, wykorzystanie sieci społecznościowych czy implementacji nowych funkcjonalności na podstawie istniejącej infrastruktury telekomunikacyjnej. Głównym celem artykułu jest przedstawienie zarówno wyzwań, jak i szans dla zarządzania kryzysowego, płynących z nowych rozwiązań teleinformatycznych.

Introduction

In recent years, there has been a significant change in the perception of challenges in the field of crisis management (CM). Instead of focusing on a major incident, there is a trend to draw special attention to several smaller incidents, which overlap/accumulate in a relatively short period of time. A perfect example illustrating this were the national crisis management system exercises – LIBERO II, organised by the Government Security Centre in collaboration with the Ministry of Internal Affairs and the PL.2012 company. During the event many scenarios were practiced, incl. energy failure, a disaster on an expressway, removing the effects of civil unrest after the football match. The scope of the exercises did not refer to one big event, but to many events that correlated with each other.

Furthermore, there is an increasing awareness of other crisis management aspects, such as use of modern information and communication technology, and the search for communication platforms able to provide adequate functionalities. News from social networks is of great importance, and is exceptionally useful during decision making process. It turns out, that the first thing that accidental witnesses tend to do is to post multimedia material on social networks, instead of reporting it to the appropriate crisis management agencies. Thus, there is a need for crisis management agencies to permanently monitor those social networks with respect to extraction of useful, up to date and unique pieces of information about given incident. In certain cases, it may become the only factual evidence.

The main scientific problem was to identify communication challenges in the field of crisis management, and to propose new solutions in this field. In the article the focus was put on broad context of crisis management rather than on a single incident.

Challenges in crisis management

Crisis management involves the coordination of activities by different groups in an effort to avoid or minimize disaster impact. This section describes the challenges that need to be confronted by crisis management in order to be more effective. There are four phases in crisis management:

– prevention,
– preparedness,
– response,
– recovery (PIĄTEK 2006).

Where the most challenging – from the crisis management communication system perspective – is the response phase. That is the area where rescue

actions are executed; given the specificity of the domain, this phase is the most dynamic. It is very difficult to precisely plan the response in advance, since it is not possible to predict when and where crises will occur. In fact, response actions always need to be undertaken in real time. Moreover, disasters often affect communication systems (e.g. natural disasters like floods or fires can seriously harm infrastructure). Therefore, the least that can be done is to prepare for the effects.

When it comes to ensuring communication between all stakeholders responsible for crisis management it is important to identify threats in real time, and coordinate the rescue actions accordingly to them. Participation of the Police, National Fire Service and Emergency Medical Service in training exercises confirmed that when an incident occurs, the number of connections to the crisis management centres increases significantly. It means that requests with the same content but through different channels (text, voice, video) are made. Quick extraction of the most important part from each message, its processing and passing to the decision makers, responsible for coordinating rescue actions in the crisis management centres, is extremely challenging, both at technical and organisational levels.

On top of that, multiple agencies as well as volunteers and passers-by are involved in the actions at the crisis scene. This creates yet another challenge which is the need to ensure communication and effective flow of information between them. That, combined with the response phase characteristics, puts an additional pressure on communication systems.

Furthermore, crisis management involves the execution of very broad and diverse actions. Possible incidents include:

– riots during mass event,
– natural disasters (earthquake, avalanche, flood, wildfire),
– man-made/terrorist attack/confrontations,
– workplace violence/misdeeds,
– accidents (crashes on land, sea and air).

For those incidents – each supporting by technology – a number of challenges might be identified. In high level of abstraction, they can be categorised into technical and organisational ones, often influencing each other. The key technical challenges include (*Metody sztucznej inteligencji*. 2009, ŚWIĄTNICKI, ŚWIĄTNICKI 1992):

– insufficient spectrum of services,
– lack of interoperability between various ICT systems,
– security aspects,
– managing user groups in real-time,
– effective information dissemination (incl. notifications to the population),

while the organisational:

– units autonomy,

– frequency allocation,
– cooperation with telecommunication operators,
– improving the work of the international community in several areas, such as decision making and situational awareness.

First responders have invested in many – often incompatible – telecommunication solutions. As a result, the possibility of exchanging information in an effective way has been reduced. In the next sections we will discuss the aforementioned technical challenges.

The technical challenges in the field of crisis management

This section provides a short description of technical challenges in the crisis management field. The current status of technical challenges is presented first, then a short description of future perspectives is given; and at the end we provide examples of how difficult crises are becoming with the purpose of illustrating the need for confronting the technical challenges.

State of the art

As it was stated previously, the response phase puts an extra pressure on the telecommunication systems. Unpredictability of time and place results in urgent needs for extra capabilities at the incident scene.

On top of that, agencies and some command chain levels have different user requirements – not only functional requirements which may concern different spectrum of services available but also non-functional (like security or performance). Additionally, the requirements may vary depending on the incident type.

Recently some investments have been done in various technologies supporting first responders. However, these investments have been done without taking into consideration the exchange of information between different crisis management actors; hence there is no unification of infrastructure, end-user devices and software applications. As a result, full interoperability is not achievable.

Perspectives

Currently, there is no single vision for the crisis management telecommunication system. Many agencies have done some technology updates without obtaining the consent of other stakeholders. There is also a lack of a *perfect* telecommunication solution, which will meet the needs of each stakeholder

(in terms of characteristics and costs). Furthermore, such a solution have not been designed yet.

Terrestrial Trunked Radio (TETRA) is an open standard, created by ETSI for dispatching digital radio-telephone communication [(Terrestrial Trunked Radio (TETRA)a]. It could be said that TETRA is the optimal choice; but its efficiency is still doubtful. One may notice that this solution is getting more and more "mature", and not even TEDS [(Terrestrial Trunked Radio (TETRA)b] (TETRA Enhanced Data Services) may guarantee the sufficient bandwidth when multimedia services are in use. Also the costs (both implementation and maintenance costs) are believed to be drawbacks of TETRA.

Crisis globalisation

The larger and larger crises, the greater number of agencies need to be involved, which puts an extra pressure on the crisis management communication system. The incidents (esp. natural ones, like floods and wildfire) also occur in cross-border areas, which require greater cooperation between nations as rescue actions involve rescue teams from several countries (vide Central European flooding in 1997 and 2010 or Haiti earthquake and Katrina hurricane in USA).There are also other types of incidents, such as terrorist attacks (incl. Madrid train bombings on 11 March, 2004, 2011 Norway attacks, 7/7 London bombings) or cyber threats (incl. attacks on SCADA systems) that have already become crises.

The crises also vary in terms of specific telecommunication needs and background, e.g.

– Prevention of disorders (e.g. riots during mass events) – a large number of volunteers are engaged, as well as third-party organisations (incl. personal security). Due to law requirements (e.g. banned access to the event for selected persons) the access to external databases would be appreciated.

– Flood – mostly involves several agencies – and also third-party organisations (e.g. construction companies) as well as volunteers, but it is almost impossible to indicate them in advance. Thus, there is a need for quick and seamless inclusion of new actors into the system. Another very important feature is the notification of residents. That could reduce disinformation as well as improve the coordination at the scene.

– Terrorist attack – where behaviour detection would have great importance. Audit trial could be very useful for public prosecutors. Different security requirements could be defined, since e.g. confidentiality may play a great role. Also actor localisation could be useful not only in terms of coordinating the

rescue teams, but also rescuing the victims (using e.g. their mobile phones) (*Bezpieczeństwo...* 2009).

The importance of ICT in crisis management is undeniable; communication is necessary in order to achieve effective coordination. ICT provides efficient coordination of activities, the sharing of information between organisations working at the scene as well as access to new data and databases, such as images, maps, and infrastructure information. The role of ICT is getting broader, since not only new threats are identified, but also new opportunities are visualised.

New opportunities for crisis management

Nowadays, crisis management is not able to operate efficiently without the support of the state of the art ICT. In order to find an optimal operation model in crisis management it becomes more frequent to take the advantage of various technological innovations (e.g. trusted computing and agent-based infrastructure) or organisational solutions (e.g. cloud computing). In this section, an outline of new technological opportunities for improving crisis management is provided.

Mobile technologies

Currently, mobile technology is advancing rapidly, both in terms of mobile phone popularity and capabilities. Modern mobile devices (palmtops, mobile phones, etc.) are capable of performing tasks that used to be reserved for personal computers.

With regard to capabilities, there is a marked trend to integrate hitherto separate devices into a single solution. Modern mobile devices are often equipped with auto-focus, a digital camera with several Mega pixels, Full HD video recording possibility (such resolution was barely achievable for dedicated digital cameras just a couple of years ago); moreover, these devices have several GBs of internal storage (with possibility to further increase using flash memory). Combined with broadband (e.g. based on HSDPA or WiFi b/g/n) data transmission and access to modern services (e.g.: online maps (even with traffic information and predictions), weather forecast or social media) mobile phones are considered to be a great tool in crisis management, used not only for communication between responders, but also for dissemination of information among the public in general (Ficoń 2007).

Social media

Social media is set of technologies that allow people to exchange multimedia information. Despite the fact that the information in social media comes from sources that are not verified, social media allow people to exchange information, ideas, opinions and experience. Therefore, social media has become very popular and this trend is growing.

The example of the 2010 flooding in Central Europe emphasizes the importance of using social media during crises situations. Citizens of the Bydgoszcz city in Poland were using a forum to inform each other about the water level; this source of information was much more effective than official communiques in traditional media. Nevertheless, with the growing popularity of social media, this information could be disseminated even faster -using applications like Facebook, Twitter, Web log and others. Comparing social media to internet forums, one may notice that the former one allows to exchange information almost in real time e.g. through smartphones. The cost in terms of development and maintenance of infrastructure as well as disseminating the information to many recipients is negligible, since social media does not require any additional costs apart from the Internet connection bills.

Cloud computing

Another new opportunity for crisis management is the use of dedicated services in modern business models – cloud computing. The main idea behind cloud computing is to provide services from remote centres using the Internet as a communication channel. In other words, cloud computing provides applications that run on the Internet. Cloud computer services are divided into four models, according to the capability provided (VOORSLUYS et al. 2011):

– IaaS – Infrastructure as a Service. This model provides all the equipment needed by an organisation to support operations, it includes hardware, servers, storage and network components. In this model, the cloud provider is responsible for maintaining the equipment.

– PaaS – Platform as a Service. In this model, cloud providers deliver a computing platform including an operating system, a programming language execution environment, database and web server. With PaaS applications developers can design, run and debug their software solutions on a cloud platform, and do not have to worry about buying and maintaining the hardware and software layers.

– SaaS – Software as a Service. It comprises software applications that are installed on the cloud and that can be accessed by cloud users. Since the

software applications are located on central hosts, the cloud users can access them through a browser. In SaaS, users do not have to maintain the data and infrastructure on which the application is running e.g. games, google docs, e-mail, etc.

– BPaaS – Business Process as a Service. This model includes any business processes delivered as a service over the Internet (for example, payroll, printing, e-commerce) and accessible by multiple web-enabled interfaces and devices such as PC, tablets and smartphones.

Cloud computing could contribute to crisis management by facilitating information sharing among first responders at different management levels (central, regional and local), and making the emergency notification more accessible to the public. Additionally, cloud computing reduces costs when it comes to data storage and recovery after a disaster. Companies that own the infrastructure locally could be severely affected by a disaster as their server may be permanently destroyed and backup may be lost. In the case of a disaster affecting a cloud computing data centre, user data will not be lost since suppliers of cloud infrastructure replicate user data and cloud servers across multiple data centres.

Furthermore, the data stored on the cloud is highly secured by cloud providers. In the data centres, the integrity of the information is protected with power generators, monitoring systems and 24/7 security personnel as well as technical specialists.

There is a wide range of possible cloud computing applications in crisis management. It not only improves the current services (in terms of e.g. costs, scalability, confidentiality, availability, security, redundancy and performance), but also provides new opportunities.

Commercial ICT in crisis management

In the previous section selected new opportunities for crisis management have been presented. Mostly they are related to the use of commercial ICT equipment in the field of public safety. Even if the infrastructure is designed for commercial use, it still can bring significant value to the crisis management field.

Current telecommunication infrastructures (e.g.: WiMAX, 3G, LTE or even WiFi) enables a wide range of services desirable in the crisis management field, like:

– (broadband) IP transmission,
– high capabilities:
  – many simultaneous voice calls,

  - video calls,
  - broadband data transmission,
  - low latency,
  - low error-rate,
- redundancy,
- positioning services,
- access to external data sources,
- a wide range of compatible, off-the-shelf devices,
- great network coverage (almost 100% in EU),
- access to numerous external services, incl.:
  - social networks,
  - on-line maps,
  - current traffic information and forecast,
  - weather forecasts (FICOŃ 2007).

At the same time, it provides an easy (often cost-effective) possibility to implement additional services:

- increased encryption,
- audit trial,
- information broadcast,
- online group management.

Further actions and conclusions

In this article selected challenges as well as opportunities in crisis management have been presented. The authors have underlined the possibility to use commercial infrastructure – with respective risks and chances – in the crisis management field.

The aim of this article has been achieved by identification of new functionalities for communication systems in crisis management, at the junction of the organisational and technical layers. The research is presented in a general context, with the focus on a number of innovations that can be adopted in the area of crisis management (e.g., social media, cloud computing, mobile phones). Current results are proofs of concepts rather than ready-to-use solutions. In addition, various approaches have been undertaken, incl. short, medium and long-term solutions, but no common vision has been established.

It is worth mentioning that no ultimate telecommunication solution for crisis management is available or expected to appear soon. As for today, the research on this problem has been undertaken by several initiatives – incl. research FP7 projects like:

- SAFECOM,

– EULER – EUropean Software Defined radio for wireless in joint security operations,

– MESA – Mobile Broadband for Public Safety,

– HIT-GATE – HIT-GATE – Heterogeneous Interoperable Transportable GATEway for First-Responders,

– SECRICOM – Seamless Communication for Crisis Management for EU safety,

– FREESIC – Free Secure Interoperable Communications.

However, the problem is still open.

Acknowledgments

This work was funded by the SECRICOM project (EC FP7-SEC 2007 grant 218123).

Translated by AUTHORS

Accepted for print 30.06.2012

References

Bezpieczeństwo w środowisku lokalnym. 2009. Red. W. Fehler, Arte, Warszawa.

FICOŃ K. 2007. *Inżynieria zarządzania kryzysowego. Podejście systemowe*. Bel Studio, Warszawa.

http://kbn.icm.edu.pl/gsi/raport.html

http://tetraforum.pl/10-lat-tetry-w-polsce.html

http://www.alert-sms.pl/alert-samorzadowy.php

http://www.ipedr.com/vol25/25-ICEME2011-N00035.pdf

http://www.sisms.pl/pl/glowna/ostrzeganie-przed-zagrozeniami.html

LEVINSON P. 2006. *Telefon komórkowy. Jak zmienił świat najbardziej mobilny ze środków komunikacji*. Muza, Warszawa.

LIDWA W. 2010. *Zarządzanie w sytuacjach kryzysowych*. Akademia Obrony Narodowej, Warszawa.

Metody sztucznej inteligencji. 2009. Eds. E. Nawarecki, G. Dobrowolski, M. Kisiel-Dorohinicki, Wydawnictwo AGH, Kraków, p. 19–22, 219–253.

PIĄTEK Z. 2006. *Procedury i przedsięwzięcia systemu reagowania*. Akademia Obrony Narodowej, Warszawa.

SIENKIEWICZ K. 2010. *Zarządzanie kryzysowe w administracji publicznej*. Difin SA, Warszawa.

ŚWIĄTNICKI W., ŚWIĄTNICKI Z. 1992. *Bronie inteligentne*. Wydawnictwo Bellona, Warszawa, p. 8, 9.

Terrestrial Trunked Radio (TETRA)a; Release 2; Designer's Guide; TETRA High-Speed Data (HSD); TETRA Enhanced Data Service (TEDS).

Terrestrial Trunked Radio (TETRA)b; Voice plus Data (V+D); Part 17: TETRA V+D and DMO specifications; Sub-part 4: Release 2.0.

VOORSLUYS W., BROBERG J., BUYYA R. 2011. *Introduction to Cloud Computing*. In: *Cloud Computing: Principles and Paradigms*. Eds. R. Buyya, J. Broberg, A. Goscinski. New York, USA: Wiley Press. pp. 1–44. ISBN 978-0-470-88799-8. http://media.johnwiley.com.au/product-data/excerpt/90/04708879/0470887990-180.pdf.

ZYCH J. 2010. *Metodologia badań bezpieczeństwa narodowego*. In: *Metody badawcze w obszarze bezpieczeństwa narodowego*. Eds. P. Sienkiewicz, M. Marszałek, H. Świeboda, AON, Warszawa.

ZYCH J. 2010. *Nowe wyzwania i wykorzystanie współczesnej nauki w zarządzaniu kryzysowym*. In: *Gry decyzyjne w zarządzaniu kryzysowym*. Ed E. Sobczak. Wydawnictwo Wydział Administracji i Nauk Społecznych Politechniki Warszawskiej, Warszawa.