Strategic Integration of Social Media into Project Management Practice

Gilbert Silvius
LOI University of Applied Sciences, The Netherlands & University of Johannesburg, South Africa

A volume in the Advances in IT Personnel and
Project Management (AITPPM) Book Series

All work contributed to this book is new, previously-unpublished material. The views expressed in this book are those of the authors, but not necessarily of the publisher.

Chapter 14

From Reactive to Proactive Use of Social Media in Emergency Response:
A Critical Discussion of the Twitcident Project

Kees Boersma
VU University, The Netherlands

Julie Ferguson
VU University, The Netherlands

Dominique Diks
Hiemstra en De Vries, The Netherlands

Jeroen Wolbers
VU University, The Netherlands

ABSTRACT

This chapter examines the introduction and implementation of the pilot project Twitcident in an emergency response room setting. Twitcident is a web-based system for filtering, searching and analyzing data on real-world incidents or crises. Social media data is seen as important for emergency response operations: it can be used as an 'early warning monitoring system' to detect social unrest, and for improving common operational pictures (COPs). This chapter shows that the expectations on the functioning of the tool were not fully met: first it was hard for the response room professionals to make sense of the data and second, the management did not develop a proper project planning. The recommendations are twofold. On the one hand, the professionals who work with Twitcident must invest in developing new information management routines. On the other hand, the response room management needs to create a much more inclusive project learning strategy.

INTRODUCTION

Over the last five years, the use of social media and social networks such as Twitter, Facebook, Yammer and Instagram by citizens at times of crisis has gained the attention of professionals operating in crisis response organizations, such as the police, fire service and medical teams (Palen, 2008; Merchant, Elmer, & Lurie, 2011). In the crisis management literature it has been recognized for decades that citizens are

self-reliant when there is social disruption and in crisis situations, whether those are incidents, emergencies or large-scale disasters (Helsloot & Ruitenberg, 2004). Nowadays, social media platforms provide a new opportunity for people to keep each other informed, adding a bottom-up information network that provides a platform for online communication (Machjzrack & More, 2010). In addition, they can potentially provide welcome additional resources for professionals in crisis response organizations. The promise is that, by using social media data, the first responders can enlarge their *common operational picture* (COP) (Yin, Lampert, Cameron, Robinson, & Power, 2012).

Yet, although the response organizations have started to recognize the importance of social media data during times of crisis, *how* this data actually can be made sense of, interpreted, validated and used is still an issue that requires further research. Therefore, professional crisis response organizations have also carried out (pilot) information management projects to understand how social media platforms actually work and how they can include social media data in their operations, both day-to-day and during crises. Over the years, many pilot projects have been implemented to test social media platforms as early warning systems, and to provide professionals with data that predicts upcoming social disruptions (Goolsby, 2010). In particular, the police have undertaken projects to determine how they could use social media data in their surveillance activities (Crump, 2011). Whereas for a long time social media data was regarded merely as 'noise' or, at best, not validated data[1], these projects indicate that crisis response managers and professionals are starting to take social media and Web 2.0 platforms seriously. Their problem, however, is how to incorporate these new information flows properly into existing information architectures in order to build a coherent crisis information system and, eventually, make the emergency response more reliable.

In this chapter we will present a project management case from the physical safety in the Netherlands, where 25 safety regions were established in 2007 to cover the crisis response across the whole country (Boersma, Groenewegen, & Wagenaar, 2010; Boersma, Wagenaar, & Wolbers, 2012). The safety regions have various functions. First, they facilitate integration between the two main first response disciplines: the fire service and the ambulance service medical teams. They work closely together with the police, who are organized at the national level in the Netherlands. Second, each safety region has had to establish a bureau responsible for developing emergency response plans and strategies and for how their professionals communicate with those in other emergency services, with policymakers and with citizens. Third, the safety region bureau is responsible for undertaking a specific risk analysis and assessment for the region. Finally, the safety region must ensure that there is a dispatch center, or *emergency response room* function, available. In the response room all three of the first response disciplines or services (police, fire and ambulance) are represented. The response room can be shared with other safety regions, on condition that the on condition that they are still able to respond adequately to incoming calls from citizens from across their own region.

Since 2012, those responsible for managing the safety regions have started to improve their crisis information management by implementing social media projects. For the various professionals working in the safety regions, however, it is still difficult to include social media data in their information management at times of emergency. The case we will present in this chapter is a pilot project from one of the 25 Dutch safety regions. In this region a project called *Twitcident* has been put in place to see how social media data – and in particular data from Twitter – could be used in the response room setting. It is a web-based system for filtering, searching and analyzing data on real-world incidents or crises. The project started in April 2014 and has been used by the region. We studied the implementation of the

project and interviewed the professionals who were directly and indirectly involved in the introduction and in the actual use of Twitcident. We studied the aims and goals of the project, the expectations of the professionals involved, how Twitcident was *used*, and the first results. Our research question is:

How did Twitcident affect the developing of a common operational picture between different professional disciplines in an emergency control room setting?

The sub-questions are:

Why did the management of the safety region initiate the Twitcident pilot project?
How was Twitcident implemented?
How did Twitcident affect the work of the emergency response room professionals?

We collected our data through observations and interviews during the first half of 2014. Our main concern was to understand both the expectations of the management and the experience of actually using Twitcident, a framework and web-based system for filtering, searching and analyzing data on real-world incidents or crises (Abel, Hauff, Houben, Stronkman, & Tao, 2012). In both of these areas, *sensemaking* in crisis situations (Weick, 1988) was a central issue for us: we were curious to know how those involved made sense of the complex coordination and information-sharing practices in emergency and crisis situations. Sensemaking is seen by Weick as a cognitive activity and ability of framing experienced situations as meaningful. Collective sensemaking is the collaborative process in which different individuals start to create *shared* awareness and understanding of the situation.

We conducted a total of 17 interviews with managers, information system engineers (who were responsible for the actual implementation of the project), professionals from the region's emergency response room, and police officers. Our most important sources of information were the centralists and generalists working in the response room. The *centralists* who do the intake (i.e., receive the incoming emergency calls), validate and, where possible, enrich the data and pass it on to the first responders in the field. The *generalists* who work with additional information sources such as social media platforms and applications that can enrich social media data – the Twitcident project being one example – to provide the centralists with additional information.

Over a period of two months, we observed how the interaction between the generalists and centralists took place, and how Twitcident added to the quality of the information exchange, if at all. We selected this style of ethnographic research and in-situ research in order to gain a fuller picture of the context of the response room and the background to the routines of the generalists and centralists (Alvesson & Sköldberg, 2009). The generalists wrote daily diaries or logbooks, which were very useful in helping us to understand their actions and see what kind of data analysis they undertook with Twitcident. We were also able to get access to formal documents about the pilot project and to the work manuals and standard operational procedures used by the generalists and centralists.

The objectives of this chapter are first of all to understand how pilot projects function as a 'protected space' for introducing and testing new, contested information technologies. Second, we would like to present an actual case in the context of a demanding environment, i.e., the emergency response room, where the time pressures constrain a smooth introduction of new technologies.

BACKGROUND

In the literature on emergency management, adopting a COP is proposed as the solution to poor communication and information-sharing practices in and between response organizations (Wolbers & Boersma, 2013). The idea is that a COP is an integrated part of an information system and used to overcome problems such as information overload, or insufficient evaluation and validation of the information. A COP is defined as the display of relevant information shared by more than one command or unit. Potentially, COPs contribute to a better *situational awareness*, which is the perception of environmental elements during incidents, emergencies and crises with respect to time, space and meaning, critical to the decision-making processes of professional first responders (Sarter & Woods, 1991; Bosse, Majdanik, Boersma, & Ingibergsdóttir, 2013). Adequate information management is seen as a precondition for creating a high-quality COP. Technical solutions are seen as the answer to failing information management. Over the years emergency response rooms information systems have been 'enriched' by a myriad of tools to enable and improve information management and thus the creation of COPs. The newest generation of tools that have been added to emergency response rooms are meant to make social media data suitable for use in emergency response information management.

Social media sites, and Twitter in particular, are seen as an important (additional) source of information in emergency and crisis situations (Mendoza, Poblete, & Castillo, 2010; Schultz, Utz, & Göritz, 2011; Hughes & Palen, 2009; Cassa, Chunara, Mandl, & Brownstein, 2013). With applications such as Twitcident the centralists in the emergency response rooms can actually follow what citizens post on social media and how citizens' information networks come into being. Twitcident can be seen as part of a larger trend in crisis management and practice to enlarge the number of sources for creation of relevant information. In particular, during actual crises and emergencies, information needs to be up-to-date and dynamic (Treurniet, Messemaker, Wolbers and Boersma, 2015). Since the crisis or emergency is constantly changing, the centralists demand sources that can deal with the speed of change. Social media sources have the potential to provide a greater quantity of information and more up-to-date information than other, more static, sources such as databases and information from incoming emergency calls.

The use of social media data in crisis and emergency situations is promising, but not without problems. There are serious concerns relating to the quality of the data from social media platforms, the validation of social media data (Yates & Paquette, 2011), the filtering of relevant information from messy social media data sources (Abel et al., 2012; Oh, Agrawal, & Rao, 2013), and the process of combining social media data with relevant data from other sources (Vieweg, Hughes, Starbird, & Palen, 2010). There are also more fundamental problems such as legal issues and questions to do with privacy and surveillance (Van de Walle, Turoff, & Hiltz, 2009; Fuchs, Boersma, Albrechtslund, & Sandoval, 2011).

Besides the more practical problems relating to the use of social media in emergency and crisis situations, we see that the expectations can be sky-high. The idea that social media data is useful for crisis situations can be seen as information technology *hype* (Meijer, Boersma, & Wagenaar, 2009). A hype can be agenda-setting, but in instances where promises cannot be met, users start to be very disappointed. Through a lack of planning or thoughtless introduction and implementation people will no longer buy in to the hype at all in particular when the claims are exaggerated (Ruef & Markard, 2010). In addition, projects always run the risk of becoming dysfunctional in different project phases, particularly in situations in which there is no common understanding of the project (Van Marrewijk, 2007; Veenswijk,

Van Marrewijk, & Boersma, 2010). Crucial for the success or failure of a project such as Twitcident is a careful and thoughtful plan for its introduction, monitoring and evaluation (Edmondson, Bohmer, & Pisano, 2001).

In order to be successful, Twitcident must be seen as a social, organizational project and not solely as a technical project (Barley, 1986; Orlikowski, & Barley, 2001). However, it has already been known for decades that IT innovation projects are often based on a relatively naïve picture of organizational change. Events, features, and behaviors that are important to the project's success or failure tend to be overlooked (Markus & Robey, 1988; Ciborra & Lanzara, 1994; Boersma & Kingma, 2005; Mirvis, Sales, & Hackett 2006). In this chapter, therefore, we will reflect upon Twitcident not only as a useful additional source of information in crisis management, but we will also consider the particular characteristics of the project, and the way it has been introduced and implemented in the organization.

THE INTRODUCTION AND USE OF TWITCIDENT IN THE EMERGENCY CONTROL ROOM SETTING

In 2012 the Dutch safety regions took an important step in optimizing their information management and information processes. This involved the establishment of *real-time intelligence centers* (RTICs) (Inspectorate of Safety and Justice, 2013). The information technologies used in the RTICs were primarily meant to support police work, but since the centers were housed next to the response rooms, they also started to collect and share information with the fire and ambulance service. The idea behind the RTICs is mainly to create an 'early warning monitoring system'. Centralists are supposed to consult the RTIC information to evaluate and monitor the atmosphere and the behavior of citizens in town centers.

Monitoring citizens' behavior became an issue for the safety regions' bureau after the so-called *project X* incident, during which social media platforms were used to mobilize people to come together for partying. In 2012 a project X party in the Netherlands got out of hand, because the police could not prevent serious rioting during the party (Van Dijck & Poell, 2013). Second, the information from the RTIC is supposed to enable centralists, and eventually officers in the field, to create an *improved COP* of the emergency situation and of the actions and interactions taking place on the ground.

The management of the safety region considered the RTIC the perfect place in which to implement the Twitcident pilot project. Before the introduction of the RTICs to the emergency response rooms, centralist only looked incidentally into social media data, and they had no analytical tools like Twitcident at their disposal.

Setting the Scene: Centralists and Generalists

In order to understand the relative value of Twitcident (and, in a broader sense, social media data), we will describe the organization of the emergency response rooms and their role in the safety region.

The emergency response room and RTIC featured in our study are housed in two rooms next to each other, separated by a glass wall. The rooms are connected by a door that is always open, so that the professionals working there can easily walk from one room to the other, to ask for feedback, exchange information in person, or request validation of decisions or actions. For the generalists it is important to

be able to see what is going on in the emergency response room so that they can respond instantly to the 'body language' of their colleagues asking for additional information. The workstations of the centralists and the generalists are very similar.

The centralists in the response room are the dispatchers; they operate the response information systems, take the incoming calls, evaluate the relevance and quality of the information received, and are responsible for disseminating the information to the appropriate first responders on the streets. The centralists have sophisticated communication and information systems at their disposal (Wagenaar, Boersma, Groenewegen, & Niemandsverdriet, 2009). About ten years ago, a new integrated information system was introduced for the response rooms, which used the software *GMS*, the Dutch abbreviation for an Integrated Emergency Room System. This system integrates various services and systems such as the 1-1-2 phone number (the Dutch equivalent of the 9-1-1 emergency number in North America), communication, radio and telephone systems used by first responders, and important databases related to the information needs of the three services, police, fire service and ambulance. One of the GMS screens is a data-entry screen where new information can be added into the database. The other screen shows geographical information about the position of the first responders (e.g., police cars), and the location of the incident. Of course, the centralists use telecommunication devices such as phones, radios and pagers to communicate with citizens and with first responders. The phones are integrated into a system that gives the centralists instant access to the most important numbers (landlines) such as those for hospitals, doctors, police stations and other organizations that are part of the critical infrastructure.

Data entered into GMS by the centralists is visible to those in the three first response services, except for data that are filtered, for example, because of confidential information. The data within GMS can also be consulted by the RTIC generalists. They know which background information will be critical to the first responders, and how to create a COP on the basis of the messages coming in. Their job description includes the need for search skills that enable them to access additional information, and the ability to filter relevant information from social media. This is in contrast to the work of a centralist, who responds to the incoming data in a reactive manner (i.e., after the call has come in, or after an incident has happened). The generalists, however, can enrich data by adding background information such as information on locations, persons, the social environment, and historical detail. This information is entered into GMS using separate files. The generalists can send it to the first responders.

The RTIC's function can be seen as that of an *intelligence service* – it collects, analyses, and exploits information to support the response room and ultimately the actual response operations (Inspectorate of Safety and Justice, 2013, pp. 33-34). The generalists also have access to additional systems such as MobiPol, a database with police information, vehicle tracking systems, specific databases, and enterprise resource systems. They can also access *Blueview*, which contains over 55 million documents with information about criminals and past crimes. And finally, of course, they can consult open information sources such as those on the Internet.

The Introduction of the Twitcident Project

The management of the safety region started to implement the Twitcident project on 1st April 2014. Their main concern was how the professionals in the response room could use social media data proactively. Our interviews with the centralists revealed that they heard about the project only two days before it was introduced. The manager responsible for the instruction used a PowerPoint presentation to explain the technical functionalities of the project. He also drew attention to the way in which the centralists and

generalists should use the tool as an addition to the systems already in use. Since the introduction was done with an emphasis on the technical aspects of the tool, the centralists and the generalists – considered to be the end-users – did not directly understand the main goal of the project and how Twitcident could be integrated into their daily routines and information management practices.

According to the managers that we interviewed some weeks after the introduction, however, the goal of Twitcident was clear: using social media websites as an 'antenna', the centralists were supposed to capture important information from citizens. Social media data could provide an answer, at least in part, to the question 'what is going on in society'. At the same time, for them Twitcident was an important project to see whether and how they could align ideas and practices about the use of social media at times of crisis at a local and national level. Twitcident was for them also a tool for organizational change. Both the centralists and the generalists were provided with a personal account (including login and password) to access Twitcident. This way, the managers coordinating the pilot could check who was using the tool, and what kind of (search) actions were taking place.

The centralists, however, interpreted the tool first and foremost as an enabling instrument that would help enlarge the *common operational picture* when incidents were taking place. In other words, for them it became an extra sensor that could be used to provide first responders in the field with relevant information about a particular incident. Also, they saw the introduction of the pilot as an attempt by the management to take initiative: with the introduction of Twitcident they could show sensitivity to the hype surrounding social media.

The rather inadequate 'management of expectations' resulted in different and at times conflicting ideas about how Twitcident could be used. The managers could fall back on a mutual feeling that social media data was potentially useful for the centralists' work, but there was no consensus about *how* that potential could be fully exploited. The centralists doubted from the start whether the Twitcident information would really be helpful to them in their daily operations and at times of crisis. To them it was unclear how they could link the information to other sources of information that they could already access. Also, the centralists had many questions about the way they could *make sense* of the additional information. While this objection could easily be interpreted as resulting from unfamiliarity with the system, there was another aspect of Twitcident that bothered them a lot. Their concern was that implementing and using Twitcident would be very time-consuming in a situation in which they were already experiencing a heavy workload.

Twitcident in Use

The Twitcident interface contains a set of filters (i.e., search options) that capture and categorize incoming information. The most important filters are tweets and retweets. Retweets are the messages on Twitter that show content that was initially posted ('tweeted') by another user. The format is RT @username where username is the Twitter name of the person one is retweeting. Within Twitcident, the tweets are categorized on the basis of predefined search terms and city names. The search terms represent the *types* of incident. Table 1 shows the Twitcident interface: the first column contains the city names, and the top row represents the types of incident.

The table shows the number of tweets per city and per incident. The city names and types of incident are not only categories but also hyperlinks. The generalist can use the links to add details *of a particular incident*, historical data, and the like. Since the software automatically generates data on the basis

Table 1. The Twitcident interface with the categories City Names and Types of Incident

City Name	Burglary	Robbery	Hacked ATM Machine	Physical Violence	Public Order	Guns	Fire
aaa	11			13	2		12
bbb	12	132	1	171	1	4	18
ccc	4	30		7	1		5
ddd	9	23		5	7	1	86
eee	9	6		24		67	154
fff	21	34	2	25	2	5	276
ggg				6	1	5	
hhh	25	55		22	4	16	13
iii	14	19		32	6	9	13
jjj	2			2			9

of the retweets, the generalist's most important task is to enrich the data with background information and details about the location and environment. The generalist can consult the content of the tweets and retweets by clicking on the numbers that pop up in the table. He or she then can decide on the relative urgency of a tweet or retweet and, if needed, delete those hits that simply cause *noise* in the information stream (e.g., because they contain false or irrelevant information). The generalist also can mark an account as spam, so that Twitcident no longer accepts incoming information from that particular account.

Twitcident also has an archival storage or preservation function because digital information – the tweets and retweets – is easily lost or corrupted. This storage function can help the generalists when they are writing after-action reports or looking at patterns of information.

Analysis and Discussion

The added value of Twitcident for the daily response room practices was disappointing. In the first eight weeks after the introduction of the tool (the same period in which we did our observations), there was no proactive use of the social media data. In other words, the expectations of the management that the tool could be used as an antenna, or 'early warning monitoring' system, were not met. Furthermore, although the generalists and centralists started to work together in the weeks after Twitcident was introduced, the centralists told us that the work of the generalists had little effect on their work routines. From our observations and interviews with centralists and generalists we could discern three main practical problems in the actual implementation and use of Twitcident.

First, the generalists complained about the constraining effect of the pre-defined search terms. The search terms are based on the categories set up by the generalists. For example, they have to categorize incoming calls under terms such as Public Order, Robbery, Fire, etc. Social media data, however, is messy and full of contradictions. Citizens who post a tweet about a burglary use terms such as 'we've had a break-in', 'theft', 'break-in', 'someone's broken in' and the like. In other words, citizens use a variety of terms, including more colloquial language. For the generalists it was challenging, if not impossible, to

use the search terms systematically in order 'filter' the social media data. The predefined search terms stopped them from making flexible choices and interpretations of the raw data. The Twitcident software allowed them to add new search terms, but it was very difficult for the generalists to come to a consensus about more adequate categories.

Second, the generalists were confronted with different uses and interpretations of the terms by the different first response disciplines. In particular the police have their own terminology, and since most of the Twitter data has to do with public order and safety, they started to dominate the discussion about terms and categories (as is also reflected in the table). The generalists started to adjust the terms, which led to an instant increase in the number of Twitcident hits. The main problem still remained: the search terms turned out to be too specific for the generic use and analysis of social media data.

Third, for the generalists geo-information is crucial for validating tweets and for linking the information to other sources and informing first responders on the ground. Therefore a tweet or retweet is only recognized in Twitcident if it contains geo-information on the sender. Tweets without a geo-location and/or a city name are filtered out. However, since most people who use Twitter do not add geo-information, most of the data from Twitter turned out to add no value to the information that was already available. Potentially, a lot of valuable data was missed or filtered out.

Alongside these practical issues, we see two more fundamental problems with Twitcident and the way that the social media is, or could be, used in the daily practices and routines of the emergency response room.

First, the generalists and centralists became demotivated in the weeks following the introduction of Twitcident. Social media, and in the case of Twitcident *Twitter*, was supposed to enrich their job, but in reality the data that came out of Twitcident appeared to be rather poor. On top of that, not a single incident or emergency was filtered out from the social media data that was not already known by the centralists as a result of the 1-1-2 calls. It meant that Twitcident could not meet the management's expectations of being an 'early warning monitoring system' or an antenna for social unrest. During our observations we noticed that some days after it was introduced, the generalists stopped using Twitcident as part of their standard procedure, but instead used it only occasionally and on a relatively ad-hoc basis. They did not invest time in establishing stable routines for using Twitcident. For the centralists it meant that they were not really able to rely on this additional source of information. What made the integration of the Twitcident data even more problematic is that no interconnection (or, in technical terms, interoperability) was possible with GMS or with other systems in use. Instead of being a help to them, Twitcident turned out to be yet another thing they had to deal with. This made it all too easy for them to ignore Twitcident completely. As they told us during the interviews, centralists still believe that Twitcident could be useful, but, given their experiences, they see its added value as being for writing after-action reports, for example.

Second, it was really hard for the centralists to fully appreciate the tool since they were not involved in its design, nor in the implementation process. They saw Twitcident as a management initiative. In the absence of an adequate monitoring process, the result was a significant mismatch between expectations and actual experiences, a problem that is commonly reported in the information technology implementation literature (Fleck et al., 1990). Twitcident was introduced in a top-down fashion and the management had high expectations, but the professionals who actually had to work with the tool felt a lack of ownership. The work of a centralist can be stressful, particularly during incidents and emergencies. Information overload and time pressures are serious concerns for them, and paradoxically this is especially the case at times when the potential of social media data is at its greatest.

SOLUTIONS AND RECOMMENDATIONS

We have shown in this chapter that the management of the emergency response room and coordinators of the tool had high expectations of the pilot project. In particular they expected Twitcident to be a rich source of instant data not just at times of crisis, but also for day-to-day operations. However, the first results turned out to be disappointing. Not only was the social media data hard to validate (i.e., it was difficult to verify the trustworthiness of the content), but it was also almost impossible to keep up with the amount of data provided by Twitcident. When the centralists tried to use Twitcident to improve their operational picture, they had a difficult time interpreting and validating social media data and linking it to other sources of information. In addition, looking through social media content for 'monitoring' purposes turned out to be useless. This does not mean, however, that the use of social media data has to be abandoned completely by the safety region response rooms.

What needs to happen is first of all that, the generalists and centralists must create a shared understanding of the intended and unintended consequences of social media data for their work. Having a more realistic view of how Twitter, and other social media, could be used in their work will help them to develop new work routines (Feldman & Pentland, 2003) in which the use of this additional information source can be embedded. Twitcident can only be a valuable extra source of information for the centralists if they are clear about why and how they should use it. The dual nature of Twitcident – an early warning monitoring system on the one hand, and a system to enlarge COPs on the other – made that it fell between two stools. Early warning systems need a different type of organizational routine (i.e., scanning big data with broad search terms) than COP development (i.e., a precise and channeled search for adequate additional information about a particular incident). Thinking through the routines in use (Orlikowski, 1992) needed for Twitcident is crucial for organizations to use the tool effectively.

Second, Twitcident was seen as yet another information source that could be easily accessed and consulted by centralists. In other words, it was seen as an 'information warehouse' where users could select information that was relevant to them in performing their tasks. Unconsciously, they assumed that they could simply select information from the warehouse database to help them in executing their task because (as with any other information database) the information was supposed to be stored in an easy and accessible form (Davenport, 1998). However, to regard Twitcident as a warehouse dataset will lead to a failure of the tool. Instead, the use of Twitcident data must be based on a collective *sensemaking* perspective. Centralists and generalists have to realize that they (knowingly or unknowingly) give meaning to information and that their sensemaking can differ from that of other people because there are differences in routines, beliefs and assumptions that can potentially lead to misinterpretation of information (Wolbers & Boersma, 2013). Upfront there is no guarantee that social media data can contribute to creating COPs or help organizations to monitor behavior. If Twitcident is to contribute to the control room information management, the stakeholders involved (the response room's management, generalists, centralists, and first responders) all have to reflect upon their sensemaking process. In other words, simply sending data from Twitcident from the RTIC room to the emergency response room and on to the first responders is useless. It has to have *meaning* attached, and the only way to do that is to talk about the information (Weick, 1988) so that people can then understand the constraints, and start to appreciate the relative value of the data source.

Finally, the Twitcident project lacked a proper project *plan* – there was no thoughtful introduction or implementation strategy, let alone a monitoring process. For Twitcident to be successful, the management needs to invest far more in 'managing expectations'. Earlier studies of new technology implementation

have shown that top-down introduction of new technologies in organizations can have a disruptive effect. Those who implemented such technologies successfully underwent a qualitatively different *learning process* than those who were unsuccessful. Important steps in this process are: enrollment, preparation, trials, and reflection (Edmonson et al., 2001). In the Twitcident case it means that the users – generalists and centralists – have to be involved in the further use of the tool, and develop the motivation needed to use it. Being more reflective about their work would encourage a learning process to begin, and would allow them to develop new routines for using social media data. From our interviews it is clear that it is not too late for this, since the centralists still believe that there is value to be gained from using social media data, but only if they can embed this in their information management routines.

FUTURE RESEARCH DIRECTIONS

Twitcident was introduced, implemented and used in an emergency response room setting as part of a *pilot* project. For further research it would be interesting to study the subsequent development of Twitcident, and to analyze the pros and cons of using social media data for emergency response in a more systematic manner. For example, one could look at the use of social media data by first responders in major crisis situations or disasters. It might be that disruptions of this kind would also make the generalists' searching of social media sites more targeted.

It is also known that the hectic environment in the emergency response room – with time pressure on the centralists – influences the way that information streams are managed. Therefore, it might be useful to look at how projects using similar applications are used in other settings where the time pressures are not so great – for example, in marketing or consumer insight activity. (Evans, 2012; Tuton & Solomon, 2014).

Clearly, projects such as Twitcident can only succeed if they are carefully embedded in an organization's information management. A future research direction might therefore be to study social media as part of the wider and more complex information architecture of an organization (Koltay, 2011) to understand the conditions in which the social media data can become part of the structural design of shared information environments.

Finally, we need to research and understand how people make sense of social media data in complex organizational settings. This chapter has shown that in order to use social media data successfully, we have to take seriously the sensemaking processes of who are trying to interpret that data. This would require us to look at the social aspects of social media implementation and use. In times of uncertainty, people try to make sense of the situation and the incoming information. It is important that we start to understand how people in organizational (in our case centralists and generalists) take cues from social media data that help them decide which information is relevant for their work. In other words, we need to explore creatively the way in which meaning is attached to social media (see, for example, Bechmann & Lomborg, 2013).

CONCLUSION

The emergency control room's management had high expectations of the pilot project Twitcident, as they expected it to be a rich source of instant data not just at times of crisis, but also for monitoring processes

in daily situations. This dual nature, however, was never adequately explained to the professionals who had to work with it - the centralists and generalist. In fact, the implementation process has been done in a top-down fashion. Therefore, the generalists and centralists never developed a full understanding of the meaning and potential usefulness of Twitcident for their work, which had eventually a negative effect on the success of the tool.

Perhaps the most important outcome of our study into the Twitcident project is that professional response organizations have to think in advance what to do with social media data and how they want to use it. Social media data is not clean; it is messy, full of contradictions, and therefore difficult to integrate into the daily operations of the centralists. The professionals have to develop the skills to actually *make sense* of social media data. They have to ask themselves the question: what does this data actually mean? What does it mean for my operations, for my information management, and how does it interfere, complement or align with other information sources that we are already using?

Our study makes clear that social media data and information are not very useful if the organization does not know how to link this additional source of information to its other information streams. In other words, social media has to be strategically *integrated* into the overall information management of the crisis response organization in order to be of use. Our case has clearly shown that the introduction of social media (i.e., here the Twitcident project) to the emergency response room must be treated as part of a careful learning process that includes enrolment, preparation, trial and testing out. This is the only way for such projects to be successful.

REFERENCES

Abel, F., Hauff, C., Houben, G. J., Stronkman, R., & Tao, K. (2012). Twitcident: fighting fire with information from social web streams. *Proceedings of the 21st International Conference Companion on World Wide Web* (pp. 305-308). doi:10.1145/2187980.2188035

Alvesson, M., & Sköldberg, K. (2009). *Reflexive methodology: New vistas for qualitative research*. London: Sage.

Barley, S. R. (1986). Technology as an occasion for structuring: Evidence from observations of CT scanners and the social order of radiology departments. *Administrative Science Quarterly*, *31*(1), 78–108. doi:10.2307/2392767 PMID:10281188

Bechmann, A., & Lomborg, S. (2013). Mapping actor roles in social media: Different perspectives on value creation in theories of user participation. *New Media & Society*, *15*(5), 765–781. doi:10.1177/1461444812462853

Boersma, F. K. Groenewegen, & P. Wagenaar, P. (2010). The information management of co-located Emergency Response Rooms in the Netherlands. In H. Rahman (Ed.), Cases on Adoption, Diffusion and Evaluation of Global E-Governance Systems (pp. 107-116). Hershey USA: IGI Publishing.

Boersma, F. K., & Kingma, S. F. (2005). From Means to Ends: The Transformation of ERP in a Manufacturing Company. *The Journal of Strategic Information Systems*, *14*(2), 197–219. doi:10.1016/j.jsis.2005.04.003

Boersma, F.K., Wagenaar, P., & Wolbers, J. (2012). Negotiating the 'Trading Zone'. Creating a Shared Information Infrastructure in the Dutch Public Safety Sector. *Journal of Homeland Security and Emergency Management, 9*(2).

Bosse, T., Majdanik, K., Boersma, F. K., & Ingibergsdóttir, K. (2013). Studying Shared Situation Awareness by Agent-Based Simulation, *Web Intelligence (WI) and Intelligent Agent Technologies (IAT)*, Atlanta, USA. *Proceedings of the 2013 IEEE/WIC/ACM International Joint Conference* (Vol. 2, pp. 201-208).

Cassa, C. A., Chunara, R., Mandl, K., & Brownstein, J. S. (2013). Twitter as a sentinel in emergency situations: Lessons from the Boston marathon explosions. *PLoS Currents*, July. PMID:23852273

Ciborra, C. U., & Lanzara, G. F. (1994). Formative contexts and information technology: Understanding the dynamics of innovation in organizations. *Accounting*, *Management and Information Technologies*, *4*(2), 61–86. doi:10.1016/0959-8022(94)90005-1

Crump, J. (2011). What are the police doing on Twitter? Social media, the police and the public. *Policy & Internet*, *3*(4), 1–27. doi:10.2202/1944-2866.1130

Davenport, T. H. (1998). Putting the enterprise into the enterprise system. *Harvard Business Review*, *76*, 121–131. PMID:10181586

Edmondson, A. C., Bohmer, R. M., & Pisano, G. P. (2001). Disrupted routines: Team learning and new technology implementation in hospitals. *Administrative Science Quarterly*, *46*(4), 685–716. doi:10.2307/3094828

Evans, D. (2012). *Social media marketing: An hour a day*. Indianapolis: John Wiley & Sons.

Feldman, M. S., & Pentland, B. T. (2003). Reconceptualizing organizational routines as a source of flexibility and change. *Administrative Science Quarterly*, *48*(1), 94–118. doi:10.2307/3556620

Fleck, J., Webster, J., & Williams, R. (1990). Dynamics of information technology implementation: A reassessment of paradigms and trajectories of development. *Futures*, *22*(6), 618–640. doi:10.1016/0016-3287(90)90131-Z

Fuchs, C., Boersma, F. K., Albrechtslund, A., & Sandoval, M. (2011). Internet & Surveillance. Introduction. In C. Fuchs, F. K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and Surveillance* (pp. 1–29). London: Routledge.

Goolsby, R. (2010). Social media as crisis platform: The future of community maps/crisis maps. *ACM Transactions on Intelligent Systems and Technology*, *7*(1), 1–11. doi:10.1145/1858948.1858955

Helsloot, I., & Ruitenberg, A. (2004). Citizen response to disasters: A survey of literature and some practical implications. *Journal of Contingencies and Crisis Management*, *12*(3), 98–111. doi:10.1111/j.0966-0879.2004.00440.x

Hughes, A. L., & Palen, L. (2009). Twitter adoption and use in mass convergence and emergency events. *International Journal of Emergency Management*, *6*(3), 248–260. doi:10.1504/IJEM.2009.031564

Inspectie Veiligheid en Justitie. (2013). *Nationale Politie op Koers?* Den Haag: IVJ.

Koltay, T. (2011). Information overload, information architecture and digital literacy. *Bulletin of the American Society for Information Science and Technology*, *38*(1), 33–35. doi:10.1002/bult.2011.1720380111

Markus, M. L., & Robey, D. (1988). Information technology and organizational change: Causal structure in theory and research. *Management Science*, *34*(5), 583–598. doi:10.1287/mnsc.34.5.583

Meijer, A., Boersma, F. K., & Wagenaar, P. (Eds.), (2009). *ICTs, Citizens & Governance: After the Hype!* Amsterdam: IOS Press.

Mendoza, M., Poblete, B., & Castillo, C. (2010). Twitter Under Crisis: Can we trust what we RT? *Proceedings of the first workshop on social media analytics* (pp. 71-79). doi:10.1145/1964858.1964869

Merchant, R. M., Elmer, S., & Lurie, N. (2011). Integrating social media into emergency-preparedness efforts. *The New England Journal of Medicine*, *365*(4), 289–291. doi:10.1056/NEJMp1103591 PMID:21793742

Mirvis, P., Sales, A., & Hackett, E. (2006). The implementation and adoption of new technology in organizations: The impact on work, people, and culture. *Human Resource Management*, *30*(1), 113–139. doi:10.1002/hrm.3930300107

Oh, O., Agrawal, M., & Rao, H. R. (2013). Community intelligence and social media services: A rumor theoretic analysis of tweets during social crises. *Management Information Systems Quarterly*, *37*(2), 407–426.

Orlikowski, W. J. (1992). The duality of technology: Rethinking the concept of technology in organizations. *Organization Science*, *3*(3), 398–427. doi:10.1287/orsc.3.3.398

Orlikowski, W. J., & Barley, S. R. (2001). Technology and institutions: What can research on information technology and research on organizations learn from each other? *Management Information Systems Quarterly*, *25*(2), 145–165. doi:10.2307/3250927

Palen, L. (2008). Online social media in crisis events. *EDUCAUSE Quarterly*, *31*(3), 12.

Ruef, A., & Markard, J. (2010). What happens after a hype? *Technology Analysis and Strategic Management*, *22*(3), 317–338. doi:10.1080/09537321003647354

Sarter, N. B., & Woods, D. D. (1991). Situation Awareness: A Critical but Ill-Defined Phenomenon. *The International Journal of Aviation Psychology*, *1*(1), 45–57. doi:10.1207/s15327108ijap0101_4

Schultz, F., Utz, S., & Göritz, A. (2011). Is the medium the message? Perceptions of and reactions to crisis communication via twitter, blogs and traditional media. *Public Relations Review*, *37*(1), 20–27. doi:10.1016/j.pubrev.2010.12.001

Treurniet, W., Messemaker, M., Wolbers, J., & Boersma, F. K. (2015). Shaping the societal impact of emergencies: Striking a balance between Control and Cooperation. *International Journal of Emergency Services*, 4(1), 129-151. http://dx.doi.org/10.1108/IJES-06-2014-0007

Tuten, T. L., & Solomon, M. R. (2014). *Social media marketing*. London: Sage.

Van de Walle, B., Turoff, M., & Hiltz, S. R. (Eds.), (2009). *Information systems for emergency management*. New York: ME Sharpe.

Van Dijck, J., & Poell, T. (2013). Understanding social media logic. *Media and Communication*, *1*(1), 2–14. doi:10.17645/mac.v1i1.70

Van Marrewijk, A. (2007). Managing project culture: The case of Environ Megaproject. *International Journal of Project Management*, *25*(3), 290–299. doi:10.1016/j.ijproman.2006.11.004

Veenswijk, M., Marrewijk, A., & Boersma, K. (2010). Developing New Knowledge in Collaborative Relationships in Megaproject Alliances: Organising Reflection in the Dutch Construction Sector. *International Journal of Knowledge Management Studies*, *4*(2), 216–232. doi:10.1504/IJKMS.2010.030793

Vieweg, S., Hughes, A. L., Starbird, K., & Palen, L. (2010). Microblogging during two natural hazards events: what twitter may contribute to situational awareness. *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 1079-1088). doi:10.1145/1753326.1753486

Wagenaar, P., Boersma, F. K., Groenewegen, P., & Niemandsverdriet, P. (2009). Implementing C2000 in the Dutch police region 'Hollands-Midden.' In A. Meijer, F.K. Boersma, & P. Wagenaar, (Eds.), ICTs, Citizens & Governance: After the Hype! (pp. 119-134). Amsterdam: IOS Press.

Weick, K. E. (1988). Enacted Sensemaking in Crisis Situations. *Journal of Management Studies*, *25*(4), 305–317. doi:10.1111/j.1467-6486.1988.tb00039.x

Wolbers, J. J., & Boersma, F. K. (2013). The Common Operational Picture As Collective Sensemaking. *Journal of Contingencies and Crisis Management*, *21*(4), 186–199. doi:10.1111/1468-5973.12027

Yates, D., & Paquette, S. (2011). Emergency knowledge management and social media technologies: A case study of the 2010 Haitian earthquake. *International Journal of Information Management*, *31*(1), 6–13. doi:10.1016/j.ijinfomgt.2010.10.001

Yin, J., Lampert, A., Cameron, M., Robinson, B., & Power, R. (2012). Using social media to enhance emergency situation awareness. *IEEE Intelligent Systems*, *27*(6), 52–59. doi:10.1109/MIS.2012.6

ADDITIONAL READING

Coombs, W. T. (2014). *Ongoing crisis communication: Planning, managing, and responding*. London: Sage Publications.

Kietzmann, J. H., Hermkens, K., McCarthy, I. P., & Silvestre, B. S. (2011). Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, *54*(3), 241–251. doi:10.1016/j.bushor.2011.01.005

Latonero, M., & Shklovski, I. (2011). Emergency management, Twitter, and social media evangelism. *International Journal of Information Systems for Crisis Response and Management*, *3*(4), 67–86.

Reuter, C., Marx, A., & Pipek, V. (2012). Crisis management 2.0: Towards a systematization of social software use in crisis situations. *International Journal of Information Systems for Crisis Response and Management*, *4*(1), 1–16. doi:10.4018/jiscrm.2012010101

Veil, S. R., Buehner, T., & Palenchar, M. J. (2011). A Work-In-Process Literature Review: Incorporating Social Media in Risk and Crisis Communication. *Journal of Contingencies and Crisis Management*, *19*(2), 110–122. doi:10.1111/j.1468-5973.2011.00639.x

White, C. M. (2011). *Social media, crisis communication, and emergency management: Leveraging Web 2.0 technologies. Tailor & Francis Group*. CRC press. doi:10.1201/b11251

Artman, H., & Wærn, Y. (1999). Distributed cognition in an emergency co-ordination center. *Cognition Technology and Work*, *1*(4), 237–246. doi:10.1007/s101110050020

Furniss, D., & Blandford, A. (2006). Understanding emergency medical dispatch in terms of distributed cognition: A case study. *Ergonomics*, *49*(12-13), 1174–1203. doi:10.1080/00140130600612663 PMID:17008252

Heath, C., & Luff, P. (1992). Collaboration and control. Crisis management and multimedia technology in London Underground Line Control Rooms. [CSCW]. *Computer Supported Cooperative Work*, *1*(1-2), 69–94. doi:10.1007/BF00752451

Suchman, L. A. (1987). *Plans and situated actions: the problem of human-machine communication*. Cambridge: Cambridge University Press.

Boersma, K., & Kingma, S. F. (2005). Developing a cultural perspective on ERP. *Business Process Management Journal*, *11*(2), 123–136. doi:10.1108/14637150510591138

Joshi, K. (1991). A model of users' perspective on change: The case of information systems technology implementation. *Management Information Systems Quarterly*, *15*(2), 229–242. doi:10.2307/249384

Lapointe, L., & Rivard, S. (2005). A multilevel model of resistance to information technology implementation. *Management Information Systems Quarterly*, *29*(3), 461–491.

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research*, *2*(3), 192–222. doi:10.1287/isre.2.3.192

Orlikowski, W. J., & Gash, D. C. (1994). Technological frames: Making sense of information technology in organizations. *ACM Transactions on Information Systems*, *12*(2), 174–207. doi:10.1145/196734.196745

Taylor, S., & Todd, P. A. (1995). Understanding information technology usage: A test of competing models. *Information Systems Research*, *6*(2), 144–176. doi:10.1287/isre.6.2.144

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *Management Information Systems Quarterly*, *27*(3), 425–478.

KEY TERMS AND DEFINITIONS

Common Operational Picture (COP): The display of relevant information shared by more than one command or unit, facilitation situation awareness.

Crisis Management: The organization function that deals with expected and unexpected, disruptive situations, such as incidents, emergencies and (natural) disasters.

Emergency Response Rooms: Dispatch centers occupied by the first response organizations (i.e. the police, fire and ambulance service) for the intake of emergency calls, the 'cleaning' of the information and for the dissemination of the information to first responders.

GMS: Integrated Emergency Room System.

Information Technology Implementation: The process through which new information technologies are introduced and enrolled in organizational settings.

RTIC: Real-time intelligence center.

Sense-Making: The process by which people give meaning to information and experiences. The sense-making becomes evident through written and spoken narratives.

Social Media: Computer-mediated platforms that enable people to create, share or exchange information, ideas, and pictures/videos in virtual communities.

Trading Zone: The notion that data from (social media) information sources is something to talk about, that is, actors must give meaning to the data in order to be able to link it to other information sources.

Twitcident: A web-based system for filtering, searching and analyzing data on real-world incidents or crises.

ENDNOTES

[1]   We define social media *data* as the raw data from social media platforms to which no meaning is (as yet) attached. Only after professionals have attached meaning to data can we speak of *information*.