



EMPIRICAL RESEARCH

Information sharing and interoperability: the case of major incident management

David K. Allen¹,
Stan Karanasios² and
Alistair Norman²

¹AIMTech Research Group, Leeds University
Business School, Leeds, U.K.; ²Leeds University,
Business School, Leeds, U.K.

Correspondence: David K. Allen, AIMTech
Research Group, Leeds University Business
School, Maurice Keyworth Building, Leeds,
LS2 9JT, U.K.
Tel: +44 (0)113 343 7015;
E-mail: Da2@lubs.leeds.ac.uk

Abstract

Public sector inter-organisational information sharing and interoperability is an area of increasing concern and intense investment for practice and an area of increasing scholarship. This paper focuses on one particular set of public sector organisations (emergency services) and illuminates the key technological and organisational issues they face concerning information sharing and interoperability. The particular contexts in which these are studied are ones where decisions are non-trivial and made in high-velocity environments. In these conditions the problems and significance of inter-organisational information sharing and interoperability are accentuated. We analyse data gathered from two studies: the first focused on 'first responders' (police, fire and ambulance services) in the United Kingdom. The second, a follow on study, with emergency service managers and interoperability project managers in the United Kingdom and the European Union. Using activity theory as a conceptual framework we describe the informational problems critical emergency responders face in their initial response to, and management of, an incident. We argue that rather than focusing on interoperability as a primarily technological issue it should be managed as an organisational and informational issue. Second, we argue that rather than designing for anomalous situations we should design systems, which will function during both anomalous and routine situations. Third, we argue for focus on harmonisation of policies, procedures and working practices.

European Journal of Information Systems (2014) 23(4), 418–432.

doi:10.1057/ejis.2013.8; published online 18 June 2013

Keywords: inter-organisational information systems; information sharing; activity theory; emergency response

Introduction

Until recently the topic of inter-organisational information sharing and interoperability has not been the focus of a significant body of work within the information systems (IS) community. Some early IS scholars noted the challenge concerning sharing data among early electronic platforms (Barrett & Konsynski, 1982) and later sharing information across systems in multi-national organisations (Ives & Jarvenpaa, 1991). Nonetheless, it is only since 2000 that it has surfaced as an area of interest for the IS community (Allen *et al.*, 2000; Park & Ram, 2004). The number of journal special issues devoted to electronic cross-organisational and cross-border collaboration and reviews (Madlberger & Roztocky, 2010; Romano *et al.*, 2010) testify to the increasing interest in the topic. Much of the research in this area has, however, focused on business environments where there are clear economic drivers and on relatively stable collaborations between partners (Dong-Heon & Ramamurthy, 2011), in clearly defined business

Received: 16 October 2011
Revised: 7 March 2012
2nd Revision: 22 October 2012
3rd Revision: 7 January 2013
4th Revision: 19 February 2013
Accepted: 22 March 2013

processes or activities often in dyadic relationships (Iannacci, 2010). Indeed, this surge in academic interest reflects the fact that for many private and public sector organisations information sharing has emerged as a major concern (Park & Ram, 2004; Pardo & Tayi, 2007; Verdecho *et al*, 2012).

In this paper, we focus on the context of high-velocity environments (Oliver & Roos, 2005), where inter-organisational information sharing and interoperability allows rapid decision making and collaboration between multiple partners in *ad-hoc* partnerships. The context we focus on is typified by its complexity, information intensiveness, speed of decision making and the non-routine nature of the activity. The collaborating partners in these environments create temporary highly reliable organisations (Bigley & Roberts, 2001). In this paper, we explore these issues by focusing on emergency responders communicating and sharing information during these incidents and discuss the influence of organisational rules and norms on information sharing and interoperability.

The particular environment that we focus on is the response to major incidents (such as man-made or natural disasters). Such incidents require rapid and simultaneous intervention and subsequent communication between several emergency disciplines, including police (to stabilise the scene and begin investigations), paramedics (to aid the injured), fire and rescue services (to manage fires and structures) and a range of other specialised agencies. This has been brought into sharp focus by several critical reports, where failure to communicate and share information led to loss of life, suffering and damage to property. Enquiries into the 2007 summer floods in the United Kingdom (Pitt, 2008), 7/7 London bombings in 2005 (London Assembly, 2006) and 9/11 attack in 2001 (NCTAUS, 2004) all revealed information sharing and inter-organisational communication shortcomings. Echoing the 9/11 Commission findings, one of the well-known conclusions of the London Assembly (2006, p. 120) report on 7/7 was that *communications within and between the emergency services did not stand up on 7 July*. It is also an area of intense investment and activity both by national governments and on a European level, as evidenced by the large-scale funding and EU projects that drive towards greater Information and Communication Technology (ICT) interoperability among different agencies, and an issue that is expected to grow in importance across the world in light of concerns about climatic change and responding to extreme weather events (Karanasios, 2011). This type of collaboration is also of wider interest, as a type of activity that is becoming more relevant in both the public and private sectors where rapid decision making in conditions of uncertainty (Hodgkinson *et al*, 2009) and *ad-hoc* decentralised and short-term collaboration becomes more normalised (Engeström *et al*, 1999a).

This paper is organised as follows: first, we review relevant literature relating to interoperability and infor-

mation sharing and identify several research gaps; second, we describe our research setting and method and outline the empirical base for this paper; third, we analyse two studies of information sharing and interoperability, and finally we discuss the analysis of the synthesis of the two cases and present several theoretical and practical implications.

Literature review

Interoperability, information sharing and emergency response

While several large-scale events and enquiries have emphasised the need for addressing information integration among emergency responders, until very recently, there have been few empirical studies and significant insights (Chen *et al*, 2008). Indeed, Coles *et al* (2012) noted that the wider area of interagency cooperation has not been clearly defined and that an understanding of the dynamics within effective partnerships remains underdeveloped.

One theme that has received a significant amount of enquiry is the technical issues and challenges surrounding the development of ICT systems. In particular, studies undertaken in the electrical engineering, law and disaster focused fields have largely approached the issue from a 'technology as a solution' perspective or examined the issues surrounding current ICT systems. These studies have augmented understanding on a number of salient technical issues that enable and inhibit interoperability and information sharing and the opportunities afforded by technological advances. This includes: the difficulty of allocating different frequency/transmission standards to individual public safety agencies; information-sharing security concerns; the dependence on legacy systems; the complication of managing systems across borders (for instance, in Europe there are 23 official languages); diverse command structures and cultures; the tailoring of systems to the specific requirement of the organisation with little consideration for vertical and horizontal integration across organisations; and the possibilities opened up by cognitive radio technology (Mayer-Schönberger, 2005; Pawelczak *et al*, 2005; Brito, 2007; Baldini, 2010).

By comparison research approaching the issue through a management or organisational perspective is scarce. Some recent research has provided insights into post-hoc case studies of disaster response, the problems facing information sharing *in-situ*, the difficulty surrounding information sharing in inter-organisational contexts and described studies undertaken during disaster management exercises as a prelude to systems design (Rietjens *et al*, 2009; Bharosa *et al*, 2010; Lee *et al*, 2011; Locatelli *et al*, 2012). A theme noted is that most approaches to remedy the problem include the development of ICT to support the collaboration process, rather than the creation, refinement or transformation of a collaboration process (facilitated by ICT) to improve information flows and patterns (Sagun *et al*, 2009). In common with the

technical studies, the approach and perspective used tilts towards the technology as a solution perspective.

An examination of the broader (non-emergency/public safety and non-technical) literature reveals several inter-related factors that problematise real progress in terms of inter-organisational information sharing and interoperability, which are magnified as the number and type of information resources, technologies and organisations to share information across grows (Pardo & Tayi, 2007). The European Interoperability Framework (EIF) identifies four dimensions of interoperability, which interact within a broader political interoperability context, they are: organisational, legal, semantic and technical (cf. European Commission (EC), 2010a, p. 12). While these dimensions have been used as a basis for differentiation by several researchers, Scholl *et al* (2012) note that academic research has neglected the organisational aspects (similar to the case in studies of emergency response). Yang & Maxwell (2011) captured 11 factors, which influence information sharing in the public sector. Similar to the dimensions of interoperability identified by the EIF, these can be grouped as organisational, cultural, incentives/reward *vs* risk, political and technical. These dimensions emphasise the complexity of the inter-related factors that public safety organisations are likely to experience in trying to achieve interoperability.

Given this complexity, a challenge for management IS scholars is the lack of conceptual frameworks to drive studies of the scale and complexity of information sharing and interoperability in inter-organisational and high-volatile, stressful and fast-paced environments. These gaps highlight fundamental theoretical openings and challenges for praxis. While useful for explaining the behaviour of individual users, of various distinctions, traditional IS adoption frameworks on the implementation, adoption and use of ICT (Davis, 1989; Cooper & Zmud, 1990; Rogers, 2003) offer only partial insight into the difficulty concerning the institutionalisation of interoperable systems and congruent information-sharing practices, as they do not customarily account for cross-organisational, cross-regional and cross-national issues.

At the organisational, level, some theories of organisational behaviour and change have illuminated the broader organisational challenges. Here we highlight two that are particularly relevant. The first is the 'irreversibility-problem', where resources are committed in a particular direction because of previous investments, which are problematic to reverse, explaining how sustained directions of innovation are enabled, but how other directions tend to be constrained (Allen, 2000). This is evident in the case of interoperability where we see patchwork solutions rather than concrete action and reflection upon organisational information-sharing practices. Others have associated the lack of action by individual emergency services to Olson's (1965) 'logic of collective action'. That is, even though interoperability might be in the common interest of all public safety

organisations, individually they have little incentive to absorb the costs of achieving it; and as no one in the group will react if no other agency makes a contribution, there is little action (Brito, 2007). These help to shed light on the organisational challenges, rather than just the technological challenges that underpin the interoperability challenge.

At the individual, user level, a critical consideration for IS in emergency response is that first responders tend to revert to normal usage habits in times of crisis, rather than modifying their use to align with the system, which many agencies have patched together (Timmons, 2007). This suggests that developing systems (whether voice or data based), which are only deployed in crises may lead to ineffective usage (Manoj & Baker, 2007). This provides a caveat to the success of the 'emergency response use only' technical solutions currently heavily invested in. Therefore, alongside technological development and overarching institutional issues there is a clear need to understand the work practices of the target users.

The foregoing discussion raises two key issues concerning IS integration and more specifically information sharing and interoperability in emergency response: (1) interoperability and information sharing across agencies (and borders) remain problematic and should be framed by a range of non-technical issues including legal, political and cultural aspects; and (2) while there is a strong focus on technology development and patching current systems there is much less attention on how organisations themselves should change to improve interoperability and information sharing enabled by advances in ICT. Underpinning these issues is a lack of understanding of the nature of emergency responder work and the interplay between technology, information and the user in order to ensure that technological solutions are contextually relevant and appropriated into work practices.

On the basis of these fundamental issues, two exploratory research questions form the basis of our enquiry:

1. How do emergency responders communicate and share information in order to achieve a shared objective?
2. How do organisational rules and norms influence information sharing and interoperability?

These questions are not trivial. They have strong implications for design and may lead to some difficult reflection on organisational work practice and current approaches to addressing interoperability and information sharing. As such, the findings in this paper are relevant to the IS community, practitioners and policymakers interested in striving towards greater interoperability and information sharing among public sector organisations on a national and international scale. There are lessons to be learnt for private organisations in contexts characterised as complex, information intensive and where rapid decision making occurs in conditions

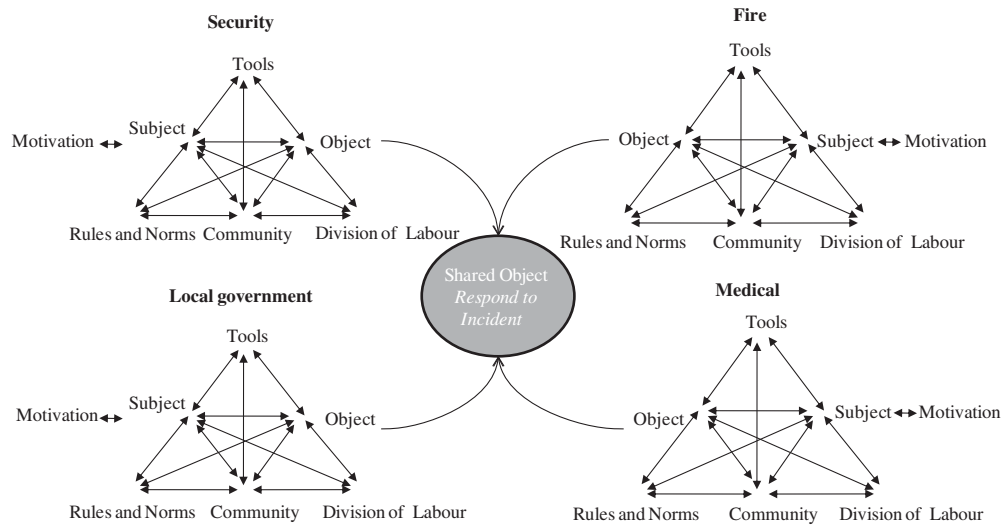


Figure 1 The shared object.

of uncertainty (Park & Ram, 2004; Hodgkinson *et al*, 2009).

Research setting and method

Conceptual framework

In order to answer the research questions, activity theory, which conceptualises the interactions between agents and their cultural–historical contexts (Vygotsky, 1978), is established as the conceptual framework. Rather than a theory that explains certain phenomena, activity theory consists of a set of basic principles, which can be used as a conceptual framework for enquiry, and a foundation for more specific theories (cf. Engeström *et al*, 1999b). Comparisons between activity theory and other contemporary social theories have been explored in detail elsewhere (Spinuzzi, 2008; Allen *et al*, 2011; Allen *et al*, 2013). Here we highlight several theoretical contributions that activity theory offers to this study. A focus on the ‘shared object’ of an activity is the first contribution. In activity theory the ‘activity’ is posited as the essential site for analysing interaction between actors and collective structures, and follows the argument that activity theory offers significant value in understanding activity ‘in context’ (Allen *et al*, 2011). Further, it provides a lens for observing the inter-connectivity between networks (Karanasios & Allen, 2013) of independent organisations (Engeström, 2001; Lyytinen & Damsgaard, 2011). The second contribution of activity theory is the achievement of the shared object (see Figure 1), which arises through the use of tools. The term tool refers to material tools and meaningful items such as signs, symbols, language and so on referred to by Ilyenkov (1977) as ‘ideal forms’. A third contribution is an understanding of the organisational ‘rules and norms’ that underpin the activity. This illuminates the organisational factors,

procedures and restrictions surrounding interoperability and information sharing.

A conceptualisation of these contributions is provided in Figure 1, which shows an emergency incident in which several agencies respond, and undertake distinct activities; however, they do so within the frame of reference of a common objective (the shared object). Further, such incidents are *ad-hoc* and the shared object is usually short-lived and once achieved each agency returns to its routinised and insular activities. This follows the notion of ‘knot-working’ (Engeström *et al*, 1999a; Lyytinen & Damsgaard, 2011), where groups of independent organisations come together to work on a shared object, then ‘un-knot’ themselves once the object has been achieved.

The studies

To answer the research questions we draw upon two studies that form part of broader programme of research spanning 10 years, which has focused on emergency services, IS and information management (cf. Allen *et al*, 2013; Allen and Wilson, 2004; Allen *et al*, 2011; Allen & Karanasios, 2011; Hassan Ibrahim & Allen, 2012; Karanasios & Allen, 2013). In line with the foundations of activity theory our research approach follows a critical philosophical perspective (Allen *et al*, 2013) and is concerned with understanding existing social systems in order to improve them.

As illustrated in Figure 2 the level of activity, and therefore response required to manage an incident, is at its peak during the initial response and consolidation phases of an incident, and it is on the initial response phase that we concentrate, where information sharing and interoperability has been highlighted as critical and has been the focus of scrutiny, significant investment and technology innovation. Therefore, the aim of this paper is not to look at the totality of the disaster cycle but to

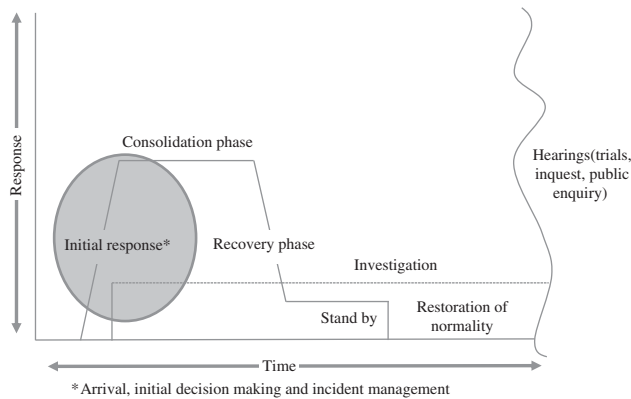


Figure 2 Stages of emergency response (LESPL, 2007, p. 8).

explore it within an initial response phase and the activities that occur at that stage.

The first study addresses the information sharing and work practices *in-situ* of services with a full set of civil protection duties, which are at the core of the response in most emergencies (such as the fire service). These are referred to as Category One responders (Cat1). This was a collaborative 18-month project entitled MAIS (Multiple Agency Information Sharing) involving a range of U.K. Government Agencies and Emergency Responders who supported the project by providing access to their staff, relevant documentation and financial support, and introductions to key individuals who had been involved in response to major incidents across the United Kingdom.

This project provided a base for understanding the need for interoperability and information sharing in context. Using a stratified purposeful sampling technique interviews were conducted with a mixture of senior (Strategic or Tactical command level) and operational personnel within a rural and urban fire and rescue service, police, ambulance, local and central government bodies. We also interviewed those involved in an emergency planning capacity and/or the development of policies, process and technology. In total 30 interviews were conducted across seven Cat1 organisations.

The second study followed on from the first and adopted a broader frame of reference by investigating interoperability and information sharing from the perspective of managers of individual agencies and individuals charged with improving interoperability of information and communication systems. We were given the opportunity to undertake this research by the National Policing Improvement Agency Multi-Agency Interoperability Programme who funded the research and provided access to their own staff, internal documentation and key stakeholders developing policy or managing programmes, which would influence interoperability for the management of major incidents within the United Kingdom. This provided a macro lens perspective on

the rules and norms surrounding incident management, the motivation behind certain ICTs used and the underlying organisational factors surrounding multi-agency interoperability and information sharing. The sample strategy used was guided initially by introductions to key informants involved in the emergency services and then the 'snow-ball' technique. In total 12 extended interviews were conducted. In parallel with these projects research was also undertaken on decision making and information sharing, which included observation of training events (Mishra *et al*, 2011) and critical interview techniques reported elsewhere (Hassan Ibrahim & Allen, 2012).

In other words, we captured the perspectives of the workers *in-situ*, of the managers of these workers and of those charged with improving information sharing and interoperability. The combination of the micro and the macro is fundamental to understanding the complex and multi-dimensional nature of interoperability and information sharing as both perspectives allow for greater understanding of how emergency responders achieve a shared objective within the contexts of both a broader set of organisational, technical and political factors and the independent work activities of the agencies involved.

Across both studies a small team of researchers conducted the data collection and analysis. Interviews were undertaken using a common interview schedule scaffolded by activity theory. Where the interviewee gave consent, interviews were digitally recorded and transcribed verbatim (or reconstructed from notes as soon as possible after the interview) and coded in Nvivo collectively by the research team (Weber, 1985). Data was initially free coded and axial coded. Through this early analysis we both formulated new questions for later follow-up interviews, and identified new subjects and other possible data sources.

While interviews formed the main source of data collection, across both studies, in order to maintain a critical perspective, we also undertook organisational scanning and the collection of supporting documentation. In this situation, organisational scanning was not limited to the individual organisation but to the type of organisation. For instance, the suggestion that 'incident action cards' used by the ambulance service should be examined in more detail led to an examination of this type of document from a number of ambulance services, not just those used by the organisations visited. Furthermore, to verify comments made by interviewees, we drew upon high-level reports and meeting minutes such as the workshop on interoperable communications for Safety and Security, involving EUROPOL and other policy-level organisations. Therefore, data was collected from a number of main sources (interviews, organisational documents, work documentation and meeting minutes), providing triangulation and a more holistic perspective as well as limiting the potential for bias that can arise from relying on a single data source. Such a pluralistic approach is an established approach in IS research (Trauth & O'Connor, 1991).

Data analysis

In both studies the conceptual framework in Figure 1 guided our analysis. In study 1, this is evident as we provide a detailed description of a response to a multi-agency incident on a chronological basis (initiation, arrival, management) and the work activities of the individual agencies as they worked towards a shared response, highlighting the relevant issues at each stage of the incident. This provides a lens to understanding the work activities of emergency responders in light of the shared object. In the second case, rather than focus on the incident level, we examine the views of those who are managing projects intended to deliver interoperability and improve information sharing among the agencies to better support the work activity. These efforts aim to lead towards the realisation of the shared object in Figure 1 through individual and collective information sharing and communication. This provides a lens to examine motivations, rules and norms and organisational issues surrounding interoperability and information sharing. The focus on the *in-situ* and macro-level perspectives provides greater insights into the research questions.

Study 1: information sharing and ICT in emergency response

Initiation of the incident A theme recurring throughout our analysis was that the information types required by an organisation are greatly influenced by the means by which it becomes aware of an incident. A senior fire officer interviewed commented:

the way it kicks off, would depend where we receive the initial call from, if it's a member of public then they wouldn't necessarily understand the magnitude of it, we would then cross-reference that with any supporting information or risk information that we would have.

Equally, a relatively insignificant event in a highly populated area may be over reported as several members of the public report the same incident. At this point the individual services hold data in separate systems, which are accessed by a human information intermediary in the command and control room (C&C). Each service then makes an initial decision on which resources to dispatch to the incident. While en route to the incident, further contextual information would be provided to the services attending, by their C&C room/function. In the United Kingdom, the different services will have different C&C functions, which are typically not co-located; even where they are, they may not be able to share data. As the services arrive at the incident, information is fed back primarily by voice to the C&C and by voice (by radio) and data (using in-vehicle mobile data terminals) to the services. This means that the activities of the personnel on the ground concentrate on information types that are seen as core for their organisation's response; these personnel do not receive information from other services, nor are they delivering information to

those services; thus, for a fire and rescue service information on the location of hydrants, water flow rates and so on would be relevant but this information would not be relevant to either police or ambulance services. All of the agencies indicated that any assessment of information needs could only begin in earnest when a representative of their organisation arrived at the scene. The lack of communication between organisations at the start of an incident can also be a part of the genesis of a more holistic problem as it leads to a lack of a comprehensive understanding of the nature of the incident. For example, an ambulance worker noted when en route to Russell Square, one of the sites of the 7/7 bombings, that:

Now, equally the police didn't help because they were directing our resources to the bus [one of the four bomb sites], they didn't know, because they weren't talking to us and didn't know, we had two separate incidents

The respondent indicated ineffective information sharing contributed to the lack of a common operational picture resulting in resources being sent to one incident site rather than both sites.

Arrival at the incident Once personnel were deployed to an incident, the priority was for information to be delivered or gathered that would be useful in an initial risk assessment. The demand was for information about the current and immediate risks or hazards present at the scene and its use to try to determine the risk to organisational personnel and 'saveable' members of the public. As part of this dynamic risk assessment, there was also interest in information that could be termed mitigation information, such as water supplies and evacuation routes. However, it was noted that this information can be highly variable in both quality and quantity. Local knowledge of a station manager, crew members or a person with knowledge of the building (such as the fire officer who could share a local risk plan and plans of the building) was also seen as being highly valuable. Tied to this was the fact that information available to one service may not be available to another service. One respondent noted:

The stupidity of that is what we don't have. That is, what records the police may hold against a building and what information they may have

This view was emphasised by other respondents who indicated that they required real-time access to historical data held by other services. For instance, the police may know that there is a high probability of used syringes being present on the floor in a known 'drug house', which would pose a risk to fire officers entering the building or they may know that gangs operate in an area and are likely to 'bottle' (throw missiles at) an incoming fire engine; however, there aren't any formal mechanisms for this intelligence to be shared.

Beyond this, while the need for further contextual information about the situation was quite high, it was suggested that for managers on the ground, obtaining this information was a lower priority than 'taking action' or rather undertaking activity once risk had been established. This meant that the initial response following the risk assessment would generally be reflexive decision making based on pattern recognition *how does this current situation resemble a previous situation I have faced?* While driven by reflexive processes this seemed to be verified by a more reflective and deliberative form of decision making as information became available as one police officer interviewed commented *you can turn up at an incident and it might be similar on the face of it but what you have to do on the ground can be very different, it's hard to compare.*

One of the key issues hampering the successful exchange and sharing of information was the information overload that was felt *within* an organisation during the initial stages of an incident. As one senior ambulance officer commented:

In a major incident, you can end up managing four separate locations and the incident commander can say 'there is so much information – what do I need to know?'

Tied to this was the issue that services were unable to share information at the scene of an incident, because each was struggling to build its own picture of what was happening. Those responsible for, or with knowledge of, C&C environments also indicated that, at the start of an incident, the rapid and chaotic flow of information caused problems for those managing and allocating resources. A police officer commented:

There is just too much to deal with. So you need someone of a similar rank filtering the information for them – saying 'This is important, you need to action this'.

During the initial period of an incident, the major source of information for each service is often the affected local community or other members of the public who may be in the area. They are often confused or disoriented and their initial reporting may not be accurate. Trying to deal with and filter this, adds to the information overload effect, as services try to deal with conflicting witness accounts. For example, in reference to the 7/7 bombing, a member of the ambulance service noted that:

The thing is that when those [bombs] went off and people were going from all tunnels and self-presenting to us – it was very, very difficult to work out where things had occurred, a very confusing picture, of course they [other emergency services] were in the same situation and were directing resources with a similar level of confusion.

The relationship with control and the use individuals make of the control resource was seen to change very quickly during the opening stages of a response. In the fire service, for example, officers attempt to obtain

additional information from control, en route. Once on the scene, the pattern of communication changes; C&C makes more requests for information while the incident commanders are more likely to make requests for resources, and updates on when those resources will arrive.

Management of the incident ground One of the issues raised by respondents was the way organisational rules and norms promoted activity, which was independent of the other services. The most fundamental of these issues was described by a respondent as the norm of *getting on with our job*; each organisation (within the agreed frameworks) will have activities critical to their own processes, which means information sharing and related activities are limited unless they affect core activities. A member of an ambulance service illustrated this in terms of an incident he recently attended:

One of the biggest barriers you see is the isolationism. A prime example is a large fire that we turned up to last week, the police were there and the fire brigade was there – the commander didn't want to talk to anyone, anybody else...it's the mental thinking.

In a similar vein a police officer noted that 'I've been at incidents and you can be standing around waiting to speak to someone and you think "...I'll just get on with it"'. Along these lines another commented 'it's not a technology issue, it's a process issue, people are not doing what they should, rather they are doing what they can'. The technology structures deployed often reinforce this silo approach. During a major incident, for example, mobile Incident Command Units otherwise known as 'Forward Command Vehicles' are deployed to act as *ad-hoc* command centres for silver commanders (tactical coordinators of the incident). In the United Kingdom these are deployed for each service. For the fire service, for example, a forward command vehicle will form part of a unit coordinating the activity of fire tenders, other vehicles (e.g., 4 × 4 vehicles) and fire crews. For particularly problematic or protracted incidents a much larger Major Incident Command Unit will be deployed. These units vary in capability and are, again, provided for and used by single services. Information sharing occurs outside these environments at the command meetings, typically face-to-face. As important, the systems that are provided focus on gathering and sharing information of relevance to a particular service. As a member of the fire service noted:

What we don't have is a consistent tool for the management of information, do we? The stuff you are learning on the incident ground, whatever role, you are in, there is no methodology for capturing that or pooling – passing, that would be via radio, into a control room.

This is also reflected in the way that incidents are handled on the ground by the different responders. For the fire service, continuity on the incident ground was not maintained in the same manner as other services.

In the fire and rescue service as and when more senior personnel arrive, they take over the management of the incident, with little or no further input from the previous incident manager. As a result, the narrative that is built around the incident and the service response can be broken.

In the preceding case, we described the way in which the different emergency services share information to achieve a common shared objective (as described in Figure 1). We indicated that the technological tools provided for information sharing are not seen as a source of tension or contradiction and fit with the current division of labour. The flow of information was described as being vertical and hierarchical within organisations with the primary location for information sharing being the strategic apex. However, we also noted that the different services have similar structuring of the division of labour indicating that they have different rules and norms and use different ideal forms (language), which is a source of tension particularly at the strategic apex. This study drew heavily upon the views of those intimately involved in managing the response to major incidents. In the second study described below, we also focus on interoperability and information sharing in emergency response; however, we draw on the perspectives of high-ranking officials involved in the development of solutions to improve interoperability within the United Kingdom and European Union (EU).

Study 2: achieving interoperability

Having presented a description of multi-agency response to an incident and the interoperability and information-sharing issues surrounding the achievement of a shared object, here we present an analysis of the perspective of public safety managers charged with implementing initiatives to better support interoperability and information sharing. In particular, we focus on their views in light of the realisation of interoperability and information sharing at the incident ground. This helps to focus on the rules and norms of the individual agencies in the context of the shared object and more broadly the motivation of working towards interoperability and the organisational, political and technical influences in order to paint a picture of interoperability and information sharing, which we turn to in the discussion section.

Problem recognition and motivation The analysis of the data revealed an unequivocal recognition of the problem surrounding information sharing and some desire to move towards greater interoperability. At the same time, there was an underlying perception that while U.K. interoperability is desirable, cross-national interoperability is not a top priority, given that the United Kingdom is geographically detached from continental Europe. However, this perspective was countered by the realisation that while EU–U.K. interoperability is not an everyday concern, the lack of it exposes emergency services in the event of a major contingency. At the policy level it

was felt that there is value in working towards EU interoperability at the high level:

I think there could be value in it (EU interoperability), depending on what the issues we deal with are, for climate issues, or other threats and hazards, certainly, a mass terrorist event... then there would be value in a high level of EU interoperability, but we haven't come up with anything yet...they (the various EU projects) are not coming very well together to be honest.¹

Tools, division of labour and rules and norms In activity theory tools can be seen as consisting of both tangible forms (such as a technological artefact) and intangible or ideal forms (such as language). One of the most interesting revelations from this study was the clear recognition that the technological artefact was not seen as a barrier. The consensus was that 'technology is not the problem' but rather people and processes are the main problems behind the inertia in moving towards interoperable systems 'the technology is way in advance of procedural stuff'.

Technical problems were acknowledged as being relatively easy to resolve and the most challenging issues were not in the technical domain, but people issues [interoperability is] *about what processes are people using* and establishing the use of these processes through *training and culture change*. One organisational factor emphasised was interoperability surrounding classified data. Again, this is not a technical barrier but one of establishing processes and procedures for efficiently achieving the shared object. For instance, respondents indicated that during the Glasgow airport attack, in 2007, there were restrictions on what information could be shared, hindering group efforts towards the shared object. Unclassified data is, however, usually relatively easy to share across different voice and data systems, interoperability and organisational processes permitting.

A further issue raised was the use of language and terminologies; that is if emergency workers do not know the *common language* then it is impossible to communicate with one another as each is using different tools to achieve the object. For responders *in-situ* often there is uncertainty concerning what information can be shared and what types of information is useful to others and vice-versa:

Challenges are things like policy and procedures about what information we can and should share, and an absence of a policy that defines that we need to share this information, about how do we go about doing it

The above quote resonates closely with the views expressed of the activity *in-situ* concerning the lack of methodology for capturing or pooling information that might be relevant. This fragmentation has been identified as inhibiting effective multi-agency cooperation as it means that each organisation will be more likely to

¹Titles/positions/agencies are not revealed in the data analysis as the research took place under a non-disclosure agreement.

concentrate on 'their' sources of information and 'their' priorities, rather than the overarching shared object.

This echoes the theme underscored in the analysis of the activity *in-situ*, which is different forms of the division of labour predicated on isolated ways of working. This is a theme that was heavily emphasised, not just with regard to language, terminology and classified data, but also across all aspects of interoperability and information sharing. Individual processes and rules and norms, bound each agency and were not necessarily congruent with other agencies [*each agency*] *has different ways of working, doing their particular role without thinking about other emergency services*. Even in the isolated country case of the United Kingdom it was suggested that there is a reluctance of police services to share information with fire services. This further illuminates the narrow frames that the individual agencies work within and the lack of consideration given to the information and communication that may be of use between agencies.

One thing you tend to notice about large public organisations is that processes become embedded in the organisation culture and it is very difficult to change that

Here also it was suggested that current technology goes far beyond the capacity that it is currently applied, and little criticism was aimed at technology; rather, at the multi-agency level, culpability was blamed on a lack of policy and processes in place to allow interoperability, *getting people to come to the party* and establishing incentive and buy-in from the services, the absence of which hinder the technology from being used to its full extent.

Examining the range of solutions currently under investigation, both nationally within agencies, regionally across agencies and across borders, it was acknowledged that there is a significant level of effort taking place, however, little cohesion has resulted, and efforts within the United Kingdom alone could be described as 'clunky', as individual agencies go about patching existing systems. While the technology may be proven to work in some cases, barriers in the form of politics and processes prevent these initiatives moving forward. For instance, policies surrounding one agency's handsets prevented them from being taken out of the country, which raises questions concerning their use in a potential EU-wide contingency.

Discussion

The data explored two fundamental questions concerning (1) how emergency responders communicate and share information in order to achieve a shared object, and (2) the organisational rules and norms that influence interoperability and information sharing. Here we provide a synthesis of the data analysis across these two studies and answer the research questions.

Information sharing

In this research, a picture was presented of independent activity systems with strong organisational norms

and rules and a division of labour based on hierarchies. This resonates with earlier work that described the organisation of emergency response by fire fighters as being close to that of a bureaucracy where the work is highly formalised and where there were specialised jobs within the system based on extensive and standardised rules and a clear hierarchy (Bigley & Roberts, 2001). Bigley & Roberts (2001) argued the organisations working within this organisational form that had the greatest potential for flexibility were those that gave more attention to connecting individuals understandings and communicating. In our research, we noted that the different emergency responders worked in separate bureaucracies each with their own set of norms and rules. While strong norms and rules are essential to management of the bureaucratic form they create a barrier to interaction and information exchange and make the creation of a common operational picture difficult. This was emphasised in both the *in-situ* analysis and the macro-level perspective [*each agency*] *has different ways of working, doing their particular role without thinking about other emergency services*. Similarly, McMaster & Baber (2012, p. 43) noted in their study of the multi-agency defence of the Walham electricity substation in the United Kingdom from rising flood water in July 2007:

responding organisations were actually working to slightly different priorities and making decisions based on different environmental cues, as well as on their own experience and expertise; whilst these priorities were broadly the same, their perspectives as to how these objectives were to be achieved differed to the extent that they conflicted

In Figure 3, we illustrate this through an activity system lens, using an example of the response activities of two agencies based on a synthesis of the studies.

It shows that while each emergency service may share the common object (management of the incident) they typically operate in an insular manner. Therefore, we see a fragmentation of the shared object. Each emergency service undertakes several actions (e.g., the police secure the perimeter, manage traffic and so on). However, these require little collaboration or sharing of information with other services. The division of labour within a particular activity system is constrained by the cultural-historical context in which it developed. For instance, in the case of police, the rules and norms that largely influence the activity system are those of routine general security or policing, rather than the anomalous and infrequent management of a disaster; these are very different rules and norms from the ambulance service (as are the actions, when taken in isolation). It is here, in the organisational rules and norms concerning working towards a shared object, that we see the greatest contradictions and highest barriers to improved interoperability and information sharing. It is also noteworthy that the division of labour does not strongly reflect a norm of informing other agencies of potential pertinent information. Another key point in the activity analysis is that

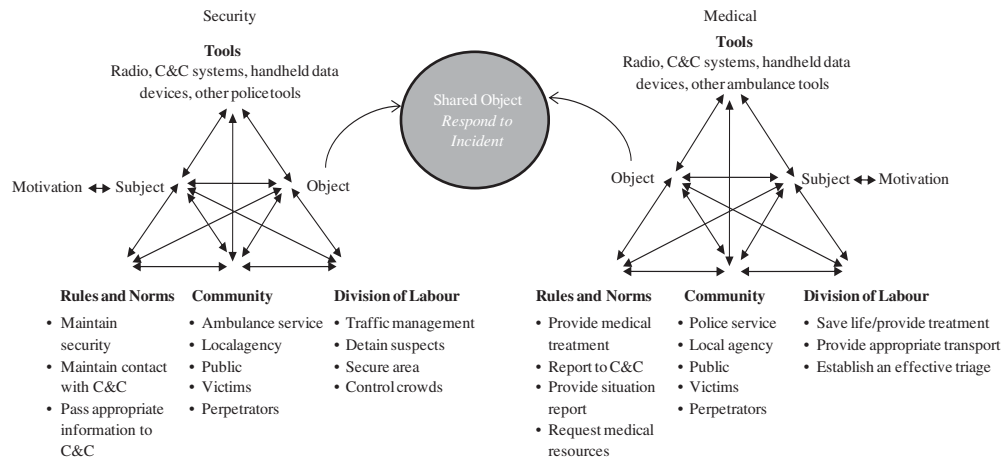


Figure 3 Response to an incident as a network of activity systems (two service response).

while the tools used are similar, information sharing remains problematic; the key issue here is how and when the tools are used (as described in study 1). These issues are discussed in detail below. This two-service example (Figure 3) raises a number of issues for interoperability and information sharing; however, if this example is then scaled up to involve other services, services from different regions within the same country, services from other countries and other organisations such as humanitarian agencies (e.g., Red Cross), local government agencies or private sector companies (e.g., utilities companies) then the scale of the organisational issues related to interoperability is evident.

Interoperability

While in our work interoperability was not explicitly raised as a fundamental concern, several critical instances were described where a lack of relevant information sharing or misinformation led to a series of safety issues. For instance, it was explained that during the 7/7 bombings ambulance staff were incorrectly concentrated at one of the bomb sites, instead of more evenly distributed to other bomb sites. There were also cases where relevant information available to one service was not available to another. For instance, the police may have information concerning threats at a building site that might be relevant to a fire service. Here technology and interoperability were not pinpointed as the underlying faults, rather the underlying processes to facilitate the correct sharing of information underpinned by organisational rules and norms were strongly reflected. As was noted in the first case, the primary focus of the services was on satisfying the information needs related to their own activity system, rather than sharing information, which allowed others to achieve the shared objective. Two issues were of particular interest: interoperability was seen as significant only at the strategic level and technology was not seen as a barrier to interoperability.

Where interoperability was referred to, it was mentioned in relation to communication between the strategic levels of the services to share information gathered from their respective organisations and coordinate activities. This in part reflects the bureaucratic and hierarchical approach taken to the management of major incidents in the United Kingdom where primary information flows are to and from the strategic apex. Information is collated at the strategic level, shared with other services and then communicated with a decision or instruction to the tactical and operational levels. The response to major incidents in the United Kingdom has also evolved within a cultural–historical context, which placed emphasis on the independence of the emergency services, allowing different norms, rules and approaches to the division of labour to be developed. When the services come together to deal with a major incident the integrity of the different organisations is maintained with their primary point of interaction being at the strategic level.

It was also clear that technological interoperability was not seen as a major obstacle to information sharing. A narrative was revealed by the research, which centred on several other more significant challenges, namely, (1) different services use different non-material tools leading to problems with semantic interoperability (e.g., a H on a map related to a hospital for the paramedics and hydrant for the fire officers leading to difficulties when sharing maps); (2) managing information overload, for instance, as the information flows a filtering process needs to take place to identify ‘what I need to know’ and uncertainty surrounds what information can be shared, and what is deemed important and useful by other agencies; (3) organisational issues around privacy and security and about what could be legally shared. Even the most sophisticated interoperability solution cannot overcome privacy barriers; (4) as noted in Walham the individual agencies also have different priorities and absorb/react to different environmental cues, suggesting

a bias in adopting a shared objective approach (as shown in Figure 3), one that presupposes a common objective. However, this lens does capture the combined outcome of overarching aims and the different priorities and outcomes of decisions of the individual agencies; and (5) a division of labour predicated on isolated ways of working.

Technology as the problem?

What is striking about the outline of the emergency response activity we sketched out in study 1 is an absence of fault attributed to the technology and integration of IS between work activity systems to allow for greater information sharing. This gathers further validation from the empirical data from the second study *the technology is way in advance of procedural stuff*. Recent case study research (Locatelli *et al*, 2012) also failed to identify technology as a barrier as did work into public sector information sharing (Yang & Maxwell, 2011). It is not technological interoperability that remains the problem, rather it is the organisational processes and other information-sharing challenges (as identified in the section 'Information sharing') that constrain interoperability. We note that the primary elements of the system are congruent and mutually reinforcing and deeply embedded in everyday practice. We characterise this as a form of 'cultural-historical structuralism', particularly evident in public sector organisations. This makes it particularly problematic to introduce new approaches to management and technologies for collaborative action, which may conflict with those deployed in routine action. This questions, for example, the ability of services to reverse the current model and put in place alternative matrix-based models of coordinating response to major incidents such as NetCentric approaches (Boersma *et al*, 2010) or Network Enabled Capability (Walker *et al*, 2008).

The current work practice of services responding to major incidents reflects the practice of the individual services in routine activity. This is enabled by a form of organisation and technology, which preserves the integrity of the elements of the activity systems while allowing coordination. This raises the issue of the potentially disruptive influence of the implementation of new technologies designed to support open communication between networked communities (such as social media) within such rigid hierarchical command and control systems. In activity theory terms such technologies could introduce contradictions, whereby the technology allows information sharing and interoperability but the organisational rules and norms do not. This contradiction between rules and norms and technology can lead to maladaptive changes. The impact of this on practice is that such technologies could damage rather than support coordination and effective response to major incidents. This in turn, perhaps explains why rather than focusing on transforming organisational structures, norms and values and processes to facilitate technology advances, the focus has been placed on how

technology can be shaped (and re-shaped) to fit and preserve the existing *status quo*, leading to patchwork technological solutions.

Routine vs emergency situations

As noted above, the analysis of the activity at the incident ground revealed important considerations concerning how responders behave during an emergency compared with more routinised activity and the consequences for information and technology use. For instance, our analysis pointed to the underlying decision-making processes where there is interplay between information-rich deliberative analyses and reflexive or intuitive decisions based on expert knowledge or knowledge embedded in policies or protocols. We found that when an incident commander or other person is engaged in an assessment of a situation, there is a tendency to try to match the current situation with those they have experienced previously (a form of sensemaking using heuristics or pattern matching) (cf. Timmons, 2007) and engage in reflexive rather than reflective behaviour. This approach resonates with the Naturalistic Decision Making (NDM) model, which suggests that experience helps decision makers to make rapid decisions as it acts as a source of information (Klein, 1989, 1997, 2008) by recognising patterns to fill information gaps and allowing them to respond quickly and reflexively. While the NDM model indicates that this is an effective form of decision making, others suggest that it can be a source of error and bias. Weick (1993), for example, indicated that during time pressure, people *regress to their most habituated ways of responding* indicating that people rely more on their past experience, which results in expectations and assumptions and thus undesirable outcomes suggesting that a more reflective information-based form of decision making is more effective. Further, work by authors on information behaviour and decision making in time-constrained practice suggests that in practice we see an interplay between both models in forming decisions (Allen *et al*, 2011; Mishra *et al*, 2011). The norm in emergency response is, however, to focus on the design of systems and processes solely to enable reflective forms of decision making, to de-legitimise reflexive decision modes and to focus on information flow to the apex of the organisation.

If this finding is allied with the earlier point that responders on the incident ground draw upon rules and norms developed within their own service to achieve a common object, this suggests that developing systems, which are used only in a major incident (assuming common norms and rules) may be problematic. Furthermore, any imposition of tools (both technologies and language) that would embed common rules may meet with resistance as they clash with service rules and norms intrinsic to routine practice. This is an interesting dimension that is not considered frequently by ICT adoption studies; that of technology fit to task *vs* familiarity, as the classical adoption studies typically neglect the complicated

dimensions of options and contexts, even though they do consider the perceptions of the user (Venkatesh *et al*, 2003). This provides a fruitful area for future research and provides further support for the view that ICT systems only deployed in crises are not likely to be effectively used (Manoj & Baker, 2007).

We would argue that there are a number of ways to increase adoption of systems developed for *ad-hoc* inter-organisational information sharing in high-velocity environments. The first way to encourage use of interoperable systems is to integrate systems used in major incidents into everyday operations to make sure they are actually used (SAFEKOM, 2006; Bharosa *et al*, 2010). The integration of systems used during major incidents into routine work practices may help resolve the contradictions between tools and rules and norms and lead to more effective use during disasters. The second is to move towards common norms and rules and language, which would then resolve the contradiction between tools and rules and norms and allow the shared use of locally developed existing systems. The third, and more radical, approach is to use new and emerging technologies to redesign activity systems, moving to alternative decentralised forms of organisation such as the Netcentric approach (Boersma *et al*, 2010). Others have suggested that one key element in resolving interoperability is through both human and technological information gateways or interfaces (Lee *et al*, 2011), which bridge the different services to overcome information problems. This final approach allows the maintenance of the bureaucratic form.

While some scholars suggest that there is still lack of clarity in demand for interoperability (Baldini, 2010), in harmony with broader European goals of integrations (EIF, 2004; European Commission (EC), 2010b) this study lends support for greater integration of information and communication systems across in the United Kingdom and across continental Europe. This was implicit in study 1, where there were clear examples of situations where a lack of information sharing had severe ramifications. In study 2, this was more explicit with statements such as *I think (EU interoperability) is definitely desirable and probably necessary especially if you look forward to 2012 (Olympic Games)*. While there was a balance of opinion leaning towards greater integration, the range of technical solutions available was described as 'clunky' and there was a concern at the lack of progress. This concern has been raised by previous researchers who commented that some solution strategies currently being pursued may actually make matters worse, instead of better, despite massive grant funding to improve communications (Timmons, 2007). Another issue is where interoperability is positioned. It was clear that when at the incident ground there is a clear demand for interoperability and information sharing at a strategic level, however, as long as a hierarchical C&C model is preserved the occurrence of interoperability at a lower level seems more problematic. Equally the challenging nature of organisational

change provides a more problematic view. The analysis suggests that there is a demand for interoperability, but what is perhaps missing is a better understanding of information challenges around building sound interoperability solutions and a bias towards technological solutions. It is only when the technology solutions are considered in light of the extant organisational rules and norms, the relationship between material tools and ideal forms, and information sharing challenges that effective systems can be developed.

This is highlighted in the analysis that revealed several factors that problematise greater interoperability between information and communication systems, which are instructive for understanding the broader challenges for inter-organisational interoperability: (1) rigid organisational structures *the technology is way in advance of procedural stuff*; (2) a silo approach towards achieving a shared object *[each agency] has different ways of working, doing their particular role without thinking about other emergency services*; and (3) issues surrounding concerning classified data and trust. These are significant organisational and political hurdles and perhaps, explain why progress at the moment is at best disjointed and described as being in the *too hard basket*, as characterised by an interviewee in the second study. Tackling this issue would involve overcoming the 'irreversibility-problem' (Allen, 2000) and addressing the 'logic of collective action' (Olson, 1965), which would require political will and possibly radical strategy.

As underscored, there is a bias in viewing information sharing and interoperability as a technical matter, which is not reflected from either the micro or macro lenses applied in this paper. Views from Cat1 responders and officials involved in interoperability projects support the contention that current technology goes far beyond the capacity currently applied in emergency organisations. This is a consideration that has been largely ignored, except by a few (Brito, 2007; Baldini, 2010), and one that policymakers, public safety leaders and system developers should be aware of.

Conclusion

In focusing on information sharing and interoperability in partnerships that occur between temporary organisations in high-velocity environments we have identified a number of issues, which are relevant both to IS research and practitioner communities. Drawing upon empirical data from both studies we argue that rather than focusing on interoperability as a primarily technological issue it should be managed as an organisational and informational issue intrinsically linked to norms and values. An alternative narrative arose from the analysis that differs from the typical calls for interoperability and rather explains that interoperability is underpinned by several information-sharing challenges that transcend technology issues.

This stands in contrast to current efforts to address this issue. Our study supports the argument that the

philosophy of designing systems specifically for major incidents is flawed. While there are a number of potential approaches we suggest that rather than designing for anomalous situations the emphasis should be on designing systems, which will function during routine situations and support anomalous ones.

In addition to identifying several information sharing challenges, significantly the work also emphasised that while the different emergency services had a common object (management of the incident) they typically operate in an insular manner. Therefore, we see a fragmentation of the shared object. Services undertook discrete processes or activities, which often did not require resource or involvement from the other services. This challenges the focus on interoperability at operational level or tactical level and increases the significance of interoperability at the strategic level.

While the organisational science and IS community have illuminated organisational change and IS implementation, these have offered only partial insights into the inertia concerning interoperability and information sharing as they do not customarily account for the cross-organisational, cross-regional and cross-national issues that bound the interoperability challenge. Using the notion of activity systems and the shared object we augmented understanding of intra- and inter-agency interoperability and the complexities surrounding information sharing. We

argue that change of this nature and scale requires procedural and strategic, operational and behavioural changes at the policy and agency level as well as a paradigm shift for system design.

Acknowledgements

The views expressed in this research are the result of two research projects: The first (Project MAIS) was supported by a number of partners including: Emergency Planning College, Norfolk Fire Service, London Ambulance Service, The Scottish Executive, West Yorkshire Police, The Department of Communities and Local Government, The London Borough of Greenwich and Lancashire Constabulary. The second was undertaken on behalf of the National Policing Improvement Agency (NPIA) Multi-Agency Interoperability Programme. The views expressed in this paper are solely those of the authors and should not be taken to reflect the judgement, understanding or opinions of any of the partners. We would like to thank Richard Baskerville and the anonymous reviewers for their support in developing the paper and Michael Hallows, Ex-Head of the Strategic Operations Unit, Director of the Multi-Agency Interoperability Programme at the NPIA and currently Emergency Services Commissioner, Victoria Department of Justice for his insightful comments. We would also like to acknowledge the work of the researchers who contributed to the projects: Dr. Nurain Ibrahim and Dr. Charles Knight

About the Authors

David Allen is Director of the AIMTech Research group. His work spans both the information systems and information science communities focusing on the way new technologies, especially mobile technologies influence information behaviour and practices. His work illuminates the significance of understanding information behaviour in the design, innovation, implementation and use of systems.

Stan Karanasios is a Research Fellow working in the AIMTech Research Group. He completed his Ph.D. at

Victoria University in Melbourne, Australia. His research and consultancy work covers evaluation and monitoring, project implementation, disaster response/emergency services and information management.

Alistair Norman is a Lecturer in Leeds University Business School and Programmes Manager for the AIMTech Research Group. His research focuses on the concept of mobility and the effects it has on the way that those equipped with mobile technologies undertake and manage their work.

References

- ALLEN D and KARANASIOS S (2011) Critical factors and patterns in the innovation process. *Policing (Oxford): A Journal of Policy and Practice* **5**(1), 87–97.
- ALLEN D, KARANASIOS S and SLAVOVA M (2011) Working with activity theory: context, technology, and information behavior. *Journal of the American Society for Information Science and Technology* **62**(4), 776–788.
- ALLEN DK, BROWN A, KARANASIOS S and NORMAN A (2013) How should technology-mediated organizational change be explained? A comparison of the contributions of critical realism and activity theory. *Management Information Systems Quarterly* [WWW document] <http://www.misq.org/skin/frontend/default/misq/pdf/Abstracts/AllenBrownAbstract.pdf> (accessed 9 May 2012).
- ALLEN DK, COLLIGAN D, FINNIE A and KERN T (2000) Trust, power and inter-organizational information systems: the case of the electronic trading community translease. *Information Systems Journal* **10**(1), 21–40.
- ALLEN DK and WILSON TD (2004) Action, interaction and the role of ambiguity in the introduction of mobile information systems in a UK police force. In *IFIP TC8 Working Conference on Mobile Information Systems* (LAWRENCE E, PERNICI B and KROGSTIE J, Eds), pp 15–37, Springer, New York.
- ALLEN JP (2000) Information systems as technological innovation. *Information Technology & People* **13**(3), 210.
- BALDINI G (2010) Report of the workshop on 'interoperable communications for safety and security'. European Commission, Joint Research Centre (JRC), Institute for the Protection and Security of the Citizen, Ispra.
- BARRETT S and KONSZYNSKI B (1982) Inter-organisational information sharing systems. *MIS Quarterly* **6**(Special Issue), 93–105.
- BHAROSA N, LEE J and JANSSEN M (2010) Challenges and obstacles in sharing and coordinating information during multi-agency disaster response: propositions from field exercises. *Information Systems Frontiers* **12**(1), 49–65.

- BIGLEY GA and ROBERTS KH (2001) The incident command system: high-reliability organizing for complex and volatile task environments. *The Academy of Management Journal* **44**(6), 1281–1299.
- BOERSMA FK, WAGENAAR FP and WOLBERS J (2010) Organizing emergent safety organizations. The travelling of the concept 'netcentric work' in the Dutch safety sector. In *7th International Conference on Information Systems for Crisis Response and Management (ISCRAM)*, Seattle, Washington DC, USA.
- BRITO J (2007) Sending out an S.O.S.: public safety communications interoperability as a collective action problem. *Federal Communications Law Journal* **59**(3), 457–492.
- CHEN R, RAO HR, SHARMAN R, UPADHYAYA SJ and CHAKRAVARTI N (2008) Emergency response information system interoperability: development of chemical incident response data model. *Journal of the Association for Information Systems* **9**(3–4), 200–230.
- COLES JB, ZHUANG J and YATES J (2012) Case study in disaster relief: a descriptive analysis of agency partnerships in the aftermath of the January 12th, 2010 Haitian earthquake. *Socio-Economic Planning Sciences* **46**(1), 67–77.
- COOPER RB and ZMUD RW (1990) Information technology implementation research: a technological diffusion approach. *Management Science* **36**(2), 123–139.
- DAVIS FD (1989) Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly* **13**(3), 319–340.
- DONG-HEON K and RAMAMURTHY K (2011) IOS resources, electronic cooperation and performance: a conceptual model. In *Proceedings of the 44th Annual Hawaii International Conference on System Sciences (CDROM)*, pp 1–10, Computer Society Press, 4–7 January.
- EUROPEAN COMMISSION (2010a) European Interoperability Framework (EIF) for European public services: Annex 2. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions 'Towards interoperability for European public services'*. Brussels, 744 final pages 1–35.
- EUROPEAN COMMISSION (2010b) The European eGovernment Action Plan 2011–2015: Harnessing ICT to promote smart, sustainable & innovative Government. *Communication from the Commission of the European Parliament, The Council, the Economic Social Committee of the Regions*. Brussels, 743 final pages 1–15.
- EIF (2004) European interoperability framework for pan-European e-government services. European Interoperability Framework, IDABC programme, European Commission, Belgium.
- ENGSTRÖM Y (2001) Expansive learning at work: toward an activity theoretical reconceptualization. *Journal of Education and Work* **14**(1), 133–156.
- ENGSTRÖM Y, ENGSTRÖM R and VÄHÄÄHO T (1999a) When the center does not hold: the importance of knotworking. In *Activity Theory and Social Practice: Cultural-historical Approaches* (CHAIKLIN S, HEDEGAARD M, JENSEN UJ and INTERNATIONAL SOCIETY for ACTIVITY THEORY and CULTURAL RESEARCH CONGRESS, Eds), p 381, Aarhus University Press, Aarhus.
- ENGSTRÖM Y, MIETTINEN R and PUNAMÄKI R-L (1999b) *Perspectives on Activity Theory*. Cambridge University Press, Cambridge.
- HASSAN IBRAHIM N and ALLEN D (2012) Information sharing and trust during major incidents: findings from the oil industry. *Journal of the American Society for Information Science and Technology* **63**(10), 1916–1928.
- HODGKINSON GP, SADLER-SMITH E, SINCLAIR M and ASHKANASY NM (2009) More than meets the eye? Intuition and analysis revisited. *Personality and Individual Differences* **47**(4), 342–346.
- IANNACCI F (2010) When is an information infrastructure? Investigating the emergence of public sector information infrastructures. *European Journal of Information Systems* **19**(1), 35–48.
- ILYENKOV EV (1977) *Dialectical Logic: Essays on its Theory and History*. Progress, Moscow.
- IVES B and JARVENPAA SL (1991) Applications of global information technology: key issues for management. *MIS Quarterly* **15**(1), 33–49.
- KARANASIOS S (2011) New and emergent ICTs and climate change in developing countries. Centre for Development Informatics, Institute for Development Policy and Management, SED, International Development Research Centre, Manchester.
- KARANASIOS S and ALLEN DK (2013) ICT and development in the context of Chernobyl nuclear power plant closure. *Information Systems Journal* **23**(2), [http://onlinelibrary.wiley.com/journal/10.1111/\(ISSN\)1365-2575/earlyview](http://onlinelibrary.wiley.com/journal/10.1111/(ISSN)1365-2575/earlyview) (accessed 9 May 2012).
- KLEIN G (1989) Recognition-primed decisions. In *Advances in Man-machine Systems Research* (ROUSE W, Ed), pp 47–92, JAI Press, Greenwich.
- KLEIN G (1997) An overview of naturalistic decision making applications. In *Naturalistic Decision Making* (ZSAMBOK CE and KLEIN G, Eds), pp 49–60, Lawrence Erlbaum Associates, Mahwah, NJ.
- KLEIN G (2008) Naturalistic decision making. *Human Factors: The Journal of the Human Factors and Ergonomics Society* **50**(3), 456–460.
- LEE J, BHAROSA N, YANG J, JANSSEN M and RAO HR (2011) Group value and intention to use: a study of multi-agency disaster management information systems for public safety. *Decision Support Systems* **50**(2), 404–414.
- LESPL (2007) Major incident: procedure manual. *Report-London Emergency Services Liaison Panel*. Norwich: TSO (The Stationery Office).
- LOCATELLI SM, LAVELA SL, HOGAN TP, KERR AN and WEAVER FM (2012) Communication and information sharing at VA facilities during the 2009 novel h1n1 influenza pandemic. *American Journal of Infection Control* **40**(7), 622–626.
- LONDON ASSEMBLY (2006) Report of the 7 July review committee. Greater London Authority, London.
- LYTTINEN K and DAMSGAARD J (2011) Inter-organizational information systems adoption – a configuration analysis approach. *European Journal of Information Systems* **20**(5), 496–509.
- MADLBERGER M and ROZTOCKI N (2010) Digital cross-organizational collaboration: a metatriangulation review. In *Proceedings of the 43rd Hawaii International Conference on Systems Science (CDROM)*, pp 1–10, Computer Society Press, 5–8 January.
- MANOJ BS and BAKER AH (2007) Communication challenges in emergency response. *Communications of the ACM* **50**(3), 51–53.
- MAYER-SCHÖNBERGER V (2005) The politics of public safety communication interoperability regulation. *Telecommunications Policy* **29**(11), 831–842.
- MCMASTER R and BABER C (2012) Multi-agency operations: cooperation during flooding. *Applied Ergonomics* **43**(1), 38–47.
- MISHRA JL, ALLEN DK and PEARMAN AD (2011) Information sharing during multi-agency major incidents. In *Proceedings of the 74th Annual Conference of the American Society for Information Science and Technology (ASIS&T): Bridging the Gulf: Communication and Information in Society, Technology, and Work (CDROM)*, New Orleans, LA, 9–11 October.
- NCTAUS (2004) 9/11 commission report. The National Commission on Terrorist Attacks upon the United States.
- OLIVER D and ROOS J (2005) Decision-making in high-velocity environments: the importance of guiding principles. *Organization Studies* **26**(6), 889–913.
- OLSON M (1965) *The Logic of Collective Action: Public Goods and the Theory of Groups*. Harvard University Press, Harvard.
- PARDO T and TAYI G (2007) Interorganizational information integration: a enabler for digital government. *Government Information Quarterly* **24**(4), 691–715.
- PARK J and RAM S (2004) Information systems interoperability: what lies beneath? *ACM Transactions on Information Systems* **22**(4), 595–632.
- PAWELCZAK P, VENKATESHA PRASAD R, XIA LGI and NIEMEGERLS M (2005) Cognitive radio emergency networks – requirements and design. In *IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DYSPAN)*, pp 601–606, Baltimore.
- PITT SM (2008) *Learning Lessons from the 2007 Floods*. London: Cabinet Office.
- RIETJENS SJH, VERLAAN K, ZAALBERG TWB and DE BOER SJ (2009) Inter-organisational communication in civil–military cooperation during complex emergencies: a case study in Afghanistan. *Disasters* **33**(3), 412–435.
- ROGERS EM (2003) *Diffusion of Innovations*. Free Press, New York.
- ROMANO NC, PICK JB and ROZTOCKI N (2010) A motivational model for technology-supported cross-organizational and cross-border collaboration. *European Journal of Information Systems* **19**(2), 117–133.
- SAFECOM (2006) Safecom: the road to interoperability. The Department of Homeland Security, Washington, DC.
- SAGUN A, BOUCLAGHEM D and ANUMBA CJ (2009) A scenario-based study on information flow and collaboration patterns in disaster management. *Disasters* **33**(2), 214–238.

- SCHOLL HJ, KUBICEK H, CIMANDER R and KLISCHEWSKI R (2012) Process integration, information sharing, and system interoperation in government: a comparative case analysis. *Government Information Quarterly* **29**(3), 313–323.
- SPINUZZI C (2008) *Network: Theorizing Knowledge Work in Telecommunications*. Cambridge University Press, Cambridge.
- TIMMONS RP (2007) Interoperability: stop blaming the radio. *Homeland Security Affairs* **3**(1), 1–17.
- TRAUTH EM and O'CONNOR B (1991) A study of the interaction between information technology and society: an illustration of combined qualitative research methods. In *Information Systems Research: Contemporary Approaches and Emergent Traditions* (NISSEN H-E, KLEIN HK and HIRSCHHIEM R, Eds), pp 131–144, Elsevier, Amsterdam.
- VENKATESH V, MORRIS M, DAVIS G and DAVIS F (2003) User acceptance of information technology: toward a unified view. *MIS Quarterly* **27**(3), 425–478.
- VERDECHO M-J, ALFARO-SAZ J-J, RODRIGUEZ-RODRIGUEZ R and ORTIZ-BAS A (2012) A multi-criteria approach for managing inter-enterprise collaborative relationships. *Omega* **40**(3), 249–263.
- VYGOTSKY L (1978) *Mind in Society: The Development of Higher Psychological Processes*. Harvard University Press, Cambridge, MA.
- WALKER GH, STANTON NA, SALMON PM and JENKINS DP (2008) A review of sociotechnical systems theory: a classic concept for new command and control paradigms. *Theoretical Issues in Ergonomics Science* **9**(6), 479–499.
- WEBER RP (1985) *Basic Content Analysis*. Sage Beverly Hills, London.
- WEICK KE (1993) The collapse of sense-making in organizations: the Mann Gulch disaster. *Administrative Science Quarterly* **38**(4), 628.
- YANG T-M and MAXWELL TA (2011) Information-sharing in public organizations: a literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly* **28**(2), 164–175.