

UNDERSTANDING THE BARRIERS TO THE INTEROPERABILITY OF DISASTER AND EMERGENCY MANAGEMENT INFORMATION SYSTEMS

E. Wilkinson ^{*1}

**Resilience Centre, Department of Defence Management and Security Analysis, Defence College of Management and Technology, Cranfield University, UK*

KEY WORDS: Disaster and Emergency Operations, Information Systems, User Requirements, Situational Awareness, Interoperability, Information Communication Technology (ICT), Information Exchange, Common Data Formats

ABSTRACT:

Emergency and disaster operations require a multi-agency approach to civil protection. However, agencies such as the police, the fire services, the health services and relevant non-governmental organisations display major differences in the way they handle information. This may be attributable to security rules, operational procedures, or even the culture that characterises each organisation. Situational awareness in a multi-agency operation is a key factor for the effectiveness of disaster and emergency response. Its enhancement is based on the building of a reliable Common Operational Picture, made up of information shared by the different teams of responders working together.

Interoperability describes the ability of systems to connect and exchange information so that they operate effectively together. This has been a long-standing requirement in the military domain, largely due to the demands of joint-service missions but also those of combined multinational operations. However, unlike the military, the civil protection sector is fragmented. Solutions for improving interoperability encounter difficulties in the face of such disjointed “markets”. The civil protection “market” does not provide clear directions for the Information Communication Technology (ICT) industry to meet the demand of commonly agreed data formats for exchange of information.

The efforts required for developing common data formats and driving them through lengthy standardisation processes may be seen as inefficient. This is particularly relevant to the fast moving ICT world where the risk of being outdated is high.

The paper suggests that in this context, the achievement of various local, regional or even national ICT strategies could be described as sub-optimal and that there is a pressing need for various stakeholders, and the user community in particular to agree on a common vision for interoperability.

¹ Resilience Centre, Department of Defence Management and Security Analysis, Defence College of Management and Technology, Cranfield University, Shrivenham, Swindon, SN6 8LA, UK – e.m.wilkinson@cranfield.ac.uk

INTRODUCTION

This paper addresses the issue of information sharing during response operations to disaster and emergencies. It focuses on the case of civil protection organisations that encounter multi-agency dealings every day. By and large, information is shared during the response to emergencies and disasters between organisations that have varied purposes and use differing processes. These exchanges are frequently described as key to the success of operations. Nevertheless, the sharing practices may be difficult as technology, procedures or even trust are not always in place to support them.

THESIS

This paper will not only examine information exchanges in their strictest technical aspects. It will examine the issue further than the dictionary definition² which characterizes interoperability as the ability of computer systems or software to operate in conjunction by considering the wider context of information sharing.

Firstly, this paper underlines what is at stake when sharing information by looking into some of the lessons learnt from the response to Hurricane Katrina. It shows that a common situational picture can only be created and is only useful when a structure of coordination mechanisms exist.

The background of the requirement for improved interoperability is explored in the second part of the discussion. Indeed, the EU's evolving strategy for Global Security will ultimately bring about more cases for inter-agency operations for which interoperability is critical.

A model offering a characterisation of the levels of interoperability is proposed in the third part of the discussion. The model describes each level by a form of output corresponding to a range of building blocks.

This paper then looks into the need for standardisation and the proposed solution of a Common Data Format by the EU FP6 funded project called Oasis.

SOURCES OF INFORMATION

The sources of information for this paper are mainly bibliographical and are also drawn from the authors' own experience in taking part in the conception and development of a Disaster and Emergency Management System. The bibliographical references used feature as footnotes throughout the paper.

² *The Concise Oxford English Dictionary*, Eleventh edition revised. Ed. Catherine Soanes and Angus Stevenson. Oxford University Press, 2006. *Oxford Reference Online*. Oxford University Press. Cranfield University. 28 Feb. 07
<http://www.oxfordreference.com/views/ENTRY.html?subview=Main&entry=t23.e29008>

FINDINGS AND DISCUSSIONS

The importance of building situation awareness through the sharing of information – the case of Hurricane Katrina

A striking example of the importance of information sharing can be found in a report³ to the US House of Representatives on the response to Hurricane Katrina. Although this Transatlantic account may seem distant and possibly irrelevant, some of the issues it raises are generic.

Following the 9/11 incidents, the US government had enhanced its framework for disaster and emergency response by creating the Department of Homeland Security (DHS) and developing the National Response Plan (NRP). During the response to Hurricane Katrina, although most emergency support functions were activated as prescribed in the NRP, it is reported that there was a major lack of situational awareness and disjointed decision making. “Too often, because everybody was in charge, nobody was in charge” as a consequence, valuable situational information was not provided to the White House and some of it was wrongly discounted (when actually accurate). The report believes that “earlier presidential involvement might have resulted in a more effective response”.

A number of coordination problems have their origins in the preparation for disasters and it is disturbing to read that top officials in the U.S. Department of Health and Human Services and in the National Disaster Medical System did not share a common understanding of responsibilities and controls.

In effect, it appears that deficient situational awareness was not present solely at the top of organizations nor on the ground, but featured right through the response apparatus. For instance, the Federal Emergency Management Agency (FEMA) lacked knowledge of requirements and resources in the supply chain.

The military provided a key part of the response, but again the lack of coordination caused delays in the Department of Defence response. The report emphasizes that there was a deficiency in adequate information sharing protocols that would have enhanced joint situational awareness. It also outlined that a lack of communication equipment and interoperability contributed to poor ground coordination in the joint military, Coast Guard and National Guard response

Furthermore, failures in communications had a profound impact on the overall response by restricting Command and Control, constraining situational awareness, creating delays in the delivery of relief supplies and limiting officials’ ability to address unsubstantiated media reports.

The description of the response to Hurricane Katrina illustrates the difficulty in building reliable situational awareness in the midst of a crisis. It also shows that common awareness must be backed up by effective coordination mechanisms.

The evolving context – the EU’s recent approach to Global Security

For the EU, security is increasingly at the forefront of policies, although in the post Cold War era the EU has become less of a “consumer” and more of a “provider” in terms of security⁴. The EU has shown it is keen to preserve peace and security in its area of direct interest, but the difficulties in differentiating between internal and external policies are becoming more apparent.

³ Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, Tom Davis, Chairman. A Failure of Initiative - The Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina. (2006)

⁴ International Crisis Group. EU CRISIS RESPONSE CAPABILITY REVISITED. (2005). Europe Report N°160, .

European Security and Defence Policy (ESDP) is moving from concepts⁵ to reality. Whereas traditionally its focus has been on the enhancement of military capabilities, recent developments in capabilities have seen a shift to rapidly deployable, technologically capable and intelligence based forces structured and equipped to perform a wide range of tasks. The focal point of the EU approach now revolves around military capability shortfall, in order to obtain a level of readiness geared to prevent conflicts or assist stabilisation in post-conflict situations.

The EU civilian toolbox has not benefited from as much attention. Paradoxically, the development of civilian capabilities is crucial as civilian missions are increasingly more likely than “high-end military” ones. Several aspects of ESDP are described as non-military. These civilian crisis management capabilities are: policing; the administration of justice (rule of law); civilian administration; and civil protection. Their purpose is to allow the EU to provide the full range of assistance to countries in crisis and a number of organizations and bodies have been set up by the EU to address this issue. The Committee for Civilian Aspects of Crisis Management was established in 2000 to ensure coherence and completeness in the delivery of an EU response to crises and is assisted by Crisis Response Coordination Teams. Since 2001, the Conflict Prevention and Crisis Management Unit has acted as a focal point within the European Commission to look at the civilian aspects of Crisis Management. A joint Situation Centre has also been established (in 2003) to combine the military and the civilian instruments and to provide an operational point of contact at EU level within the Council. In addition, the provision of civilian capabilities were defined in 2000 and Member States pledged to provide 5000 police officers that could be deployed in 30 days as well as 200 experts in the fields of rule of law, civilian administration and civil protection.

The EU recently assessed its collective civilian capabilities⁶ for crisis management and began to articulate how these should be expanded, both in scope and quality. The subsequent agreement of a Civilian Headline Goal launched in December 2004 sets out a number of ambitions for the development of ESDP.

This initiative⁷ called for the development of capacities in order to allow the EU to:

- Deploy integrated civilian crisis management packages. The definition of these ‘packages’ and their tasks are derived from the specific needs on the ground and exploit the full range of EU crisis management capabilities.
- Conduct concurrent civilian missions at different levels of engagement. The EU should be equipped to conduct several missions concurrently, including at least one large civilian follow-on mission at short notice in a non-benign environment. These should be sustainable over a longer period of time
- Deploy at short notice. The EU should be able to take a decision to launch a mission within 5 days of the approval of the mission concept and certain capabilities should be deployable within 30 days of the decision to launch.
- Work with the military. The EU missions can be deployed autonomously or in close co-operation with the military. In the latter case, a coherent coordination of civilian and military means in response to crises should exist in order to allow the smooth transition from ESDP operations to long-term EC programmes. This requires a clear functional division of responsibilities and close co-operation in planning of ESDP efforts and exit strategies.
- Respond to requests from other international organisations, notably the UN.

⁵ International Crisis Group. EU CRISIS RESPONSE CAPABILITY REVISITED.(2005). Europe Report N°160. .

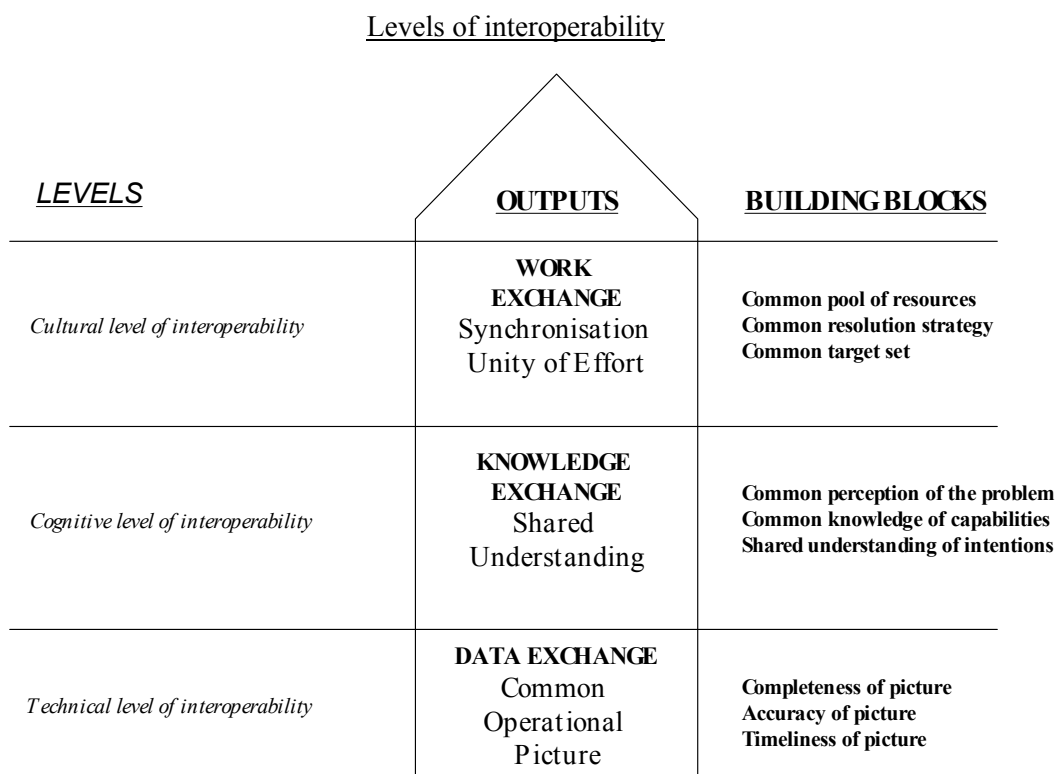
⁶ Isis. European Security Review, Number 25, EU Civilian Crisis Management : preparing for flexible and rapid response (March 2005)

⁷ EU security and defence.(2005). *Chailot Paper no. 75, Core Documents 2004, Volume V.*

It appears that the conduct of multinational security operations will increasingly have a multi-agency aspect to it. There seems to be a trend in associating military and civilian means in tasks such as conflict prevention, peacekeeping and tasks of combat forces in crisis management. Hence, the capability shortfalls within the EU should not just be assessed in terms of quantity or quality, but also very importantly, interoperability.

Defining levels of interoperability - the military benchmark

Interoperability is key to success in multinational operations. Military forces are aware of this fact due to their long experience of combined coalition operations. Much of the early research for greater interoperability has been conducted by the military. Recently, there has been a new focus to define the various levels of interoperability,⁸ which aims to bridge the gap between coalition partners' differences in doctrine, organization, concepts of operation and culture.



Model adapted from U.S.-CREST, RUSI,FRS, SWP. Coalition Military Operations - The Way Ahead Through Co-operability (2000)

This model suggests that there are various levels at which exchanges can be achieved when organisations work together. The basic exchange of data can be described as a technical level of interoperability. It aims at building a common operational picture in a timely, accurate and complete manner. An augmented exchange of knowledge will allow shared understanding of the situation. This can be described as a cognitive level of interoperability where information

⁸ U.S.-CREST (Center for Research & Education on Strategy & Technology), RUSI (Royal United Services Institute for Defence Studies), FRS (Fondation pour la Recherche Stratégique) & SWP (Stiftung Wissenschaft und Politik). Coalition Military Operations - The Way Ahead Through Cooperability - Report of a French-German-UK-U.S. Working Group.(2000).

exchanges are not purely descriptive. They are accompanied by a common perception of problems, knowledge of what tasks are being carried out to solve them and a comprehension of how this might have an effect on the situation. Further amplified is the work exchange, whereby the cooperating organisations work not just alongside each other, but actually share some of their tasks and synchronise their efforts. This improved level of interoperability can be referred to as cultural or doctrinal. It suggests that at a high level in the Command and Control chain there will be common definition of strategies and associated targets and a common pooling of resources.

The boundaries between these levels of interoperability are not clear-cut. Nevertheless, many examples illustrate that there are indeed a range of various levels of interoperability or information exchange.

This can be observed for instance through the confirmed interest of the US Department of Defence into effects-based approaches. An effects-based approach⁹ seeks to establish the “why” of a mission rather than just the “how”. Such an approach encourages a holistic approach where “all of the sources of power and influence that can be applied” and orchestrated so that the synergies that result in effects are greater than those that are additive. In his book, Smith (2006) highlights that “even though the info-structure has improved, being able to conduct effects-based operations has proved challenging” This is generally attributed to a lack of commonly defined “organizational processes, trained individuals, and appropriate tools.” Again this suggests that the issues of interoperability need to be tackled at each of the various levels and not just at the strategic or tactical level.

In the same way, a recent RUSI Paper¹⁰ suggests that the exchange of information is not necessarily impeded by technical constraints and that it must find its roots in organisational culture. In fact, an interoperability agreement drawn up in the UK between the emergency services illustrates just how this will change the culture from the top.

In recent legislation¹¹ to develop an integrated emergency management system, the British Government recognized that a fine balance must be found between making decisions based upon comprehensive and fit for purpose information and acting on that information as swiftly as possible. It underlines that “establishing systematic information management systems and embedding them within multi-agency emergency management arrangements will enable the right balance to be struck”. It also goes on to state that “terms and definitions should, wherever possible, come from national standards and publications rather than local initiative.... Otherwise, there is a risk that parochial usage may interfere with interoperability and co-operation with local partners and neighbouring areas and hinder co-ordination at the regional and national levels. The same applies to concepts of operation, doctrine and structures.”

The call for standards – the Tactical Situation Object as a proposed solution

It is a fact that interoperability relies on standardisation. In itself, the concept of standardisation is not highly controversial, but implementing it may prove difficult to achieve. Implementation requires political will to organise coherent procurement programs. More importantly it requires the resolve to update capacity, which equates to committing financial resources in the long term.

⁹ SMITH, E.A. Complexity, networking, & effects-based approaches to operations. Anonymous Library of Congress Cataloging-in-Publication Data (2006).

¹⁰ Bell, S. & Cox R. (2006). Communications Inter-operability in a Crisis. *Whitehall Report - RUSI*.

¹¹ HM Government. Emergency Response and Recovery, Non-Statutory Guidance to Complement Emergency Preparedness.(2005). , Chapter 2 - Principles of effective response and recovery.

The sources of standards in Europe¹² are varied and can be categorised as follows:

- single-company *de facto* standards;
- multi-company commercial standards, developed by trade associations or ad-hoc standards organizations, often leading to a patent pool;
- formal commercial standards bodies with mixed membership;
- government standards

For private companies, in the first two instances, it is easily understandable that there may be natural tension between two objectives¹³: on the one hand, protecting market share and establishing proprietary positions; and, on the other hand, opening markets through industry-wide acceptance for new technologies, particularly by having the technology accepted as standard. In the fast moving field of electronics and computing it is particularly important to plan technical developments so as to create a balanced portfolio of essential and non essential rights framed around a business strategy. Consequently, the selection of technologies to go through a lengthy and heavy standardisation process is a tricky issue which requires a thorough awareness of future markets. This possibly means that drivers are too weak and wrongly focused rather than barriers too great.

The ability to share information in a timely and secure manner is often critical to the conduct of operations. In order to enhance situation awareness and facilitate information exchanges, the definition of a "standard instrument" which carries the description of the tactical situation between systems is necessary. The OASIS project funded by the European Commission under the FP6 Information Society Technologies program has done significant work of this issue¹⁴. Its strategy has expanded to include the new CEN (European Committee for Standardisation) workshop to prepare specifications for the interoperability of information systems and further consultation on its work on the Tactical Situation Object" (TSO).

This interface is derived from a NATO standard and more details are available on the project web site. The TSO is able to vehicle the following type of information:

- Identification of the information: the identifier of this TSO, the originator of the information and the date of creation of the TSO,
- Description of the event: the type of the event, its extent, the number of casualties, the consequences on the environment, its criticality,
- Description of the resources: which resources are already used, which resources are available,
- Description of the missions: the tasks that are on going, their status, the teams and resources that are engaged for them and their planning.

Ultimately, this standardisation process should provide the market with the tools required for the operation of advanced systems deployed in disaster and emergency management and is expected to feed into the ISO - International Organisation for Standardisation (Technical Committee for Societal Security -ISO/TC 223) as a contribution to the international work plan for Societal Security standardisation (ISO/TC223).

Concluding remarks

¹² Dolmans M. STANDARDS FOR STANDARDS (2002).

¹³ Watts, J.J.S. & D.R. Baigent. Intellectual property, standards and competition law: navigating a minefield.(2002). Volume 2, Page(s):837 - 841 vol.2, .

¹⁴ See the OASIS project website: www.oasis-fp6.org

It is noteworthy that, in essence, the difficulty in understanding the markets of Crisis and Emergency Management Systems is inherent in the fact that these markets are fragmented. The division does not reside only in the lack of coherent acquisition contracts – a major barrier is that the various organisations involved in disaster and emergency operations do not adopt the same perspective when providing a response. Ultimately, their common purpose is about saving lives and recovering from crises, but as the police might need to focus on investigative aspects or the protection/restoration of a scene, the fire service will conduct search and rescue or fight fires and the ambulance service will attend to the health of casualties, sometimes with little consideration of other agencies' requirements. A joint response must offer a united vision of the 'why' and what is the overall strategy to all parties involved.

AUTHOR BIOGRAPHY:

Edith Wilkinson currently works for the Resilience Centre of Cranfield University on various EU-funded projects. The OASIS project aims to design and develop an open, modular and generic Crisis Management System in order to improve the effectiveness of the information sharing and interoperability of all agencies involved in disaster emergency response. The MARIUS project aims at developing a pre-operational autonomous initial tactical Command Post that can be deployed very quickly. Its set up and activation are aimed to support operations large-scale disaster or when existing arrangements are incapacitated.

She previously worked as one of the Cranfield Mine Action Team on of the revision of international mine clearance standards, developing sampling procedures for quality assurance of cleared areas.

Edith's background is in European affairs; she worked for the Directorate General for Research of the European Parliament and then as a Consultant monitoring and advising on EU policy.

She was educated in Montpellier (France), obtaining her first degree in Economics and an MSc in Statistics, and also at the University of Reading where she gained an MA in European Studies.