Interoperability: Diagnosing a novel assessment model

Sérgio Felgueiras
Lúcia G. Pais
Sónia M. A. Morgado
Major Events Laboratory, Research Centre (ICPOL), Instituto Superior de Ciências Policiais e Segurança Interna, Lisbon, Portugal[1]

Abstract

Today, uncertainty is what is most certain in our daily living. In the domain of security and protection, uncertainty becomes a critical condition for the decision-making process. Crowd's protection is a complex and arduous problem in what concerns to guarantee security and safety during mass gatherings. In Europe, after several terrorist attacks targeting crowded places, the first responders had to cooperate to mitigate the terrible effects of a terrorist attack, violence or an accident. The promotion of a better cooperation amongst first responders should be based on a multilevel interoperability model to solve potential and real coordination problems during rescue operations. It is clear that an interoperable system will respond in a better and integrated way to save lives. Preparedness is the key element. We all know that there are some traditional barriers for the interoperability implementation, such as technological, cultural, organisational and individual. The presentation of a general reflexion about the critical aspects of interoperability governance (plan, decision-making and training) tackles key issues such as innovation, harmonisation of safety and security culture, articulation of top-down and bottom-up approaches, operational procedures, technological support and general training. The discussion of a diagnosis model to assess the European interoperability continuum will give some food for thoughts to draft a roadmap to enhance the potential of each organisation and the overall interoperability system.

Keywords: diagnosis model, first responders, governance, innovation, interoperability

Introduction

´The two biggest challenges for police are interoperability and security between the information systems´ (Scarborough & Rogers, 2007: 666). In the domain of security and protection, uncertainty becomes a critical condition for the decision-making process. Crowd's protection is a complex and arduous problem in what concerns to guaranty security and safety during mass gatherings. In Europe, after the several terrorist attacks targeting crowded places, the first responders had to cooperate to mitigate the terrible effects of a terrorist attack, violence or an accident. But due to their diversity and the diverse multicultural approaches between European countries, and within the organisations, the response to critical incidents differs among them.

1 Corresponding author's email: sfelgueiras@psp.pt

Building trust between the different organisations involved in the first response activities is essential. Though, it may take too long to achieve regardless the urgency of the interventions, namely considering the jurisdictional disputes and the closeness of the organisations, their competitiveness, and the contemporary security demands. Sharing, integrating and managing of the information coming from the different stakeholders seems to be an impossible mission to accomplish.

This paper aims to contribute to the comprehension of the interoperability process, which considers different factors, dimensions, events and values of stakeholders, and helps to better understand how they can or interact in order to accomplish the interoperability potential. We propose to design a model for data collection and analysis that will allow the characterisation of the standard procedures as well as the malfunctions in each of the organisations studied. A survey will be conducted using this model and as a result it will help us to build a dynamic map where links and disruptions amongst them can be identified, thus enlightening us about current best practices and points of attention.

The usual focus for interoperability is information sharing (Allen, Karanasios & Norman, 2014; Chen et al., 2008; Desourdis, 2009; Miller et al., 2005; Thatcher, Vasconcelos & Ellis, 2015). However, working collaboratively implies achieving coordination between multi-team agencies at various levels. Therefore, the concept exceeds and goes beyond the strict sense of interoperability as information flows. For instance, the technological dimension is frequently approached on the basis of communications' equipment (Miller et al., 2005). Nevertheless, governance, usage, training and operations (Department of Homeland Security [DHS], 2005) are also elements for and of intervention with high levels of complexity that needs to be acknowledged.

In the context of multi-agency cooperation, interoperability is ´the capability of organisations or discrete parts of the same organisation to exchange operational information and to use it to inform their decision making´ (ACPO NPIA, 2009: 14).

The promotion of a better cooperation amongst first responders should be based on a multilevel interoperability model to solve potential and real coordination problems during rescue operations. It is clear that an interoperable system will respond in a better and integrated way to save lives.

Preparedness is the primary element. In fact, assuring readiness must rely not only on an adaptive response (Jenkins, 2006), but on a projected roadmap for first responders to deal with soft or hard incidents, in traditional or emergency missions, despite their unpredictability due to their dynamic nature.

This implies that police managers have to consider money expenditure, logistics, and opportunity-cost evaluation. In the end, the outputs of the organisations have to be questioned, and the whole missions will have to be reconfigured. A dilemma emerges: being focused on emergencies, routine activities are left aside... Regarding economic management, money expenditure in units that have to be stationed most of the time in a standby position is immediately questioned and put under criticism. Furthermore, it can be asked if this dilemma is pondered the same way by different organisations and in different countries, mainly if we bear in mind that the political climate may have a clear influence on these matters.

On the other hand, having a taxonomy and unifying procedures between first responders would ensure and improve the compatibility of approaches and interventions in critical incidents. As stated by Timmons (2007: p.3) 'it is imperative to devote resources to developing and implementing new procedures for responders during emergencies'.

And so, code sharing is essential for people to talk and understand each other. The human factor must be properly recognised, so the learning and training process is fundamental to raise awareness and thus improve the communication skills of everyone involved. This seems to be another item for proper consideration – the integration of these specific issues in the academies' curricula.

In this sense, not only the communication improves but also the decision-making process.

> ´More than a simple patch between two adjoining radio networks or a few officers talking on interoperability channels at a crisis, shared digital networks give all officers the ability to communicate with the right people to acquire the right information to accomplish their mission and solve problems whenever and wherever they need it.´ (Cowper, 2007: 1249-1250).

Some well-known traditional barriers for the interoperability implementation are technological, cultural, organisational and individual. Different organisations in the same country and in various countries as well, may be in different stages of development, acting based on different concepts of governance which are also differently operationalised.

Also, the constant technological development is another factor that separates countries, placing them apart from each other and thus compromising cooperation. The financial limitations police organisations are facing puts them in different levels of maturity in technological intervention. Therefore, they usually have a diverse perception of the same incident, and so engage in different activities to respond according to the organisational diversity.

In fact, some of the characteristics of the modern policing information technology systems, mentioned by Manning (2005: 230-231), such as the existence of ´nonlinked databases that are locally sourced, numerous software systems, the secrecy and nonlinked access points (multiple and incompatible channels of communication between the public and the police within the police department), the inconsistent user and backside technology interfaces, the tendency to use mapping information for short-term tactical interventions absent "problem solving"', must be overcome by coordinating with interoperability.

This fragmented approach may actually put people´s lives at risk. It seems imperative the first responders design a common language and method to boost the whole interventions. One of the best-known laws of Gestalt tells us that "the whole is other than the sum of the parts", so it seems mandatory to find a minimum common denominator. To accomplish this goal, different parties have to trust each other, understand the added value of interoperability, in order to pool and share resources, information, etc.

Building trust between stakeholders involves aggregating diverse information, models of intervention, eliminate isolated systems to manage and process information. The integrative and sharing mode would enable evocative information usage and boost operation, decision-making and security of crowds. The major problem here seems to be the time and length of the trust-building process because of the usual secrecy of police organisations culture. Thus, interoperability is the solution to facilitate data processing, management and decision-making.

A major question has to be answered: How to diagnose a model to assess the European interoperability continuum?

Method

General remarks

Building up a questionnaire demands to adequately address the issues that we want to learn about. First, we have to find out the proper dimensions to be addressed. Second, some linguistic precautions have to be taken, namely regarding the idiomatic expressions and some specific discourse technicalities, to maximise clarity. This issue directly links with the different professional specialities and organisations that will be under analysis. Also, the way the questionnaire has to be delivered must be taken into account – in this case, by mail.

Participants

The main idea is to apply this instrument in several European cities, in a multilevel approach (inter- and intra-organisation).

Procedure

The core dimensions were highlighted during the literature review and some (more or less) informal talks with operatives and experts in the knowledge domain. Also, they were based on the JESIP Multi Agency De-Brief Template[2] and the Homeland Security Interoperability Continuum (U. S. Department of Homeland Security, 2015). As far as the U.S. Department of Homeland Security (2015: 1) aims 'to assist emergency response agencies and policy makers to plan and implement interoperability solutions for data and voice communications', the JESIP template was designed to have a common approach for the post event assessment. Some examples of the dimensions are: context/framework, standard operational procedures, communication, and technology, amongst others.

2 www.jesip.org.uk/upload/media/pdf/JESIP_Interoperability_De_brief_.4.pdf

Results

Based on the specific goals established, some close-ended and open-ended questions were designed to collect different kinds of data. According to these different types of questions, statistical tests will be made. The questions will be ordered so that they follow each other logically and the diverse topics were organised clearly in between them. Demographic data is to appear at the beginning of the questionnaire, as usual. The questionnaire will be tested in different professional groups to ask for some feedback. The need for rewording or rephrasing, the order of the questions along the questionnaire, and/or the necessity of deleting or presenting new items, will be cleared in this phase.

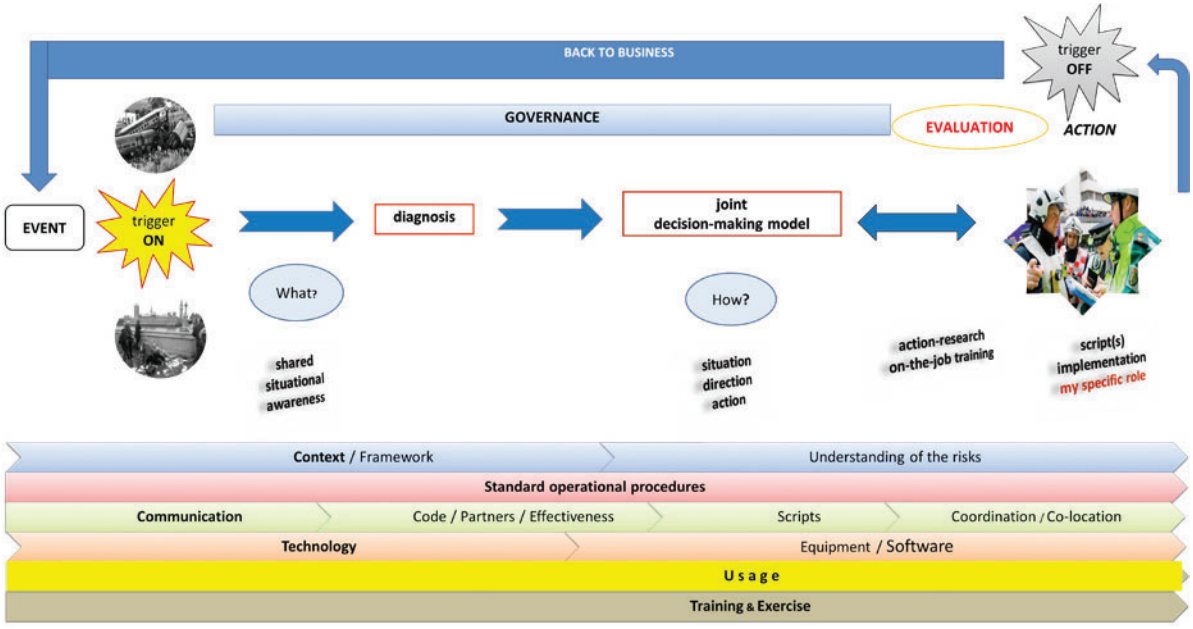
The meaning of interoperability in first responders is both intrinsically complex and dynamic and tends to fluctuate with context, type of event and time of occurrence. We intend to gather information about networking, processes involved, and technologies applied to improve interoperability, reliability and security.

We intend that interoperability involves a chain of processes (see Figure 1) starting from the event characterisation which according with its nature, context, etc. may or may not demand an interoperable approach. So, the first decision to make is to classify the event and, consequently, involve the necessary types of first responders. The proper identification of the concrete problem (or problems) at stake imply the existence of a shared situational awareness, and must consider the context features and the diverse institutional frameworks. This will permit to answer the main question in the first moment: What is happening? This is the phase in which the diagnosis is performed. At this stage, the conditions for the emergence of a common vision about the event should be met.

For this to happen, communication is crucial. It will allow to establish the necessary common-code to promote the effectiveness of the whole response. A common-code as well as a shared understanding of the standard operational procedures, supported by the technologies, may answer the second major question: How to deal and solve the problem? In this moment, it is possible to envisage a joint decision-making model and define the action course to manage the risks and implement the agreed scripts where each partner knows his role within the event operational coordination.

The after-event phase should let everybody go back to business. By then, it is possible to evaluate the whole operation, mainly in what concerns governance, data and information sharing, use of technology and the effectiveness of communication. In a word: Interoperability.

Figure 1 – Conceptual model of intervention



Therefore, the results of the survey to be conducted, that is the first stage of the process, will allow for a close picture of the interoperability situation in several European cities, according with the conceptual model of intervention. Actually, systemising the issues related to interoperability, acknowledges services, information and processes features, being the core and leverage for building a model that can be used to good governance in action. Considering the questionnaire also as a methodological tool for collecting data concerning the entire intervention, it is an action-research tool, and its results provide elements to conduct on-the-job training for all first responders' organisations.

Discussion

As stated by Allen et al. (2014), interoperability should be managed in organisational and informational aspects, developing systems that work in either routine or anomalous situations, within a common framework and taxonomy concerning procedures, working practices and harmonisation of first responders.

Building a cohesive interoperability platform would ensure that end-users can combine strategies and interact in order to serve a common purpose, regardless the differences between the services.

As so,

— the harmonisation of the different organisations regarding its subcultures, and in terms of the safety and security culture,
— the articulation of top-down and bottom-up approaches, operational procedures, technological support and general training,

will demand for a new and innovative decision-making model, that will withstand the reflexion about the critical aspects of interoperability governance and compose solutions highly optimised towards the needs of the first responders.

House, Power and Alison (2014) also argue that in the actual conceptualisation decision-making is at risk, considering that a non-hierarchical and decentralised network would benefit interoperability.

The diagnosis model as a roadmap for first responders can be considered a win-win situation. Its benefits for the intervention in different kinds of events seems obvious. It would increase the trust between partners, enhance collaborative processes, improve the homogeneity of process and information systems, and decrease disruption in data integrity that affects the collaborative processes, thus decreasing the responsibility and accountability gap.

References

- ACPO NPIA (2009) *Guidance on Multi-Agency Interoperability.* Available from: http: http://library.college.police.uk/docs/acpo/Multi-agency-Interoperability-130609.pdf [Accessed 10th January 2018].
- Allen, D. K., Karanasios, S. & Norman, A. (2014) Information sharing and interoperability: The case of major incident management. *European Journal of Information Systems*. 23 (4), 418-432. doi:10.1057/ejis.2013.8
- Chen, R., Sharman, R., Chakravarti, N., Rao, H. R. & Upadhyaya, S. J. (2008) Emergency response information system interoperability: Development of chemical incident response data model. *Journal of the Association for Information Systems*. 9 (3), 1-8.
- Cowper, T. (2007) Technology and the police. In: Greene, J. (ed.), *The Encyclopedia of Police Science*. 3rd ed. New York, Routledge, pp.1249-1250.
- Desourdis, R. I. (2009) *Achieving Interoperability in Critical IT and Communication Systems*. London, Artech House.
- House, A., Power, N. & Alison, L. (2014) A systematic review of the potential hurdles of interoperability to the emergency services in major incidents: Recommendations for solutions and alternatives. *Cognition, Technology & Work*. 16 (3), 319-335. doi:10.1007/s10111-013-0259-6
- Jenkins, W. O. (2006) Collaboration over adaptation: The case for interoperable communications in Homeland Security. *Public Administration Review*. 66 (3), 319-321. doi:10.1111/j.1540-6210.2006.00588.x
- JESIP (2015) *JESIP Interoperability De-Brief*. Available from: http: www.jesip.org.uk/upload/media/pdf/JESIP_Interoperability_De_brief_.4.pdf [Accessed 2nd November 2017].
- Manning, P. K. (2005) *Environment, Technology, and Organizational Change.* In: Pattavina, A. (ed.), *Information Technology and the Criminal Justice System*. Thousand Oaks, CA, SAGE Publications, pp. 221-239.
- Miller, H. G., Granato, R. P., Feuerstein, J. W. & Ruffino, L. (2005) Toward interoperable first response. *IT professional*. 7 (1), 13-20.
- Scarborough, K. E. & Rogers, M. K. (2007). *Information security*. In: Greene, J. (ed.), *The Encyclopedia of Police Science*. 3rd ed. New York, Routledge, pp.664-669.
- Thatcher, A., Vasconcelos, A. C. & Ellis, D. (2015) An investigation into the impact of information behaviour on information failure: The Fukushima Daiichi nuclear power disaster. *International Journal of Information Management*. 35 (1), 57-63.
- Timmons, R. (2007) Interoperability: Stop blaming the radio. *Homeland Security Affairs*. 3 (1), 1-17.
- U. S. Department of Homeland Security (2015) *Interoperability Continuum: A Tool for Improving Emergency Communications and Interoperability*. Washington, DC, Department of Homeland Security.