SECURE DYNAMIC CLOUD FOR
INFORMATION, COMMUNICATION AND RESOURCE INTEROPERABILITY
BASED ON PAN-EUROPEAN DISASTER INVENTORY

Deliverable 2.6 21st Century Crisis Management

Final

Edited by Paul Hirst
British APCO
March 2017

Work Package 2

Project Coordinator
Prof. Dr.-Ing. Rainer Koch (University of Paderborn)

7th Framework Programme
for Research and Technological Development
COOPERATION
SEC-2012.5.1-1 Analysis and identification of security systems
and data set used by first responders and police authorities

Distribution level		**Public**		
Due date		31/03/2017		
Sent to coordinator		26/03/2017		
No. of document		D2.6		
Name		21st Century Crisis Management		
Type		*Public*		
Status & Version		*Final version 1.0*		
No. of pages		*36*		
Work package		*2*		
Responsible		*BAPCO*		
Further contributors		*KEMEA, ULANC*		
Authors		*Edited by Paul Hirst*		
Keywords		*Practices, Standards, Guidelines, …..*		
History	Version	Date	Author	Comment
	V0.1	10/01/2017	BAPCO	For Discussion
	V0.2	09/03/2017	BAPCO	TO ULANC & KEMEA for comment
	V0..3	23/03/2017	BAPCO	For QA
	V1.0	26/03/2017	B-APCO	Final version incorporating all above

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n°607832.

Authors

British APCO

Paul Hirst
Email: paul.hirst@bapco.org.uk

Contributors

Mobilities Lab
Centre for Mobilities Research
Department of Sociology
Lancaster University
LA1 4YD
UK

Katrina Petersen
Email: k.petersen@lancaster.ac.uk

Centre for Security Studies (KEMEA)
P.Kanellopoulou 4
1101 77 Athens
Greece

Ioannis Daniilidis
Email: i.daniilidis@kemea-research.gr

Reviewers

Airbus Defence and Space

Olivier Paterour
Email: Olivier.Paterour@airbus.com

TU Dortmund
CNI

Daniel Behnke
Email: Daniel.behnke@tu-dortmund.de

Executive summary

The frequency of disaster events being natural disasters, terrorism, intense and protracted conflicts, corporate crises, threats to critical infrastructures (possibly to mega-events such as Olympic games) as well as related problems of governance, civil involvement and self-reliance take on new dimensions. Crises confront public authorities, corporate leaders and the public at large with challenges to the traditional policy assumptions of crisis management, having a wide, if not global impact, being difficult to contain in the short and long run, and generating diverging notions about appropriate solutions. The forms of crises have evolved too, with features such as severe threat, uncertainty, urgency.

The threats we face today are more numerous, more substantial and more complex than ever before. Threats of large-scale violence, such as terrorism and conflicts within and between fragile states augmented by new risks and crises (affecting our communications and information technology, food production, new viruses etc.). In comparison with the kinds of disaster we experienced in the past, today's misfortunes seem to elicit an unprecedented level of uncertainty and an urgent need for government intervention. This calls for policy that is focused on managing these threats to our national security.

This document will examine the history behind the concept of 'Crisis Management', before going on to examine the factors affecting change in the 21st Century, the variations in national models within the European Union and finally, will look at what the future holds.

Table of contents

1 Introduction

1.1 Purpose of this document

This document is included in the overall work plan of the SecInCoRe project under WP2.

The purpose of this document is to examine existing and emergent practices of crisis management, drawing on the implication not only of previous deliverables in WP2.
It also discusses the relationship of emergent crisis management models to the results of WP3 and WP4, including general how SecInCoRe's results in relation to information systems and data set use for information, communication and resource interoperability, business models, and barriers and opportunities for common information space technologies. Building on the previous deliverables, literature reviews, and advisory board workshops, this primary objective of this document is to present emergent crisis management models, exploring in particular the diversity of what the terms means and the new challenges and opportunities that are appearing as new technologies and are increasingly incorporated into risk management practices (T2.2). The second objective of the document is to draw out the ethical, legal and social issues (ELSI) challenges and opportunities, offering insight into how SecInCoRe addresses these (T2.3). It follows with a reflection on the implication of such socio-technical challenges for future design and crisis management to envision the shape of new crisis management models (T2.4).

1.2 Validity of this document

This document is not a report on technological developments: it is a research and literature paper on the history and current and future trends in crisis management and as such does not require quality assurance from a scientific or technical perspective, other than to ensure accuracy of reporting and content.

The analysis and conclusions in this document are based upon the empirical work, literature reviews, EIA, and PIAs, and Collaborative-Design Workshops that have been conducted to this point.

1.3 Relation to other documents

This Document is related to the following SecInCoRe project documents:

[1] Grant Agreement

[2] Consortium Agreement

[3] D2.1 (WP-2) – 'Overview of disaster events, crisis management models and stakeholders' [in the form of T2.1 as input to T2.2/T2.3/T2.4; T2.2 and as input to T2.3/T2.4]

[4] D2.2 (WP-2) – 'ELSI guidelines for collaborative design and database of representative emergency and disaster events in Europe' [in the form of T2.1 as input to T2.2/T2.3/T2.4; T2.3 and as input to T2.4]

[5] D2.3 (WP-2) – 'Report on Performance, Goals and Needs and First Draft of New Crisis Management Models and Ethical, Legal and Social Issues' [in the form of [T2.2/T2.3/T2.4]

[6] D2. (WP-2) – 'Domain Analysis: Baseline and Emergent Future Practices' [in the form of T2.2; T2.1 as input to T2.2]

[7] D2.5

[8] D3.1 (WP-3) – 'Setup of inventory framework and specification of research requirements' [in the form of T3.1 as input to T2.2/T2.3/T2.4]

[9] D3.2 (WP-3) – 'Second publication of inventory results including ethnography and holistic process models and statements on future evolutions' [in the form of T3.1as input to T2.2/T2.3/T2.4; T3.5 as input to T2.4]

[10] 4.1 (WP-4) – 'Requirement Report' [in the form T2.3]

Outputs:

[11] D2.7 (WP-2) – 'ELSI in Crisis Management through the Secure Dynamic Cloud' [in the form of T2.4]

1.4 Contribution of this document

This deliverable is a high-level research document which is not intended to contribute directly to the developments of the project: rather, it is intended to highlight the way in which crisis management is developing for the future and therefore, where the outcomes of the SecInCoRe project might assist in those developments.

1.5 Target audience

This document is for general publication and should be treated as a research paper for anyone with an interest in the subject matter.

1.6 Glossary

Acronym	Expression	Explanation
BCM	Business Continuity Management	
ERM	Enterprise Risk Management	
FA	Football Association	Professional football governing body
JESIP	Joint Emergency Services Interoperability Programme	UK programme
PPDR	Public Protection & Disaster Relief	

1.7 List of figures

1.8 List of tables

2 A Brief History of Crisis / Incident Management

The EU's increasing foray into crisis management, which began in the 1980s (Boin and Ekengren 2009;[1] Wendling 2010[2]), can be linked to at least three key forces. First, EU integration, which has meant that 'border thinking' when it comes to safety and security no longer makes sense (Boin et al. 2014a[3]). Second, various 'threat' events such as the fall of the Berlin Wall, terrorist attacks, large scale natural disasters, and disease pandemics (Boin and Ekengren 2009[4]; Boin et al. 2014a[5]; SEEDRMAP 2008[6]). Third, the strategic initiative of individual Commissioners (Wendling 2010[7]). Consequently, the EU has increasingly emphasised a comprehensive approach to crisis management (Attinà et al. 2014[8]; Boin and Ekengren 2009[9]; Tercovich 2014[10]).

However, there are signs that what this means is both changing and under debate (Pirozzi)[11]. Moreover, it is becoming increasingly clear that more traditional ways of managing crises no longer suffice (Attina et al. 2014)[12]. A major impetus for such changes is the increasing scale and frequency of disasters. Another confounding factor is emerging information and communication technologies (ICT) that have the potential to increase collaboration and coordination while changing the expectations of what communication is and does in relation to disaster response. The EU has been focusing on developing new tools and technologies to enhance coordination of the various instruments at its disposal (Al-Khudhairy 2010)[13].

In order to better understand these changes, this document examines historical and emergent socio-technical elements that comprise these changes in order to better understand the future directions, challenges, and opportunities crisis management faces. As a starting point, this chapter offers an overview of the emergence of crisis management in the EU as a concept and frame of practice. This sets the backdrop for the following chapters that explore emerging ICT and their implications for crisis management.

2.1 20th Century – 21st Century

There is some difficulty in comparing crisis management as a 'discipline' from the previous century to the current one: the key reason for this being that the subject was not really referred to as a concept until just over 30 years ago. The pace of change over those intervening years has been rapid, which made defining crisis management models a continual challenge and an on-going process. Even with increasing documents and directives within the EU intended to co-ordinate what this means conceptually and in practice, there is still no clear notion of what a 'comprehensive approach' between EU nations is (Tercovich 2014).[14]

Looking back to when crisis management as a discipline started to emerge, it is helpful to look at the social, political and technological complexities of that time period. To go back to the European Union in, for example 1985 (which seems to mark a significant turning point in various technologies), would see Spain and Portugal in the process of joining; Greenland in the process of leaving; the issue of the first European passports; and the beginning of the Schengen agreement on the elimination of border controls, signed by Belgium, Germany, France, Luxembourg and the Netherlands. 1st January 1985 saw the first public mobile telephone call made in the UK. The internet did not really exist in the public consciousness; indeed the domain-name system only came into being on that same date and Microsoft Windows v1.0. was released in the November of

that same year. Emergency service communications were generally UHF / VHF analogue and the fixed-line telephone. Such incident management systems as were then in existence were usually custom designed, 'green-screen' or monochrome and based on nothing more sophisticated than MS-DOS. In most cases, there was no need to define labels such as the 'command and control' system as there were few, if any other systems to distinguish it from: it was simply 'the computer'.

Perhaps of significance in the context of this paper, 1985 alone saw:

- large-scale public disorder at a Luton -v- Millwall football match
- Bradford City stadium fire, killing 56 and injuring at least 265
- The English FA bans all clubs from playing in Europe following the Heysel riots.
- Manchester air disaster – 55 dead when Boeing 737 burst into flames
- A riot in Brixton, London erupts after accidental shooting of a woman by police
- Polish police arrest seven members of the 'Solidarity' group
- 150 killed when Spanish jet crashes on approach to Bilbao airport
- Mikhail Gorbachev replaces Konstantin Chernenko as Soviet leader
- 'Communist' bomb attack kills 2 firemen in Brussels
- Booby trap bomb kills 86 people in India
- Israel exchanges 1,100+ Arab prisoners for 3 Israeli soldiers
- Bomb destroys Air India Boeing 747 in air near Ireland, 329 die
- Val di Stava Dam in Italy collapses killing 268 people
- Earthquake in Mexico kills 2000 people
- Nevado del Ruiz volcano erupts in Colombia, killing 25,000

In terms of disasters, 1985 may not have been an exceptional year but perhaps taken together with advances in technology around the internet and mobile communications and key political changes, the mid-to-late 1980's might well be seen as a period where the need to collaborate and co-operate was increasing, but for the first time ever, the ability to be better able to do so was starting to appear.

The frequency and intensity of natural or man-induced disasters has increased over the last few decades, accounting for huge cost in both lives and property[15]. Public Protection and Disaster Relief (PPDR) agencies, also known as first-responders, are the primary forces dealing with incident response. These agencies operate now as they always have; in a hierarchical structure, working together to take decisions, identify strategy and tactics and to manage the incident through to its conclusion. Relatively recent improvements in communications and computer-based information retention systems has improved the ability to work in this way, although the lack of true interoperability is still some way off. Many agencies throughout Europe operate on independent systems, either at an organisational, regional or national level. This is not driven by a desire to remain autocratic, but is often due to organisational governance and (most often) budget restrictions. Other obstacles might include the lack of a common reference vocabulary

– even in the same language, across organisations. One example which comes to mind is a simple one: in Police Force A, the Operational Support Unit (OSU), is a unit, which supports front-line officers by taking statements and interviewing witnesses; in Police Force B, the OSU is the provider of specialist firearms and public-order officers. Other issues at higher levels include cross-border and trans-national collaboration and the spoken languages. In the latter case, even given a common language (for example English in the EU), there is always a difference between learnt English as a second language and the colloquial English spoken by natives of the UK.

These PPDR organisations traditionally deal with an incident from its inception until the point where it no longer requires such services – the point where a process of 'return to normality' commences. For example, a large-scale forest fire will require PPDR organisations to manage, contain and extinguish the fire; to warn and evacuate residents and visitors; and to maximise public safety in the affected area. Once the fire is extinguished and the area declared safe, their services are no longer required but the 'incident' is not finished: homes must be rebuilt, trees replanted, debris cleared, services replaced, costs assessed and compensation paid. The fire may last a few days, but the overall incident and the impact from it will run for many months, if not years.

The description of a major incident as defined in the diagram below is accurate, though simplistic. It commences at the on-set of an incident and applies to those agencies with a responsibility for managing the incident. In many ways, though necessary to serve its purpose within a larger publication[16], the diagram largely ignores the ongoing, detailed and often complex processes of contingency planning, training and general preparedness which takes place on an on-going basis behind the scenes.

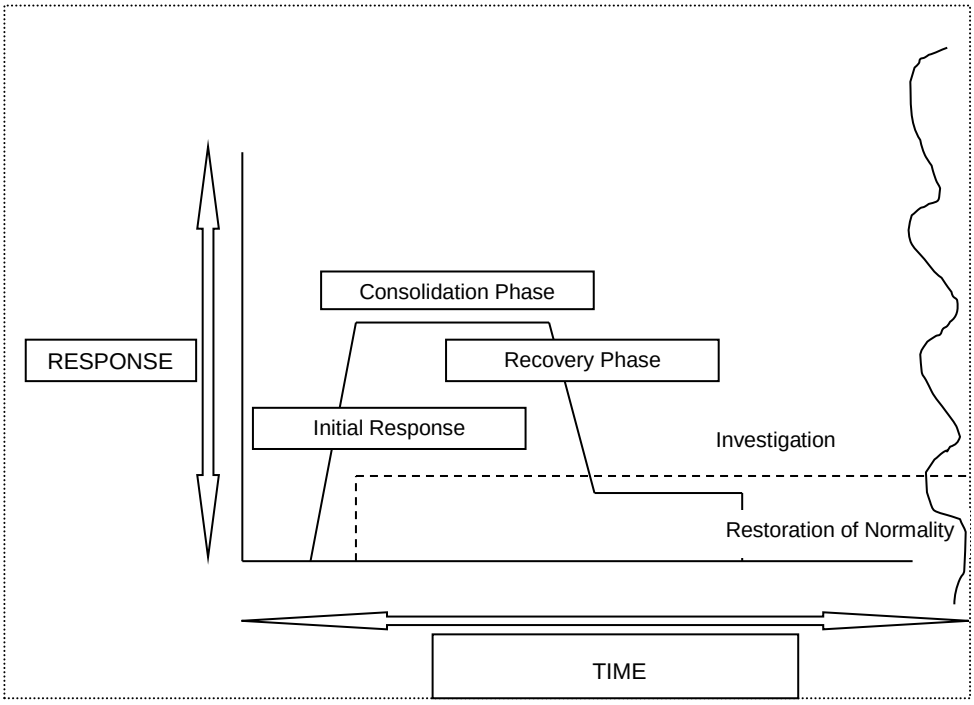

Figure 1: Stages of a Major Incident

It is argued that this is the area of most significant change in disaster management in recent years. It is a change which affects a far wider sphere than simply PPDR organisations. Previously little-used phrases such as 'business continuity' and 'organisational resilience' not only affect many businesses and other organisations but have in themselves resulted in the formation of a whole new area of education, service delivery, consultancy under the banner of 'risk-management'.

As one organisation states in its internal policy document[17]:

> Business Continuity Management (BCM) is a core component of good governance and is integral to our Enterprise Risk Management Framework. Business Continuity Management is applied across the entire organisation – central office divisions, regions, schools and TAFE institutes.
>
> Business Continuity focuses on our capacity to achieve our objectives.
>
> Our first priority in the case of a disruptive event is the immediate and ongoing safety of customers and staff. Department for Education, Training & Employment's (DETE) emergency management arrangements help us to be prepared for, and respond to emergency situations.
>
> Following the event, we will ensure that our critical services are operating, and that normal business is resumed as quickly as possible.
>
> Finally, we will learn from our experiences of disruptive events to minimise (where possible) their likelihood and consequence in the future.
>
> The BCM Framework links with DETE's emergency management arrangements and with whole of government business continuity arrangements. The Department of Premier and Cabinet has endorsed security and response strategies to increase government agency preparedness for critical incidents including:
>
> - Queensland Plan for the Protection of Government Assets from Terrorism
> - Queensland Pandemic Influenza Plan
> - Brisbane Central Business District Emergency Plan

The short introduction to this document succinctly describes the circular process of learning: preparation, response, recovery and finally, lessons learned fed back into preparation processes.

3 Factors for change into the 21st Century

New and emerging information and communication technologies can transform crisis management models and disaster risk management practices. They have increasing flexibility and capabilities, pairing well with the standard yet improvisational needs of command and control functions and creating shared situational awareness. They act both as sources of data as well as represent techniques for extracting data, analysis, information sharing and management, leading to challenges both in retrieving data and extracting information from that data (Al-Khudhairy 2010).[18] If designed right, they can help process signal from noise and they can complement workflows and increase trust between organisations with each other and between organisations and the public.[19] However, if not properly designed or used in integrated and adaptable ways to keep up with every increasing innovations, these ICTs can lead to information overload as systems become increasingly connected, lack of continuity with people and infrastructures and they are increasingly mobile.

3.1 The Nature of Incidents

Natural disasters – unpreventable occurrences which take place and whose impact can range from mild to highly destructive – appear to be on the increase. This appearance is borne out by studies: In 1970, the average of natural disasters that were reported was 78; in 2004, this number jumped to 348. According to AccuWeather, since 1990, natural disasters have affected 217 million people every single year. From 1980 to 2009 there was an 80 percent increase in the growth of climate-related disasters. Between 2001 and 2010, more than $1.2 trillion was lost to the increased rates of natural disasters. This was a dramatic rise, which between 1981 and 1990 had been roughly $528 billion.[20]

One other area which is on the increase of course, is terrorism. Having previously peaked globally in 2005, 2015 saw a massive increase of some 650% - largely due to the activities of the so-called Islamic State.[21]

As population grows and infrastructure, both physical and technical, becomes more vital in so many areas of modern life, so does the potential of any disaster to impact significantly on people and property. With reference to the importance of technology, the growth of what has become known as ‘cyber-crime‘ or ‘cyber-terrorism‘ takes on major importance. Reports of attacks have become common-place. Cyber-crime may be a modern innovation, but it is carried out by criminals for the same reasons always: boredom and vandalism, ideological or political motives, malice or revenge, monetary gain through extortion or sale of illegally obtained data, terrorism or notoriety and sensationalism. The techno-word ‘hacker’ tends to be used in reference to such people, but in reality they, like so-called ‘shoplifters’ are simply ‘thieves’. The aesthetic may be different – breaking into a bank to steal money is different to ‘hacking’ into a computer system and doing the same thing, but the results are the same. Or are they? There are in fact several very significant differences between cyber and conventional crime and that is:

- Scale.
    - Breaking into a bank premises or security vehicle can only net the criminals at most the contents of the building or vehicle. A cyber-crime attack in contrast can potentially target millions of victims. The other major

difference of course is that a bank robbery will result in loss of cash and other physical property: a cyber-attack can result in (and is frequently the reason for) the loss of personal data, which in turn can lead to further attacks on other systems, using that data.

- Speed
    - A cyber-attack is carried out, not at the speed of the criminal, but at the operating speed of the machines or networks targeted, usually measured in seconds.
- Scope
    - A physical crime happens in a geographical location. Computer networks and the internet in general make it possible to target systems anywhere in the world, making detection and prosecution much more difficult.

An extension of cyber-crime in general is cyber-terrorism. In its most recent manifestations, even specific countries are being blamed for state-sponsored activity of this type of crime: China[22] and Russia[23] to name but two.

Some may not see this type of incident as 'crisis' management in the pure sense, but consider the issues as a result of interruption to energy supplies, unauthorised accessing of the computers which power nuclear power stations, etc. and the problems become much clearer.

Taking the nuclear scenario a little wider and we find the Chemical, Biological, Radiological and Nuclear (CBRN) incident and consequent training, monitoring, management and response. In each case, these hazards are man-made, either accidental or deliberate. Examples might include deliberate contamination of drinking water, accidental radio-nuclear contamination or the emergence of a new infectious disease including those that take the form of a pandemic.

The EU activities to prepare for such emergencies include the following:

- crisis-management arrangements and strategies
- communication systems linking up EU countries
- expert advice on prevention, treatment and mitigation
- health risk assessments
- promoting research in CBRN related topics

There is an overarching organisational framework in the form of the EU Health Security Committee, with representatives from all EU countries: this works in conjunction with the Global Health Security Initiative, a partnership of health official from the G7 countries, Mexico and the EC, with eh World Health Organisation as a participating observer. This provides a platform for health security preparedness at global level and provides advice during health emergencies.[24]

3.2 Mobile communication

It seems as if they have been around all the time (indeed to anyone under 30, they have been) but mobile telephones are a relatively recent technology. Now, in the second decade of the third millennium they are all-pervasive: there are almost as many cell-phone subscriptions (6.8 billion) as there are people on this earth (7 billion), and it took a little more than 20 years for that to happen. In 2013, there were some 96 cell-phone service subscriptions for every 100 people in the world.

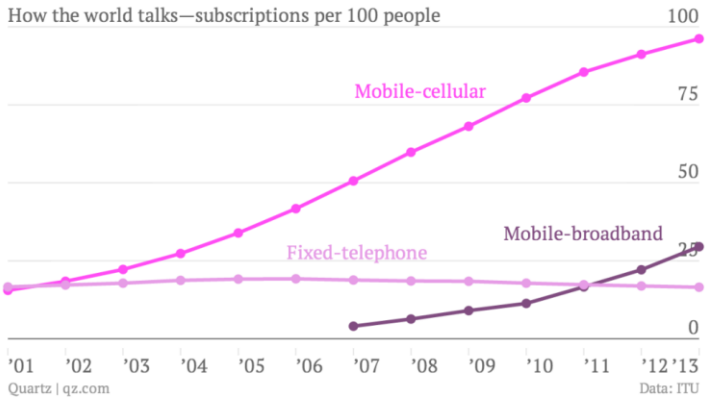

Figure 2: Global mobile telephone subscriptions[25]

Those figures[26] are from the United Nations' telecommunications agency, the International Telecommunications Union which keeps track of the rise and fall of various kinds of communications technology. In wealthier countries, penetration rates exceed 100% because of individuals with multiple subscriptions, making up for the disparity in developing economies. Still, penetration rates are impressive even in poor countries, with an average of 89.4 subscriptions per 100 inhabitants.

By contrast, fixed or landline telephone subscriptions have been falling since cellular phones really took off: the world peak for landlines was in 2005 and now the rise of mobile broadband subscriptions for smartphones is putting the legacy technology under further pressure. There are a few notable exceptions, mostly small, rich states—Monaco has 121 land-line subscriptions per 100 inhabitants, for example. The USA peaked in 2000 with just under 70 subscriptions per 100 population; this figure had fallen by 2013 to less than 45 subscriptions.

Today, almost everywhere has more mobile phone penetration than land-lines: the continent of Africa has a very low level of landline penetration of 1.4 subscriptions per 100 people, but 63.5 cell subscriptions.

We have also seen how the internet has advanced at incredible speed over recent years: in parallel, computer speed, processing power and memory capacities have increased exponentially. A home computer in the early 1990's was considered 'state-of-the-art with 512 Kilobytes of RAM: just a few years later and the equipment designed for the modern home and office measures its RAM in terabytes – an increase of a factor of one billion and in computer circles memory is talked of in units of up to the 'geopbyte', six steps beyond the terabyte with each step increasing capacity by a factor of 1000 over the previous one.

Such computer processing power, sophisticated communications programmes and memory capacity has been instrumental in changing the way individuals and organisations work. Working-from-home and distributed networking are commonplace today – unthinkable only a few years ago. We should note that these practices are not a panacea: they bring their own problems as we shall see later on.

As never before, technology provides the ability for organisations to manage their data and to interoperate with each other; for organisations to communicate with citizens and for citizens with each other, all with ever-decreasing restrictions on location and physical connections to buildings. Organisational interoperability is still limited by a lack of common systems but one of the benefits of advanced technology is that we are witnessing the evolution of communications between organisations and systems which do not of themselves require a common system across organisations.

3.3 Communication with Citizens

In addition to the way organisations communicate with each other and individuals communicate with themselves, modern technology provides not merely the means, but the obligation for government and PPDR organisations to communicate with the population within their respective jurisdictions. Digital technology is rapidly transforming the way authorities are engaging with their citizens, and vice versa. The problem often is that citizens are bombarded with information from all manner of sources and so the simple fact that "our information to you is important for your safety" is often not sufficient to attract and hold peoples' attention. Conversely, when a serious situation occurs, people are apt to bombard both government al organisations and the media with images, video recordings and demands for information and clarity on the situation. For a government body or PPDR to stand out from the crowd, it is critical to embrace and implement the following four citizen engagement trends: [27]

- Multichannel Approach

  An offline-only approach to citizen engagement is already a thing of the past. Modern governments think digital first, for many obvious reasons. The cost of online communication is significantly lower compared to offline means. Engaging citizens online attracts more people, particularly the young, than any other method. In addition, thinking of citizen participation, giving them the option to share their input on a digital platform dramatically reduces the overall cost per engaged citizen.

Channel	Cost per transaction
Face-to-face	€11,50
Telephone	€4,50
Postal	€8,70
Online	€0,27

Figure 3: Comparative communication cost per citizen by method

- Personalised Interface

The likelihood of citizen participation will increase in direct proportion to its relevance: with the availability of so much information, the forced presentation of irrelevant information will only lead to the important data being ignored in the wash of 'data-overload'.

One way forward appears to be the personalised interface such as a mobile application or web platform: a prominent example of this would be the BBC mobile application, which allows users to select and prioritise the areas of news which interest them.

- Citizen Engagement Analytics

  Increasingly, government organisations and departments are adopting citizen engagement dashboards which help them gain insights to their citizens' opinions from widely available streams of data.

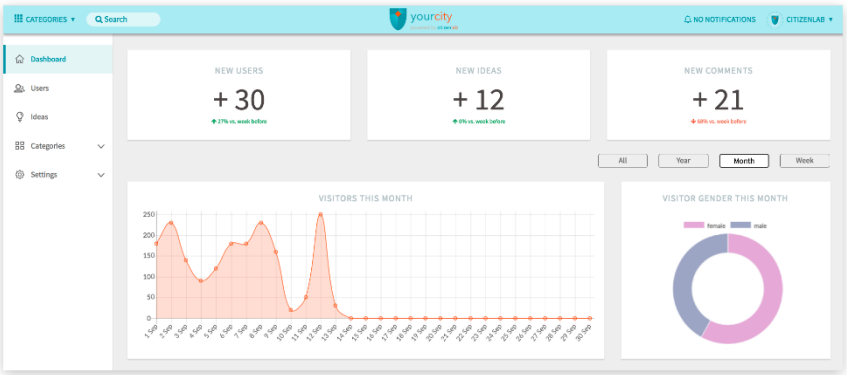

Figure 4: Example Citizen Engagement Dashboard

- Open Data

  The number and variety of web application programming interfaces (API) and public open data sets continues to proliferate. At a basic level, open data is believed to enhance transparency[28].

  The down-side to this approach is that organisations can become fearful of going beyond the elementary steps of uploading pdf meeting minutes or expenses of senior officials: increased visibility = increased accountability = fear of vulnerability.

This issue exists not only in the relationship between citizens and organisations but between organisations themselves and can be a serious obstructing factor in the sharing of information which can be made technically possible through developments such as SecInCoRe. ICT can provide a productive means of information sharing for disaster management, but it is only effective and efficient if frameworks and standards for such stems are improved and maintained, if they are used in all phases (including planning), if general risk communication models are balanced with local community needs.[29]

This is one of the main impetuses for some of the decisions in SecInCoRe's conceptual design (e.g. semantic search to help limit information overload) need to be developed further in the future for ICTs to have a productive role in crisis management.

3.4 Citizen mobility

Martin Lund[30] suggests that if 'infrastructure' was the buzzword of the 20th century, (physical) 'mobility' and (technical) 'connectivity' are the keywords of the 21st. He argues that infrastructure in its totality (whether roads, railways, bicycle paths or fibre-optic cables) should serve as a means of enhancing mobility in society; of connecting people and goods, knowledge and innovation, cities and regions.

Mobility is required not only for developing efficient liveable cities but also for attracting top talents and investments. There is no time like the present to invest in public infrastructure, concluded the International Monetary Fund (IMF) in 2014 its World Economic Outlook for 2014[31]. Low loan rates combined with stagnant growth in many advanced economies make investments in infrastructure – the backbone of everyday life – more relevant than ever.

The UK government recently announced a five-year programme to invest GBP 38 billion – USD 59 billion – in railway networks, but that alone cannot create mobility and connectivity, according to Alan Pauling of Ramboll, a global engineering consultancy group. He added that the basic infrastructure across Europe is generally satisfactory. The weak point is short-distance connectivity, also known as the 'last-mile barrier': people's need to get to public transport, the train station, for example, from their homes and offices and vice versa.

There is a strong argument that connectivity is necessary for mobility: connectivity can maximise the use of all available transport systems and cover the majority of those short-distance trips, which are the core of liveable, sustainable cities. On the negative side, technical connectivity is not the complete answer to the issues of ever-increasing cost of owning or renting property space and managing a business. A dispersed workforce is difficult to manage effectively; may result in loss of efficiency when other distracting factors around working from home take effect; and can result in individual workers feeling out of touch and isolated from both work colleagues and the business itself (see 3.1 above).

3.5 Social Media

One method of communication wholly grounded in the 21st century goes under the umbrella title of 'social media'. Hosted on applications such as Twitter, Facebook, YouTube, and Flicker, this form of media "is characterised by interactive communication, in which message content is exchanged between individuals, audiences, organisations and sectors of the general public" (Alexander 2014: 718). Social media challenges the idea of communication "to" the public within command and control, and the public seeks active participation in how they seek information and how the response and longer term recovery unfolds.[32] Not including social media within crisis management models risks the loss of public confidence, due to a lack of use of normal and expected communication networks, or even uncontrollable and irresponsible public and media participation that puts more lives at risks and exacerbates the effects of a disaster.[33] However, including it risks including unverified information, making information public that might otherwise remain private for security reasons, and representing uneven breadths of society further marginalising vulnerable groups.[34] The answer is not simple

or one-sided, but affects both a communities ability to get the information they seek and a responders ability to have the community trust their decisions when all the information is not knowable. Consequently, it is important to consider the growth and place of social media in society especially when dealing with the emerging trend in crisis management to address business continuity and organisational resilience.

Social media sites in general have changed the way in which people and organisations interact with each other. Sites like Facebook, Twitter, LinkedIn, Vine and others make it simple to stay connected in people's lives. Friends can keep up to date with others statuses, activities, photos and videos that they post. Social media is not just seen as important for individuals, it has become a key influencing tool for businesses or anyone trying to develop their professional network or look for a job.

When it comes to business, current wisdom suggests it is important to be on as many social media sites as possible.[35] These sites offer many different options to share information and have different users on each one. As a result, the more sites a business is on, the more people will see it. There are different benefits to different sites, hence many businesses encouraging visitors to 'like' them on Facebook and 'follow' them on Twitter.

In brief, the variations between the most popular social media platforms are as follows:

- **Facebook**

  Facebook allows users to get to know a business more intimately, communicating through status updates, photographs, messages and more. The key to being successful with Facebook is interaction. If patrons post a question on a business's page, they need to respond. The more the business responds and interact with the people who 'like' their page, the more they will talk about that business to others and share that page, thus getting it more 'likes' and further promoting the business. The company must also tell followers what is going on in the company: staff changes, new products and so on.

- **Twitter**

  With Twitter, news and updates can be shared quickly. As with Facebook, it is important to interact with followers. It also gives users a chance to find like-minded people through 'hashtags'. If a user tweets about hedge trimmers, they can hashtag it as '#hedgetrimmers' and that tweet will be put in any searches with 'hedgetrimmers' in it. Using hashtags in this way can help others to discover that user and also that user to discover those who are talking about similar subjects to themselves.

  In April 2014 there were some 974 million Twitter users[36]. Significantly, and in contrast to Facebook, it is reported that many 'users' are not especially active. Statistics published in 2016 indicated that there were around 1.3 billion accounts with 310 million monthly active users, Around 44% of all those signed up to the system have never sent a single tweet[37]; 500 million people visited the site each month without logging on; 83% of the world's leaders are on Twitter, but singer Katie Perry has the most followers (87 million) compared to the average number of followers, which is 208.[38]

- **Instagram**

  Instagram is, for want of a better phrase, a 'show-and-tell' social media tool. Like Twitter, it utilises hashtags to make it easier for like-minded people to discover businesses or individuals and to follow them. Its advantage for business is that It is easy to present existing and new products in a visual, pictorial format.

  Instagram users have grown from 90 million in 2013 to 600 million in 2016.[39] According to other sources, 60% of users log in daily and 30% of all internet users are now on Instagram[40]. In slightly more intellectual contrast to Twitter, the most followed brand on Instagram is National Geographic, although it then reverts to type with actress Selena Gomez as its most followed name.

This form of public communication and networking can act as 'a listening function' and a monitoring device allowing organisations to gain insight into and help manage public sentiment and reaction; it can be integrated into emergency planning and crisis management models and plans, whereby agencies and organisations use crowdsourcing and collaborative development; it can help create 'social cohesion' in times of crisis and promote 'therapeutic initiatives' and volunteerism; it can be drawn upon to communicate with friends and family when other communication technologies fail; and, finally, it can also be used to make donation appeals and for research purposes (Alexander 2014: 720-723).[41] Through such uses, social media has already contributed to various disaster responses.

One particularly promising way in which social media has been enrolled in disaster response is through 'crowdsourcing'. Crowdsourcing has been defined in numerous and often unsatisfactory ways (see Liu 2014;[42] Starbird 2012[43]). In general, crowdsourcing implies connecting to and utilizing the collective intelligence of 'the crowd' to generate, organize, and manage information and solve problems. Crowdsourced data can be collected almost immediately after a disaster has occurred through social media; crowdsourcing tools and applications (e.g. Ushahidi.com) can collect data from various different sources (e.g. tweets, geo-located images on Flickr) as well as do quick summaries, categorization, and analysis (e.g. tag clouds, trends, filters); in this process 'the crowd' can locate requests for help and validate information (Gao et al. 2011).

Engaging with social media, can provide a productive tool for crisis management models to switch from treating the public as passive to engaging the public participation, something that always happens during disasters. But these advantages come paired with challenges.

Given the facts in the previous section, it might appear that any individual or business not making full use of all social media tools available is behind the times – perhaps even stagnating and no longer relevant. Social media however is not without its down-side. A number of disadvantages to its use are reported by researchers: .[44]

- *It perpetuates false and / or unreliable information*
  Information, however unsubstantiated can spread to millions of people within hours on social media.
- *Cyber Bullying Is A Growing Problem*

Having virtually unrestricted access to people's lives at is not always a good thing. The trend of 'cyber-bullying' is generating new levels of distress and corresponding legislation all the time.

- *Decreases Face-to-Face Communication Skills*
  "Computer reliance could hurt a person's ability to have a face to face conversation by making it awkward and unusual to hear something and respond with a thoughtful message through the spoken word because of one's dependence on a keyboard to convey a message."
- *Causes Face-to-Face Interactions to Feel Disconnected*
  "When I see my friends on their phones and I am around them, I feel disconnected even though we are only two feet apart….. Unfortunately, sometimes friends use their phones so much that it is difficult to have an actual conversation with them. Sometimes friends can get so socially attached to something such as a blog or gaming console that they lose touch with friends, creating small gaps and holes in close friendships/relationships."

Perhaps surprisingly, some of the loudest critics of social media come from areas where they might be least expected to be found. [45]

> "*Steve Jobs in 2010 was on the stage at the Apple event releasing the iPad and he described it as a wonderful device that brought you educational tools. It allowed you to surf the web, it allowed you to watch videos, it allowed you to interact with other people. And he basically said it's the best way to do all those things.*
> *Two years later when he was asked "Your kids must love the iPad?" He said "Actually we don't allow the iPad in the home. We think it's too dangerous for them in effect." The reason why he said that was because he recognized just how addictive the iPad was as a vehicle for delivering things to people. That once you had the iPad in front of you, or when you took it away from the home with you, you'd always have access to these platforms that were very addictive. That were hard to resist.*
> *So where his kids were very well adapted, well adjusted, may not have been prime targets for say substance abuse, they like everyone else, are susceptible to the charms of something like an iPad and what it delivers".*[46]

and perhaps even more significantly:

> "*Honestly, I sometimes truly wish that 'tools' such as the iPhone (or any smartphone), laptops, iPads, tablets, etc. hadn't been invented. Sure, they're great, incredibly useful, and fun time-killers. But the way teenagers abuse them, and turn them into mini social control rooms is frankly awful.*"

At first glance, this quote might have come from a parent or grandparent lamenting on the disadvantages of social networking and how social media has doomed today's children. In fact, it was written by a Seattle-area school-age teenager as part of an assignment to answer the question, "How has online social networking influenced your relationships with friends and family?"

This student goes on to write,

> "*The teenage way of life has completely changed from what it was only twenty years ago. Now, there is a dramatic decrease in face-to-face communication,*

which reduces our generation's ability to interact with others on a speaking level."

By way of confirmation, Price-Mitchell, as a result of interviewing young people cites a number of disadvantages to the use of social media and asserts that youth engaged in their communities claim that face-to-face interaction is what motivates them to make a difference in the world.[47]

There is now less expectation in face-to-face communication, which is the highest commodity form of communication in traditional disaster management. This is leading to a generation gap that interviewees and SecInCoRe workshop attendees have continually described: newer and older responders expect to networks, connect, and communicate via different methods. These differences cannot be erased by simply not including social media. Nor can the problems be fully addressed just by including it, as clearly stated in the quotes above. Instead, new challenges posed by social media in coordinating responders with each other as well as coordinating responders with the public need to be addressed in future crisis management models.

- *Diminishes Understanding and Thoughtfulness*

  "Since the inception of social networking, the quality of conversations has dropped. I believe that people are spending so much time online that they don't always understand the feeling, emotion and/or character of the person they are talking to. When you talk to someone through a message or even a voice, you can't always fully understand them."

Such loss of understanding and thoughtfulness, or assumption that simply sharing equals that, can lead to both the public and responders not seeking contextual and situational understandings of the information they see.

- *Causes Face-to-Face Interactions to Feel Disconnected*

  "When I see my friends on their phones and I am around them, I feel disconnected even though we are only two feet apart….. Unfortunately, sometimes friends use their phones so much that it is difficult to have an actual conversation with them. Sometimes friends can get so socially attached to something such as a blog or gaming console that they lose touch with friends, creating small gaps and holes in close friendships/relationships."

- *Facilitates Laziness*

  "The new socially active era causes laziness because instead of running to your friends you can message them. Or instead of walking upstairs to notify the family of dinner, I can blog it. Social networking makes life so convenient that it creates laziness. In my opinion staying fit is important, but it is difficult to go beyond the newly developed status quo."

  "It's really easy to spend hours doing nothing….It's a fantastic way to waste time."

The disadvantages of social networking and social media will doubtless be studied for decades to come. In the meantime, we already know it is a significant source of concern among privacy advocates as well as parents who worry about their children's safety. Clearly, the disadvantages of social networking go much deeper than privacy and safety; and the school students quoted earlier describe some of the serious drawbacks to relationships, which in turn are one of the foundation stones of human development.[48]

3.5.1 Social Media in Crisis Management

Social media is an ever-growing phenomenon that is changing the way in which people and organisations interact with each other. It cannot be ignored by crisis management practices because for crisis management to succeed, it is essential to know what the public believes and how they are interpreting the situation (Stal 2015).[49]

However, it is also apparent is the fact that the use of social media can often take priority over things which logic would indicate are far more important. This latter point has expanded to the point where humour has entered into warning notices;

Figure 5: Evacuation social media-style 1

Figure 6: Evacuation social media-style 2

Viewers of the television news broadcasts of the sinking of the cruise liner Costa Concordia will have seen footage of passengers, having been given the order to abandon ship, taking their time and potentially risking life and limb to record their own evacuation on mobile phones.[50]

Remaining on the subject of trivia for a moment, recent European Commission research has studied the possibility of analysing social media feeds for the purpose of assessing the 'mood of the citizen' during a crisis.[51] An analysis of thousands of Tweets during the Hurricane Sandy incident affecting the Eastern USA in 2012 in an attempt to classify

them into 'anger', 'fear', 'positive' and 'other', proved less than beneficial. By far the majority of tweets consisted of inane comments such as "*Can Sandy like blow north away so that we don't have school please I hate school*" and "*Hurricane Sandy just disrespected the f**k out of my umbrella*". Very little content could be genuinely attributed to anything apart from the 'other' category.

This propagation of misinformation is a real fear. Alexander (2014: 725)[52] notes that after hurricane Sandy:

> 'Photoshop-style image manipulation was widely used by people who shared photographs of the storm. Exaggerated and false news items, for example, about which places in New York City were flooded, were shared and reposted by so many social media users that they were picked up by mainstream media and thus began to assume the status of true stories until they could be discounted by field checking'.

On the other side of the fence, some emergency service organisations were arguably slow[53] to adapt to make the best use of social media platforms: rather, they reluctantly moved onto them on the basis that they were current, trendy and the place to be seen; that otherwise, they would be seen as being behind the times if they were not visible on such platforms, despite not always knowing the best ways in which to exploit them. Moreover, as more private businesses engage with the public through social media, ignoring these pathways can be detrimental to response, despite the privacy and data protection issues, as privacy companies, such as airlines or utilities, are increasingly necessary partners in crisis management (Watson, H., & Finn, R. L. 2013).[54]

Since around 2008 there has been a growth in interest in European police forces in the use of social media as a basis for engagement with the public. This interest is set in the context of a political agenda for increasing public trust and confidence in the police and enlistment of the public as jointly responsible for crime reduction. An ambitious national police agenda led by the (then) Association of Chief Police Officers (National Police Chiefs' Council since 2015) has promoted the use of social media to engage groups previously uninvolved in discussion of local policing, and has envisaged its use as a basis for deliberation about priorities. Some studies have examined how successful this endeavour has been, and how far any hierarchical organisation such as the police service, has been able to exploit the networked characteristics of social media and the potential of user created content. One conclusion suggests that the constraints of police culture have meant that social media in general has been used cautiously and as a reinforcement for existing means of communication. [55] Issues such as this would need to be addressed if more ambitious aims for social media are to be achieved.

Social media provides the police with new opportunities to engage with the public; to collect and impart information; and to gather intelligence – to listen to the needs of the local communities, as stated above. It can also help raise local concerns to the awareness of the officials that were otherwise being ignored/missed and creating distrust (see, for example, http://www.bbc.co.uk/news/magazine-32203907). Lastly, command and control models of crisis management do not easily adapt to information seeking activities by the public, leading to the public continuing to improvise information.[56] Local community engagement also has the potential to strengthen data gathering providing the opportunity for these communities to claim ownership of and

investment in the outcomes (Stal 2015).[57] Social media offers opportunities to address these challenges.

However, these opportunities come with challenges which are yet to be fully addressed. There is still no UK national strategy on police use of social media and every force is left to develop its own approach. Scholars have noted that there is unequal distribution and use of social media technologies and applications within societies, for example along the lines of class, gender, 'race', age, disability, and skill (Alexander 2014).[58] Thus, while social media can, on the one hand, lead to a democratisation of voices, attention has to be paid to how this 'democratisation' is socially structured.

There is also considerable debate about the accuracy or necessity of the information produced. Scholars point to the potential propagation of unintentionally or intentionally false information, even if eventually self-correcting, raising the question of both organizational as well as public trust in regards to crowdsourced data.[59] Moreover, to look beyond individual tweets, for instance, social media use wanders crisis management into the realm of big data, which has the potential to obscure situational knowledge and build a limited understanding of how a disaster is unfolding.[60] This further raises questions regarding the decision-making practices of first responders who, in the event of relying upon 'unreliable data' may be seen as liable. There is also the concern of too much data and a lack of ability to adequately turn it into useful information in a timely manner.

These debates about social media can affect the fundamental structures of crisis management, not just the tools and ICT they use. The civilian and military branches of EU crisis management are built into separate directorates and capabilities and historically are not well coordinated often leading to a lack of shared vision or understanding of what has unfolded (Pirozzi 2013).[61] Add to this the distance in expectations created in what could be done in crisis response by the everyday use of social media and other 'in-an-instant' technologies and what can be done at present by response agencies. Unless the reasons for such differences are addressed and the public expectations are productively acknowledge, then there will likely be a continued surge in public seeking their own information and putting themselves and others in risky situations in doing so.

Work remains to be done on developing systems and strategies that help embed the use of social media into everyday working practices, and ensure that lessons are learnt in terms of what constitutes best practice. Research into the public perception of the police's use of social media may be of benefit, particularly if it helped to pin down what the public wants from a police social media account, how they view different types of tweets or posts and what impact social media has on public confidence in the longer-term. With 87 per cent of young people using social media, it represents a crucial form of communication now and in the future and could become a vital element in helping to build trust and confidence and improve policing in years to come.[62]

3.6 Crisis Management – Before First Responders

Over recent years and often due to the critical infrastructure on which business depend, the science of Business Continuity Management has grown to become a major part of societies preparation and planning for emergencies. Both national and international events have led Governments, regulators, insurers and other public and private sector

bodies to emphasise and actively promote the view that a robust, proactive, effective and appropriate level of organisation resilience and proven BCM preparedness and capability is essential. As part of the overall enterprise risk management (ERM) of an organisation[63] and in the face of the challenges and threats that inevitably arise in today's national and global business and public sector service environment complacency is wholly unacceptable.

Despite their best endeavours no organisation can have complete control over its business environment especially its supply chain. It is therefore essential for both public and private sector organisations to have an effective and appropriate business continuity management (BCM), incident and corporate crisis management capability. Even the terminology is chosen with care: 'Business Continuity Management' is used rather than 'business continuity planning'. This approach is deliberate because 'planning' implies there is a start and end to the process and can lead to unwanted planning bureaucracy. However, business continuity planning is still a critical and key component of the BCM process. In contrast to the earlier narrow and reactive approaches to BCM it is now recognised as a dynamic, proactive, and ongoing business as usual management process. To be effective it must be aligned with or complete against a standard, appropriate (fit for purpose), practical, realistic, up-to-date, effective and a plausible (proven) capability.

At a time when 'Just In Time' (JIT) delivery, procurement and supply chain issues in general have a high profile there is a need to consider the big picture and both the fragility and resilience of an organisation's capability to deliver its own products and services. In particular the organisation's supply chain and their dependency upon it.[64] In addition there are regulatory, legal, insurance, licence and contractual requirements to consider whereby contract management takes on a different role to that traditionally recognised.[65] Within this context there is the ever growing differentiator within the procurement process where organisations are asked to provide demonstrable 'verifiable' proof of their BCM capability and resilience. The failure to respond or be able to demonstrate or verify what is required will provide an 'exit' within the process creating a 'lost opportunity' rather than providing a strong evidential based 'competitive advantage'.[66]

3.7 Crisis Management – First Responder Agencies

The process of Business Continuity Management has, in the UK and many other countries been extended into law as far as first-responder organisations are concerned.[67] New developments in technology have seen the advent of new and improved capabilities for incident management: trunked digital communications; mapping tools; resource management tools; drones; predictive modelling software; command solutions; to name just some generic examples.

Ironically, the pressure to improve their performance is increasing on the emergency services not because of these additions to the armoury but more as a result of improvements in communications for the public at large and the media. One person, trapped in an overturned railway carriage can transmit a message via social media which can go 'viral' in minutes, resulting in almost immediate demand for information – sometimes even before the responders have arrived at the scene. The public can

communicate with speed, so they expect the same of the organisations that keep their society functioning.

Increasing restrictions on budgets, together with demands to increase performance and efficiency are driving emergency organisations to work together on a more formalised basis than the previous method of simply calling on 'mutual aid' when required. This process is complicated by the need to reduce human resource levels (the most expensive resource in the public services) to manage budget reductions.

Initiatives such as the UK Joint Emergency Services Programme (JESIP)[68] are in existence with the sole purpose of improving the response of the emergency services to multi-agency incidents.

Commencing initially as a 2-year programme in 2012, it was intended to deliver practical guidance to assist organisations to improve. Amongst other things, it delivered a Joint Doctrine: Interoperability Framework,[69] setting out a standard approach to inter-agency working, together with training and awareness products to assist in staff development.

The principle of JESIP is to be scalable: the five joint working principles;

- Co-locate
- Communicate
- Co-ordinate
- Jointly Understand Risk
- Share Situational Awareness

and associated joint decision models can be applied to any type of multi-agency incident and in fact could be utilised in a multitude of environments where organisations need to work together more effectively. The programme initiated the largest and most successful joint training initiative across the emergency services. Now JESIP is about all services integrating the JESIP ways of working and models into all policies, procedures until staff use JESIP as a matter of course.

JESIP has introduced a national standard to multi-agency joint working in the UK. When it is used every day by responders, the emergency services will be able to provide a consistent joint emergency response to incidents, wherever the incident may take place across the country. It will take some time for all services to integrate JESIP and for staff to use JESIP as a matter of routine. Below is a table that shows the intended positive improvements JESIP will bring across its four areas of work as it integrates and matures.

JESIP Maturity Matrix

	Level One (Chaotic/Intuitive) A fundamentally ingrained culture of single service working	Level Two (Informal/Ad-Hoc) Some positive examples of an 'interoperable culture', but a highly inconsistent national picture	Level Three (Managed/Effective) A nationally consistent commitment to interoperable working, but not yet fully ingrained as part of the culture	Level Four (Optimal/Best Practice) A fundamentally ingrained culture of interoperable working
Doctrine	Single service doctrine	Joint doctrine exists, but not widely accepted or understood	Universally accepted and understood joint doctrine on interoperable working	Joint doctrine on interoperable working fully embedded and aligned with all current & future single service and specialist doctrine
Training	Single service training	Some isolated examples of joint training, but a highly inconsistent national picture	A nationally consistent approach to joint training, though not formally integrated into existing training programmes	Joint training fully embedded as the default position for the Emergency Services and integrated into existing training programmes
Testing & Exercising	Single service testing & exercising	Some isolated examples of joint testing & exercising, but a highly inconsistent national picture	A joint testing and exercising strategy developed and accepted by all services	A joint testing and exercising strategy fully embedded within all services
Joint Organisational Learning	Consistent failures to respond to lessons that have been identified	Some positive examples of responding to lessons identified, but a highly inconsistent national picture	A joint organisational learning strategy developed and accepted by all services	A joint organisational learning strategy fully embedded, nationally

Figure 7: *JESIP Maturity Index*[70]

4 National crisis management models within the EU

As the EU does not have its own capacity and resources, any joint response to a cross-border threat requires the cooperation and resources of one or more members states.[71] To complicate matters further, neither is there a common civil protection system within the member states of the EU: even within a country there can be significant differences at regional and local levels. These differences are due largely to the unique cultural, historical and political contexts of each country as well as to their various demands, experiences and exposure to crises. Some examples are given below.

UK	Spain	Portugal	Sweden	Germany
Senior Government Ministers / Cabinet Officers	Senior Government Ministers	National: Ministry of Interior / National Committee of Civil Protection	Municipal administrations	Politically responsible chief of administration
Relevant Government or other national agencies	Appropriate Government Agencies	District: Civil Governor / District Civil Protection Committee	County councils	Appropriate staff of administration
Regional / Local Resilience Forum(s)	Regional Government Senior Management	Mayor / Municipal Civil Protection Committee	County administrations	Local Authorities or Municipalities Senior Management
Local Authorities Senior Emergency Mgt.	Local Authorities or Municipalities Senior Mgt.		The government office (emergency mgt. functions)	Local Civil Protection Senior Management
Local Emergency Services Senior Management	Regional Civil Protection Senior Management		SOS Alarm Sweden	National or Local Transport and Utility Providers Senior Mgt.
National or Local Transport and Utility Providers Senior Management	Local Civil Protection Senior Management		National authorities with civil protection / emergency mgt. functions & responsibility.	
	National, Regional or Local Transport and Utility Providers Senior Mgt.			

Table 1: *Comparative Command & Control Levels*[72]

To expect these variations to be standardised in the foreseeable future would be an exercise in futility, but this variation need not be an obstruction to efficient incident management. The EU can and does play a role in coordinating a multilateral response to boundary threats.

4.1 EU Crisis Management Models

In recent years Europe has experienced a number of cross-border events including terrorist attacks, airplane crashes, flooding, disease pandemics, and pollutant spills that have fallen across international infrastructures and called for a multi-lateral response. While responsibility for disaster response rests with EU member states, to do so they also "acknowledge – on paper, at least – that they must increase their mutual cooperation capabilities given the rising number of transboundary crises" (Tercovich 2014: 150).[73] To add to these coordination needs between nations, the EU, UN and

NATO also have all been active in helping to facilitate cooperation and collaboration between the member states.

EU Joint Communications acknowledge that a common plan is still needed, one that "effective and proactive EU policy responses to conflict and crises should draw on the different strengths, capacities, competencies and relationships of EU institutions and Member States" (HREURASP 2013: 7). Among the many challenges of doing so are:

- Strengthen early, pro-active, transparent and regular information-sharing, co-ordination and team-work among all those responsible in the EU's Brussels headquarters and in the field
- Improve combined situational awareness and analysis capacity in particular by better linking up the dedicated facilities in the various EU institutions and services
- Further develop and systematically implement a common methodology to conflict and crisis analysis
- Work across EU institutions and with Member States to translate conflict and crisis risk analyses into specific conflict prevention measures, drawing on lessons learned from previous conflicts and crises
- Strengthen mechanisms for pooling and sharing European capacities and expertise
- Take stock of lessons learned, including within the EU institutions, with Member States

The EU assists member states by collating, analysing, and sharing information and lessons learned (Boin et al. 2014b[74]; SEEDRMAP 2008[75]); it develops emergency management guidelines, offers member states advice, and holds trainings, and aims to increase response efficiency through coordination and cooperation (Boin and Ekengren 2009[76]; SEEDRMAP 2008[77]). More resistance arises in areas in which the EU has developed capacities which "operate independently from the member states", such as an EU civil protection force, EU disaster supply chains, or a central crisis management unit (Boin and Ekengren 2009: 290).[78]

As a result, the EU and other European bodies have developed a variety of policies, agencies, tools and institutions for responding to crises. Some of the key policy developments are outlined in the table below.

Key EU Policies and developments in Crisis Management
1991 – Resolution adopted: request of Member State aid in times of disaster
1992 – The European Community Humanitarian Aid Office (ECHO) established
1993 – Common Security and Defence Policy
1998 – European Security and Defence Policy
2001 – Establishment of the EU Civil Protection Mechanism and the Monitoring and Information Centre (MIC) as its key operational tool.

2009 - The Crisis Management Planning Directorate created to establish of a single civilian-military strategic planning structure for EU peace-keeping and humanitarian operations and missions
2009 – Lisbon Treaty, Solidarity Clause, Article 222
2010 – EU Internal Security Strategy in Action (2011-2014)
2013– The Emergency Response Coordination Centre (ERCC) replaces the MIC
2015–Renewed European Union Internal Security Strategy (2015-2010) (in process)

Table 2: *Key Developments in EU Crisis Management and Security Policy*

Some further structures are already in place to assist in crisis management at EU level:

- The EU Civil Protection Mechanism

  Established in 2001 to facilitate cooperation between European states in responding to natural and human-made disasters both within and outside of Europe. It incorporates 28 member States plus Montenegro, Norway, Serbia, Macedonia and Turkey. Mechanism activated on over 220 occasions between 2001 and 2015. Requests for assistance and coordination of response in coordinated through the Emergency Response Co-ordination Centre.

- The Emergency Response Co-ordination Centre (ERCC)

  Established by the EC in 2013 and aims to coordinate a coherent European response during emergencies: part of the Humanitarian Aid and Civil Protection department (ECHO) the ERCC is staffed around the clock and is the co-ordinating hub of the Civil Protection Mechanism.

- The Early Warning and Response System (EWRS)

  Based in the European Centre for Disease Prevention and Control (ECDC) and gathers, analyses, and shares data among participants pertaining to public health threats. The EWRS users include: nominated national contact points, experts from national ministries and agencies of the EU and EEA countries, the European Commission, DG SANCO, ECDC, the European Medicines Agency and the WHO. Available around the clock, activity is triggered by a national contact point posting a message in a system thread. One complaint is that during crises the EWRS becomes flooded with information, making it hard to sort through it. It is also of concern to users that not all relevant stakeholders have access, the information can sometimes be of poor quality, also resulting in duplication of effort with data entry into multiple systems. The proposed SecInCoRe cloud-based inventory and CIS provides a potential solution to these issues.

Further detailed reading on this subject matter can be found in project SecInCoRe D2.4 ‘Domain Analysis: Baseline and emergent future practices’.

The EU’s comprehensive approach, supported by all these mechanism, intended to bring all the various national focuses and strengths into alignment, requires the institutionalization of coordination mechanism (Pizzolli 2013).[79] However, one key feature that has emerged from this is that for each crisis a new “crisis management concept” has to be proposed to the EU ministers for approval.[80] Moreover, as the EU

participates in all sorts of crisis events, from terrorist attacks to financial crises, and there are crisis management capacities spread throughout many of the different DGs relating to different kinds of threats, leading to considerable fragmentation across the EU and sometimes crisis domain competition between different EU DGs/agencies (Boin and Ekengren 2009;[81] SEEDRMAP 2008[82]; Tercovich 2014,[83]). Despite resistance, the increased threat of transboundary crises, such as the eruption of Eyjafjallajökull volcano, has helped give credence to the need for increased EU ability to quickly come to a 'shared situation awareness' (Boin et al. 2014b)[84].

Along with the increasing role in guiding crisis management within and between its member states, there has been an emergence of a plethora of EU "tools and systems related to sense-making" such as early warning systems, rapid alert systems, communication platforms, or situational awareness networks (Boin et al., 2014b: 43). However, despite these tools, there is still a gap in knowledge and data management that require better mechanisms for collection, access, and sharing of knowledge and data, gaps that need to be addressed because how you communicate can change decision making practices (Stal 2015)[85]. One major challenge within all this is the power to address, with these coordination tools, culturally sensitive situations and demographic changes (Stal 2015).[86]

5 What does the future hold?

In practice, forging cooperation between diverse nation states, each with their own national civil security systems and diverse cultural and historical traditions, laws, structures and procedures can be 'particularly challenging'.[87]

At the EU level, crisis data is shared according to various themes: these themes do not align neatly to the agencies at the national level. We have seen elsewhere in this project[88] that ostensibly similar agencies in different nations do not necessarily share the same tasks. Legacy systems and budgetary restraints make the possibility of truly common systems unlikely in the future, although those same budgetary restraints may well be responsible for the amalgamation of various individual organisations in the POPDR field in the short to medium term; indeed the current frequency and intensity of events has already signalled the need for close collaboration to overcome the obstacles of incident preparation and management.

In the absence of the streamlining described in the previous paragraph, the logical way to proceed would seem to be improvements in the sharing of information between organisations for training, planning and preparation and ultimately, in real time for the management of incidents. To this end, EU projects such as SecInCoRe, REDIRNET, SECTOR and others are contributing potential technical solutions and methodologies.

As is so often the case, it appears that the technology which would enable improvement in interoperability either already exists or is not very far away. The obstacles to its success appear to be more related to organisational cultures and governance than to technical restraints and this change process.

One area in which PPDR organisations could well streamline their approach is in the area of communication with the public over social media: the reason of course is that they all use the common commercially available systems (Twitter, Facebook etc.) in order to do so. Policy-makers and organisation executives should look for a seamlessly integrated communication model that potentially strengthens the depth and width of citizen engagement by combining digital instruments (such as citizen engagement platforms and social media channels) with the more traditional methodologies (such as focus groups and public meetings).

At the highest level, Europe is changing: as this paper is being written, the UK is going through the process of leaving the EU; the Euro currency is under pressure and who knows where the EU structure will be in a few years' time. In PPDR organisations, it may be argued that those at the highest level are becoming increasingly political in their outlook and motivation, as a result of changes in governance and responsibility. However, those responsible for the tactical and operational management of incidents are motivated far more by demand and necessity: it will not matter to them in the future that Northern Ireland is part of the United Kingdom and therefore outside the EU any more than the fact that Eire remains part of the EU. PPDR organisations on both sides of the border will continue to co-operate as they always have.

6 References

[1] Boin, Arjen and Ekengren, Magnus. (2009). 'Preparing for the World Risk Society: Towards a New Security Paradigm for the European Union'. *Journal of Contingencies and Crisis Management*, 17(4): 285-294.

[2] Wendling, Cécile. (2010). 'Explaining the Emergence of Different European Union Crisis and Emergency Management Structures. ' *Journal of Contingencies and Crisis Management*, 18(2): 74-82

[3] Boin, Arjen, Rhinard, Mark and Ekengren, Magnus. (2014a). 'Managing Transboundary Crisis: The Emergence of European Union Capacity'. *Journal of Contingencies and Crisis Management*, 22(3): 131-142.

[4] Boin, Arjen and Ekengren, Magnus. (2009). 'Preparing for the World Risk Society: Towards a New Security Paradigm for the European Union'. *Journal of Contingencies and Crisis Management*, 17(4): 285-294.

[5] Boin, Arjen, Rhinard, Mark and Ekengren, Magnus. (2014a). 'Managing Transboundary Crisis: The Emergence of European Union Capacity'. *Journal of Contingencies and Crisis Management*, 22(3): 131-142.

[6] South Easter Europe Disaster Risk Mitigation and Adaptation Programme (SEEDRMAP). (2008). *The Structure, Role and Mandate of Civil Protection in Disaster Risk Reduction for South Eastern Europe*. World Bank and United National International Strategy for Disaster Reduction Secretariat (UNISDR). http://www.unisdr.org/files/9346_Europe.pdf [Accessed 01.10.2015].

[7] Wendling, Cécile. (2010). 'Explaining the Emergence of Different European Union Crisis and Emergency Management Structures. ' *Journal of Contingencies and Crisis Management*, 18(2): 74-82

[8] Attinà, Fulvio, Boin, Arjen, and Ekengren, Magnus. (2014). 'Designing EU Crisis Managemetn Capacities: Filling the Glass'. *Journal of Contingencies and Crisis Management*, 22(3): 129-130

[9] Boin, Arjen and Ekengren, Magnus. (2009). 'Preparing for the World Risk Society: Towards a New Security Paradigm for the European Union'. *Journal of Contingencies and Crisis Management*, 17(4): 285-294

[10] Tercovich, Giulia. (2014). 'The EEAS Crisis Response System'. *Journal of Contingencies and Crisis Management*, 22(3): 150-157

[11] Pirozzi, Nicoletta. (2013). 'The EU's Comprehensive Approach to Crisis Management'. Crisis Management Papers Series.

[12] Attinà, Fulvio, Boin, Arjen, and Ekengren, Magnus. (2014). 'Designing EU Crisis Managemetn Capacities: Filling the Glass'. *Journal of Contingencies and Crisis Management*, 22(3): 129-130.

[13] Al-Khudhairy, Delilah H.A. (2010) Geo-spatial information and technologies in support of EU crisis management, International Journal of Digital Earth, 3:1, 16-30, DOI: 10.1080/17538940903506014

[14] Tercovich, Giulia. (2014). 'The EEAS Crisis Response System'. Journal of Contingencies and Crisis Management, 22(3): 150-157.

[15] (https://www.unisdr.org/we/inform/disaster-statistics)

[16] London Emergency Service Liaison Panel: Major Incident Procedures Manual; 8th Ed.

[17] Queensland Government Business Continuity Management Framework 2014 -18 'Building Organisational Resilience'

[18] Al-Khudhairy, Delilah H.A. (2010) Geo-spatial information and technologies in support of EU crisis management, International Journal of Digital Earth, 3:1, 16-30, DOI: 10.1080/17538940903506014

[19] http://www.preventionweb.net/english/hyogo/gar/2015/en/bgdocs/inputs/Stal,%202014.%20Disaster%20and%20crisis%20communication%20trend%20analysis%20of%20technologies%20and%20approaches.pdf

[20] https://borgenproject.org/natural-disasters-increasing/

[21] http://edition.cnn.com/2016/11/16/world/global-terrorism-report/

[22] https://www.theglobalist.com/china-united-states-cyber-crime-politics/

[23] http://www.telegraph.co.uk/news/2016/10/31/spy-chief-says-british-intelligence-has-foiled-12-terror-plots-s/

[24] https://ec.europa.eu/health/preparedness_response/cbrn_threats_en

[25] https://qz.com/179897/more-people-around-the-world-have-cell-phones-than-ever-had-land-lines/

[26] http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[27] https://www.citizenlab.co/blog/civic-engagement/4-emerging-technology-trends/

[28] https://www.citizenlab.co/blog/civic-engagement/4-emerging-technology-trends/

[29] http://www.preventionweb.net/english/hyogo/gar/2015/en/bgdocs/inputs/Stal,%202014.%20Disaster%20and%20crisis%20communication%20trend%20analysis%20of%20technologies%20and%20approaches.pdf

[30] http://www.ramboll.com/megatrend/feature-articles/mobility-and-connectivity

[31] International Monetary Fund: World Economic Outlook for 2014

[32] http://www.tandfonline.com/doi/abs/10.1080/10807039.2014.947866

[33] http://help.iscram.org/legacy/ISCRAM2014/papers/p27.pdf

[34] http://burnsr77.github.io/assets/uploads/burns_shanley_workshop_report.pdf

[35] https://blog.udemy.com/why-social-media-is-important/

[36] http://www.cbsnews.com/news/many-twitter-users-dont-tweet-finds-report/

[37] http://markets.cbsnews.com/TWTR/news/

[38] https://www.brandwatch.com/blog/44-twitter-stats-2016/

[39] https://www.statista.com/statistics/253577/number-of-monthly-active-instagram-users/

[40] https://www.brandwatch.com/blog/37-instagram-stats-2016/

[41] Alexander, D. E. (2013). Social Media in Disaster Risk Reduction and Crisis Management. *Science and Engineering Ethics*, 1–17. http://doi.org/10.1007/s11948-013-9502-z

[42] Liu, S. (2014). Crisis Crowdsourcing Framework: Designing Strategic Configurations of Crowdsourcing for the Emergency Management Domain. *Computer Supported Cooperative Work (CSCW)*, 389–443. http://doi.org/10.1007/s10606-014-9204-3

[43] Starbird, K. (2012). What “Crowdsourcing” Obscures: Exposing the Dynamics of Connected Crowd Work During Disaster. *Ci2012*, 8. http://doi.org/arXiv:1204.3342

[44] http://futureofworking.com/10-advantages-and-disadvantages-of-social-networking/

[45] http://www.rootsofaction.com/disadvantages-of-social-networking/

[46] Steve Jobs (Apple CEO) quoted in Alter. A: Irresistible: The Rise of Addictive Technology and the Business of Keeping Us Hooked; Penguin Press, 2017

[47] Price-Marshall, M: Tomorrow's Change Makers: Reclaiming the Power of Citizenship for a New Generation: Eagle Harbour publishing, 2015

[48] http://www.rootsofaction.com/disadvantages-of-social-networking/

[49] Stal, Marc. 2015. *Disaster And Crisis Communication: Trend Analysis Of Technologies And Approaches*. Input Paper. Prepared for the Global Assessment Report on Disaster Risk Reduction 2015. UNISDR and GAR

[50] http://www.telegraph.co.uk/news/worldnews/europe/italy/9015901/Amateur-video-captures-cruise-ship-evacuation-panic.html

[51] EU FP7 Project 'Alert4All' at http://www.dlr.de/kn/en/desktopdefault.aspx/tabid-4309/3222_read-29975/admin-1/

[52] Alexander, D. E. (2013). Social Media in Disaster Risk Reduction and Crisis Management. *Science and Engineering Ethics*, 1–17. http://doi.org/10.1007/s11948-013-9502-z

[53] Alexander, D. E. (2013). Social Media in Disaster Risk Reduction and Crisis Management. *Science and Engineering Ethics*, 1–17. http://doi.org/10.1007/s11948-013-9502-z

[54] Watson, H., & Finn, R. L. (2013). Privacy and ethical implications of the use of social media during a volcanic eruption : some initial thoughts. In Proceedings of the 10th International ISCRAM Conference – Baden-Baden, Germany, May 2013 (pp. 416–420).

[55] Crump J.: 'What Are the Police Doing on Twitter? Social Media, the Police and the Public' in Policy & Internet Journal: vol.3 issue 4, December 2011

[56] http://courseweb.ischool.illinois.edu/~katewill/fall2009-lis590col/PalenEtal_2007_CitizenCommuInCrisis.pdf

[57] Stal, Marc. 2015. *Disaster And Crisis Communication: Trend Analysis Of Technologies And Approaches*. Input Paper. Prepared for the Global Assessment Report on Disaster Risk Reduction 2015. UNISDR and GAR

[58] Alexander, D. E. (2013). Social Media in Disaster Risk Reduction and Crisis Management. *Science and Engineering Ethics*, 1–17. http://doi.org/10.1007/s11948-013-9502-z

[59] https://www.ideals.illinois.edu/bitstream/handle/2142/47257/308_ready.pdf?sequence=2

[60] http://burnsr77.github.io/assets/uploads/burns_rethinking_big_data.pdf

[61] Pirozzi, Nicoletta. (2013). 'The EU's Comprehensive Approach to Crisis Management'. Crisis Management Papers Series.

[62] The Briefing - Police Use of Social Media: Police Foundation, June 2014

[63] ISO 31000:2009 and Global Institute for Risk Management Standards.

[64] ISO 22301: Clause - 4.3.2 Scope of BCMS - and ISO 22313: Clause - 4.3.2 Scope of BCMS

[65] ISO 22301: Clause - Scope and ISO 22313: Clause - Scope and 4.2.2

[66] ISO 22313: Clause - Business Continuity, p.viii

[67] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61029/Chapter-6-Business-Continuity-Management_amends_04042012.pdf

[68] http://www.jesip.org.uk/home

[69] http://www.jesip.org.uk/uploads/media/pdf/Joint%20Doctrine/JESIP_Joint_Doctrine_The_Inter.pdf

[70] http://www.jesip.org.uk/what-will-success-look-like

[71] Kuipers, S., Boin, A., Bossong, R. And Hegemann, H. (2015). Building Joint Crisis Management Capacity? Comparing Civil Security Systems in 22 European Countries, Risk, Hazards and Crisis in Public Policy, Vol 6, No. 1.

[72] EU FP7 Project Alert4All Deliverable 2.2 'Analysis of Current Practices Report'

[73] Tercovich, Giulia. (2014). 'The EEAS Crisis Response System'. *Journal of Contingencies and Crisis Management*, 22(3): 150-157

[74] Boin, Arjen, Ekengren, Magnus and Rhinard. (2014b). *Making Sense of Sense-Making: The EU's Role in Collecting, Analysing, and Disseminating Information in Times of Crisis*. The Swedish National Defence College: Elanders Sverige AB: Vällingby. Accessed online at: http://www.societalsecurity.eu/uploads/Articles/2014_Boin%20Ekengren%20Rhinard_Sensemaking_FHS%20Book.pdf [Accessed: 01.10.2015]

[75] South Easter Europe Disaster Risk Mitigation and Adaptation Programme (SEEDRMAP). (2008). *The Structure, Role and Mandate of Civil Protection in Disaster Risk Reduction for South Eastern Europe*. World Bank and United National International Strategy for Disaster Reduction Secretariat (UNISDR). http://www.unisdr.org/files/9346_Europe.pdf [Accessed 01.10.2015].

[76] Boin, Arjen and Ekengren, Magnus. (2009). 'Preparing for the World Risk Society: Towards a New Security Paradigm for the European Union'. *Journal of Contingencies and Crisis Management*, 17(4): 285-294.

[77] South Easter Europe Disaster Risk Mitigation and Adaptation Programme (SEEDRMAP). (2008). *The Structure, Role and Mandate of Civil Protection in Disaster Risk Reduction for South Eastern Europe*. World Bank and United National International Strategy for Disaster Reduction Secretariat (UNISDR). http://www.unisdr.org/files/9346_Europe.pdf [Accessed 01.10.2015].

[78] Boin, Arjen and Ekengren, Magnus. (2009). 'Preparing for the World Risk Society: Towards a New Security Paradigm for the European Union'. *Journal of Contingencies and Crisis Management*, 17(4): 285-294.

[79] Pirozzi, Nicoletta. (2013). 'The EU's Comprehensive Approach to Crisis Management'. Crisis Management Papers Series.

[80] https://eeas.europa.eu/headquarters/headquarters-homepage_fr/8477/The%20Crisis%20Management%20and%20Planning%20Directorate%20(CMPD

[81] Boin, Arjen and Ekengren, Magnus. (2009). 'Preparing for the World Risk Society: Towards a New Security Paradigm for the European Union'. *Journal of Contingencies and Crisis Management*, 17(4): 285-294.

[82] South Easter Europe Disaster Risk Mitigation and Adaptation Programme (SEEDRMAP). (2008). *The Structure, Role and Mandate of Civil Protection in Disaster Risk Reduction for South Eastern Europe*. World Bank and United National International Strategy for Disaster Reduction Secretariat (UNISDR). http://www.unisdr.org/files/9346_Europe.pdf [Accessed 01.10.2015].

[83] Tercovich, Giulia. (2014). 'The EEAS Crisis Response System'. *Journal of Contingencies and Crisis Management*, 22(3): 150-157.

[84] Boin, Arjen, Rhinard, Mark and Ekengren, Magnus. (2014a). 'Managing Transboundary Crisis: The Emergence of European Union Capacity'. *Journal of Contingencies and Crisis Management*, 22(3): 131-142.

[85] Stal, Marc. 2015. *Disaster And Crisis Communication: Trend Analysis Of Technologies And Approaches*. Input Paper. Prepared for the Global Assessment Report on Disaster Risk Reduction 2015. UNISDR and GAR.

[86] Stal, Marc. 2015. *Disaster And Crisis Communication: Trend Analysis Of Technologies And Approaches*. Input Paper. Prepared for the Global Assessment Report on Disaster Risk Reduction 2015. UNISDR and GAR.

[87] Boin, Arjen, Ekengren, Magnus and Rhinard. (2014). Making Sense of Sense-Making: The EU's Role in Collecting, Analysing, and Disseminating Information in Times of Crisis. The Swedish National Defence College: Elanders Sverige AB: Vällingby. Accessed online at: http://www.societalsecurity.eu/uploads/Articles/2014_Boin%20Ekengren%20Rhinard_Sensemaking_FHS%20Book.pdf

[88] EU FP7 Project SecInCoRe Deliverable 2.3 'Report on performance, goals and needs and first draft of new crisis management models and ethical, legal and social issues'