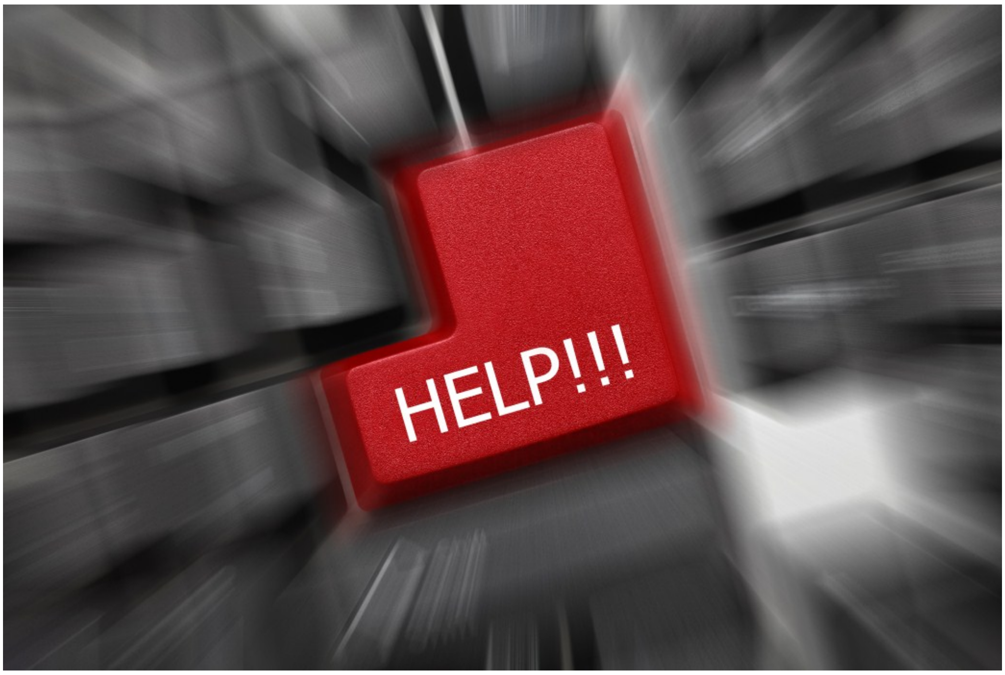
enisa
European Network
and Information
Security Agency



Emergency Communications Stocktaking

A study into Emergency Communications Procedures

Contributors to this report

ENISA would like to recognise the contribution of Mr. David Cohen of Analysys Mason Limited, who prepared this report in collaboration with and on behalf of ENISA.

Acknowledgements

ENISA would like to acknowledge the contributions of the following experts, who provided valuable input and comments during the preparation of this report.

- Hans Akermark, Swedish Post and Telecom Authority, Sweden
- Mircea Ghita, Special Telecommunications Service, Romania
- Andreas Garyfallos, Ministry of Infrastructure, Transport and Networks, Greece
- John Healy, Federal Communication Commission, USA
- Anita Kołodyńska, State Fire Service, Poland
- Ulrich Latzenhofer, Rundfunk und Telekom Regulierungs- GmbH, Austria
- Gerald McQuaid, Vodafone, United Kingdom
- Stefan Mikus, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Germany
- Manuel Pedrosa de Barros, Autoridade Nacional de Comunicações, Portugal
- David Trissell, Federal Emergency Management Agency, USA
- Reiner Wyphol, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Germany

Published: December 2012

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact details

For contacting ENISA or for general enquiries on Emergency Communications, please use the following details:

- E-mail: Resilience@enisa.europa.eu
- Internet: http://www.enisa.europa.eu
- Follow us on Facebook Twitter LinkedIn YouTube & RSS feeds

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Contents

List of Tables

1 Executive summary

The Emergency Communications Stocktaking project is an initiative of the European Network and Information Security Agency (ENISA) to determine how emergency services communicate within their own organisations and with each other in times of emergency or crisis, in order to respond to a serious incident. The aim is to identify how processes and technology might be improved, and to provide guidance to policy makers in Member States and the European Union.

Using a comprehensive methodology of primary research and interviews with relevant stakeholders in the regulatory, service provision and crisis response sectors, the study was able to identify that:

- Terrestrial Trunked Radio (TETRA) is widely used (but is not ubiquitous) across Europe by emergency services
- some emergency services do use data services, often on commercial networks, but data is not used between the emergency services and the public
- some civil defence organisations have a military background and are subject to national security restrictions, limiting inter-agency working
- standards and policies for emergency communications are often developed in vertical silos, making inter-agency communication (e.g. between police and ambulance organisations) difficult
- inter-agency communication problems are a common issue identified in post-crisis reviews of major incidents
- integrated inter-agency communications and aggregated information from the public can improve situational awareness for crisis responders
- technology failure is often an issue identified in post-crisis reviews of major incidents, and having broader technical back-up capabilities that anticipate and mitigate such failures is useful; data services (especially from the public) fit into this model
- EU treaties set an expectation for cross-member-state crisis responses, if required, and crisis responders need to be prepared to operate in this way.

These findings were summarised into three key objectives:

- **develop improved inter-agency crisis communications technology and procedures**
- **define standards in crisis communications technology and procedures**
- **encourage the uptake of data services in emergency communications, particularly in the area of public interaction.**

On the basis of meeting these key objectives, a series of recommendations was made to Member State governments, competent authorities, service providers and the bodies of the European Union.

2 Introduction

The Emergency Communications Stocktaking project is an initiative of the European Network and Information Security Agency (ENISA) to determine how emergency services communicate within their own organisations and with each other in times of emergency or crisis, in order to respond to a serious incident.

2.1 Rationale

The aim of the study is to identify technical and policy practices currently used, or which could be used, to prioritise availability and continuity of emergency communications in cases of major crisis. The resulting output will be used to provide guidance to policy makers in Member States and within the European Union in the effective support of emergency communications for the future.

2.1.1 Background information

According to the INDIGO project "Modern societies have experienced a spate of catastrophic events in recent years. Terrorist attacks (London, Madrid, Mumbai), factory explosions (Enschede, Toulouse), floods and storms (Louisiana) – these are but a few examples of crises and disasters that threaten the security, prosperity and wellbeing of citizens. […]

The recent crises have demonstrated the inherent difficulties that urban safety and crisis managers face when a large-scale disaster threatens an urban environment. In this ever-changing environment, it is hard to design proper emergency plans, to train security organizations and effectively handle crisis management procedures."[1]

A crisis is typically defined as an event that increases the insecurity of an environment, disturbing a group, a community or the whole society. A crisis should be presumed whenever an event with a high impact on national security, public health and public safety, national economy, environmental effects, geographical spread, public confidence or media attention occurs.

For dealing with a crisis, a response plan needs to be put in place. Usually, the measures which need to be taken are captured in a contingency plan. The definition[2] used by the United Nations (UN) describes a contingency plan as "a forward planning process, in a state of uncertainty, in which scenarios and objectives are agreed, managerial and technical actions defined, preparedness measures undertaken to mitigate the effects and response systems put in place in order to prevent, or better respond to, an emergency".

[1] *The INDIGO project, which is supported by the European Commission through the Security Research programme under FP7, **http://indigo.diginext.fr/EN/index.html***

[2] *Handbook for Emergencies, UNHCR, 2007, http://www.unhcr.org/472af2972.pdf*

In the Good Practice Guide on National Cyber Contingency Plans (NCPs)[3], the following definition is used: NCPs are the interim structures and measures to respond and recover services following major incidents that involve Critical Information Infrastructures (CIIs) and that lead to a crisis. Interim structures may involve the formation of committees and response teams (at various levels), the initiation of secure, robust means and platforms for communication, possibly the assembly of a crisis cell, and the involvement of different actors from the private sector(s) that have predefined roles during the crisis response.

For assuring a co-ordinated response to a crisis, the contingency plan will define the involved actors and their roles. Such actors are usually named ‘emergency responders’, which are organisations that safeguard public safety and health by tackling different emergencies.

The existence of resilient and reliable communication channels for such responders, including the crisis management cells[4], becomes crucial when dealing with the security and safety of the public. According to Koivukoski[5], the communication needs of public safety authorities are:

- reliable and robust voice communication everywhere
- allowing for co-operation and easy communication between all organisations
- short messaging for alarming and field task delivery, and to secure the validity of the information
- file transfer from the place of incident to support sites as the command or 112 centres
- offering of communication from the field for daily office work.

The INDIGO project points out the fact that “Communications have traditionally been the Achilles’ Heel of response operations. During disasters, communications networks often break down. The effect on information exchanges and, consequently, crisis coordination and effectiveness, has been widely described. A precondition for any working software system is a reliable communication network.”[6]

This report aims to take stock of this key topic by assessing existing practices in this area, with a view to understanding the mechanisms, the policies and the legal frameworks used in Europe and in selected countries to facilitate emergency communication, including voice and data (wireless, wired, and satellite), during a crisis.

[3] *ENISA Good Practice Guide on National Cyber Contingency Plans, https://www.enisa.europa.eu/activities/ Resilience-and-CIIP/national-cyber-security-strategies-ncsss*

[4] *Crisis management cells are pre-planned organisational arrangements, facilities and command structures that can be activated on demand when a crisis arises*

[5] *J. Koivukoski, “What are the future solutions and technologies of national security communications?” VIRVE Day -seminar, Helsinki, Finland, March 2011*

[6] *The INDIGO Project,* ***http://indigo.diginext.fr/EN/index.html***

2.1.2 Target audience

The target audiences for this study are:

- government ministries in Member States with responsibilities for crisis management (and emergency communications)
- competent authorities in Member States with responsibilities for crisis management and emergency communications (regulators, civil defence organisations and emergency services)
- policy makers at the EU level (the European Commission and relevant EU agencies).

3 Emergency Communications Stocktaking Study

This section introduces the definitions used, outlines our methodology, and discusses the findings of the study.

3.1 Definitions

Before the findings of the study are considered, it is worth defining some of the concepts and terms that relate to emergency communications.

- **Emergency services** – "The set of specialized agencies that have specific responsibilities and objectives in serving and protecting people and property in emergency situations."[7]

  Three main functions are provided by the emergency services – police, fire and rescue, and emergency medical services. These functions can be provided by separate organisations or a single service. The terms 'first responders' or 'crisis responders' are also used, as these services are normally initiated directly in response to an incident.

- **Civil protection** – "… the aim of Civil Protection is to minimise the impact of catastrophic events. Civil Protection organisations are those which coordinate the necessary actions to mitigate and, where possible, prevent the risk of disasters. Civil Protection is involved with the construction of specific knowledge, the ability to issue early warnings, the ability to reach people through different information channels, the capacity to coordinate human resources and the technology needed to cope with calamities. It includes the non-structural measures that will positively impact on governments' abilities to respond effectively to disasters."[8]

  During the cold war, civil protection was principally focused on defence from large-scale military attack (especially nuclear bombardment), but recently has become more generally applied to large-scale emergencies or disasters. Typically, civil protection will be invoked in an incident response when the responding emergency services feel that the scale of the incident is larger or more widespread than normal.[9]

- **Disaster** – "A serious disruption of the functioning of a community or a society involving widespread human, material, economic or environmental losses and impacts, which exceeds the ability of the affected community or society to cope using its own resources."[7]

- **Crisis** – an ongoing unstable or dangerous situation affecting a group or society. A crisis is typically considered to be degradation in the normal functioning of a system, and, in the context of a disaster, the infrastructure damage or loss of life that results can precipitate a

[7] *Terminology for Disaster Risk Reduction, United Nations Office for Disaster Risk Reduction (UNISDR), Switzerland, 2009. Available at http://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf*

[8] *The Structure, Role and Mandate of Civil Protection in Disaster Risk Reduction for South Eastern Europe, UNISDR, Switzerland, 2008. Available at http://www.unisdr.org/files/9346_Europe.pdf*

[9] *In some jurisdictions, civil defence remains the responsibility and prerogative of the military. Military communications are outside the scope of this study and none of the discussion, assessment or recommendations of the study apply to military procedures or infrastructure, even where these overlap with crisis response requirements.*

civil crisis. A key element of a crisis is the need for ongoing out-of-the-ordinary decision-making and management response to ensure that the situation improves rather than gets worse, and that the system in crisis reverts as quickly as possible to normal operation and management.

- **Emergency communications** – systems and processes that allow the emergency services, civil protection authorities, governments and the populace to communicate or interact, and, as such, to manage responses to an incident, disaster or crisis. The typical communications systems used in an emergency are:
  - broadcast – radio and television signals transmitted for reception by the public for the purposes of providing situational awareness and general directives to the populace
  - telephony – commercial voice systems (both fixed and mobile) that allow individuals to request aid from the emergency services (using a national emergency number scheme), or to contact each other for information exchange or reassurance
  - Internet – commercial data systems used for electronic communication, either person-to-person (email, messaging, voice over IP) or for broadcast purposes (social media and Web blogging)
  - data networking – private IP networks (normally sourced from commercial service providers) that are used for electronic exchange of information. Often provide secure gateways to the Internet or other Government networks
  - emergency radio – private radio systems operated by the emergency services, civil protection agencies or government, designed to be highly available (even in disaster conditions) and optimised for the command-and-control requirements of emergency services.

3.2 Methodology

The methodology for the project was as follows:

- project initiation – setting up of goals of the project
- information gathering – understanding current approaches and thinking around emergency communications
- analysis and output – a consideration of the information gathered, looking for common requirements, gaps in provision and a series of proposed recommendations to improve emergency communications provision.

3.2.1 Objectives of information gathering exercise

The information gathering exercise for this project had three main objectives:

- understanding of the emergency communications policies, procedures, technology and supporting arrangements for countries across the EU
- identifying how emergency communications are being developed by policy makers and practitioners across the EU, in particular where it is felt that improvements are required

- identifying how emergency communications services and systems have performed during actual incidents around the world, and seeing what lessons can be learned from these incidents.

These objectives were met through a combination of desktop research and stakeholder engagement.

3.2.2 Desktop research

The desktop research phase involved using established, referenced sources to gather relevant information pertinent to the project. Sources considered included:

- websites of stakeholder organisations (telecoms operators, telecoms regulators, civil defence organisations, emergency services)
- published white papers from the telecoms industry and academia
- speeches and presentations given on relevant topics at industry events.

A citation list of desktop research references that contributed to the report can be found in Annex I: References.

3.2.3 Stakeholder engagement

The preferred method for information gathering for this project was direct stakeholder engagement, by holding discussions with appropriate stakeholders to gather their input. This was performed by contacting likely stakeholders directly, offering them a chance to participate, and then arranging a teleconference call, guided by a pre-shared document in the form of a questionnaire.

The direct teleconference format with guided discussion has the following advantages:

- stakeholders can ensure that the information received for the project is of the highest quality and accuracy
- stakeholders can provide direct input into the project, ensuring that any agendas for structural improvements in emergency communications are directly reflected in the final output
- stakeholders can be sure that any sensitivities or dependencies that may arise from the project can be expressed directly to the ENISA project team and, as such, can be accounted for in the final output
- stakeholders who have been consulted directly can review and comment on the final report before publication
- stakeholders can advise their colleagues and partner organisations of the project and the final output, ensuring that they are aware of their country’s participation in the project effort.

Potential stakeholders were selected with a view to getting a wide range of responses from across the broad range of bodies responsible for communications in general, and emergency communications in particular: mobile operators, regulators, civil protection authorities and emergency services.

3.3 Information gathering findings

This section provides an overview of the project findings from the information gathering exercise.

3.3.1 Emergency communications across Europe

Emergency communications systems within each Member State are typically provided as a private radio network – radio works best for emergency services as their requirements are for voice communication devices that are mobile and can be worn by individuals in diverse, unknown environments.

The dispositions of different types of radio system across Europe are as shown in Figure 1.

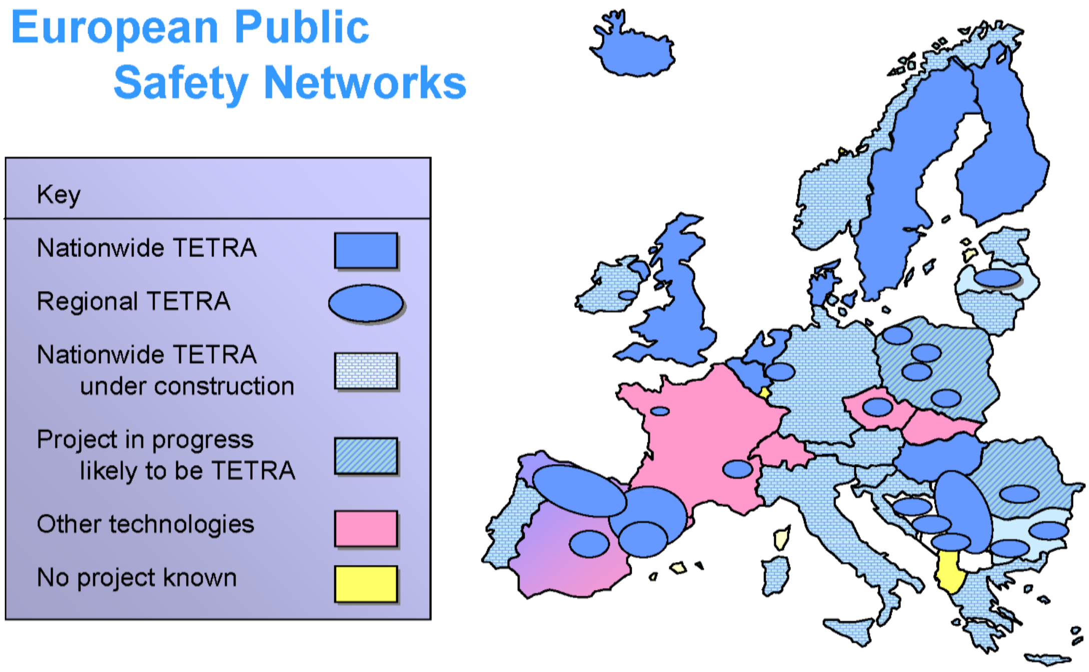


Figure 1: European public safety network deployment [Source: Vts Police Netherlands]

Technology in use is primarily Terrestrial Trunked Radio (TETRA), a digital radio standard, although a competing standard, TETRAPOL, is in use in France. Where other non-TETRA systems are used, these are typically older analogue radio systems.

Telecoms regulators support emergency communications within each Member State by ensuring that commercial communications operators comply with legal requirements on telecoms services availability, interaction with the emergency services and provision of emergency number call reporting services. The level of support that each state's regulators offer their local communications operators in meeting their statutory obligations in regard to emergency communications varies. As the managers of each state's radio spectrum, regulators also have an indirect role in the provision of the radio systems used by the emergency services (except where that service provision is provided by a commercial entity).

When asked about the use of data services in the emergency communications arena, the stakeholders reported that some emergency users are using commercial data services for command-and-control functions (on smartphone handsets), with procedures to fall back to radio and voice if necessary. Some use of the data capabilities of TETRA was also reported, though this is limited by the capabilities of the system and terminals available. Regulators recognise that data services are becoming a much more important communication tool for the public, and are beginning to respond by examining policies around the resilience and availability of data services.

3.3.2 Legacy of military provision of civil defence functions

An issue that was encountered from some potential participants in the information gathering process was an inability to provide detailed answers to the questions raised in the study because of potential national security concerns.

This situation arises because many countries have extended their civil defence arrangements (conceived during the cold war to help citizens respond to a military attack) to cover crisis response for the public – as the organisational arrangements and physical infrastructure required for mass shelter in a crisis are broadly similar to those required for protecting the public from a military attack.

However, where this occurs, the civil defence organisation can often be dependent on military infrastructure for its communications and logistical arrangements, even where the civil defence service itself is no longer provided by the military. As such, these arrangements will be subject to confidentiality requirements in the interests of national security that can restrict the ability to share or discuss these arrangements without the appropriate security clearances. In addition, any such sharing of information would not be able to be publicly disseminated.

Key observations

A legacy of military involvement in civil defence can create national security concerns about the sharing of information regarding civil defence arrangements.

These national security concerns could limit the ability of the organisation concerned to collaborate with similar agencies in other jurisdictions.

3.3.3 Standardised approach adopted – but often only within each emergency responder

An examination of the general approach to crisis management shows a common structure is in use in most crisis response organisations: a tiered command structure (such as the UK's

Gold-Silver-Bronze arrangement within each of the emergency services) allowing for hierarchical decision making within each emergency service. The concept is that the top tier of command within each emergency service can liaise with the others for a co-ordinated response – but this does create tensions in decision-making, with differing priorities and requirements from each organisation. An additional problem can arise when an executive decision maker (such as a government minister) interfaces at the Gold command level, and this can interfere with the standard approach.

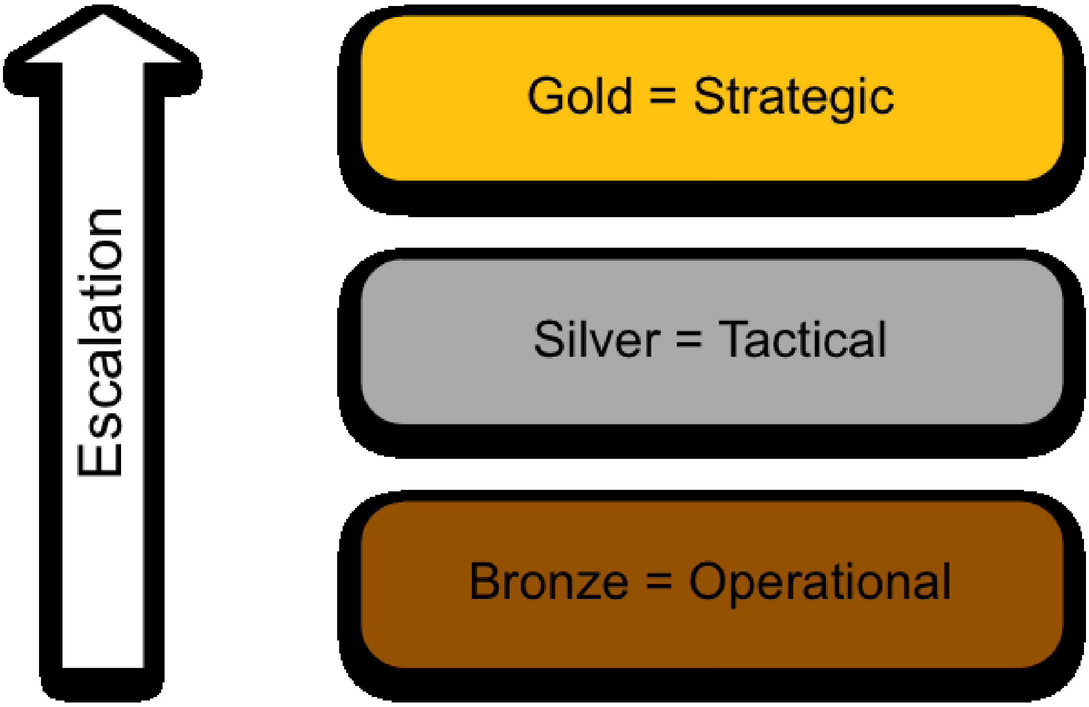


Figure 2: Gold-Silver-Bronze command structure [Source: Analysys Mason, 2012]

The different emergency services use their communications systems in different ways, as shown below.

Emergency service	Use of communication
Police	• Centralised control of officer and unit dispatch • Individual officer two-way communication with central control for data access and situation updates • Group voice messaging (talk groups) • Officer-to-officer direct communication
Emergency Medical	• Centralised dispatch model • Communication primarily to vehicles rather than officers • Text information transfer (dispatch addresses, patient details) important • Low level of traffic back to central dispatch
Fire and Rescue	• Centralised dispatch model • Dispatch performed over fixed lines to stations rather than radio • Communications requirements focused on on-site incident control and communication • Only incident command needs communication back to centre

Table 1: Emergency Services Communications Use [Source: Analysys Mason Emergency Services Consultancy Experience, 2012]

A common theme from the interviews with stakeholders is that there are often several streams of emergency communications operating within EU states, under the purview and responsibility of different organisations. For example, for some respondents, crisis communications with the public are the responsibility of the ministry of communications, and the mechanisms for government decision makers to communicate with crisis first responders is provided by the telecoms regulator. As discussed in Section 3.3.2, in other states, legacy organisational arrangements of military responsibility means that all crisis responses and provision (including communications) sit within a civil defence organisation.

It was noted during the stakeholder interviews that the development of standardised approaches to voice for emergency communications (procedures, command engagement structures, technical operational arrangements etc.) has come from the sharing of experience and best practice between organisations. This experience is not so well established for data services, and the use of social media or engagement with the public, and developments in this area, are much more specific to each responder, rather than adopting common approaches.

The stakeholder interviews also revealed the success that some countries have had with a centralised umbrella organisation for crisis management and co-ordination between different first responders.

Key observations

Different types of crisis responder have different communications processes, making inter-agency communication more of a challenge.

Standardisation of process and technology is a route to address such inter-agency communication.

A centralised umbrella organisation can also promote standardisation and co-ordinate between different agencies.

3.3.4 Lessons learned from crisis events – communications improvements required

There are numerous occasions when reports into major crises have found failings in the way emergency responders and decision makers have been able to communicate with each other. Some notable examples are outlined below.

- Queensland floods, January 2011[10] – interoperability communication problems between the fire and rescue/ambulance service, the police service and the state emergency service (a civil protection volunteer service) led to confusion, non-optimal responses, and a lack of confidence from the public in the ability of the emergency services to cope with the situation. In addition, interoperability deficiencies within the police service's call response centres meant that some dispatch requests for officers had to be performed manually over radio or fixed communications.
- Victorian Bush Fires, February 2009[11] – a lack of co-ordination between emergency services responding to multiple simultaneous incidents, an inability to share information between ICT systems, multiple radio systems that could not cross-communicate, and an inability to effectively communicate revised evacuation policies, hampered the response to ferocious fires in which nearly 200 people were killed.
- Hurricane Katrina, August 2005[12] – lack of communication between local and state-level responders and officials led to underestimates of the initial impact of the storm impact and slow mobilisation of support services, food and water to last-resort shelters within New Orleans.
- London bombings, July 2005[13] – there were multiple emergency service responses, but even three hours into the incident, the ambulance service was unaware of the true number

[10] *The State of Queensland, Australia, 2012. Queensland Floods Commission of Enquiry final report. Available at http://www.floodcommission.qld.gov.au/publications/final-report*

[11] *The State of Victoria, Australia, 2009. Victorian Bushfires Royal Commission Final Report Recommendations. Available at http://www.royalcommission.vic.gov.au/getdoc/5bc68f8a-a166-49bc-8893-e02f0c3b37ab/VBRC-Final-Report-Recommendations*

[12] *Appleseed, USA, 2006. A Continuing Storm: The On-Going Struggles of Hurricane Katrina Evacuees. Available at http://www.appleseednetwork.org/wp-content/uploads/2012/05/A-Continuing-Storm.pdf*

[13] *The Guardian, London, 2011. Communications underscores London's emergency planning. Available at http://www.guardian.co.uk/public-leaders-network/2011/aug/24/communication-emergency-planning-london*

and locations of the explosions, despite this having already been ascertained by the police and fire services. This resulted in substantial delays in mobilising services.

- Elbe Floods, 2002[14] – key recommendations in the subsequent enquiry into this disaster included revising command-and-control arrangements to ensure that information travels from responders to decision makers and back again, rather than being a one-way flow, and that inter-agency disaster management communication is vital.

The example of the Victoria bush fires is particularly pertinent, as the aftermath was investigated by a Royal Commission. The report stressed the need for effective inter-agency communication. Key quotes from the final report[15] include:

> "When the State's approach to fighting ferocious fires is so highly dependent on cross-agency coordination it is unacceptable that effective coordination of information systems has not been achieved"
>
> "[...] effective access to and use of technology is important to effective detection and management of fires and tracking of resources on the ground. As noted, various problems became evident with information technology at incident control centres, including because the CFA and DSE used different systems and incident management team staff sometimes had difficulty gaining access to both systems. This inhibited the use and transfer of information such as warnings, maps and situation reports"
>
> "Communications systems on 7 February were also hindered by poor coverage, lack of interoperability between emergency services agencies, and insufficient investment in new technologies. For example, the transmission speed of the paging system had been reduced in order to expand reception coverage, and this caused serious delays in other than the most urgent messaging. There were also communication difficulties between metropolitan and regional police because of incompatible radio systems".

Of the 67 recommendations made as a result of the Royal Commission investigation, seven related in part to the effectiveness of agency interoperability, and two specifically recommended improvements in communications systems

[14] *Saxon State Government, Germany, 2002. Report of the Independent Commission of the Saxon State Government into the 2002 Flood. Available at https://publikationen.sachsen.de/bdb/artikel/10825/documents/10951*

[15] *The State of Victoria, Australia, 2009. Victorian Bushfires Royal Commission Final Report Recommendations. Available at http://www.royalcommission.vic.gov.au/getdoc/5bc68f8a-a166-49bc-8893-e02f0c3b37ab/VBRC-Final-Report-Recommendations*

Recommendation no. in final report	Detail
22	The Country Fire Authority and the Department of Sustainability and Environment standardise their operating systems and information and communications technologies with the aim of achieving greater efficiency and interoperability between agencies.
23	The Country Fire Authority review and improve its communications strategy as a matter of priority and develop a program for identifying and responding to black spots in radio coverage. Only incident command needs communication back to centre.

Table 2: Communication interoperability recommendations [Source: Victorian Bushfires Royal Commission, 2009]

Stakeholder discussions as part of this study emphasised importance and value of the engagement that first responders have with each other and the industry and regulators in their countries to develop and improve services and policy.

Key observations

Lack of interoperability between first responders and communication problems are the most common findings in post-crisis lessons learned exercises.

Both standardisation and the resilience of infrastructure have been cited in post-crisis reviews as issues that need to be addressed.

3.3.5 Clarity of situational awareness

As exemplified by the examples above, the development of a good understanding of the crisis situation is key to effective responses. Good inter-agency communication is crucial to achieving this, and in the age of 24-hour news, Internet news and social media, information from the public also has a role to play in providing a breadth of situational information.

- During the Deepwater Horizon oil spill in 2010, live video monitoring feeds of the capped oil well showed a sudden increase in oil flow when the cap slipped. A member of the public spotted this and blogged about it; the media then picked it up and began querying the Joint Information Centre (which was managing the spill operation) about it. The speed of this interrogation by the media, based on observations by a member of public, was faster than the internal reporting of the increase in leakage to the operation's leadership team.[16]
- Recognising the need for improved situational awareness, the City of Madrid commissioned an integrated advanced command centre for the city, bringing together

[16] *O'Brien's Response Management, USA, 2010. Unending Flow – Case Study on Communications in the Gulf Oil Spill. Available at https://www.piersystem.com/external/content/document/3571/1009367/1/Unending Flow_v1.01.pdf*

software and communications services for all of the city's first responders to provide a co-ordinated view of any crisis situation. It was found during the bombings that developments during an event (subsequent explosions and the pursuit of the bombers) strained resources that had already been fully committed to the initial explosion rescue.[17]

- In the United States, the Department of Homeland Security is pursuing a federal emergency communications plan and a nationally interoperable first responder broadband network, aimed at assisting local responders in building integration and co-operative communications into their planning and systems to improve the exchange of situational data.[18,19]
- The ICT Centre at the Commonwealth Scientific and Industrial Research Organisation (which is the Australian government's national science laboratory) has developed and successfully demonstrated a statistical algorithm for analysing social media trends to highlight emerging incidents as they happen and allow for situational information to be aggregated and collated for senior decision maker use. This system identified and reported on 12 major emergency incidents in the Asia–Pacific region over an 18-month period of monitoring, with a throughput of 600 million social media messages.[20]
- The Kirchbach report[21] into the 2002 Elbe floods made a number of comments and recommendations about providing better situational information to the public by crisis responders:

> "The local authorities and lower emergency response authorities were forced, under the pressure of events, to inform and warn the population about measures. The information provided was of variable quality and in many cases in the early stages of the disaster was issued too late.
>
> In some cases the questionable decision was made to withhold warnings because of concerns about creating panic. Lack of information is often a cause of panic.
>
> The lower emergency response authorities had no secure access to regional media. Occasional interviews are no substitute for official announcements or statements.

[17] *IBM, USA, 2010. City of Madrid: Coordinated emergency response raises public safety to a new level. Available at http://www-01.ibm.com/software/success/cssdb.nsf/CS/JSTS-7ZWSPF?OpenDocument&Site=default&cty=en_us*

[18] *Department of Homeland Security, USA, 2008, National Emergency Communications Plan. Available at http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf*

[19] *Department of Homeland Security, USA, 2012, Public Safety Broadband: Fulfilling a 9/11 Commission Recommendation. Available at http://www.dhs.gov/public-safety-broadband-fulfilling-911-commission-recommendation*

[20] *Commonwealth Scientific and Industrial Research Organisation, Australia, 2012. Tapping into Social Media to Build Emergency Situation Awareness. Available at http://www.apcoaust.com.au/2012/presentations/2012APCOA_Mark_Cameron.pdf*

[21] *Saxon State Government, Germany, 2002. Report of the Independent Commission of the Saxon State Government into the 2002 Flood. Available at https://publikationen.sachsen.de/bdb/artikel/10825/documents/10951*

> In many cases loudspeaker systems for providing locally relevant information were unavailable. Loudspeakers alone were found to be insufficient at night and under difficult weather conditions. Sirens are needed to attract attention to the loudspeaker announcements."
>
> "**The commission recommends** […]
>
> […] designing the notification system as a two-way street and fundamentally overhauling the system [...]
>
> […] funding and implementing an appropriate warning system that both warns and informs the public […]"

It was clear from the stakeholder discussions for this study that the focus of emergency service crisis management remains on voice communications – though this remains an inefficient method for promoting situational awareness, especially when the voice traffic concerned comes from untrained members of the public. The aggregated view of data from social media and other online reporting tools has been embraced by the media, and yet, for the moment, plans for emergency service use remain nascent.

Key observations

Integration and interoperability of communications and command and control of different crisis responders dealing with the same incident can improve overall responses and effectiveness.

Information from the public can be captured, assessed and aggregated to reliably improve the situational awareness available to incident commanders.

3.3.6 Technology loss

Many emergency services invest heavily in separate, robust and resilient communications infrastructures for the purposes of operational security and high availability, while the public are also increasingly reliant on the use of commercial mobile phone services. However, people and processes can become overly dependent on these technologies, and, should they fail, operational processes can become less effective and public responses to the inability to communicate can exacerbate technical difficulties. Some examples are provided below.

- In the Great East Japan Earthquake of 2011, much of the earthquake monitoring and emergency communications infrastructure survived the earthquake itself, but was rendered inoperative due to power loss; receiving equipment used by citizens was similarly disabled. This hampered efforts to warn citizens of the incoming Tsunami and the need to seek higher ground.[22]

[22] *Electronics News, Australia, 2011. Japan's 2011 earthquake and tsunami: communications and networks. Available at http://www.electronicsnews.com.au/news/japan-s-2011-earthquake-and-tsunami-communications*

- After the Moscow subway bombings in March 2010, the volume of mobile phone calls between the travelling public and their families (trying to reassure each other about their safety) rapidly overwhelmed the mobile phone networks' capacities, and the systems went down. This led to further confusion regarding a hoax report of a third explosion, and the perception remains among critics of the Russian government that the networks were deliberately closed down by the Ministry of Emergency Situations.
- In the Victorian Bush Fires of 2009, the problems of communication that were encountered on that day were added to by the loss of radio coverage that arose as the fires destroyed regional radio mast equipment.[23]
- In the case of the London bombings in July 2005, the inability to operate the emergency services' Airwave TETRA radios underground led to delays in rescue efforts, through a combination of lack of situational awareness, indecision arising from a lack of communication with seniors, and time spent improvising ad-hoc communications procedures to compensate.[24]
- In the 2002 Elbe floods, loss of communications networks due to electricity failure was an issue in the emergency services' ability to respond.[12]

A corollary observation is that in a crisis any available technology that is unaffected by the crisis will be used for communication, with ad-hoc processes being created. For example, experience shows that the public will make use of Internet-based social media and voice over Internet technology when conventional systems are unavailable in a disaster (such as after the Great East Japan Earthquake[25],[26]), and many emergency responders carry private mobile phones or smartphone devices as a supplementary communication and data access tool. However, the creation of ad-hoc processes carries risks of sub-optimal organisation and duplicated 'islands' of effort.

The stakeholder interviews for this study revealed that all organisations involved in crisis response conduct regular exercises to measure the effectiveness of their processes, procedures and infrastructure. It was not clear, however, to what extent loss of infrastructure is simulated in such exercises.

[23] *The State of Victoria, Australia, 2009. Victorian Bushfires Royal Commission Final Report Recommendations. Available at http://www.royalcommission.vic.gov.au/getdoc/5bc68f8a-a166-49bc-8893-e02f0c3b37ab/VBRC-Final-Report-Recommendations*

[24] *The Guardian, London, 2011. Communications underscores London's emergency planning. Available at http://www.guardian.co.uk/public-leaders-network/2011/aug/24/communication-emergency-planning-london*

[25] *Inderscience Publishers, USA, 2011. Twitter for Crisis Communication: Lessons Learnt from Japan's Tsunami Disaster. Available at http://www.sciencedaily.com/releases/2011/04/110415154734.htm*

[26] *Information-technology Promotion Agency, Japan, 2012. How Cloud Survived the Earthquake and Served People. Available at https://cloudsecurityalliance.org/wp-content/uploads/2012/07/Day1_1645_Track1_Session_KatsumiBen_-_IncMan_Katsumi_Ben.pptx*

Key observations

Despite high levels of investment and planning, loss of technology is a factor in many incidents and can hamper the crisis response.

A breadth of capability and coverage in communications technology can mitigate these issues – but it would be preferable if this were planned and integrated into the crisis response operations, rather than developing in an ad-hoc manner.

3.3.7 EU commitments to co-operation

Article 222 TFEU of the Treaty of Lisbon is a solidarity clause that places obligations of mutual assistance on EU members if requested in times of natural disaster or terrorist incident. Natural disasters (in particular storms and flooding) are more likely to affect one Member State at a time, and inter-agency communication issues take on an extra dimension of complexity when trying to enable co-ordination between different states.

The UK Parliament House of Lords considered the EU Internal Security Strategy in a report published in 2011[27], and clearly recognised calls for improved communication and co-operation between Crisis Situation Centres of Member States to support efforts under Article 222.

The need to respond to this commitment is therefore already in place for Member States and it is possible that this commitment will be tested (and even strengthened post-crisis) should the EU suffer a major cross-border crisis incident.

Key observations

There is a requirement on Member States to assist each other during crises, with a corollary requirement for effective inter-agency and inter-state emergency communications.

These requirements may increase in importance with time, and, as such, current decisions on common approaches and interoperability should reflect this.

[27] *Parliament House of Lords, UK, 2011, European Union Committee – Seventeenth Report: The EU Internal Security Strategy. Available at http://www.publications.parliament.uk/pa/ld201012/ldselect/ldeucom/149/14902.htm*

4 Outcomes and recommendations

This section summarises the outcome objectives identified from the information gathering and makes recommendations as to how these objectives could be achieved.

4.1 Key observations summary

From the information gathering exercise, a number of key observations were made. These are summarised in Table 3.

Key Observations
Different types of crisis responder have different communications processes, making inter-agency communication more of a challenge.
Standardisation is a route to address such inter-agency communication.
A centralised umbrella organisation can also promote standardisation and co-ordinate between different agencies.
Crisis responder interoperability and communication problems is the most common finding in a post-crisis lessons learnt exercise.
Both standardisation and the resilience of infrastructure have been cited as issues to be addressed in post-crisis reviews.
Integration and interoperability of communications, command and control of different crisis responders dealing with the same incident can improve overall responses and effectiveness.
Information from the public can be captured, assessed and aggregated to reliably improve the situational awareness picture available to incident commanders.
Despite high levels of investment and planning, loss of technology is a factor in many incidents and can hamper the crisis response.
A breadth of capability and coverage can mitigate these issues – but would be better planned for and integrated into the crisis response operation rather than dealt with in an ad-hoc way.
There is a requirement on Member States to assist each other in crisis response, with a corollary requirement for effective inter-agency and inter-state emergency communications.
These requirements may increase in importance with time, and as such current decisions on common approaches and interoperability should reflect this.

Table 3: Summary of key observations [Source: Analysys Mason]

4.2 Key objectives

The key observations can be condensed into series of key objectives for improvements in emergency communications within the EU and Member States. These key objectives can then be used to derive recommendations for stakeholders within Member States. The objectives cover the following areas, which are outlined in the sections below:

- inter-agency communication
- standards in process and technology
- increased use of electronic data and online services in emergency response.

4.2.1 Inter-agency communication

A common theme in post-crisis studies is the identification of shortcomings in communication between different agencies during a crisis. A NATO-Russia Council (NRC) conference in 2005 heard four separate briefings from teams in the USA, Russia, Spain and Turkey looking at responses to terrorist incidents; each independently identified inter-agency communication as a specific problem to be addressed.[28] Post-incident reviews of the London bombings were heavily critical of inter-agency communication shortcomings, as were those of the US response to Hurricane Katrina.[29] In the 2010 Haiti Earthquake response, disparate aid organisations lacked co-ordination due to poor communications.[30]

Consideration: How can inter-agency communication between responders and other stakeholders be improved across Europe, in a harmonised manner? And how can improved inter-agency communications be extended beyond the borders of Member States to allow a multi-state response to a crisis?

4.2.2 Standards in process and technology

A repeated finding from the information gathering process was that standardisation of process and technical interoperability is an aid to interoperability and effective communication.

This can be pursued with two approaches – a 'bottom up' approach where crisis responders themselves work in a collaborative fashion to plan, develop and implement appropriate standards, or a 'top-down' approach where a new organisation (such as a federal-level

[28] *NATO, Brussels, 2005. Lessons learned from recent terrorist attacks: Building national capabilities and institutions. Available at http://www.nato.int/docu/conf/2005/050727/index.html*

[29] *Appleseed, USA, 2006. A Continuing Storm: The On-Going Struggles of Hurricane Katrina Evacuees. Available at http://www.appleseednetwork.org/wp-content/uploads/2012/05/A-Continuing-Storm.pdf*

[30] *IEEE Spectrum Magazine, USA, 2010. Why Haiti's Cellphone Networks Failed. Available at http://spectrum.ieee.org/telecom/wireless/why-haitis-cellphone-networks-failed/*

Urgent Communications, USA, 2010. A Painful Lesson – Haiti suffers communications failures after earthquake. Available at http://urgentcomm.com/networks_and_systems/mag/disaster-communications-201006/

agency) acts as a conduit and co-ordinator of standardisation establishment between crisis responders.

Consideration: What is the best way to consider, plan and develop standards in crisis response communications across Europe?

4.2.3 Increased use of electronic data and online services in emergency responses

In the modern world, citizens are highly dependent on mobile telephone and data messaging systems to communicate with their friends and family. In times of crisis, media outlets increasingly rely on the 'citizen journalism' effect to receive on-the-spot reports from mobile data users, with phone camera images, social media reportage and the mapping and tracking capabilities of modern devices all used to evaluate events as they happen.

In the Great East Japan Earthquake and Tsunami in 2011, power loss disabled much of the conventional telephony infrastructure. However, cellular systems with high towers and battery back-up were able to function for longer, allowing citizens to communicate over social networks. In the aftermath, mapping and reporting websites were crucial in identifying injured and displaced people and eliminating them as fatal casualties.[31]

In contrast, during events such as the Haiti Earthquake[32] and the London bombings, mobile networks were overwhelmed by demand and failed. This hampered their use by emergency services, which often had data equipment that used commercial networks for communication and so were unable to function.

Fixed and mobile telephony services all have in-built support for call prioritisation of key individuals or service user groups (intended to allow first responder services or other critical users to communicate when voice networks are congested). However, in practice these functions are not well used due to the operational difficulties in managing the associated assets (numbers, SIM cards, devices etc.)

Consideration: How should data services (rather than voice) be used by responders as part of their communication plans, given the advantages in situational awareness they can potentially bring?

4.3 Recommendations to meet policy objectives

In order to see emergency communication improvements across the European Union in line with the key objectives identified, we make the following recommendations.

[31] *Electronics News, Australia, 2011. Japan's 2011 earthquake and tsunami: communications and networks. Available at http://www.electronicsnews.com.au/news/japan-s-2011-earthquake-and-tsunami-communications*

[32] *IEEE Spectrum Magazine, USA, 2010. Why Haiti's Cellphone Networks Failed. Available at http://spectrum.ieee.org/telecom/wireless/why-haitis-cellphone-networks-failed/*

4.3.1 Recommendations for Member States

Within Member States, there are two agents for change and improvement in the emergency communications sphere – government ministries and competent authorities:

- government ministries are organisations within a Member State government responsible for executing government legislation and policy
- competent authorities are non-government authorities with a responsibility for communications or crisis management – typically this will include regulatory authorities, civil defence organisations and the Member State's emergency services themselves.

The following two sections provide recommendations for both these agents.

4.3.1.1 Recommendations for government ministries

As has been discussed, the adoption of common standards and processes can serve as a facilitator for communication between different crisis responding agencies.

The areas where standardisation can assist in this regard are:

- common technical standards for crisis responder communication, which opens up the possibility of direct on-the-ground communication between responders from different agencies
- common technical standards could allow for equipment, staff or role sharing between disparate responders, giving crisis commanders more flexible options for resource deployment in a crisis
- common processes and standards allow for clarity in the exchange of information and decisions between different agencies, providing a better co-ordinated response to a crisis
- government adoption of the same standards allow for ministers and civil servants to interact where necessary with crisis responders.

In order to achieve this level of standardisation, government policy would be required to establish the principles of standardisation and to provide the appropriate consultative mechanisms to derive and implement such solutions. Such policy changes would also need to consider the wider implications of the Treaty of Lisbon solidarity clause and the Member State's attitude to compliance, including the possibility of establishing common standards with nearby states.

As discussed in the information gathering findings, some states have implemented standardisation and inter-agency communication improvements by establishing a federal agency to co-ordinate such activities. However, this approach may not fit politically in all Member States.

In terms of technical standards, TETRA is well established across the EU and proven in meeting the needs of crisis responders. However, it is not ubiquitous across all Member States, and government policy would need to reflect the local landscape in establishing the correct standards.

The findings also demonstrated that the use of Internet services such as social media have a part to play in crisis management, both as a situational awareness tool and a responsive, direct communication channel between crisis managers on the ground and the public. However, taking advantage of these opportunities will require co-ordination by government – particularly as, for many stakeholders interviewed during the information gathering exercise, government ministries are responsible for communicating with the public in a crisis.

However, most governments are working to develop e-services for their citizens, meaning that such capabilities could be developed as an extension of these efforts – and the policy frameworks required for establishing technology and standards in this area should already be in place.

Making best use of such capabilities requires correct technical solutions: the need to aggregate and summarise data from different online sources, to allow rapid configuration of new input and broadcast channels, and to allow multiple emergency service operators to update diverse Internet channels to the public in a structured manner. Government would need to direct policy towards these goals to spur adoption by the emergency services as part of the wider government e-services agenda.

Where the civil defence arrangements in place have historically come from the military, and are therefore still subject to national security concerns, governments should consider how these linkages might be broken or reorganised to enable proper inter-agency communication – both within the state and across borders.

4.3.1.2 Recommendations for competent authorities

In a similar vein to the recommendations for government ministries, competent authorities will need to recognise and embrace the benefits of improvements in inter-agency communication, and to adopt policies that fully balance local operational requirements with this wider goal.

However, beyond policy definition, competent authorities have responsibility for actually implementing and achieving the objectives, without compromising the current operational arrangements in place for crisis response.

Competent authorities will need to assist government in assessing the appropriate standards to be adopted for inter-agency working, and will also need to work closely with each other to determine how such standards can be best adopted and implemented.

It should be noted that competent authorities will already have established programmes for collaborating and sharing lessons learned and best practice, especially with similar agencies in other countries. By working with government to secure the appropriate resources they should be well placed to migrate to a more collaborative and common footing under a standardised technical and operational framework. Where this is precluded by national security concerns (due to a military background), authorities should work with government to reorganise around any national security concerns to allow open, public collaboration with other authorities.

However, the information gathering revealed that competent authorities are not currently working on developing data services capitalising on Internet and social media for crisis situational awareness and public information. Competent authorities will need to work with the non-emergency organisations that have skills and experience online data aggregation in order to develop the appropriate technology and skills to add these capabilities to the crisis response infrastructure.

In addition, competent authorities will need to promote and develop the utility of online services for situational awareness inside their own organisations – the use of statistically aggregated data does not naturally integrate into the crisis response process, where the delivery of succinct information from trained observers is the norm.

4.3.2 Recommendations for service providers

Within Member States, providers of communications services have a role to play in the adoption of new ways of handling emergency communications in a crisis.

This role will go beyond that of traditional fixed communications (i.e. three-digit public emergency telephone services) as crisis responders make increasing use of data. The traditional high-resilience voice systems favoured by emergency services are not well suited to large volumes of data transactions, and the need to use public data services such as social media will mean that the use of commercial data communications systems will be an increasing requirement.

Service providers will need potentially to provide the following capabilities to crisis responders and other competent authorities.

- Technical support to competent authorities as part of the technical standards adoption – particularly in the area of integration of standardised services.
- Support for improved commercial services where these services are used by crisis responders. In particular, improved capacity for mobile networks and data services may be a requirement in a crisis, and this may require direct intervention to support services in a crisis.
- Recognition of the criticality of newer services such as mobile networks and data services to the public, and the importance of public access to services to assist crisis responders. This could include services such as providing additional coverage or Wi-Fi networks in critical response areas, and the distribution of network credit vouchers to areas affected by a crisis.
- Assistance to competent authorities in the use of Internet services for situational awareness and public communications.

The information gathering for this report showed a positive level of collaboration and dialogue between state level regulators and their local telecommunications providers. The development of the recommendations within this report will represent commercial opportunities to these providers for service development, but a balance between new commercial provisions and development of new statutory obligations will need to be struck, and this may require transitory economic support to suppliers.

4.3.3 Recommendations for European bodies

European organisations such as the EC and its agencies will have a key role to play in the promotion and acceptance of the findings of this report in order to effect change with policy makers and crisis responders within the Member States.

4.3.3.1 Recommendations for the European Commission

As indicated by the Treaty of Lisbon solidarity clause, the EU recognises that responses to crises may require intervention at the European level. The approach of the EC in directing its agencies to investigate and recommend ways to improve cross-European working between Member States endorses and promotes this view.

Within the scope of this study, the principle role that the EC can fulfil is supporting the alignment of standards and policies by Member States as they move towards a more integrated approach to crisis response. This will involve the elements outlined below.

- Supporting Member State governments in their own policy developments with European-level policies that recognise and promote the ideas of standardisation and inter-agency working for crisis management.
- Making funding available to Member States and their competent authorities to support the development of their emergency communications infrastructure where appropriate. Such funding would need to be targeted at those areas (e.g. research and development) where adopting standardisation of emergency communications infrastructure requires substantial re-engineering or migration away from legacy systems.
- Supporting the agencies of the EU in their efforts to execute the policies required to enable better inter-agency communication between competent authorities.
- Incorporating the ideals of using Internet services to improve the transfer of information to and from the public regarding an unfolding crisis as part of the European Digital Agenda.

4.3.3.2 Recommendations for European agencies

European agencies have a crucial role to play in the development of better emergency communications capabilities across the EU, by acting as the catalyst for change within the Member States.

Specific activities that will be required include:

- working at the Member State government level to share best practice in the development of standardisation
- working at the competent authority level to co-ordinate and aid collaboration and information sharing on best practice and lessons learned

- reporting back to the EC on progress and alignment within the Member States towards the desired improvements and capabilities in crisis communications
- working with the emergency service communities to ensure that exercises test all aspects of the emergency communications infrastructure, account for the possibility of system loss, and can scale out to incorporate inter-agency working across Member State borders.

4.4 Conclusions

This study has identified a number of areas where communications between crisis responders, decision makers and the public can all be improved – with a view to providing more effective crisis responses in the future.

Recommendations as to how to achieve these improvements have been made to policy makers and practitioners at various levels within the EU.

These improvements have the potential to allow the emergency services to have a better understanding of the situation on the ground, to gather information from the public in an electronic manner, and to have new conduits to inform the public authoritatively about how they might best respond to the unfolding crisis to protect themselves and their property. These improvements have the potential to maintain communications channels even when infrastructure is damaged or destroyed.

More importantly, the improvements should allow crisis-responding bodies ultimately to communicate more effectively with each other and to provide a more efficient, more cohesive and, therefore, more effective response to an unfolding crisis in the interests of protecting human life.

5 Annex I: References

ENISA Good Practice Guide on National Cyber Contingency Plans. Available at https://www.enisa.europa.eu/activities/ Resilience-and-CIIP/national-cyber-security-strategies-ncsss

Department of Homeland Security, USA, 2008, National Emergency Communications Plan. Available at http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf

Appleseed, USA, 2006. A Continuing Storm: The On-Going Struggles of Hurricane Katrina Evacuees. Available at http://www.appleseednetwork.org/wp-content/uploads/2012/05/A-Continuing-Storm.pdf

City University, London, 2005. Eliminating the Communication Black Spots in Future Disaster Recovery Networks. Available at http://www.staff.city.ac.uk/~veselin/publications/Rakocevic_WPMC.pdf

The Guardian, London, 2011. Communications underscores London's emergency planning. Available at http://www.guardian.co.uk/public-leaders-network/2011/aug/24/communication-emergency-planning-london

Bennett, D., Jahankhani, H. and Jahankhani, H. (2009), 'The UK government's Critical National Infrastructure policy for emergency services communications platforms: vulnerabilities in the TETRA architecture', Communications in Computer and Information Science, 45, pp.43-55. Available at http://dspace.uel.ac.uk/jspui/bitstream/10552/1483/1/2009_Bennett_jahankhani_Jahankhani_TETRA.pdf

Parliament House of Lords, UK, 2011, European Union Committee – Seventeenth Report: The EU Internal Security Strategy. Available at http://www.publications.parliament.uk/pa/ld201012/ldselect/ldeucom/149/14902.htm

IBM, USA, 2010. City of Madrid: Coordinated emergency response raises public safety to a new level. Available at http://www-01.ibm.com/software/success/cssdb.nsf/CS/JSTS-7ZWSPF?OpenDocument&Site=default&cty=en_us

Inderscience Publishers, USA, 2011. Twitter for Crisis Communication: Lessons Learnt from Japan's Tsunami Disaster. Available at http://www.sciencedaily.com/releases/2011/04/110415154734.htm

NATO, Brussels, 2005. Lessons learned from recent terrorist attacks: Building national capabilities and institutions. Available at http://www.nato.int/docu/conf/2005/050727/index.html

Electronics News, Australia, 2011. Japan's 2011 earthquake and tsunami: communications and networks. Available at http://www.electronicsnews.com.au/news/japan-s-2011-earthquake-and-tsunami-communications

IEEE Spectrum Magazine, USA, 2010. Why Haiti's Cellphone Networks Failed. Available at http://spectrum.ieee.org/telecom/wireless/why-haitis-cellphone-networks-failed/

Urgent Communications, USA, 2010. A Painful Lesson – Haiti suffers communications failures after earthquake. Available at http://urgentcomm.com/networks_and_systems/mag/disaster-communications-201006/

Idisaster 2.0, USA, 2010. Social media during crisis response: Five general lessons for emergency managers. Available at http://idisaster.wordpress.com/2010/10/20/social-media-during-crisis-response-some-general-lessons/

O'Brien's Response Management, USA, 2010. Unending Flow – Case Study on Communications in the Gulf Oil Spill. Available at https://www.piersystem.com/external/content/document/3571/1009367/1/Unending_Flow_v1.01.pdf

TNO Defence, Security and Safety, The Netherlands, 2011. Insufficient situational awareness about Critical Infrastructures by Emergency Management. Available at http://www.primo-europe.eu/content/wp-content/uploads/2011/02/Symposium-or-Lecture-Series-_EN-MP_-_paper_10_Luiijf-A4_rev.pdf

The State of Queensland, Australia, 2012. Queensland Floods Commission of Enquiry final report. Available at http://www.floodcommission.qld.gov.au/publications/final-report

TETRA + Critical Communications Association, UK, 2012. Public Safety Radio communication in Europe. Available at http://www.tetramou.com/Library/Documents/TETRA_Resources/Library/Presentations/Turkey2011Borgonjen.pdf

National Policing Improvement Agency, UK, 2009. Guidance on Multi-Agency Interoperability. Available at http://www.npia.police.uk/en/docs/Multi-agency_Interoperability_Secure_130609.pdf

European Emergency Numbering Association, Belgium, 2012. Next Generation 112 Long Term Definition. Available at http://www.eena.org/ressource/static/files/eena_ng112_ltd_v1-0_final.pdf

The State of Victoria, Australia, 2009. Victorian Bushfires Royal Commission Final Report Recommendations. Available at http://www.royalcommission.vic.gov.au/getdoc/5bc68f8a-a166-49bc-8893-e02f0c3b37ab/VBRC-Final-Report-Recommendations

Commonwealth Scientific and Industrial Research Organisation, Australia, 2012. Tapping into Social Media to Build Emergency Situation Awareness. Available at http://www.apcoaust.com.au/2012/presentations/2012APCOA_Mark_Cameron.pdf

Federal Emergency Management Agency, USA, 2010. Federal Emergency Management Agency Publication 1. Available at http://www.fema.gov/pdf/about/pub1.pdf

Information-technology Promotion Agency, Japan, 2012. How Cloud Survived the Earthquake and Served People. Available at https://cloudsecurityalliance.org/wp-content/uploads/2012/07/Day1_1645_Track1_Session_KatsumiBen_-_IncMan_Katsumi_Ben.pptx

Saxon State Government, Germany, 2002. Report of the Independent Commission of the Saxon State Government into the 2002 Flood. Available at https://publikationen.sachsen.de/bdb/artikel/10825/documents/10951

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu