OECD Reviews of Risk Management Policies

The Changing Face of Strategic Crisis Management

OECD

OECD Reviews of Risk Management Policies

The Changing Face of Strategic Crisis Management

Please cite this publication as:
OECD (2015), *The Changing Face of Strategic Crisis Management*, OECD Reviews of Risk Management Policies, OECD Publishing, Paris.
http://dx.doi.org/10.1787/9789264249127-en

ISBN 978-92-64-24903-5 (print)
ISBN 978-92-64-24912-7 (PDF)

Series: OECD Reviews of Risk Management Policies
ISSN 1993-4092 (print)
ISSN 1993-4106 (online)

Revised version, June 2016
Details of revisions available at:
www.oecd.org/about/publishing/Corrigendum-TheChangingFaceofStrategicCrisisManagement-2015.pdf

Photo credits: Cover © Rawpixel.com/Shutterstock.com

Corrigenda to OECD publications may be found on line at: *www.oecd.org/about/publishing/corrigenda.htm*.

Foreword

Recent large-scale natural hazards, terrorist attacks, global pandemics, refugee crises and industrial accidents have demonstrated the diversity and complexity of today's crises. The increasing interconnectedness of modern societies makes them even also vulnerable to shock events occurring beyond their country, whose socio-economic impacts can rapidly cascade across borders.

Citizens expect effective leadership from their government in planning for and managing crises. This is fundamental for maintaining public trust, which is put at particular test during emergencies. But traditional approaches to crisis management, based on standard operating procedures and built on the history of past events, are no longer sufficient to respond to shock events of unprecedented nature. Close media scrutiny – including on social media – is also putting increasing pressure on governments to be more open, transparent and accountable in crisis situations.

This report proposes a fundamental shift in crisis management to help governments adapt to the new risk landscape through agile systems that can handle the unexpected. It presents practical recommendations on how to develop strategic crisis management capacities in order to minimise the impacts of large-scale shocks, which will help implement the OECD Recommendation on the Governance of critical Risks.

First, governments must set up robust governance frameworks for managing both classic and more complex crises. It is important to engage multiple agencies as well as the private sector in crisis management and to put in place arrangements for co-ordinating among these stakeholders both nationally and internationally.

Second, governments need to establish a network of actors with multi-disciplinary expertise and the capacity to provide digestible information to support leadership decision-making during crises. Unbundling complexities and identifying uncertainties are essential for making sense of what is happening in emergency situations, and for foreseeing similar situations in the future.

Third, governments should develop dedicated crisis communication strategies for social media. The opportunities for two-way communication provided by social media can significantly contribute to improving crisis management.

Finally, governments must design training programmes for professionals and leaders in managing and preparing for complex crises.

This report was co-ordinated by the Secretariat of the OECD High Level Risk Forum, as part of the OECD Public Governance and Territorial Development Directorate. The Forum aims to develop a shared vision of integrated risk management, with strategic crisis management a core component and brings together policy makers from OECD member countries and key partners, practitioners from the private sector and civil society, and experts from think tanks and academia.

This report draws on the discussions held in a series of workshops between 2012 and 2015 on strategic crisis management; organised jointly with the Swiss Federal Chancellery and the International Risk Governance Council. These workshops contributed significantly to the development of the Recommendation of the OECD on the Governance of Critical Risks, adopted in May 2014, which sets an OECD standard to better manage risks and crises.

The community of strategic crisis managers engaged in the activities of the OECD High-Level Risk Forum allows countries to share lessons and support international co-operation in crisis management. This constitutes a key contribution to more resilient societies and safer livelihoods through a better response to complex crises.

ACKNOWLEDGEMENTS

This report was prepared under the OECD High Level Risk Forum of the OECD's Public Governance and Territorial Development Directorate, led by Rolf Alter.

The report was co-ordinated by Charles Baubion and prepared under the supervision of Jack Radisch, Risk Management Project Manager; and Stéphane Jacobzone, Deputy Head of the Reform of the Public Sector Division. It was written by the following authors: Charles Baubion (Chapter 1); Prof. Eric Stern, Swedish National Defence College (Chapters 2 and 4); and Cécile Wendling, Jack Radisch and Stéphane Jacobzone (Chapter3). The authors are grateful to Luiz de Mello, Deputy Director, Public Governance and Territorial Development for giving strategic feedback and to Ryan Androsoff from the OECD Secretariat for comments.

The OECD Secretariat is grateful for support received from the Swiss Federal Chancellery in organising the joint workshops with the OECD on strategic crisis management. This report draws on the discussions held at these workshops in 2012, 2013 and 2014, as well as the workshop on crisis communication organised in partnership with the International Risk Governance Council (IRGC) in 2012. We wish to thank Dr. Nicolas Mueller and Dr. Christoph Doktor from the Swiss Federal Crisis Management & Strategic Leadership Training Center; and Marie-Valentine Florin, Managing Director of the IRGC, for this fruitful partnership.

Substantive comments were provided by Richard Smith Bingham from Marsh & McLennan Companies; Prof. Arjen Boin from Leiden University, Bengt Sundelius, Strategic Advisor to the Director General of the Swedish Civil Contingencies Agency.

Editorial support given by Lynda Hawe, Andrea Uhrhammer, Lia Beyeler, Liz Zachary and Kate Lancaster is gratefully acknowledged.

Table of contents

Tables

Boxes

Figures

Acronyms and abbreviations

BSE	Bovine spongiform encephalopathy (mad cow disease)
CBS	Cellphone Broadcast Service
CCC	Crisis Communication Centre
CCTV	Closed-circuit television
CDC	Centre for Disease Control and Prevention
CERT	Community Emergency Response Team
CIA	Central Intelligence Agency
CJS	Creutzfeld-Jakobs syndrome
CM	Crisis management
COBR	Cabinet Office Briefing Room
CSO	Civil Society Organisation
DRR	Disaster risk reduction
EC	European Commission
EU	European Union
EPIC	Empowering the Public with Information in Crisis
EWS	Early warning systems
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GIS	Geographic Information Systems
GPS	Global Positioning System
HADR	Humanitarian assistance and disaster relief
ICS	Incident Command Systems
ICT	Information and communication technology
ISC	Integrated Situation Centre
KM	Knowledge management
MoMs	Maximum of Maximums
NATO	North Atlantic Treaty Organisation
NBRC	Nuclear, biological, radiological or chemical

NGO	Non-governmental organisation
NIMS	National Incident Management System
NRA	National risk assessment
NSA	National Security Agency
OEMC	Office of Emergency Management and Communications
RSS	Really Simple Syndication
SAGE	Scientific Advisory Group for Emergencies
SARS	Sudden acute respiratory syndrome
SAVER	System for the Analysis and Visualisation of Risk Scenarios
SHOC	Strategic Health Operations Centre
SMS	Short Message Service
SOP	Standard operating procedure
SUMMIT	Standard Unified Modelling, Mapping and Integration Toolkit
TEPCO	Tokyo Electric Power Company
UNDAC	United Nations Disaster Assessment and Coordination
VGI	Volunteered Graphic Information
VTC	Volunteer Technology Community
WHO	World Health Organisation

Executive summary

Governments play a crucial role in strengthening the resilience of their populations, communities and critical infrastructure networks: managing crises is a key part of this. Recent crises, such as industrial accidents, large-scale flooding, terrorist attacks, cyber attacks, global pandemics, earthquakes and tsunamis, have challenged political leadership and risk managers in many countries. The icelandic volcanic ash cloud, the great east japan earthquake and subsequent tsunami and Fukushima crises, the Deepwater Horizon oil spill in the Gulf of Mexico, the sinking of the ferry Sewol in Korea, the Tianjin industrial blast in China or the European refugee crisis are vivid examples of challenging crises.

This report highlights new approaches to address novel types of crises, and reflects on how governments can best adapt to rapidly changing social and economic conditions while maintaining the ability to deal with traditional crises. The report discusses the capacities required to ensure that the complexity of modern crises are identified and understood early, and that communications, particularly through social media, are effective. It also provides practical policy guidance for strategic crisis management.

Adapting government approaches to a new crisis landscape

Globalisation has led to the concentration of people and assets in cities and coastlines, created interconnectedness and interdependencies through global value chains and critical infrastructure systems, and increased the mobility of people, goods, capital, information and infectious diseases. These factors create more possibilities for unexpected and uncommon crises. The scale and transboundary nature of novel crises means governments not only have to contend with direct impacts on their populations, but also secondary consequences on their reputation and economies. Governments thus need to learn how to work with partners across boundaries, to co-ordinate among different sectors, and to integrate new stakeholders – especially from the private sector – in their crisis management efforts. Greater media scrutiny and the development of social networks put increasing pressure on governments to excel in this complex policy area.

Understanding and identifying strategic crises through early warning and "sense-making"

Leaders in charge of crisis decision-making must recognise the issues at stake in a crisis, its potential development, and the associated uncertainties. This "sense-making" function complements early-warning systems and requires dedicated methods and structures often located within Centres of Government.

Despite great strides in administrative practices and scientific and technological advances, crises often take governments by surprise and lead to great difficulties in sense-making. When an unexpected crisis occurs, it is necessary to quickly obtain, digest and channel accurate information and trustworthy expertise. Too often, leaders have not been

adequately informed before taking crucial decisions at times of deep uncertainty, conflict over values and high expectations. Crisis sense-making is context-dependent: group, organisational, and political contexts will both enable and constrain the decision-making ability of leaders and advisors.

Advances in science and technology have led to vast improvements in early-warning systems, both at national and international levels: hydro-meteorological phenomena, infectious disease outbreaks, volcanoes, tsunamis and many other hazards are now continuously monitored. Crisis managers must ensure effective use of these information systems in order to quickly advise decision makers.

Social media use for crisis communication

Social media can create opportunities and present challenges in times of crisis. It allows for multiple players and communication channels to participate in risk communication, which can facilitate two-way communication between the authorities and society and improve crisis management functions. The expectations of citizens to receive information drives demand for more communication, but greater complexity and uncertainty make crisis communication more difficult.

Using social media effectively in crisis communication requires avoiding certain pitfalls, and appropriate resources need to be devoted to the management of social networks during a crisis to ensure responsiveness. Ensuring the reliability of information circulating through social networks, managing rumours and avoiding panic is fundamental. Information overload can cause distractions for crisis mangers. As some segments of the public may not be easily reachable through social media, inclusive crisis communication also requires using traditional communication channels.

Strategic crisis management exercises

Crises force strategic-level decision makers to act under very difficult circumstances. Leaders, along with their teams, organisations and key partners, must be prepared to cope with the rigours of contemporary crisis management. Training leaders is thus a pre-requisite for efficient strategic crisis management.

International co-operation and partnerships should be further strengthened in areas such as joint response planning, early warning and sense-making through information exchange and joint exercises and drills. Despite the challenges involved, engaging with the private sector internationally in strategic crisis management exercises is necessary for the development of a shared crisis management culture and for creating trust across borders.

Key messages and recommendations:

1. **Governments must develop robust crisis management frameworks** to cope with the complexity, uniqueness, ambiguity and uncertainty that characterise many modern crises. New crisis governance frameworks are needed for these major "black swan" events.
2. **Leadership during a crisis is fundamental for maintaining trust in public institutions**. It requires developing professional capacity and skills through specialised training; addressing in particular crisis sense-making, decision-making and meaning-making.
3. When confronted with **unprecedented emergency**, **strategic crisis managers should be able to quickly identify and mobilise the most relevant and trustworthy expertise** to help make sense of the crisis. Such knowledge management systems and experts networks need to be set up in advance and across multiple sectoral, professional and disciplinary boundaries.
4. **Social media present opportunities to enhance crisis communication but also come with new challenges.** Governments should therefore develop dedicated crisis communication strategies for the use of social media in crisis management.
5. **Engaging the private sector in crisis management efforts is essential** as the scale and complexity of major crises requires a "Whole of Society" approach. Governments should set-up the right incentives for cooperation with the private sector in times of crisis.
6. **International co-operation offers fruitful opportunities with the need to strengthen international partnerships. This may concern** areas such as joint response planning, early warning and sense-making, and may involve information exchange, joint exercises and drills.

Chapter 1

Adapting government approaches to a new crisis landscape

Governments are confronted with many types of crises that can trigger significant economic knock-on effects. These crises often happen outside their national borders. Managing crises is a key responsibility for governments who have a crucial role to play in strengthening the resilience of their populations, communities and critical infrastructure networks. This chapter highlights the changing landscape of crises that governments are confronted with. It discusses new approaches in dealing with both traditional and new crises. It invites a reflection on how governments can adapt better to change, while maintaining the capability to deal with more classic types of crises.

This chapter draws on Baubion, C. (2013), "OECD Risk Management: Strategic Crisis Management", *OECD Working Papers on Public Governance*, No. 23, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k41rbd1lzr7-en.

Key messages

1. Governments must develop crisis management capacities to cope with the complexity, novelty, ambiguity and uncertainty that characterise many modern crises.
2. Emergency response plans are necessary tools for conventional crisis management. They are designed with reference to past events and work well for routine events. New approaches are needed for "black swan[1]" events.
3. National crisis governance frameworks need be set up to ensure that the appropriate structures and institutional frameworks are put in place to deal with both classic and unprecedented crises.
4. Multi-disciplinary expertise needs to be organised for sense-making before and during crises.
5. Leadership during a crisis is fundamental for restoring public trust. It requires developing professionalism through specialised training.
6. The ability to manage large multi-stakeholder and multi-form public/private/non-governmental organisation (NGO) response networks is a new challenge that central government must invest in to strengthen crisis responses.
7. International co-operation and partnerships can support many functions of crisis management and should be further strengthened.

Governments are confronted with an increasing number of crises, some resulting from unprecedented and poorly understood hazards and threats. Crises can spread beyond national borders and trigger significant economic knock-on effects due to the interconnected nature of the global economy (*Future Global Shocks,* OECD, 2011). In the aftermath of the 2008 financial and fiscal crises, global leaders are acutely aware that further systemic shocks could severely challenge economic recovery, social cohesion and even political stability. Government responsibility is key to managing these disruptive events. Citizens' trust in government is directly affected by how quickly, efficiently and transparently government decisions are taken in crisis situations.

The complexity of managing modern crises requires the involvement of many actors above and beyond emergency services, and requires the efficient co-ordination of emergency response units in order to protect citizens and businesses and mitigate the impacts of disasters. This creates governance challenges, as crisis management operations are often carried out at sub-national levels, but co-ordinated by the centres of governments. The capacity to co-ordinate crisis management and provide appropriate responses at the right time is a fundamental element of good governance. Ensuring that national authorities have the right tools and institutional framework for co-ordinated action is critical.

Many OECD governments have taken developments over the last decade into consideration when revising their crisis management systems. However, crises continue to evolve, requiring even the most recent and robust systems to continue to adapt.

This chapter highlights the changing landscape of the crises that governments are confronted with today. The chapter discusses different approaches and practices in dealing with both traditional and novel crises, asking how best governments can adapt to change while still maintaining capabilities to deal with more classic crises.

Managing crises: a key responsibility for governments

Citizens require governments to provide robust leadership in crisis management or they may be held accountable. Governments can benefit from exchanging practice and experience with other governments to deliver better leadership in an evolving context of trans-boundary risks. This is especially the case for countries that manage critical hubs of the global economy. Crisis management takes place within a range of disaster risk management activities that fall under government responsibility.

Disaster risk management has often focused on planning the organisation of emergency responses after disruptive events. Recent progress in science, technology and information management allows governments to better understand how built environments are exposed to hazards and threats, and the vulnerabilities of populations, economic assets and environmental resources.

Prevention and mitigation policies

This greater understanding of hazards and threats has enabled better risk assessment to better target prevention policies and mitigation programmes to reduce exposure and vulnerability. These phases of risk management take place before an event occurs and are keys to many of the strategic approaches discussed below. Building capacities in these areas will be vital to the successful adaptation of countries to the new risk landscape. The economic argument for governments to invest more in disaster risk prevention is that a

net gain could be achieved, when compared to sums spent on recovery and reconstruction after a disaster.

Long-term investment in prevention has been shown, in many cases, to provide a significant positive return (World Bank, 2010). Efforts to build and develop more robust societies and economies are fundamental, however emergencies continue to occur and crises are perhaps even more frequent. Countries that have invested heavily in prevention through the development of protective infrastructure, early-warning systems, regulations on land use, and building codes still experience major disasters, as illustrated by the Great East Japan earthquake in 2011 and Hurricane Sandy in the United States in 2012. This illustrates that building crisis management capacities to reduce the economic impacts of crises still has to deserve primary attention.

Building resilience

The policy research community working on government preparation for large-scale risks has promoted the concept of resilience, which is derived from ecology and based on the notion of ecosystems (Beddington, 1976). Applied to risk management, resilience is "the ability of a system, community or society exposed to hazards to resist, absorb, accommodate and recover from the effects of a hazard in a timely and efficient manner, including through the preservation and restoration of its essential basic structures and functions." (UNISDR, 2009) Building the resilience of societies is consistent with investment in prevention and preparedness, as well as with enhancing crisis management capacities. Promoting the concept of resilience is a powerful driver for encouraging different levels to boost their capacity for risk and crisis management. For example, business continuity ensures businesses have identified and can continue to perform their core functions during crisis, even at a reduced scale, and recover as quickly as possible. It illustrates the concept of resilience applied to a company or a service, including public services.

Under this conceptual approach, governments have a crucial role to play in strengthening the resilience of their populations and critical infrastructure networks. While promoting the concept of resilient communities and systems at all levels can be addressed through regulation and is reflected in the national policy frameworks in some countries, governments are looked to as the ultimate guarantor when resilience capacity is disrupted at any level.

New crises call for new and innovative crisis management responses

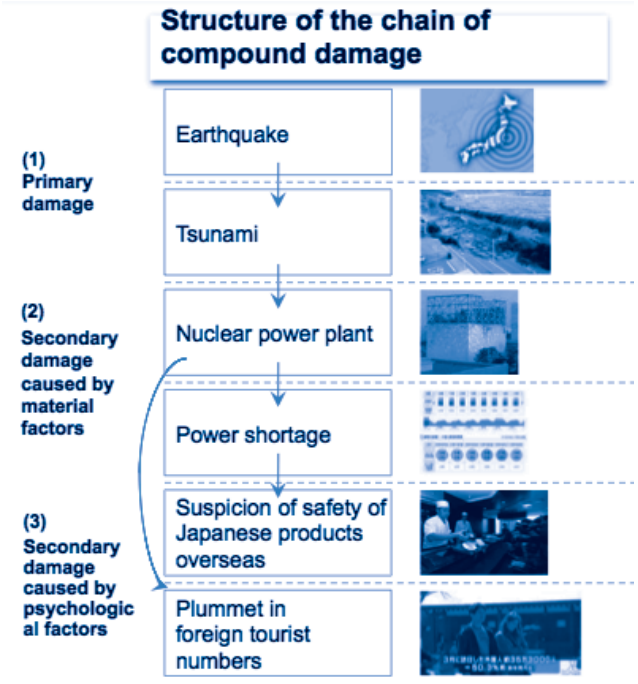
Defining new crises

Recent crises have challenged political leadership and risk managers in many countries, often due to unexpected or unforeseen circumstances, but also due to weak links and breakdowns in information flow. Examples include the events of 11 September 2001, the sudden acute respiratory syndrome (SARS) and H1N1 outbreaks in 2003 and 2009, the 2004 Indian Ocean tsunami, Hurricane Katrina in 2005, the 2010 volcanic ash cloud over Europe, and the 2011 Great East Japan earthquake, in which the tsunami and the Fukushima Daiichi nuclear accident resulted in cascade effects (Figure 1.1.). Risk managers, processes and structures were unprepared to deal with these new crises, which differed significantly from past crises in several respects:

- Their novel or unprecedented nature – at least in human or crisis managers' memories – or their unusual combination (Leonard, 2012).

- Their unexpectedly large scale or geographic distribution.
- Their trans-boundary nature (Boin et al., 2010), which here refers not only to their effects having crossed physical geographic borders, but also the involvement of public authorities from national and sub-national levels, relevance of several policy fields, and mobilisation of different sectors (public, private, non-governmental etc.).
- Their consequences, which stir deep uncertainties in the minds of the public, challenge government structures, and aggravate tensions between many stakeholders in the public and private sectors.

Figure 1.1. Cascading effects of the Great East Japan earthquake



Source: Kaji (2012)

These trans-boundary effects can expand to become what the OECD has characterised as a "global shock", that is, a "rapid onset event with severely disruptive consequences covering at least two continents" (OECD, 2011). This concept takes into account another pattern of novel crises: cascading risks that become active threats as they spread across global systems, such as transport, health, financial or social systems. A traditional crisis can become trans-boundary and develop into a global shock at a later stage, through non-linear processes.

The increased vulnerability of modern societies

Societies have improved living standards with complex and interconnected systems. However, reliance on these systems also makes them increasingly exposed and vulnerable to the effects of natural hazards and threats and their second-order effects, which may spread more quickly through spill over or amplifier effects.

Future Global Shocks (OECD, 2011) identified key drivers that increase vulnerability and amplify the consequences of more classic crises. Heightened mobility within the global economy facilitates the spread of risk carriers or vectors, such as viruses or terrorists. Globalisation has also led to an increased interdependence of production and delivery systems and their infrastructure, as well as to the centralisation and concentration of critical systems. As supply chains and networks of vital services attain an increasingly global reach they are exposed to many more hazards and threats. A crisis affecting one key node, or hub, of such a system could cripple the whole system, with large-scale cascading impacts. Urbanisation and the concentration of populations and assets further exacerbate societies' vulnerabilities by creating hotspots that have a high potential for direct losses during catastrophic events. They are also attractive targets for terrorist attacks.

The characteristics of hazards and threats change over time. An increase in the frequency and severity of extreme weather events may be expected to accompany climate change; and rising sea levels could endanger inhabited coastal areas where some megacities are developing. New infectious diseases evolve and appear to spread more quickly with increased mobility of economic activities. Terrorism and other intentional acts are taking new forms as their agents adapt their operations to a globalised landscape.

Changing roles of governments and increased demand from citizens and the media

In addition to the emergence of new threats and vulnerabilities, crisis managers need to consider the evolution of governments and governance as factors in an ever-changing sector. While crisis management will always remain a fundamental role of government, privatisation and decentralisation has altered the capacity of governments in many countries, including OECD countries, to take direct action to prevent or mitigate risks in sectors that are critical for the well-functioning of societies, such as transport, utilities and infrastructure. Government crisis managers need to adapt their approaches to deal with a variety of different stakeholders who all have different interests, priorities, and values. Critical infrastructure in many OECD countries is largely operated by the private sector. Citizens also tend to organise themselves to respond to crisis through civil society and non-governmental organisations (Civil Society Organisations [CSOs] and NGOs), thus adding new players to the field who expect to be consulted during preparations and utilised during operations.

Governments and their decision-makers need to meet expectations of openness and transparency and contend with media scrutiny and widespread dissemination of information online and through social media. This pressure is all the more acute when a crisis occurs as citizen expectations are high: they demand more transparency, accountability and high standards of ethics from their governments, which need to react promptly or risk a political backlash. Pressure to act quickly and decisively is usually at odds with acting on comprehensive information.

A changing landscape for risk managers

These trends paint a picture of global complexity that challenges risk managers, especially at the level of central government. The changing landscape requires governments to adapt their processes, structures, tools and equipment to manage new crises. Today, risk managers are confronted with:

- Dealing with the unknown.

- Dealing with different and multiple administrative levels, foreign governments, and/or international organisations.
- Reduced capacities of central government due to decentralisation and/or privatisation.
- New actors with different agenda and approaches, such as the private sector and NGOs/CSOs.
- Constant scrutiny from the media and citizens through social media.
- Higher citizen demands and expectations.

As well as dealing with new crises, governments also need to maintain capacity to deal with more traditional crises that continue to occur. The innovations required to adapt to new features of crises and societies are not replacements for, but rather complement and can be built on existing capacities.

How to adapt crisis management to the new risk landscape

Crisis management frameworks and concepts

Crisis management comprises three key phases: 1) preparedness before a crisis; 2) response to limit damages during the crisis; and 3) feedback after the crisis.

Before a crisis, **preparedness** requires developing knowledge and capacities in order to effectively anticipate, respond and recover from a crisis. Elements include:

- Risk assessment constitutes the fundamental first step in preparedness for a crisis and involves identifying and analysing major threats, hazards and related vulnerabilities.
- Early warning systems based on the detection of these threats serve to activate pre-defined emergency or contingency plans.
- Stockpiling, maintaining equipment and supplies, training and exercising emergency response forces and related co-ordination mechanisms through regular drills all contribute to preparedness.
- Appropriate institutional structures, clear mandates supported by comprehensive policies and legislation, and the allocation of resources through regular budgets are instrumental to thoroughly prepare for crises.

Once a crisis actually materialises, the **response phase** begins:

- Detection of a crisis may come about through various sources (e.g. monitoring networks and early warning systems, public authorities, citizens, media, private sector). It may build up over time or happen suddenly.
- An appropriate intelligence organisation is required to monitor the development of a crisis and maintain situational awareness, and to make sense of its characteristics and ascertain the operational picture.
- Understanding the crisis permits the selection of appropriate contingency plans and the activation of appropriate emergency response networks.
- Response efforts need to be co-ordinated, monitored and adapted as the crisis develops through the tactical and strategic oversights of crisis units or cells at the appropriate levels.

- Standard operating procedures (SOPs) should govern operations and co-ordination and include information sharing and communication protocols, as well as scaling-up mechanisms to mobilise additional emergency responses.
- Leadership ensures co-operation and decision making, but it also plays a key role in crisis communication through communicating with the media to help the general public understand events, to maintain trust in the emergency responders and government, and to transmit specific messages.

Ultimately, a crisis usually ends, which completes the crisis management phase. Bringing a crisis to a close requires clear messages to the public. After a crisis, feedback mechanisms should review in detail the actions taken to limit damage. Drawing lessons from past crises or disastrous events helps to improve preparedness and response processes. Evidence of lessons learned may take the form of changes to legislation, regulation or any of the capacities outlined above.

This brief overview of crisis management concepts provides the basis from which to review the challenges facing the various phases, processes and tools of crisis management, and how they may need to adapt to the changing nature of crisis.

Crisis preparedness

Preparing for crises used to consist of developing capacities and tools to tackle crises that had occurred in the past. In the new landscape, preparing for crises requires adapting approaches to be able to respond to the unknown.

Risk assessment

Sectoral risk assement

Risk knowledge is the foundation of crisis and emergency preparedness. Analysing hazards, threats and vulnerabilities through risk assessment enables response planning. Risk assessment approaches and methodologies are linked to their purpose: risk assessment for traditional crises aim to develop emergency response plans, while novel or trans-boundary crises need more flexible and adaptable capacities for responses, thus implying a more holistic and dynamic approach to risk assessment.

Traditionally, sectoral risk assessments were conducted for natural hazards, pandemics, industrial accidents or terrorist attacks in order to identify the number of people locally who might require emergency support; the number of vaccine doses or hospitals beds required to treat infected patients; safe evacuation roads in case of a hurricane or a flood; or containment measures if a nuclear, biological, radiological or chemical (NBRC) attack were to diffuse hazardous elements in a city or network. Conducting such analyses requires combining information from technical agencies, such as hydrometeorological services or health agencies on hazards and threats, the potential exposure of the population, settlements, and critical infrastructures and their vulnerability.

Government services have often taken a piecemeal, silo approach to risk assessment, whereby the scope of the activity is determined by the nature of a hazardous phenomenon. For example, health services focus on the assessment of infectious diseases; meteorological services focus on weather; hydrological services focus on water; geological services focus on earthquakes, avalanches and landslides; and intelligence services focus on terrorist threats. Most of these risk analyses have tended to be based heavily on data describing historical events.

Local authorities and local emergency services need hazard and threat information to develop appropriate emergency plans. The availability of data and information to conduct risk assessments and mapping has been growing, along with the development of monitoring networks, databases and archives, and modelling and mapping tools. Institutional frameworks have helped to foster the availability and sharing of information at the national and local level, as well as technical guidance to realise risk assessments and mapping. Guidelines should provide details about the exact events local emergency services should prepare for, where available information is to be found, and identify agreed methodologies and standards. This information can be usefully combined at the national level to develop national plans and additional support capacities for large-scale emergencies, but the practice of sectoral approaches remains prominent at all levels. There are examples in some countries of efforts to integrate risk assessment into emergency preparedness through the use of new data gathering technologies and mapping tools. In Mexico, the System for the Analysis and Visualisation of Risk Scenarios (SAVER) is a multi-agency approach to risk mapping and scenario development for emergency response planning (Box 1.1.).

Box 1.1. Mexico - The System for the Analysis and Visualisation of Risk Scenarios (SAVER)

Since 2010, civil protection authorities in Mexico have used SAVER to include risk scenarios in emergency preparedness planning. The system integrates risk maps and geo-referenced information on vulnerability of hospitals, schools, public infrastructure and the population into one single database. Currently, its capacity to create risk scenarios is one of its most important characteristics. SAVER is the result of a horizontal and vertical co-ordination effort across the public administration. The ministries of Social Development, Communications and Transport, and Public Education provided location data and descriptive information about infrastructures under their responsibility as inputs to the system's database. Currently, the system comprises 700 hazard layers together with socio-economic and vulnerability data. With the development of SAVER 2.0 in 2011, authorised organisations may provide input to the database online. Public entities in charge of social, territorial and human development may also use the system to support policy decision making. The system provides them with information on potential damages and what populations may be affected based on disaster occurrence records. In its next version, SAVER 3.0, the objective will be to integrate all of the 32 state risk maps.

Source: OECD (2013)

Dealing with novel and/or trans-boundary crises calls for a more holistic approach to risk assessment at the national level. Ideally, such an approach should address the following challenges:

- **Developing a broader and shared view on risks** at the national level through a multi-hazard/multi-threat approach that includes new and emerging potential threats and vulnerabilities through frequent updates. Identifying interdependencies, potential cascade effects and tipping points should also be part of the analysis.
- **Sharing this risk assessment widely, but with appropriate limitations,** to emergency response stakeholders such as national and local emergency services, health agencies, police and security forces, critical infrastructures operators, NGOs and volunteer organisations, media and the public at large, and at the international level with neighbouring countries.

Both of these challenges require significant co-operation between different disciplines and stakeholders. Scientists, intelligence services and engineers need to combine their data and information of hazards and threats and their knowledge of systems to conduct risk analyses and scope emerging risks and threats. Additionally, governmental agencies, local authorities, NGOs, the private sector and society at large need to understand risk analyses and integrate them into their preparedness strategies at all levels. An appropriate national authority should lead these processes to ensure co-ordination and co-operation through integrative partnerships.

National risk assessment

In recent years, a number of OECD countries have adopted national risk assessments (NRAs) to address the challenges of a holistic approach to risk assessment (Box 1.2.). The aim of a national risk assessment is to evaluate threats and hazard scenarios at the national level to assess the potential impacts and likelihood of each identified scenario according to common criteria. The result is visualised on a risk matrix, which ranks the major risks and threats that could affect a country. Used in conjunction with the results of a capabilities analysis (i.e. whether a country has the concrete capabilities to handle an emergency), the national risk assessment supports capabilities-based planning for emergency response in a resource-constrained environment. The United Kingdom has been a pioneer in this area, and its national risk register (an unclassified version of the national risk assessment) has been publicly available since 2008. Norway, Switzerland, Canada, the United States and the Netherlands have displayed similar efforts, and Germany and Sweden are advancing their programmes in this area.

Box 1.2. National Risk Assessment in the Netherlands

Since 2007, the Netherlands' National Safety and Security Strategy has promoted a holistic approach to risk management. It has determined five vital areas for the country: territorial, physical, economic and ecological safety, and social and political stability. The main objective of the Netherlands' NRA is to define priority risks for which the Netherlands should prepare and plan capacity development. The NRA consists of two parts: analysis and impact assessment. The analysis phase is managed by a network of independent experts who operate under the leadership of the national security steering committee, which is composed of ministries, businesses and intelligence services. The NRA method is scenario-based. Risk scenarios are assigned scores for their likelihood and impacts according to 10 criteria related to vital safety and security interests. The results give low and high estimates of a risk occurring. The impact assessment permits the Netherlands to determine which capabilities are needed for each type of risk. In this way, high estimates contribute to the development of resilience capacities and preparedness. The NRA develops estimates for a five-year period. However, analyses and capabilities can be reassessed frequently by expert groups according to new information or a new context. A report on the risks is sent each year to the parliament. It is also published on official websites and sent to stakeholders. This NRA is then used to assess capacity gaps and identify where capabilities should be reinforced.

Source: Dutch Ministry of Security and Justice/Ministry of Interior and Kingdom Relations (2009), Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands, Directorate-general for Public Safety and Security, the Hague.

International co-operation in the area of risk assessment could be further developed in a variety of ways. Sharing methodologies and tools for risk assessment, developing a common view on cross-border risks, and developing common tools at the international

level could increase the quality of risk assessment and potentially reduce costs. Detecting emerging risks requires significant efforts. Initiatives such as the World Economic Forum's annual *Global Risks* report or the risk radar developed through the European Emerging Risk Radar Initiative could be used to support the specific efforts of national authorities.

In addition to crisis preparedness, risk assessment can inform other phases of the risk management cycle, including vulnerability reduction through long-term territorial management, infrastructures and other policies, as well as disaster risk financing strategies. In this way it is a fundamental tool for harmonising risk management policies and practices through its coherent vision of risk priorities.

Emergency planning

Emergency planning is directly linked to risk assessment. Once risks have been identified, resources can be allocated to develop emergency response capacities and emergency plans can be developed to respond to pre-defined scenarios.

In most countries, emergency response capacities are spread across several agencies from the local to the national level. Emergency management agencies, civil protection departments, health services, fire-fighting units, police forces, armed forces and the emergency units of transportation, energy and communication operators can contribute capabilities to emergency response depending on the nature of the crisis and their institutional structures and mandate. The aim of emergency planning is to ensure that the various organisations possess sufficient capacities (emergency centres, human resources, equipment and supplies) throughout the national territory to respond to emergencies identified in the risk assessment process. The decision whether to have highly specialised expert centres or ensure proximity of response services wherever an event might occur has to be addressed in this process. Ranking risks through the NRA facilitates resource allocation from national governments to prepare for the priority risks and related scenarios.

Box 1.3. Plan SISMO: Scenario-based emergency planning in Mexico

An 8.0 to 9.0 magnitude earthquake in the Guerrero gap is considered the most important threat in Mexico as it could severely damage Mexico City as well as generate a strong tsunami. For this reason, a special civil protection programme for earthquakes was established by the Ministry of the Interior with a specific committee on earthquake emergency preparedness that brought together key stakeholders from the Army, the Navy, state civil protection departments, academic and civil society organisations. A plan entitled "Strategy for preparedness and response of the Federal Administration to a high-magnitude earthquake and tsunami" ("Plan Sismo") was published by the Ministry of the Interior in 2011. Plan Sismo represents a major attempt to define more clearly what each agency should do in the case of a major earthquake. It consists of four directives decided by the President that instruct and order Federal agencies to support the population to preserve the rule of law and the governability of the country. The plan foresees procedures that run counter the normal practice. For example, the President would order the Army and Navy to activate their respective emergency plans the DN III Plan and the Plan Marina. States and municipalities would be called on to activate their civil protection councils and co-ordinate with the Federal level. Organised in relation to three response areas (operational, logistics, and administrative), 14 working groups are defined with their co-ordinating agencies and their members.

Box 1.3. Plan SISMO: Scenario-based emergency planning in Mexico (continued)

This plan represents the first comprehensive emergency plan with clear co-ordination mechanisms in Mexico. Although Plan Sismo means that Mexico City is far more prepared now for a major earthquake than it was in 1985 (when two tremors led to massive damages and fatalities), whether it would really be sufficient and effective in case of a major disaster remains open to question.

Source: OECD (2013)

Once emergency response capacities have been established, operational plans should be developed to mobilise capacities when a crisis occurs. Contingency or emergency plans can take many different forms: continuity plans for specific organisations or vulnerable locations (schools, hospitals, tunnels, industries); continuity plans for specific disaster events (floods, bioterrorist attack, earthquake) (Box 1.3.); or plans per administrative unit (city, local authority, region, state). Most of these plans are usually scenario-based and include a series of standard operating procedures that are automatically applied when an emergency occurs. The chain of command is detailed and responsibilities, communication protocols, and the organisation and functioning of crisis cells are defined. Increasingly, co-ordination mechanisms between different stakeholders, and scaling-up procedures in case a crisis develops beyond the coping capacities of a certain level, tend to be included in contingency planning. However, most plans are based on the pattern of a classic command and control system from top to bottom.

Capacity and planning assumptions constitute an essential element of crisis preparedness, both for classic crises and more uncommon events. However, 21st century crises often challenge this pre-defined planning and organisation. Classic preparedness leads to established routines, but could limit capacity to "think outside the box". Dealing with novelty requires a different quality of preparedness and the capability to deal with any kind of unprecedented and large-scale event.

As they are often unprecedented, novel crises cannot be tackled with a comprehensive and executable plan, as this does not exist. Emergency responders need to be able to improvise and innovate. Developing capacities to adapt to and innovate in various crisis environments and building a response network that can mobilise all the required capacities across a variety of stakeholders thus becomes a new approach in emergency preparedness and planning.

With a novel crisis, the ability to effectively co-ordinate actions and steer the whole response system with shared information and clear objectives can make a difference. Inter-agency co-ordination mechanisms and scaling-up procedures across levels of government and jurisdictions need to be very effective and flexible. The key to preparing for a trans-boundary crisis lies in the capacity to organise a common response that focuses on shared objectives and uses all the necessary capacities from different organisations with different points of view and practices. Strong strategic leadership is fundamental, as is a common set of principles and values across the network (Box 1.4.).

Box 1.4. Sharing common values in a diversified response network

The French White Paper on Defence and National Security (2008), the Netherlands' 2009 NRA, and the United States National Response Framework have all established objectives and common values to be shared along an extensive inter-agency response network.

- The French White Paper of Defence and National Security underlined the importance of new technologies and efficient communication and stated that management planning should strengthen communication as an operational dimension of emergency response. It promoted the creation of an inter-ministerial crisis network to facilitate joint management and inter-operability.
- The Netherlands adopted a bottom-up, whole-of-government process that underlined the interconnections between risks and promoting security for public and private actors. Co-ordination of diverse actors can be found in boards such as the Cyber Security Board, which provides the government with different perspectives (government, business, science) in formulating independent policy advice.
- The US approach favours various scales of response through close collaboration with the private and non-profit sectors. This 'whole community' approach enables the development of relationships and provides an opportunity to learn about the complexity of the community to reveal inter-dependencies. The final developed scheme is a diversified response network that is flexible and adaptable under a unified command system and shared common strategies.

Sources:
Dutch Ministry of Security and Justice/Ministry of Interior and Kingdom Relations (2009), *Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands*, Directorate-general for Public Safety and Security.

Présidence la République Française and Mallet. J.C. (2008), *Défense et Sécurité Nationale: le Livre Blanc (White Paper on Defence and National Security)*, Editions Odile Jacob and La Documentation Française, Paris.

US Department of Homeland Security (2011), *Risk Management Fundamentals, Homeland Security Risk Management Doctrine*, US Department of Homeland Security, Washington.

Emergency planning consists of building an inter-agency response network based on shared values; developing and training leaders/co-ordinators who are able to co-ordinate and manage this network and innovate in their approach; and creating common tools including crisis cells, integrated command centres and communication and information exchange systems. In addition, specific emergency units can be specifically trained to innovate, and flexibility can be introduced in the response network that has a strict hierarchical control in order to strengthen the resilience of the response. Breaking the chain of command can sometimes facilitate a better response. In addition to inter-agency co-operation, international co-operation mechanisms can be designed to deal with cross-border and international crises.

The need for training

Exercises and training are key tasks to prepare for a crisis. Most emergency response agencies have dedicated departments that provide on-going training for their staff. In many emergency response units, training exercises are an important daily activity.

Training and exercises for crisis preparedness may focus on building the capacities of individuals; testing equipment and the ability of staff to deploy and use equipment;

controlling stocks of supplies; and testing contingency plans, from staff knowledge of the detailed protocols and procedures to stress testing the plan itself. Table-top or large-scale exercises can be organised to test a specific response plan and its related co-ordination mechanisms. Feedback from training can then be used to improve planning.

As novel crises do not have pre-defined plans, the concept and purposes of training for them are different. The two key functions of modern crisis response – leadership and network co-ordination – require specific training. Strategic crisis management training tests leadership and develops the capacity of civil servants who could be deployed when crises occur. This simulation training does not test the knowledge of protocols or the procedures themselves, but rather the ability to innovate in a stressful environment when "the fear factor" is present. These strategic crisis management exercises require in-depth preparation to ensure realistic conditions and focus mainly on the human elements (Box 1.5). Further details on how to design strategic crisis management exercises are provided in Chapter 4.

Strategic management training should be complemented by training and exercises that are dedicated to inter-agency co-operation and large network management and interaction. While managing this wide response network from a strategic perspective is essential, the network itself must be trained to learn how to interact. Table-top exercises among strategic crisis managers of different agencies, including large private sector organisations where interactions at different levels are needed, may help build familiarity and trust within the network. Trust, based on understanding each other's capacities and approaches, can only be built through regular interaction. Regular training helps networks to become more efficient as exchanges and relationships grow.

While feedback from training for classic crises usually serves to improve the plan or procedures, feedback for novel crises mostly leads to a better understanding of the functions of key partners, a definition of common priorities against a set of shared values, and tests flexibility and the capacity to innovate. The idea is not to test the structures, but rather people and their capacities to design, lead and function in a new response organisation adapted to the current threat.

Box 1.5 Strategic crisis management exercises: Examples from Germany and Switzerland

In recent years, Germany and Switzerland have conducted strategic crisis management exercises that test co-ordination, resilience, response capacities and continuity management in crisis situations. These national exercises follow an inter-agency and cross-disciplinary approach and involve participants from all sectors and political levels in plausible risk simulations with consequences that could significantly harm the country. The exercises also focus on crisis information and communication and aim to attract media interest to foster awareness raising. One of the essential benefits of these exercises comes from the post-exercise phase. Evaluation reports, based on expert observer and participant assessments, enable the identification of capabilities that need to be strengthened and contribute to further development or shifts in crisis management strategies and structures.

For Switzerland the Federal Crisis Management Training (CMT) Unit of the Swiss Federal Chancellery is mandated to strengthen the crisis management structures, processes, tools and infrastructure in Switzerland. One of the core activities of this unit is the preparation and conducting of the Strategic Crisis Exercises that take place every four years.

Box 1.5 Strategic crisis management exercises: Examples from Germany and Switzerland (continued)

The SEISMO 12 exercise of May 2012 was based on the potential occurrence of a 6.5 to 7 magnitude earthquake in the Basel region. 1 600 people participated in this trans-boundary exercise, which was developed at the international level between Swiss authorities and German administration units. The crisis scenario included the need to prepare for cascading effects, such as a nuclear accident. In 2009, the evaluation report of a similar exercise organised on "long-term power failure" led the Swiss Federal Office for the Country Economic Supply to re-examine emergency planning related to general power failure. This was followed up in 2014 by another exercise combing a pandemic and power shortage. Germany established the National Strategic Crisis Management Exercise (LUKEK), which takes place every two years and aims to raise awareness among top government officials. The LUKEK provides training for cross-ministerial management and crisis response staff and includes the participation of political authorities, relief organisations, scientific institutions, critical infrastructure operators and key service providers. The entire cycle of the strategic exercise lasts 16-18 months. The exercise is intended to be as complete as possible and comprises table-top activities to introduce the scenario to the operational staff in their normal working environment and real-situation simulations.

Sources:
Swiss Federal Chancellery (2013) Strategic Leadership Exercise 2013. Federal Office of Civil Protection and Disaster Assistance (2011), Guideline for Strategic Crisis Management Exercises, Bonn.

Early warning systems

Early warning systems (EWS) have been instrumental in reducing loss of life and damage caused by natural hazards and other threats (WMO, 2012). Through the detection of potential risks and the information of emergency services and the populations at risk, EWS support timely activation of emergency measures.

Box 1.6 Integrated early warning system in Korea

Korea has adopted an integrated risk-management approach that leverages the country's strong early warning systems. EWS monitor information pertaining to potential natural, man-made and social disasters. This information is captured in the Integrated Situation Centre (ISC), which includes four sub-systems to monitor and disseminate information before and during a crisis. Through the Disaster Prevention and Meteorological Information System, the ISC monitors satellite images, radar images and the contents of special weather reports. Specific monitoring systems are also established for floods, rainfalls, tsunamis, earthquakes and highway accidents (closed-circuit television [CCTV] real-time monitoring). In the event of a threat, alerts are sent out though the Internet to the report centre and through a Cellphone Broadcasting Service (CBS) that sends a message to citizens' cell-phones to inform them about evacuation measures. In the event of an emergency, the ISC acts as a disaster management control tower to support response measures in a 10-minute maximum lapse of time. Using the Disaster Information Sharing System, which connects 34 organisations, it proceeds to real-time disaster information collection. It also brings together information from affiliated organisations, national and local authorities, civil protection entities, the media and affected citizens. Finally, the Disaster Management Information Database Centre provides information on the damage status while the Central Disaster Management System provides information to manage facilities, refugees and assess the damage situation.

Source: Kang (2012)

Scientific and technological progress, and better linkages between technical and risk management agencies, have strengthened the capacity of many countries to forecast, warn, and activate emergency plans. For crises relating to extreme weather and natural disasters, tropical cyclone tracks are forecasted with a five-day lead-time in all cyclonic basins. Floods, storms, heat waves and cold waves, and other hydro-meteorological hazards are monitored and forecasted through hydro-meteorological services. The daily worldwide exchange of information among national services is ensured through the tools and frameworks of the World Meteorological Organisation. In the case of earthquakes, some systems are in place that can warn people in advance of the arrival of seismic waves when the vulnerable hot spots are far enough away from the epicentre (Mexico City and its Seismic Alert System, for instance, or Japan). A few seconds warning can be sufficient to save lives and shut down critical industries and infrastructure that otherwise would be more heavily damaged if they had continued operating. A global system for epidemiologic data and information monitoring is also in place through the co-ordinated network of the World Health Organisation to detect potential pandemics. Some pioneering efforts are also underway to create EWS for ethnic and international conflicts, as well as for the risk of terrorism, where an increased threat levels as determined by intelligence services may lead to advanced warning.

EWS are by definition systems designed to observe specific parameters and issue warnings when established thresholds are exceeded, thereby leading to pre-defined actions. The integration of all this information into multi-hazard EWSs could be a key tool to help governments prepare for a crisis, activate plans or elevate warning levels for a certain threat (Box 1.6.). However, the non-linear dynamics and complexity of modern crises make them more difficult to detect and describe in advance. These challenges are further explored in Chapter 2.

Governments should develop strategic foresight capacities to detect the early signs of crises and better anticipate uncommon crises. Horizon-scanning and risk radars are among the methods and tools some governments have experimented with to detect weak signals that could potentially turn into a crisis. Similar to integrated risk assessment, these tools must leverage expertise from different disciplines. Using crowd-sourced information to monitor social networks can provide early information before crises develop. The aim for governments is to develop a capacity that can detect emerging crisis factors (Box 1.7.). For this, it is critical to develop the capacity to "think outside the box" and continue to imagine scenarios that could expose vulnerabilities. Whatever new tools a government adopts, they need to detect a broader scope of links to the source hazard or threat and ensure the implementation of preparedness measures.

Box 1.7. Measuring geopolitical tensions based on market forces

Following a similar model to existing betting markets, the Defense Advanced Research Projects Agency in the United States ran a project on Futures Markets Applied to Prediction (Future MAP). Future MAP aimed, in particular, to forecast Middle East geopolitical tensions and political events. The tool involved a closed pool of investors betting small amounts of money in a simulated market that a particular event, such as a coup, terrorist attack, or assassination, would take place in the Middle East. Participants placed bets on political and economic events happening or not based on their information and expert view. The programme began with 100 traders from Middle East universities and think tanks who were seeded with USD 100 each to buy and sell futures contracts based on plausible events in eight countries of the region. The themes of the bets mostly related to military preparedness, civil stability, economic health, military involvement and economic investment. The Department of Defense ended the project in 2003.

Source: Schoen (2013)

The crisis response

Crisis response begins either when a significant threat is clearly forecasted, or when an undetected event or series of circumstances provoke a sudden crisis.

Crisis monitoring and sense-making

Obtaining a clear operational picture of the development of a crisis is the basis for decision-making both at the operational and strategic levels. Questions that leaders need answers to for taking decisions include: what happened? How many people are or might be affected? What valuable assets and interests are at stake? How might the crisis develop? What capabilities are available in the operational field? Harmonised monitoring systems and situation reports from all active operational entities should be gathered to inform the crisis cell. Information and communication systems, as well as standard reporting protocols among the emergency response network, enable easier analysis and the sharing of situation awareness (Box 1.8.).

Box 1.8. United States Incident Command System

Since the 1970s, the United States has managed and organised emergency responses through the Incident Command Systems (ICS) in various institutions. This scheme was reshaped in 2005 in the context of the National Incident Management System (NIMS) to settle common competencies and behaviours for emergency management. The current ICS consists of a standardised emergency management structure that is implemented in Federal, State, tribal, and local governments, NGOs and the private sector to respond to the demands of a crisis situation, regardless of jurisdictional and political boundaries. Aimed at fostering inter-operability and inter-agency co-operation, the ICS provides schemes for 14 management characteristics related to incident command, operations, communication, planning, logistics, finance and administration, and intelligence and investigation. Management objectives and action planning are centralised in a single unit of command to prevent diverging orders and promote accountability to a unified command and reporting institution. This allows agencies to respond to emergencies in a cost-effective and co-ordinated way that helps develop mutual objectives and strategies. At the same time, the ICS is flexible enough to be implemented for all kinds of incidents, small or large. To ensure communication, the system has developed a common inter-agency terminology.

Box 1.8. United States Incident Command System (continued)

Information exchange is co-ordinated by public information officers who are in permanent contact with the incident command organisation and the safety officer. In order to promote an inter-disciplinary approach, training and specific guidelines on ICS are provided to agencies such as the Food and Drug Administration, healthcare providers and hospitals, and institutions of higher education.

Source: U.S. Department of Homeland Security (2008)

Due to their unprecedented nature, novel crises cannot be monitored. When a novel crisis occurs, the first requirement is to make sense of what is happening. Technical or scientific expertise is often needed to break down the various dynamics of a complex situation into simpler scientific or technical elements. One way of preparing for novel crises is to establish in advance pools or rosters of national experts from different disciplines and organisations so that their expertise can be mobilised effectively and quickly to inform crisis management (Box 1.9.). Trust in expert advice has to be built over time and, on the expert's side, clarity regarding the liability attached to their advice is essential.

Box 1.9. UK Science Advisory Group in Emergencies (SAGE)

Effective emergency management relies on decision-makers having access to the best available advice in a timely fashion to ensure that the full range of issues and crisis dynamics are considered. In this context, the United Kingdom has established SAGE, which independently advises the Cabinet Office when an unprecedented crisis requires expert views. SAGE convenes in situations that require cross-government co-ordination, notably when the Cabinet Office, in consultation with the Prime Minister, decides to activate the Cabinet Office Briefing Room (COBR). SAGE convenes to provide scientific and technical advice on the way the emergency could develop and on potential scenarios and their impacts. The advisory group is both flexible and scalable as its tasks adapt to the nature of the incident and evolve as the emergency unfolds. Under the authority of the government's Chief Scientific Advisor, SAGE includes experts from all sectors and disciplines to analyse data, assess existing research, and commission new research. It can create sub-groups or liaise with devolved institutions or scientific groups and in complex emergencies it can have access to intelligence service information. To inform UK cross-government decision-making during the emergency response and recovery phases, SAGE submits policy option papers that outline scientific and technical solutions and their pros and cons and response scenario papers. At all stages, SAGE representatives attend the COBR to explain scientific issues. SAGE was activated during the 2009 H1N1 influenza pandemic, the 2010 volcanic ash cloud and the 2011 Fukushima nuclear incident. It deactivates once there is no longer a need for cross-government decisions on emergency response or recovery. An evaluation process is then triggered to review SAGE's performance and identify lessons for the next crisis.

Source: U.K. Cabinet Office (2012)

Managing the emergency response network

Rapid and properly scaled deployment of emergency forces, means and supplies is expected in the crisis response phase. In many countries, emergency response is based on the principle of subsidiarity: first responders come from the local level, and if their coping capacities are exceeded by the scale of the crisis, they request support from higher levels

of government/organisations. SOPs govern the operations of most of the entities involved in emergency response operations.

Trans-boundary crises require strategic engagement from centres of government at the outset. While scaling-up procedures are often designed to respect the institutional setting and the mandate of local jurisdictions, different mechanisms should be set-up to allow the rapid involvement of higher-level authorities when a threat is detected or a crisis forecast. Managing a large response network of stakeholders from different backgrounds and values requires highly professionalised emergency management leaders with sufficient authority and adaptability to use the strengths of the various responders in a co-ordinated network. Trade-offs between emergency responses at the local level and strategic engagement at the national level should be clearly addressed through clear institutional and legal frameworks.

Decisions often have to be made as the crisis develops, even when consequences are not always thoroughly weighed. Measures to facilitate difficult decision-making when various factors remain unknown should be put in place. For instance, the architectural design of crisis rooms should take into account the function of emergency decision-making processes. Developing a consensus among the various stakeholders present in a situation room requires full transparency in information sharing (Box 1.10.).

Box 1.10. Italy's Civil Protection Operational Committee

The Operational Committee (OC) of the Italian Department of Civil Protection (DCP) illustrates an organisational approach to creating consensus among different stakeholders. This consensus supports, at a national level, the joint management and co-ordination of emergency activities. It is comprised of representatives from operative structures of the national civil protection agencies and, notably, from the DCP, the armed forces, the fire department, police forces, the Italian Red Cross, the National Health Service, voluntary organisations and technical and scientific agencies. The Committee ensures inter-governmental co-ordination for decision making and also comprises civil protection representatives from regions and municipalities and critical infrastructure providers.

Chaired by the head of the DCP, it is convened whenever the head deems it necessary. The committee meets in the National Operational Room at DCP premises, which converts into a crisis cell in case of an emergency. The room is equipped with technical and communication systems that provide assistance for meetings and is designed to keep pertinent information online and provide an integrated picture of unfolding events through monitoring surveillance. In this way, the committee can receive, collect, process and verify information. It is responsible for assessing requests from areas affected by an emergency in order to define intervention strategies, guarantee the co-ordinated deployment of resources, and determine the intervention of emergency response participants. The committee also disseminates emergency information with the objective of immediately alerting and activating the different structures of the National Civil Protection Service. Depending on the situation, connections can also be established through a secure system with the affected regions or with entities responsible for critical infrastructures, notably with the civil protection operational rooms of regional provinces or municipalities.

Source: Rossi (2012)

Central governments need to be able to scale-up emergency response capabilities as the extent of trans-boundary crises is often broader than initially expected. Mutual-aid agreements can be developed in many sectors, which enable utility companies, city fire-fighting units and police forces to be deployed across neighbouring regions. Additional national emergency forces can also be specifically trained by the national government to

provide "surge" capacities. Effective co-operation depends on the interoperability of equipment resources that agencies use in emergency response.

The role of civil society is growing as part of the new environment of crisis management. Citizens, volunteer organisations, and national and international NGOs should be included in the response system. Properly articulating their roles and functions with other emergency response actors is fundamental. The capacities of civil society must be appropriately considered and supported to support an open and transparent approach to crisis management. The personal safety and security of the personnel and citizens involved in these actions is a major consideration.

Leadership through "meaning-making"

Leadership plays a major role in crisis communication. During a crisis, the emotions of the population may lead to demands that cannot be met. Leadership must convey messages that answer the public's need to know what is happening and what to do, but it must be careful not to build-up expectations for clarity and resolutions that it cannot deliver. It is also essential to disseminate messages to the public at risk for its own safety, which requires appropriate crisis communication techniques and tools.

Traditional crisis communication consists of communicating messages on the status of a crisis, its impacts, and the actions and measures that have been mobilised. It is usually designed to feed the media with facts and demonstrate to citizens that the government is managing the incident as well as possible. Political leaders are often called upon to communicate through broadcast media, and therefore require specialised training.

In the age of social media, where both essential and false information is communicated widely from a large number of sources, crisis managers need to use these tools to share information and communicate. Dedicated social media response teams can be very useful for sharing crisis information with citizens. Traditional ways of communication should not be abandoned, however, as certain population groups do not make use modern social media. Furthermore, certain crises may entail damage to telecommunications networks and thereby disrupt access to many social media platforms. In such cases, diversified communications platforms prove their value. Crisis communication and the use of social media are further explored in Chapter 3.

When a crisis reaches a level of severity that means the trust in the government is severely challenged, crisis communication enters into a new phase, where leadership is critical. When citizens' expectations are at their highest, leaders need to find the right words to provide meaning to what is happening. This "meaning-making" function of leadership refers to the capacity to provide not only information, but also a narrative that responds to public expectations. Reducing public and political uncertainty is fundamental to enhancing crisis management. The leader needs to convince the public that they should trust the government at a very critical moment. Finding the right words or the capacity of "persuasion" sometimes requires taking a step back from the event to tailor key messages that focus on the values of society. Setting a few officials aside from the heat of the crisis can be a useful tactic in crisis cells to protect them from the unsettling dynamics of the events and from the media's demands for immediate information.

The end of a crisis and rebuilding trust

As a crisis winds down, officials should clearly indicate closure to the public through a formal, well-communicated process that helps alleviate continuing anxiety and

encourages the return to a state of normality. This also helps transition to the next phase of risk management, such as the reconstruction process, with a new mind-set. The role of political leadership and co-ordination is crucial in this step. While the end of a classic or routine crisis may be clear from emergency services reducing their mobilisation or warning levels, a trans-boundary crisis may be more difficult to end and could flare-up again if different government authorities send inconsistent messages.

Large-scale crises where there was severe damage can have a critical impact on people's trust in government. The level of trust can be undermined because the government did not take the right decisions or did not appear to make a concerted effort to deal with the crisis. It can be even worse when the public feels that the government did not have a transparent and open approach, or that they were hiding either important aspects of the crisis or the failure of their approach. Clarifying how decisions were made and showing clear government accountability are the best ways of avoiding the post-disaster phase turning into a looming political crisis, which would further diminish levels of trust.

After the crisis it is time for in-depth analysis to review what has happened and how response actions were conducted. It is important to conduct this feedback process at the levels of each response institution as well as at the inter-agency and strategic level.

Identifying key cross-cutting issues in strategic crisis management

Table 1.1. summarises key differences between traditional crisis management and how to deal with novel crises. While governments need to adapt their crisis management capacities to the characteristics of novel crises through developing new doctrines and tools, they should also maintain the ability to deal with more classic crises, where robust preparation is vital.

Table 1.1. Different approaches in crisis management: traditional crises vs. dealing with novelty

Traditional crisis management	Dealing with novelty
Preparedness phase	
• Risk assessment based on historical events • Scenario based emergency planning • Training to test plans and procedures • Early warning systems based on monitoring, forecasting, warning messages, communication and link with emergency response	• Risk assessment includes horizon scanning, risk radars and forward-looking analysis to detect emerging threats. Frequent updates and different time-scales, international analysis sharing, and multi-disciplinary approaches are key attributes • Capability-based planning and network building • Strategic crisis management training to learn agility and adaptability and create networks and partnerships • Strategic engagement from centres of government
Response phase	
• Command and control system • Standard Operating Procedures • Strict lines of responsibilities • Sectoral approaches • Principle of subsidiarity • Feedback to improve SOPs	• Crisis identification/monitoring: role of expertise • Flexible and multi-purpose crisis management teams and facilities • Common concepts across agencies to inform leadership with high adaptive capacities • Similar tools and protocols that could be utilised for multi-crises • International co-operation • Management of large-response networks • Ending crisis and restoring trust • Feedback

Each government, depending on its institutional structure, history, and exposure to hazards and threats, has developed specific institutional and governance mechanisms to support emergency and crisis management.

Recommendations for government approaches to crisis management

The complexity of novel crises and the increased inter-connectedness of societies require government to adapt its roles and capacities to meet the expectations of citizens. To this end, the following actions should be considered:

- **A national crisis governance framework should be set up to ensure appropriate structures and institutional frameworks are in place that can deal with both classic crises and unprecedented crises**. The framework needs to be able to deal with trade-offs attached to these two approaches: preparing for classic crisis through standard operating procedures and pre-defined plans, and developing adaptable and flexible capacities for new crises (preparing for the unknown and attracting public finance). The national framework should define the key values for all stakeholders engaged in crisis management and refer to boundary-spanning mechanisms for the crisis response. Mechanisms for rapid scaling-up are crucial.
- **Multi-disciplinary expertise should be organised to help understand crises ("sense-making") before and during their occurrence**. Multi-disciplinary expertise should be mobilised to prepare and respond to crises. Long-term risk assessment and horizon scanning and the development and operation of monitoring and early warning systems require a variety of expertise from different disciplines. Novel crises require the capacity to understand and untangle the complexities of an event into knowable and manageable elements. To this end, organisational structures should be put in place to mobilise expertise very quickly when a crisis happens. Trust and accountability related to expert advice, especially in a time of crisis, is of an upmost importance.
- **Leadership during a crisis is fundamental for restoring public trust and requires developing professionalism through specialised training**. Understanding the crisis, decision-making in the crisis cells, and crisis communication directed at the emergency response network and citizens are key leadership functions that require the appropriate tools, skills and training. Clarity regarding the respective leadership roles of professional risk managers and political leaders facilitate crisis management.
- **The ability to manage large multi-stakeholders and multi-form public/private/NGO response networks is a new capability that central government should invest in to strengthen crisis responses**. Building, training, maintaining and managing a large inter-agency response network that involves the private sector and civil society/volunteer organisations requires the capacity to mobilise stakeholders around common values and objectives. Regular training, common tools, and efficient communication mechanisms enable the network to function during a crisis.
- **International co-operation and partnerships can support many functions of crisis management and should be further strengthened**. International and regional co-operation can help national crisis management through exchanging

good practices and/or defining common standards for inter-agency crisis management. Areas for co-operation include: global monitoring systems, shared risk radars or early warning systems, the inter-operability of emergency forces, the availability of specialised teams capacities, tools and supplies at transnational levels, the interconnection of strategic crisis management structures, and harmonised crisis communication processes. Co-operation in these areas can both enhance responses and achieve cost savings.

Note

[1] "Black-swan" events refer to rare and unpredictable events as explained in the book "the Black Swan: The Impact of the Highly Improbable" published in 2007 by Nassim Nicholas Taleb.

References

Beddington, J. et al. (1976), "Concepts of stability and resilience in predator-prey models", Journal of Animal Ecology, vol. 45, 791–816, London.

Dutch Ministry of Security and Justice/Ministry of Interior and Kingdom Relations (2009), Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands, Directorate-general for Public Safety and Security, the Hague.

Federal Office of Civil Protection and Disaster Assistance (2011), Guideline for Strategic Crisis Management Exercises, Federal Office of Civil Protection and Disaster Assistance, Bonn.

Kaji, Y. (2012), "Inter-agency crisis management", presentation at First OECD/Swiss Federal Chancellery Workshop on Strategic Crisis Management, Geneva, Switzerland, 28 June 2012, http://www.oecd.org/governance/risk/Japan.ppt.

Kang, S.J. (2012), "Integrated situation management in Korea", Presentation at First OECD/Swiss Federal Chancellery Workshop on Strategic Crisis Management, Geneva, Switzerland, 28 June 2012, http://www.oecd.org/governance/risk/korea.ppt.

Leonard, D. (2012), "Rethinking the management of large-scale national risks", Presentation at First OECD/Swiss Federal Chancellery Workshop on Strategic Crisis Management, Geneva, June 28, 2012.

OECD (2011), Future Global Shocks: Improving Risk Governance, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264114586-en.

OECD (2013), OECD Reviews of Risk Management Policies: Mexico 2013: Review of the Mexican National Civil Protection System, OECD Publishing, Paris.

Présidence la République Française and Mallet. J.C. (2008), Défense et Sécurité Nationale : le Livre Blanc (White Paper on Defence and National Security), Éditions Odile Jacob and La Documentation Française, Paris.

Rossi, L. (2012), "The Italian emergency management system", presentation at First OECD/Swiss Federal Chancellery Workshop on Strategic Crisis Management, Geneva, Switzerland, 28 June 2012, http://www.oecd.org/governance/risk/italy.ppt.

Schoen, J. W. (29 July 2013), "Pentagon kills 'terror futures market'", NBC News, http://www.nbcnews.com/id/3072985/t/pentagon-kills-terror-futures-market/.

Swiss Federal Chancellery (2009), Exercice de conduite stratégique – ECS 2009

UK Cabinet Office (2012), Enhanced SAGE Guidance, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/80087/sage-guidance.pdf.

UNISDR (2009), UNISDR Terminology on Disaster Risk Reduction, United Nations Office for Disaster Reduction, Geneva, www.unisdr.org/we/inform/terminology, accessed on 1st October 2012.

US Department of Homeland Security (2008), National Incident Management System, https://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf, FEMA Publishing, Washington, DC.

US Department of Homeland Security (2011), Risk Management Fundamentals, Homeland Security Risk Management Doctrine, US Department of Homeland Security, Washington.

World Bank (2010), Natural Hazards, UnNatural Disasters, The Economics of Effective Prevention, The World Bank and the United Nations.

World Economic Forum (2012), Global Risks 2012 Seventh Edition, an Initiative of the Risk Response Network, Insight Report, World Economic Forum, Geneva.

World Meteorological Organisation (2012), Institutional Partnerships in Multi-Hazard Early Warning Systems, M. Golnaraghi Ed., Springer-Verlag, Berlin.

Further reading

Boin, A. et al. (2005), The Politics of Crisis Management, Public Leadership under Pressure, Cambridge University Press, Cambridge.

Boin, A. (2012), "Thinking the Unthinkable: The Limits of Traditional Crisis Management and the Necessity for New Approaches", Presentation, First OECD/Swiss Federal Chancellery Workshop on Strategic Crisis Management, Geneva, June 28, 2012.

Boin, A. et al. (2005), The Politics of Crisis Management, Public Leadership under Pressure, Cambridge University Press, Cambridge.

Duiven, R. (2012), "Inter-Agency Crisis Management in the Netherlands", Presentation, First OECD/Swiss Federal Chancellery Workshop on Strategic Crisis Management, Geneva, June 28, 2012.

Ghosh, P. (2011), "Emergency Plans 'needs scientists'", BBC News, online edition, 2nd March, 2011, www.bbc.co.uk/news/science-environment-12623089, accessed on 1st October 2012.

IRGC (2011), Improving the Management of Emerging Risks, Risks from new technologies, system interactions and unforeseen or changing circumstances, International Risk Governance Council, Geneva.

IRGC (2010), "Emerging Risks, Sources, drivers and governance issues", Concept Note, discussions at a roundtable on 8-9 June 2009 and a workshop on 16-17 December 2009.

IRGC (2012), "Social Media for Crisis Communication", Concept Note, IRGC, Geneva.

Japanese Prime Minister's Office, (2012), Presentation, First OECD/Swiss Federal Chancellery Workshop on Strategic Crisis Management, Geneva, June 28, 2012.

Jobet, J.C. (2012), "Lessons, improvements and challenges after the 2010 earthquake in Chile", Presentation, First OECD/Swiss Federal Chancellery Workshop on Strategic Crisis Management, Geneva, June 28, 2012.

Kang, S. J. (2012), "Integrated Situation Management in Korea", Presentation, First OECD/Swiss Federal Chancellery Workshop on Strategic Crisis Management, Geneva, June 28, 2012.

Magazine for National Safety and Security and Crisis Management (2012), National Safety and Security and Crisis Management, Special Issue, April 2012, National Coordinator for Counterterrorism and Security, Ministry of Security and Justice, The Hague.

Ministry of the Interior and Kingdom Relations (2007), National Security Strategy and Work Programme 2007-2008, Ministry of the Interior and Kingdom Relations, The Hague, http://merln.ndu.edu/whitepapers/Netherlands-2007-2008.pdf, accessed on 1st October 2012.

Mueller, N. (2010), "Proposition for a multi-dimensional, integrated approach for a crisis management system on a national level", 14th Annual Conference of the International Research Society for Public Management (IRSPM), Berne, 2010.

OECD (2003), Emerging Risks in the 21st Century: An Agenda for Action, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264101227-en.

Orantes Zenteno, J.C. (2012), "Mexico's National Experience", Presentation, First OECD/Swiss Federal Chancellery Workshop on Strategic Crisis Management, Geneva, June 28, 2012.

Rossi, L. (2012) "The Italian Emergency Management System", Presentation, First OECD/Swiss Federal Chancellery Workshop on Strategic Crisis Management, Geneva, June 28, 2012.

Sécurité et Stratégie (2012), "Dossier Spécial : La Gestion des Crises, Méthodologies et Retours d'Expériences", Sécurité et Stratégie, No°10, Le Club des Directeurs de Sécurité des Entreprises, Paris.

Smit, P. (2012), "Emergency and crisis management: the Swiss federal staff group ABCN", Presentation, First OECD/Swiss Federal Chancellery Workshop on Strategic Crisis Management, Geneva, June 28, 2012.

Sundelius, B. (2012), "Swedish Inter-Agency Crisis Management - mission and working approach", Presentation, First OECD/Swiss Federal Chancellery Workshop on Strategic Crisis Management, Geneva, June 28, 2012.

World Bank (2010), Natural Hazards, Unnatural Disasters, The Economics of Effective Prevention, The World Bank and the United Nations.

World Economic Forum (2012), Global Risks 2012 Seventh Edition, an Initiative of the Risk Response Network, Insight Report, World Economic Forum, Geneva.

Chapter 2

Understanding and identifying strategic crises through early-warning and sense-making

Though important advances have occurred in recent years, governments are regularly surprised by the emergence of crises and still struggle to identify and understand them. This chapter examines the challenges of early warning and sense-making associated with strategic crises. It explores the multiple contexts - group, organisational, and political - in which leaders and their advisers are embedded. These contexts enable and constrain leaders and their advisors. The role of current and emerging information and communications technology (ICT) is discussed in relation to finding ways to harness technology to increase sense-making capacity and identify potential vulnerabilities and risks. In addition, problems of effectively managing expertise, information, and knowledge with regards to early warning and crisis management are examined. The chapter concludes by presenting a set of critical topics that require further capability development and policy reform efforts.

This chapter builds upon research funded by the Swedish Civil Contingencies Agency, the Swedish Defense University, and the Swedish Institute for International Affairs. In addition, it draws upon and selectively reports preliminary results from the European Union 7th Framework Research Program funded project ATHENA.

Key messages

1. The capacity to detect and make sense of a crisis in a timely fashion is key to strategic crisis decision-making. This entails understanding the broader political significance of events beyond the narrow focus on physical impacts.
2. The development of early warning systems benefits from significant improvements in hazard detection and monitoring and ICT over the last decade. Integrating this scientific expertise across organisations and improving risk awareness are key to triggering action on the ground from both emergency responders and the public once warnings are issued.
3. When confronted with unfamiliar emergencies, strategic crisis managers should be able to identify and quickly mobilise relevant and trustworthy expertise to make sense of the crisis. It is important to set-up knowledge management systems and expert networks in advance across multiple sectoral, professional and disciplinary boundaries.
4. In order to properly utilise expertise in strategic crisis decision-making, expert judgements should be made in plain language, be accessible, and respond to opposing views. Clarifying the associated uncertainties of these judgments is essential.
5. Strategic crisis managers need to be prepared to take difficult trade-off decisions and cope with conflicts between core values that are threatened by the crisis (e.g. human life, public health, democracy, civil liberties, rule of law, political autonomy, economic viability, and public trust). Identifying the core values at stake in the crisis or its potential future development is a fundamental aspect of sense-making.
6. Sense-making processes should be adapted to crisis situations, avoid information overload, take full attention of time pressures and stress conditions, and leave room for strategic leadership reflection and deliberation.
7. Experience is a key asset for sense-making and officials should have opportunities to practice their sense-making and warning skills through strategic crisis management exercises.

Despite great strides in administrative practices as well as key scientific and technological advances, governments are regularly surprised by the emergence of crises and have great difficulty in making sense of them (Boin et al., 2005). Recent history points to many cases where familiar hazards have manifested themselves in unexpected ways, and new hazards will continue to arise to test leaders and organisations.

Many governments have tried to better anticipate and prepare for increasingly uncertain risks and "black swan" events, as well as classic forms of crises. Monitoring and early warning systems have been developed to detect signs of impending crises. These tools can detect and understand a wide range of events, but they need to be properly established and co-ordinated with decision-making mechanisms so that they lead to an efficient crisis response. The "chaotic" domain, also known as "unknown unknowns", requires different tools that are more conceptual than technological: this requires a capacity to build and share multidisciplinary expertise under intense time pressure. Taking the right decisions despite the many unknown elements requires real-time understanding of economic, social, environmental and political causes and effects. This is the "sense-making" function before, during and after a crisis, which goes beyond information and intelligence sharing.

This chapter explores the functions of early warning systems and sense-making for critical risks in an inter-agency crisis management context. Underdeveloped early warning systems, failures to act in response to warnings, and inadequate crisis sense-making can reduce the ability of governments to respond to crises. This chapter underlines opportunities for governments to prevent, mitigate and better manage crises.

The concept of sense-making

Recent crisis and sense-making failures

The importance of effective crisis sense-making can be examined using recent cases. Hurricanes, tornadoes, derechos (linear wind storms), cyclones and typhoons are a recurring feature of life in OECD countries and around the world. However, despite advances in storm and hydrological modelling, strategic decision-makers at national, regional, and local levels still face considerable difficulties in anticipating and responding to the consequences of major storms and the flooding that often follows. Despite considerable investment in preparedness (organisation, planning, training, and exercise) and storm monitoring and modelling, strategic decision-makers in the United States federal government struggled to maintain situational awareness of key issues such as fuel availability and distribution in the wake of Hurricane Sandy in 2012.

Though Sandy was a relatively moderate storm in terms of wind-strength category, other features of the storm greatly magnified storm surge damage to the country's mid-Atlantic coast, and caused tremendous destruction/disruption of critical transport, energy (electric and gasoline) infrastructure and housing. The example of Hurricane Sandy indicates that natural hazards can interact with human environments and technologies in ways that will produce cascading impacts that challenge and frequently outstrip the capacity of governments to follow rapidly unfolding and escalating events.

Hurricane Sandy highlights the difficulties associated with managing a moderately severe event. Increasingly, the United States is emergency planning for 'Maximum of Maximums' (MoMs) scenarios. According to Federal Emergency Management Agency (FEMA) administrator, Craig Fugate: "Historically in emergency management we have only planned for what our capabilities can handle or only looked at what we can do to

respond as government. But what we really need to be doing is planning for disasters that go beyond our capabilities. That's why we have to look beyond our government-centric approach and see what outside resources we can bring to the table. We need to better engage our volunteer and non-profit partners, work with the private sector, and most importantly involve the public."[1] Making sense of events on the scale and complexity of Hurricane Sandy requires government to engage in new forms of collaborative information sharing across not only the "whole of government" but also the "whole society".

The crisis triggered by the Great East Japan earthquake of 11 March 2011 reveals both the strengths and vulnerabilities in Japanese preparedness at the time. The undersea earthquake (which measured 9.0 on the Richter scale) resulted in a devastating tsunami that impacted on more than 500 km of coastline and caused damage as far inland as 5 km. More than 15 000 persons are confirmed to have lost their lives (with more than 4 000 additional persons reported missing) and another nearly 6 000 were reported injured. Hundreds of thousands of buildings were damaged or destroyed and nearly 600 000 persons displaced. The disaster had tremendous impacts on critical infrastructure, initially leaving 4.4 million households without electricity and an additional 1.5 million without water.

Despite these great losses, tsunami detection and early warning systems and evacuation routines in Japan are thought to have saved many lives.[2] Social media were used to good effect and in innovative ways, which contributed to enhanced situational awareness for government and non-governmental response and recovery efforts (Slater et al., 2012). The crisis escalated when it became clear, after a period of ambiguity and conflicting reports, that the tsunami had compromised cooling systems at the Fukushima nuclear plant, resulting in core meltdowns and hydrogen explosions producing uncontrolled releases of radiation and necessitating the evacuation of 80 000 persons. This nuclear accident, one of the most severe in history, produced not only radioactive fallout, but also considerable political and economic impacts that reached far beyond Japan's shores (Kingston, 2012: 1-2). Crisis sense-making on the part of the Japanese government was greatly hampered by serious difficulties in obtaining accurate information from key private sector actors such as the Tokyo Electric Power Company (TEPCO).

Planned acts that are executed by human antagonists can also challenge pre-crisis and crisis sense-making. The Oslo terrorist attacks of 22 July 2011 demonstrate that not only states and terrorist networks, but also "lone-wolves", can cause major shocks. Prior to the elaborately planned and staged attacks, Norwegian counter-terrorism heavily focused on the threat of jihadi terrorism and did not respond effectively to warning signals of a mounting threat from right wing extremists, such as Anders Behring Breivik. Breivik's preparations, such as purchases of large quantities of fertilizer (a key ingredient in the bombs he used to attack the Norwegian government), could have set-off a number of counter-terrorism "tripwires". However, he did not match the prevailing ethnic/religious profile for a likely terrorist and his purchase of a small farm masked his true purpose for buying the fertilizer. The July 22 Commission and other evaluations/studies have noted lapses not only in the ability of the Norwegian authorities to generate and act on early warning signs, but also to maintain qualified and timely situational awareness while under attack (Agrell, 2013). Similar difficulties plagued efforts in the United States to prevent and respond to the 9/11 attacks and, more recently, the Boston bombings of 2013.

Defining and characterising crises

Given the dramatic nature of the cases highlighted above, all of these events could be defined as major crises. However, this labelling leads to questioning the common characteristics they share. A crisis can be defined using three subjective criteria, as perceived by strategic leaders (and those for whom they are responsible): threat, uncertainty, and urgency (Rosenthal, Hart, and Charles, 1989; Stern, 2005; Hermann, 1963).[3] These criteria are helpful in distinguishing crises from other types of situations and provide a means for probing and preparing to act during a crisis.

First, crises are associated with threats to (and often potential opportunities to promote) the core values held by decision makers and/or their constituencies. These include human life, public health and welfare, democracy, civil liberties and rule of law, political autonomy, economic viability, and public confidence in leaders and organisations. Leaders must also be prepared to cope with conflicts between such values (Farnham, 1997). The threat of terrorism, for example, entails potential conflicts between security considerations and civil liberties, as demonstrated by the post-9/11 debates on the Patriot Act, Guantanamo Bay, and, more recently, electronic surveillance practices. Corresponding tensions can also emerge regarding the potential public safety and health measures associated with other contingencies, such as quarantine restrictions in epidemics and mandatory evacuation orders in the face of hazards such as storms, wildfires, or toxic spills.

Second, crises are associated with a high degree of uncertainty regarding the nature of the threat (i.e. the known and unknown unknowns), the composition of an appropriate response, or the possible ramifications of various courses of action. For example, the causes and means by which sudden acute respiratory syndrome (SARS) was transmitted were not known during the initial outbreak in 2003. , It was difficult for Chinese and Canadian authorities to deal with the public health challenges and the political, social, and economic consequences of the disease in the absence of this knowledge (Olsson and Xue, 2011).

Some analysts distinguish between “familiar” and “novel” contingencies, when it comes to crises. All else being equal, the more familiar the contingency (and the more it resembles scenarios used during planning, training, and exercising), the more likely it is that crisis managers will face moderate levels of uncertainty and be working in the domain of structured problem-solving. The more unexpected and novel the event, the greater the uncertainty and the more ill-structured the domain in which crisis managers must operate. Coping with novel contingencies and the associated cascading shocks makes the already difficult challenges of crisis sense- and decision-making even more demanding.

Third, crises are associated with a sense of urgency. Crises force decision makers to take consequential decisions in public life under extremely difficult circumstances. Events are perceived as moving quickly and there are small windows of opportunity to influence their course. Effective and proactive intervention can minimise vulnerability (such as by getting citizens or mobile assets out of harm’s way before a storm hits), and help to prevent or mitigate the impact of a potential threat (e.g. disrupting a terror plot or isolating carriers of a highly infectious disease.) Additional time pressures stem from the relentless pace of the 24-hour news cycle. Strategic decision makers and their organisations must cultivate the capacity to diagnose situations and formulate responses under severe time pressures.

Diagnosing a crisis situation

The three criteria of threat, uncertainty and urgency provide the basis for a practical diagnostic tool (Stern, 2009) that is particularly useful for novel crises and that can help crisis managers take control. Confronted with a threatening situation, the components of crisis definition can be turned into three diagnostic questions, as explored below.

What are the core values at stake (and for whom) in this situation?

This question helps crisis managers to identify key constituencies, threats and opportunities embedded in the crisis. It also encourages managers to craft solutions that tackle these key elements in a consciously balanced and measured way. A common source of difficulty in crises is when the initial framing of problems does not identify the full range of values and stakeholders concerned. Sometimes, policy-makers rush to develop options for action without taking the time to fully consider the nature of the problem they are faced with. This can lead to unbalanced response strategies. Explicitly focusing on identifying values (c.f. Keeney, 1992) can be useful to direct the attention of policy-makers to exploring this key dimension of crisis sense-making. Crises commonly demand hard choices, and dilemmas and value conflicts such as those mentioned above arise frequently (George, 1980; Farnham, 1997). The capacity of decision makers to formulate strategies that are well adapted to the situation and that protect key values will be increased if they engage in rigorous value-probing.

What are the key uncertainties associated with the situation and how can they be reduced?

This question enables decision makers to identify key variables and parameters and better prioritise intelligence and analytical resources. A simple but effective means of coping with uncertainty is to make the identification of multiple scenarios a standard practice of crisis sense-making (Stern, 2009). Development of best, worst, and middle case scenarios can be very helpful.

Identifying multiple scenarios forces sense-makers to extrapolate from current information and formulate prognoses. This type of thinking can help crisis sense-makers break out of a reactive mode and be more proactive in their response to the crisis. Comparing scenarios can help policy-makers identify critical variables that can be monitored closely for indications of how and in which direction the crisis is developing. Recognition of and preparation for the worst case not only tends to be helpful with regard to improving readiness and capability, but is generally good politics as well as it tends to adjust expectations in helpful ways. The general public and journalists tend to be far more critical of complacency or negligence in the face of a previously uncertain threat that subsequently occurs than of vigilant over-reaction, which is generally forgiven if perceived to have been in good faith. For example, the costly efforts to prepare for and reduce exposure to the-- as it turned out-- relatively anticlimactic "Y2K" computer bug scare at the turn of the millenium were not particularly controversial (c.f. Quigley, 2005). "Better safe than sorry" is relatively easy to defend in today's risk society.

How much time is available (or can be 'bought') to deal with this situation?

It is increasingly recognised that strategic leaders must make meta-decisions—decisions about how to decide. This includes determining what kind of sense-making and decision-making process is appropriate to the situation and context. Effective and

legitimate crisis sense- and decision-making processes may look very different depending upon whether the time frame is measured in minutes, hours, days, weeks, or months. As the time frame widens, there is increasing room for analytical, deliberative, consultative and coalition building processes (e.g. George, 1980). Effective systems for early warning, accompanied by vigilant, proactive responses to warning, create larger temporal windows for prevention, mitigation, and preparation of policy and operational responses.

Why sense-making failures are so common

One of the most fundamental and difficult tasks for crisis managers is to make sense of what is happening and develop an understanding of what the evolving situation means for them, their missions, their organisations, and various effected stakeholders (Boin et al., 2005; Boin and Renaud, 2013). Failures of sense-making contribute to over-, under- or mis-estimations of emerging threats (Karl Weick, 1988, 1993). Correspondingly distorted decisions and stationing of forces and resources may have tragic consequences. Inadequate sense-making is a key contributor to "type three" errors (Mitroff and Silver, 2009), in which decision makers spend scarce cognitive and material resources developing and implementing precise (and sometimes less precise) solutions to the wrong problems - a common phenomenon in crisis situations.

Assessments of the magnitude of public disorder and security threats to first responders during Hurricane Katrina of 2005 illustrate the profound operational and political consequences of inadequate sense-making. As local and state response resources were overwhelmed and there was an urgent need for federal assistance, the provision of federal aid was significantly delayed due to a perception among strategic decision makers in Washington that violence in New Orleans posed a threat not only to the population but also to responding federal and National Guard units. Given the breakdown of communications (Farazmond, 2007: 153), and the prevailing information deficit, media reporting was key to crisis decision makers' perception of the situation and contributed to an emphasis on public order and "force protection" issues at the expense of other priorities. Subsequent research has demonstrated that much of this reporting was unsubstantiated and sensational, dominated by media "frames" such as "civil unrest" and "urban warfare" (Tierney et al., 2006: 57).

A particular problem was "looping", in which clips of isolated incidents in a particular area of the city (such as scenes of boat-borne rescuers coming under fire from hidden assailants) were continuously rebroadcasted by the media and sustained the impression that violence (and other forms of anti-social behaviour, such as looting) was widespread and ongoing. The available evidence strongly suggests that these lapses of sense-making inhibited not only the public sector, but also the emergent voluntary response from providing timely assistance to the stricken city and contributed to a widespread perception that the federal government had not responded effectively to the disaster (US Senate, 2006; Tierney et al., 2006: 75-76).

Difficulties in framing and making sense of crises are not limited to natural disasters. During the 1990s, the European Union (EU) and its member states experienced a series of crises in the food and agriculture sectors. On what has become known as "Black Wednesday" (March 20, 1996), the British authorities announced a suspected link between bovine spongiform encephalopathy (BSE, commonly known as mad cow disease) and a fatal neurological disorder in human beings called Creutzfeld-Jakobs Syndrome (CJS). Confronted with this potentially threatening signal, the European Commission (EC) chose to frame the problem in largely scientific terms and launched

expert consultations and investigations designed to reduce uncertainty and form a response. This approach to the situation neglected political and psychological aspects of the rapidly escalating crisis and resulted in a regional leadership vacuum that was filled by uncoordinated and conflicting responses from member states. EU officials underestimated the potential of this issue to create economic disruption, citizen confusion, and bitter political conflict within the EU.

Three years later, the Commission faced a new challenge when it was revealed that dioxin, a toxic substance, had been discovered in Belgian chicken products that had been distributed throughout the country, Europe, and to other regions of the world. The Belgian government delayed disclosing the contamination for nearly a month. This time the European Commission acted immediately to ban exports of Belgian chicken products, without waiting for expert risk assessments and policy consultations. The Belgian dioxin crisis was framed in very different and much more political terms. (It later turned out that the ban, while good politics, was probably ineffectual since the contaminated foodstuffs had been produced some six months before and had mostly likely already been consumed). Comparing these cases yields interesting results. In the first case, a narrow framing of the BSE problem resulted in a missed opportunity for the Commission to be proactive and take charge of a pan-European problem. In the case of Belgian chicken products, there was a very different approach that generated a hasty and operationally ineffective response.[4]

These examples illustrate the importance of effectively framing problems and striking the right balance between different dimensions and considerations of crisis management. Prudent policy-makers may "look before they leap", but in a crisis it often turns out that "he who hesitates is lost". In each of the cases highlighted above, an adequate and balanced framing of the situation - a vital precondition of a sound crisis response - was lacking for different reasons.

Making sense in (and of) crises is a daunting task. In crises, human leaders and fallible organisations are called upon to make and implement complex and highly consequential decisions under incredibly difficult conditions. The high degree of uncertainty that characterises such situations creates a typical dilemma: act on the basis of imperfect, incomplete, inconclusive and partially digested information or risk missing fleeting windows of opportunity to affect a fast-moving course of events. In crises, the difference between success and failure often hinges upon the ability to produce and revise adequate (plausible, reasonable, coherent, actionable, justifiable) strategic and tactical assessments of rapidly moving events.[5]

Decision-makers act (and are activated) on the basis of a subjective picture of an emerging situation.[6] When occupying what organisational psychologist Rhona Flin (1996) has called "the hot seat", they cannot have perfect, complete, and uncontested information about the potentially escalating challenges they face. Instead they begin with a preliminary and provisional picture of what is happening and, equally importantly, what it means. Any actions taken or not taken will largely derive from the content the quality of situational assessments that took place prior to the crisis and as it began to emerge. Furthermore, the possibility of producing intended and desirable consequences through action or inaction depends largely upon the compatibility between the assessment and what is actually occurring. The possibility of good fortune exists, where action based on an inaccurate situational assessment turns out to have beneficial consequences in a crisis, however, policy-makers should certainly try to avoid relying on such serendipity.

Strategic surprise and the warning-response problem[7]

Strategic surprise can be characterised as an abrupt revelation that leaders have been working with a faulty threat perception regarding an acute, imminent danger or vulnerability (Levite, 1987: 1). The literature suggests that surprise can be conceived as stemming from a victim's lack of preparedness based on erroneous judgments of whether, when, where, and how a negative event (such as an attack or catastrophic accident) might occur (Betts, 1982: 11). In the all hazards realm, this may be reformulated in terms of a failure to anticipate, prevent or prepare adequately for the occurrence of societal shocks that stem from structural processes (e.g. natural or industrial), accident or malevolence.

There are many examples in history and the literature where strategic leaders (and those who serve them) have failed to pay attention to indications and/or warnings of a mounting threat. Many of the classic cases, such as Pearl Harbor, the German surprise attack on the Soviet Union, and the Middle East War of 1973, involve warfare between states. However much of the literature on strategic surprise and the "warning-response problem"—in which warnings are not acted upon in a timely and appropriate fashion in relationship to the indications of mounting threat-- is also applicable to and suitable for an all hazards approach to societal security/safety (Golnaraghi ed., 2012). This approach is useful for understanding asymmetrical antagonistic threats, such as terrorist attacks or acts by organised criminals, as well as surprises that stem from natural hazards and critical infrastructure failures, etc. (Parker et al., 2009).

More complex conceptualisations distinguish between surprise and unpreparedness, and general warning versus credible, conclusive, and specific warning (Levite, 1987: 3, 26) of particular threats. Kam (1988: 8) focuses on three main elements inherent to a surprise event: 1) the event is contrary to the victim's expectations; 2) there is a failure of advanced warning; and 3) the event exposes the lack of adequate preparation. Although there are different degrees of surprise (like warning), studies of past surprise attacks (and other largely unanticipated negative events) have led most scholars to conclude that surprise was often not inevitable based on the available indications of mounting threat and warnings that existed prior to the event (e.g. Wohlstetter, 1962). Furthermore, there are numerous documented examples of cases in which the intelligence picture was accurate, but appropriate action was not taken by strategic leaders in response to the warning.[8] Thus, warning alone is insufficient; both warning and response are needed" (Betts, 1982).

Falling prey to a surprise attack generally indicates failure in one or more links along a complex chain of policy, intelligence, warning, and response. Classical strategic surprise analysis has focused predominantly, if narrowly, on the core questions of whether or not specific warning existed, whether or not it was accurately interpreted, and whether or not policy-makers responded adequately. While these are central questions, it is important to address the responsiveness of the system to more generalised warnings and proposals for threat and vulnerability mitigation reforms in the months and years prior to the surprise.

Designing and calibrating early warning systems

Conceptualising warning/response as part of a chain of events runs parallel to current thinking regarding the design and development of multi-hazard early warning systems. For example, a recent multi-nation study (including cases from France, Germany, Japan, the United States and China) proposes dividing early warning systems for natural hazards into four interdependent components: 1) hazard detection, monitoring, and forecasting; 2)

analysing risks and incorporation of risk information in emergency planning and warnings; 3) disseminating timely and authoritative warnings; and 4) community planning and preparedness and the ability to activate emergency plans to prepare and respond, with co-ordination across agencies, at national to local levels. (Golnaraghi, 2012: 230)

Designing and calibrating early warning systems, and judgment in their use, pose difficult challenges. Designers and users of these systems must navigate between twin difficulties and modes of failure: systems that set the warning threshold too high may fail to sound the alarm or warn too late if the warning signals detected are too "soft" or ambiguous; whereas failure to warn in the face of what turns out to be a devastating event (false negatives) will discredit the warning system and those responsible for the system.

A warning system that produces chronic false positives (crying wolf) tends to produce warning fatigue and experiences eroding credibility over time. Although false positives can be costly in economic and political terms, false negatives and failure to act in the face of potential catastrophe tend to be far more costly in terms of lives, assets, and political legitimacy. Leaders must strive to create organisational and societal cultures of tolerance for occasional false positives if false negatives are to be avoided. An example is local firefighting: the price of vigilant response to real fires is acceptance of the costs associated with vigorous response to false alarms (Parker and Stern, 2005).

Science and technology have great potential to develop means of tracking and predicting the onset of various natural and man-made hazards. The rise of "big data" and capacities for monitoring social media feeds (see the section on information and communications technology below) present opportunities to develop new types of early warning systems to complement those that exist. However, technology will only provide leverage on certain aspects of the warning-response challenge.

Developing effective early warning systems is a difficult task and various problems can occur at different stages of the process. Warning-response problems can contribute to failures of early warning and negatively impact on crisis sense-making. Analyses of early warning failures (and successes) should be contextually grounded to take into account the chronically overcrowded state of the policy agenda and the politicised nature of agenda setting, as well as relevant organisational and psychological factors. Kam (1988: 213) observes that the "failure to prevent a surprise…does not evolve overnight" and is "not the result of any single factor…[or] mistakes committed on any one level." Policy processes and factors that contribute to warning response failures and/or failures of crisis sense-making are too complex to be able to easily explain their origins or identify isolated quick fixes.

In the following section, several of the ways in which threat recognition impacts on warning-response/crisis sense-making will be explored.

The multiple contexts of sense-making and early warning

Sense-making before and during crises takes place within organisational, socio-technical and political contexts that both enable and constrain the ability of decision-makers to understand potential threats and opportunities.

Sense-making in organisations and groups

The capacities of strategic decision-makers to make sense of crisis situations are heavily influenced by the characteristics of the organisationals environments in which they work. This is highlighted in three examples from historical crises documented in literature.

The US administration of President John F. Kennedy discovered the Soviet placement of missiles in Cuba due to the resumption of U2 spy plane flights over Cuba, but only after a prolonged delay due to the nature of the human and photo intelligence processing routines (and backlogs) of the day (Welch, 1992: 125-6).

In 1986 the Soviet Union did not warn its European neighbours that a catastrophic nuclear accident had taken place at Chernobyl, the radioactive fallout was first detected several days later at a Swedish nuclear power plant, Forsmark. The plant manager, diagnosing the mysterious radiation as a possible local malfunction, promptly activated his emergency organisation and evacuated 800 persons - inadvertently sounding the Chernobyl alarm for the Western world. The radiation was registered at several Swedish radiation measurement stations in other parts of country prior to the Forsmark alert, however, these measurement stations were not equipped with alarms and were only checked periodically. As a result, the heightened radiation readings were not brought to the attention of the authorities until after the Forsmark scare. It is very likely that the authorities would have explored a variety of other hypotheses and initially framed the problem very differently, had the radiation been noticed elsewhere first (Stern, 1999a).

The 1986 assassination of Swedish Prime Minister Olof Palme illustrates failures of inter-organisational information sharing in a crisis. The Prime Minister was shot at 11:21 pm and due to fears that it may be a first step in a strategic removal of the Swedish leadership preceding a military attack, contingency plans called for the immediate notification of military headquarters. Once notified, military intelligence would assist their civilian counterparts and, if necessary, the Swedish military could be placed on alert. However, neither the local police, nor the relevant units of the national police authority notified the military that the Prime Minister had been shot. The military leadership was apprised of the situation two hours later by the military attaché in Washington who had heard the news on the BBC.[9]

As these examples illustrate, what crisis decision makers know, when they know it, and what it means to and for them are largely a result of the information technology in place and the gathering, sharing, analysis and assessment practices of the organisation or organisations involved. Individuals acting in a public capacity should be seen as role-players who are embedded in groups, networks, and organisations.[10] Thus, the ways in which policy making is organised and structured in practice, as opposed to on paper, profoundly affect the flow and interpretation of information, as well as the distribution of political-administrative power.

Authority often contracts in crisis situations, leaving a small circle around a leader who has the task of sense- and policy-making for the crisis. However crisis operations often involve a large number of organisational actors and administrative levels.[11] This institutional complexity generally has both horizontal and vertical dimensions. The horizontal dimension concerns multiple agencies at the same level of government who may perceive themselves as having a stake in the crisis problem. For example, crises with a foreign policy dimension in the United States may be perceived as concerning not only the Department of State, but also departments such as Defense, Commerce, Energy;

intelligence agencies such as the Central Intelligence Agency (CIA) and the National Security Agency (NSA); and other organisations such as the Joint-Chiefs of Staff, the National Security Council staff, and relevant Congressional committees. Achieving a qualified and current operating picture that enables a whole of government response to a crisis is a difficult task.

It is also increasingly recognised that strategic crisis leadership must often be based on situational awareness that draws upon information and expertise from across the whole of society; covering not only the various parts of government, but also integrating information and capabilities from the private and non-profit sectors and from citizens directly through avenues such as social media. As noted above, the Fukushima nuclear accident illustrates the vulnerability of national leadership to breakdowns of situational awareness across the public-private divide, and the compensating decentralised dynamics that emerged across a whole society response to the catastrophe (Kingston, 2012).

The vertical dimension of organisational complexity focuses on the potential involvement of actors across levels of government. Many crises begin at the local level, where an often uneven process of political-administrative escalation commences. For example, crises provoked by acts of terrorism and natural/industrial accidents often begin in a specified geographic location and administrative jurisdiction before escalating into national or international crises. Though much of the criticism of the US response to Hurricane Katrina focused on the federal government, many other actors from local, county, and state government share responsibility for the successes and failures associated with the case (Parker et al, 2009).

It is essential to recognise that: "different actors hold different perceptions stemming from differences in tasks, jurisdictions, education, geographical location, level of preparedness, and other political and administrative considerations. Consequently decision makers and agencies are drawn into a crisis at different moments, from different points of view, and with different purposes."[12] Thus both horizontal and vertical forms of institutional complexity may have profound impacts upon sense-making in crises (Stern, 2009).

This implies that even if every actor had access to the same basic information about a crisis situation, interpretations and priorities are likely to diverge considerably. The various participating actors tend to focus on different aspects of the situation, assess the plausibility and credibility of conflicting situation reports differently, draw upon different analogies, make different inferences and prognoses, and see different interests at stake as they are each attending, analysing, and interpreting events from their own vantage points. This problem becomes even more complex when considering the likelihood of various relevant actors having access to the same information base. Although this is not impossible, it is more likely with particularly open, reliable, and vigilant organisations (Laporte, 1996; Weick and Suttcliffe, 2002; Sagan; 1993).

Poor information sharing in crisis situations is not only a function of inefficiency or deficient information technology, but often the result of policy or (bureaucratic) politics. Sensitive issues are often handled on a "need to know" basis, which makes good sense from a security perspective as the fewer who are in the know means the less chance of leaks to the press, political (or bureaucratic) rivals, or foreign governments. In practice, it is often difficult to understand who needs to know what, and officials deprived of critical information may be seriously hindered in attempts to discharge their functions and fulfil their missions under crisis stress.

As information is a key currency of power in governmental and other political settings, officials are often allocated information in a relatively arbitrary fashion. At times it is provided as a reward or sign of favour; or it can be withheld as punishment or to neutralise a potential adversary.[13] Such practices may result in distorted sense-making in crisis situations, sometimes with tragic consequences. Conflict and competition within government can have severe consequences for crisis sense-making/management if not managed and constructively moderated. This dynamic has been documented not only in national security and political crises, but also in other domains including natural disasters and industrial accidents; and large-scale public order events, such as riots associated with sporting events and political protests (Rosenthal et al, 1991; Hansen and Hagstrom, 2004).[14]

While management theories have promoted the virtue of small groups as problem solvers, several decades of small group research suggests that groups may fulfil multiple roles in policy-making settings. Not all of these are compatible with or conducive to vigilant sense-making under crisis conditions. If small groups are composed, directed, and animated by a working culture appropriate for their task and function, they may be highly effective sense-making units. In the right circumstances, diversity and synergy effects may make small groups more able than individuals to make sense of complex and ambiguous situations.

However, there are many ways group sense-making processes can go wrong and make groups less likely to produce adequate situational assessments than individuals. Groups are liable to extremes of both conformity and conflict, both of which can impede collective sense-making efforts. Historical and laboratory studies have demonstrated that individuals in groups often do not share and use information effectively. Leaders, and other members, may resort to manipulative tactics and suppress information that is damaging to a favoured problem diagnosis or course of action. Small groups are also prone to co-ordination and accountability problems where individual members may fail to take practical or ethical responsibility in ways that damage the group's sense-making capacity. Therefore, although groups have virtues that can contribute to crisis sense-making, they can also be ineffective.[15]

Awareness of the enabling and constraining aspects of the socio-technical, organisational, and small group contexts is essential for improving sense-making before and during crisis situations. Leaders can greatly enhance the sense-making capacity of crisis monitoring/management groups by fostering organisational and small group cultures and processes that are conducive to information sharing and critical deliberation ('t Hart et al, 1997; George and Stern, 2002).

The political context and sense-making

Decision makers and organisations operate within particular political contexts and the degree of politicisation associated with an issue has a profound impact on policy action. Similarly, security politics concerns the definition of existential threats and the policy measures enacted to safeguard against these threats (Buzan, Wæver, and de Wilde, 1998). Work on security politics has concentrated on trying to understand why some security issues and threat images at any given time are accorded a high degree of importance and thus rise above the increasing number of competing threats and risks. Why do some issues capture a privileged place at the top of the political and policy agenda, while others languish in relative obscurity and neglect? (Kingdon, 1995; Eriksson, ed. 2001) The literature also helps to address the closely related question of under what circumstances

and to what extent does recognition of a given threat lead to meaningful policy change and/or organisational reform.

The Copenhagen school of security studies has developed a theory of "securitisation" that examines how issues are framed in competitive communication and dramatised as security threats worthy of being treated "through extraordinary means" (Buzan, Wæver, and De Wilde, 1998: 23). A similar focus can be found in the agenda-setting literature. Kingdon, for example, concentrates on the process of "problem definition" and "categorisation." If a condition is designated as a "problem" it is more likely to be elevated onto the agenda and inspire the belief that change is needed (Kingdon, 1995: 198). Studies on threat politics examine the struggle between advocates of competing problem frames over what issues have the highest "societal salience" and are therefore regarded as the most important (Eriksson, 2001: 4–5).

Whether an issue achieves prominence and is acted upon depends, to a large extent, on the amount of attention that bureaucrats, politicians, the media, the public, academia, and pressure groups devote to it, and whether they are able to draw attention to it successfully. It is of great importance, therefore, to ask who is engaged in the process of issue definition and agenda setting, and to what extent and why their advocacy impacts on policy, especially when it comes to spurring or failing to spur major policy shifts. Whether it is agenda-setting theory's "policy entrepreneur"—creatively connective problems with solutions and pushing them through fleeting "policy windows" (Kingdon, 1995), the securitising actor in securitisation theory (Buzan, Wæver, and de Wilde, 1998), or the framing actor of threat politics (Eriksson, 2001), there is a strong emphasis on policy actors, advocacy, and the circumstances under which policy change can take place.

The agenda-politics perspective points to three main sources to explain unaddressed vulnerabilities and warning-response problems: overcrowded agendas, the failure of key actors to place issues high enough on the agenda to be acted on adequately, and competing priorities. Political and policy agendas are chronically overcrowded. A wide variety of domestic, regional, and international issues compete for the limited attention of policy makers, political opposition, mass media, and citizens. Immediate issues, unscheduled and scheduled, tend to dominate the political space and bottlenecks of attention and time lead to policy-makers working on goals selectively and sequentially rather than simultaneously (Kingdon, 1995; March, 2006)

The process by which an issue is perceived as a security threat worthy of consideration and, most importantly, action, is largely dependent on the effectiveness of key "policy entrepreneurs" in placing the issue on the agenda. For example, then CIA director George Tenet had great difficulty in placing counter-terrorism on the G.W. Bush administration policy agenda prior to September 11, 2001, despite considerable effort (Parker and Stern, 2005). Another example is that despite recognition by US FEMA that hurricane-related flooding posed an acute danger to New Orleans, a danger clearly documented in risk analyses and simulated during the Hurricane Pam exercise of 2004, political interest in addressing these vulnerabilities was limited prior to the impact of Hurricane Katrina in 2005 (Parker et al., 2009).

In many countries, substantial crisis staffing arrangements have been put in place to support strategic policy-makers with the aim of improving their capacity to prevent and manage crises. This helps to bring potential crisis issues to the attention of policy-makers in a timely fashion and provides resources for: detecting and responding to crises, facilitating inter-ministerial and/or inter-agency co-ordination, and monitoring crisis policy implementation. For example, the National Security Staff in the United States, the

Cabinet Office in United Kingdom (which hosts the Cabinet Office Briefing Room, COBR), and, more recently established, the Prime Minister's Office Crisis Management Chancellery in Sweden, are designed to help fulfil these functions. Significant reorganisation of resources have recently or are currently taking place in a number of OECD countries, including the United States, Sweden, France, and Japan.

Leaders and advisers as sense-makers

How do leaders (and those who advise them) make sense of the bewildering flow and/or lack of critical information when making crisis decisions? Fifty years of cognitive research supports the view that prior experience–mental is the basis for sense-making in crisis as in everyday life. Expectations are highly significant: under conditions of ambiguity people often see what they expect to occur (Bruner, 1957; Jervis, 1976: 144-154; Weick, 1995).

For example, in the absence of reliable information, some decision makers and observers of the 1995 Oklahoma City bombing initially assumed that Islamic fundamentalist terrorists were responsible due to the recent experience of the 1993 World Trade Center bombing, which was the work of such a group, and the fact that domestic groups were not expected to conduct operations of this scale within the US. These assumptions and expectations proved incorrect: the perpetrators were US citizens associated with an extremist militia organisation (Nacos, 1994). Similarly, when Norwegian right wing extremist Anders Breivik launched his attacks on Oslo and Utoeya, many initially assumed his deeds to be the work of jihadi terrorists (Stern, 2011; Agrell, 2013).

These examples are suggestive of the way that sense-makers use encoded experience and a small piece of information (often called a cue by cognitive psychologists) to create a scenario. Sometimes this kind of cue enlargement points in the right direction, however it can just as easily lead to misperception.[16] The tendency to focus on circumstantial cues or similarities between current and previous events can be particularly harmful, especially if the sense-maker is overconfident in the accuracy of his or her interpretation.

Individuals tend to be attentive to a set of issues while ignoring others. What is on a person's mind (the content of the cognitive "agenda") at any given time heavily affects the monitoring and sorting of signals from the environment and their interpretation. This selectivity points to a highly distinctive feature of the cognitive "revolution" in psychology: recognition of the limitations of the human ability to acquire and process information.[17]

While the human mind is capable of great intellectual feats, it is also beset with great limitations regarding monitoring and analysing highly complex physical and social environments.[18] Individuals are bombarded with stimuli to such an extent that it threatens to overwhelm the human capacity to absorb and make use of the incoming information. As a result, it is necessary to selectively monitor the environment and "tune out" much of the incoming information in order to reserve the capacity to attend to the most pressing issues at any given time. Cognitive agenda-setting is a key part of this, although even the most skilful cognitive managers are liable to miss important information from time to time. Even when an issue is identified as important and attention is devoted to it, as is generally the case with crisis decision making, crucial information may be missing or uncertain. As a result, it is often necessary to go beyond the information given in order to interpret the world and make necessary judgements and decisions.[19] Cognitive science tells us that human brains collect, organise, store and recall information, making use of

packaging and organising devices that are generically called "cognitive structures". These cognitive structures – which include a family of cognitive concepts including schemas, scripts, analogies, metaphors, and stories – enable us to perform cognition by drawing upon encoded and selectively recalled experiences to interpret the present and prepare for the future (Klein, 2001; Vertzberger, 1990). Humans also make use of a number of mental "tricks" (heuristics) to facilitate classification, interpretation, and judgment. However, research findings indicate that this is often done in a haphazard fashion due to a number of biases and other questionable patterns of information processing. In order to cope with information overload and deficiencies humans take short cuts of various kinds (Kahneman, 2011). Sometimes these short cuts point in the right direction, other times they do not.

For example, the Swedish response to the tsunami crisis of 2004-5 provides examples of the different effects of analogical reasoning (c.f. Brandstrom, Bynander, and 't Hart, 2004). For example, the tsunami was initially framed by many Swedish decision makers as a problem of humanitarian aid. The first minister to appear on television was foreign aid minister Carin Jämtin, who reportedly initially used her experience of responding to a recent earthquake in Bam, Iran to orient herself in the current situation. This analogy focused attention on the fate of the non-Swedish victims of the tragedy, but initially obscured other aspects of the problem, such as the plight of the estimated 30 000 Swedish vacationers in Thailand. Prime Minister Göran Persson, in an interview later broadcast on Swedish television, described how he came to appreciate other aspects and the degree of urgency of the problem the following morning when Permanent Under-Secretary of Foreign Affairs Hans Dahlgren compared the tsunami with the 1994 sinking of the MS Estonia. This analogy brought into focus the prospect of national tragedy and prolonged political trauma (Brändström, Kuipers, and Daleus, 2008; Daleus, 2005).

The strong emotions aroused during crisis decision-making can impact on problem framing. Sense-makers, especially in emotionally engaging crisis situations, should be seen "…not as a rational calculator always ready to work out the best solution, but as "a reluctant decision maker, beset by conflict, doubts, and worry, struggling with incongruous longings, antipathies, and loyalties".[20] Several decades of crisis research has shed light on the ways in which various types of behaviour driven by motivated biases – such as denial, wishful thinking, betrayal, and value conflict - can influence problem framing and decision-making. A robust body of findings suggests that these motivational forces can distort information processing and ethical judgement and contribute to producing various policy errors. Analyses of historical cases such as the ill-fated attempt to change the Cuban regime via a proxy invasion at the Bay of Pigs, the Iran Hostage Crisis and the Iran Contra Affair which damaged the presidencies of Jimmy Carter and Ronald Reagan, and US counter-terrorism and homeland security policy prior to September 11, 2001, all illustrate the propensity of decision makers to succumb to motivated bias in their information processing. [21]

As already explored, crises entail threats to one or more key values. For example, coping with the hostage-taking of a significant figure or a group of people such as the 2013 attack on the Nairobi Shopping Mall, the 1975 occupation of the West German Embassy in Stockholm, the 1996-7 hostage crises in Lima, Peru, and the Moscow Theater Drama of 2002, entail balancing long term requirements, such as deterring future events and legal accountability, with the short term interest of protecting the lives of hostages and those who would be at risk from a military or para-military rescue operation.

Value complexity and conflict are considerable sources of stress in crisis situations. This stress may arise not only from threat-based value complexity, but also from potentially fleeting opportunities that affect multiple values. When framing problems under stress (and also under more favourable circumstances) decision makers do not always probe issues vigorously enough to identify and deal with value conflict. This may be the result of hasty problem analysis, limited consultation, or in some cases, denial or avoidance of value conflicts.

Education and training[22]

Pre-crisis and crisis sense-making are particularly demanding tasks for leaders and their organisations, which leads to the question of how to enhance individual and collective capacity in this area. Understanding the nature of sense-making and having the opportunity to practice before facing real life crises are very helpful. Leaders must try to ensure that they, their team members, key subordinates, and key partners are educated, trained, and exercised in preparation for crisis management and crisis sense- and decision-making. For best results, crisis management education must be both conceptual and practical. Individual and collective crisis management skills are best acquired and honed through hands-on practice. There are a wide variety of powerful instructional designs and techniques (both traditional and technology enhanced) suitable for crisis management training and exercises.[23] Instructional designs and techniques should be consciously and explicitly adapted to the target group and the goals and purposes of a given training or exercise. One size (and one instructional design) does not and cannot fit all. Chapter 4 provides more details on education and training through strategic crisis management exercises.

The two sides of information and communications technology (ICT) in strategic crisis sense-making[24]

ICT has great potential for leveraging crisis sense-making (and early warning) capabilities, but to realise that potential, ICT systems must be resilient and grounded in a holistic human-machine-social (organisational and normative) framework. ICT is often seen as a key element in improving sense-making before, during, and after crises. However, it is important to realise that although technology can greatly leverage capability, it can also be associated with various forms of vulnerability, the distraction of leaders away from their core role, and constitute a serious threat to privacy, civil liberties and trust.

When it comes to developing and deploying ICT for crisis management, there is currently a period of "rich experimentation" where governments (national, regional, local) are creatively drawing upon both off the shelf and custom designed systems and applications (Heaton, 2013). Over time the costs and benefits of these efforts will become clearer: some of these innovations will fall by the wayside; others will diffuse and become standard practice.

The design, development and deployment of ICT systems must take into account current and future needs and the cognitive limitations of real world crisis managers. Design criteria must not only excel in technical terms, but also be useful and usable under the difficult conditions associated with sense-making before and during crises. Technology, however powerful, can leverage, but not replace, the good judgment of crisis managers and their political leaders.

The examples discussed below suggest that ICT can contribute greatly to enhancing capabilities in several areas by improving internal and external communications capacity and providing platforms that enable information sharing and co-ordination among actors and stakeholders, including the general public, survivors, and relatives of survivors and victims. Some innovative and potentially useful ways of using ICT will be discussed as well as some of the downsides, risks and hazards associated with the incorporation of technologies into crisis management systems.

The upside of ICT

It is increasingly realised in both civilian and military domains that superior access to and use of information can have decisive advantages in a crisis (all hazards as well as crises stemming from political, social, and economic turbulence) and war. The so-called "revolution in military affairs" (O'Hanlon, 2000) emphasises the role of technology in cultivating information superiority over potential adversaries and facilitating timely, effective and co-ordinated operations. This can also be applied to other forms of crisis deriving from natural, human, and intertwined natural-human phenomena (Akghar and Yates, 2013). Timely and up-to-date information regarding the situation on the ground (e.g. floods, earthquakes, forest fires, terrorist attacks, social unrest), at sea (e.g. tsunamis, piracy, oil spills) or in the air/in space (e.g. volcanic ash clouds, radioactive or toxic chemical plumes, solar storms) can improve situational awareness and enable crisis leaders to make the most of opportunities to prevent/mitigate escalating crises and make better use of their response assets. ICT can be of great help in rapidly securing and providing access to critical information that might otherwise not be available to leaders at all levels, including strategic decision-makers.

The Swedish experience of the Boxing Day Tsunami in 2004-5 is an example of the use of technology. The Swedish Foreign Ministry leadership (and other strategic leaders in the Swedish government) initially lacked situational awareness regarding the scope of direct Swedish exposure to the event (of the 30 000 plus Swedish citizens in Thailand at the time, the bulk were in coastal resort areas). Establishing the status and consular assistance needs of these individuals initially posed a significant challenge (Daleus and Hansen, 2011). An improvised use of text-message broadcasting (which was not part of any programmed emergency communication system at the time) was used to send messages requesting status reports to all Swedish cell phone subscription holders detected on Thai networks. This successful improvisation resulted in the incorporation of emergency text messaging into the emergency communication system in Sweden, a practice that is increasingly common in many countries. The Swedish Foreign Ministry has now developed means of tracking the movements of Swedish travellers in collaboration with the Swedish travel/transport industry.[25]

In contrast, cellular networks and other telephone service were reportedly widely disrupted in affected areas of Japan following the earthquake and tsunami that devastated the Fukushima nuclear facility and large areas of Japan in 2011. However, the Internet proved more resilient and web-based services, such as those set up by Google, enabled the registration of status reports by individuals and queries by those concerned about their well-being. Crowdsourcing—using social media and the Internet to gather information, equipment or resources-- was also used to track levels of radiation in various locations, to understand survivor needs and to co-ordinate the allocation of mass care resources.[26]

Emerging practices

Big data

When applied to the domain of crisis/emergency management, big data refers to the large-scale accumulation of data from various feeds (including social media), sensors, geographic information systems (GIS) and other databases that are increasingly available to governments in crisis (and non-crisis) situations. The scale of these systems (and systems of systems) and the volume of data traffic creates challenges in terms of equipping governmental and other actors to be able to effectively scan, mine, refine, and apply data to improve situational awareness, inform decision-making, and enable co-ordinated action. Preparing organisations to be able to exploit big data is not merely a matter of providing adequate ICT infrastructure, it is also about adapting organisational cultures, processes, and human capital in ways that facilitate the harnessing of technology's potential.

For example, during Hurricane Sandy in the United States, various competing meteorological models were used to predict the trajectory and severity of the storm, with varying degrees of success. A wide variety of ICT platforms and tools were used to make strategic and operational decisions. These included GIS, aerial photography, hydrological monitoring, incident command support tools, and analysis of various social media feeds (Heaton, 2013).

Crowdsourcing crisis policy development

Social media platforms were initially conceived of as additional channels for pushing out information to the public, complementing established channels such as conventional media and other forms of messaging. A second wave now in progress focuses on "i-reporting", where the public and other groups are enabled to act as eyes and ears on the ground and provide alternative sources of situational awareness to complement official or "organised" situational reports by first responders, local government, established non-governmental organisations (NGOs), and corporations etc. (Hughes and Palen, 2009). ICT platforms, such as apps and web-based displays, enable integration, accessing, mapping, and selective display of such information, which may also be used to facilitate decentralised citizen self-help. Chapter 3 provides more in depth analysis on the use of social media in risk and crisis communication.

Traditionally, time pressures and high stakes of crisis management, combined with governmental tendencies towards applying a "need to know" principle, has resulted in researchers identifying empirical support for a "contraction of authority" phenomenon whereby fewer people within (and outside) government are likely to be consulted in crisis policy development compared to more typical non-crisis policy processes (Hermann, 1963). However, given the nature of the all hazards threat picture, as well as a partial shift to a "need to share" paradigm of information distribution, there is potential to engage a substantially larger group of analysts and experts in attempting to understand and manage the problems that emerge in a crisis. ICT enables the engagement of experts in real time and can select the size and composition of the circle that is made privy to situational information and normative parameters for problem solving. If it is deemed inappropriate to engage the general public, it is possible to include participants by invitation, pre-established credentials, or security classification level. The US Navy Office of Naval Research (in collaboration with the Naval Post-Graduate School) has developed a

platform and methodology for crowdsourcing policy development that is suitable for use in future crisis situation.[27]

Modelling, simulation, and visualisation

Another area of emerging technology and practice is the use of advanced modelling and visualisation to support decisions and the development of higher fidelity and more flexible training and exercise scenarios. For example, The INDIGO project, financed by the EU Research Programme FP7, aimed to develop an innovative virtual reality system for operational preparedness and management of complex crises.[28] The project explores the potential for creating a common set of map virtual symbols across Europe, moving towards enhanced interoperability of crisis geographic information systems (GIS). In the United States, the Department of Homeland Security has developed a Standard Unified Modelling, Mapping and Integration Toolkit (SUMMIT) that integrates suites of modelling tools and data sources for planning, exercise, or operational response.[29] Technology-supported exercising (and corresponding operational tools) aims to facilitate improved situational awareness and sense-making (in simulated and ultimately operational environments). These technologies, among many others currently being explored in the domain of training, exercise, and decision support, aim to leverage human sense-making capacities in ways conducive to improving crisis management education, preparedness, and strategic/operational response capability.

The downside of ICT

When developed, deployed and employed effectively, ICT can be a great benefit in crisis management. However, to realise its potential, the development and use of technology must be embedded in a context of resilience and a holistic human-machine-social (organisational and normative) framework. In the absence of these preconditions, the benefits of ICT may be elusive when most needed, or even worse, be outweighed by associated vulnerabilities and the potential for abuse. Four potential downsides have been identified: 1) pace, overload and distraction; 2) critical infrastructure failure and ICT fragility; 3) data concentration and vulnerability (e.g. Manning/Wikileaks); and 4) threats to privacy, civil liberties, and trusted partnerships.[30]

Pace, overload and distraction

The availability of ICT creates potential problems and temptations. The ability to access enormous amounts of information in real time can lead to distraction or paralysis if it is not accompanied by the means to identify the most essential and relevant bits of information amongst semi- or irrelevant information. The means of sorting, analysing and integrating, and effectively displaying information are critical (Vertzberger, 1990).

In cases of international conflict (and other types of strategic interaction crises), advances in ICT, especially communications technology, can speed up interaction and escalation processes in a way that may not be conducive to maintaining control in a volatile confrontation. Sometimes, time is needed to allow for a calm approach; these pauses may be crowded out by the overuse of instantaneous communications.[31]

Similarly, the capability to share operational information feeds with strategic leaders in real time has the potential to tempt them into micromanaging operations to the detriment not only of the operational decision-making, but also of strategic considerations. If the strategic decision makers are focusing on operational matters, who is focusing on strategy?

Critical infrastructure failure and ICT fragility

The trend towards increasing dependence on ICT for governmental (and first responder) processes and capabilities also has a downside. Government officials dependent upon ICT systems may experience substantial stress when these systems are not available. Furthermore, recent history suggests that these systems have a certain tendency to fail as a cause (or consequence) of critical events. Natural or man-made disasters (large-scale accidents or attacks) can destroy or degrade critical ICT infrastructure and deprive crisis managers of their customary or crisis specific ICT tools. Even in the absence of physical damage to key systems, usage surges may overload systems and render them unavailable to users at key points of a crisis situation.

Data concentration and vulnerability

The downside of the need to share paradigm, which tends to make large amounts of historical, contextual, and situational information readily available, is that this data may be accessed by actors whose purposes are at odds with the objectives of the organisations that collected the information and built the ICT systems. Recent cases of unauthorised information disclosure demonstrate the impacts of espionage and information theft for political or financial motives. In addition, some ICT (as well as physical) systems have shown to be vulnerable to cyber-attacks where the aim is to destroy capabilities or temporarily deny key services, not to steal data or information.

Threats to privacy, civil liberties and trusted partnerships

Debates surrounding unauthorised access to and distribution of secret/sensitive information illustrate another potential downside of ICT. The widespread diffusion of ICT in domestic and international society and the ever-increasing dynamic density of communications create a potential threat to citizen and consumer privacy.

The scale and scope of ICT capabilities can be shocking, perhaps more to the general public than to practitioners, professional observers of the ICT and the intelligence communities, and politicians. The collection of large amounts of information (meta-data as well as content) regarding communications to, from, or among US citizens has proven controversial. Similarly, revelations that allies and key economic partners have been targeted (as well as geopolitical and military rivals/adversaries) have been seen by many as breach of trust, causing substantial diplomatic turbulence and reputational cost for the United States and others revealed to be engaging in such practices.

Managing expertise, information and knowledge under complex crisis conditions[32]

Knowledge and information management for sense-making

Contemporary crisis management is an intensive knowledge and information enterprise. The ability to identify, access, and integrate critical information and expertise into sense- and decision-making processes in a timely fashion is a key determinant of success. Effective information sharing in a crisis is more likely to occur when the use of collaborative information is planned well in advance of the event. Such efforts help to identify and locate critical information needs and resources associated with various contingencies. Planning for information sharing can also help to remove legal and technical obstacles to sharing, and facilitate efforts to improve information system interoperability.[33]

As highlighted above, complex, cascading crises are becoming a regular feature of public life and are, as demonstrated by the examples of Fukushima and the Hurricane Sandy, typically surrounded by complex social and technical factors that are likely to be beyond the competence of generalist leaders, be they politicians or senior civil servants. Furthermore, crises are, by definition, associated with considerable uncertainty that may be reduced or better specified through expert assessment(s). As a result, crisis managers frequently call upon experts to provide relevant data and opinions on specific (and often arcane) subject matter. The ability to find and make good use of expertise and information for sense- and decision-making is a key crisis management capability (George, 1980).

A theoretical and methodological field of study has emerged out of the administrative sciences that explicitly addresses the issue of how to find missing knowledge, transfer it to where it is most needed, and institutionalise it for future use. This field is known as "knowledge management" (KM) and is rooted in previous theories of organisational knowledge and organisational learning.[34] Though the knowledge management field initially focused upon longer term issues of development; distribution; and institutionalisation, utilisation and adaptation of knowledge within organisations, it is increasingly recognised that parallel issues also emerge in the domain of crisis management. However, potential and actual crisis conditions tend to necessitate the enactment of knowledge management tasks under particularly challenging conditions that are characterised by high stakes, time pressure, and uncertainty. For example, the possibility of tapping into KM techniques for finding and accessing new or unfamiliar knowledge (e.g. calling in experts) is very tempting, but it is questionable whether such techniques can fit into the tight time frame associated with crises.

Three key challenges of knowledge/information management in a crisis should be considered: 1) identifying and accessing expertise and information; 2) communicating expertise across disciplines and (professional) sub-cultures; and 3) integrating expertise into strategic crisis decision-making. This section will explore briefly the intersection of crisis management (CM) and KM with a focus on enriching the study and practice of CM with "tools" from the KM "tool box."

Identifying and accessing expertise and information

Novel crises tend to produce acute needs for specialised knowledge. When this occurs, governments, and the agencies that serve them, often struggle to identify and access high quality experts and information. The more unusual the knowledge domain and the shorter the time frame, the more difficult this is likely to be. For example, when it first became apparent that the ash cloud from an Icelandic volcano could have serious consequences in parts of Europe that do not have their own volcanoes or large communities of experts studying them, this knowledge specialty was suddenly very much in demand.

Another example is the Waco siege of 1993, where a raid by the US Bureau of Alcohol Tobacco and Firearms turned into a prolonged siege at the compound of the Branch Davidians - a then relatively obscure religious sect lead by David Koresh - outside of Waco, Texas. The high profile case was discussed at the highest levels of the Federal Government and key decisions were made personally by the Attorney General. It became apparent that there was little knowledge of the Branch Davidians inside the Department of Justice and the Federal Bureau of Investigation (FBI) (and the rest of the government). It also became apparent that not only did the FBI lack the relevant

expertise, it also did not know how to identify and access reliable experts/expertise. Spontaneous offers of help from a substantial number of religion scholars of varying degrees of qualification were received, but the FBI did not know how to vet the offers and was hindered by its culture of being suspicious of outsiders offering unsolicited assistance (Koraeus, 2008).

Investigations following the siege identified how to rectify the problems identified. It was noted that the FBI needed someone positioned to mediate between the Bureau and the community of religion scholars to better prepare for similar future cases. A conflict resolution specialist position was therefore created, charged with exploring and networking with religion scholars. The role envisioned coincided in important respects with the notion of a knowledge broker from the KM literature. Though not uncontroversial, the utility of this role and its associated networks and seminars (which came to encompass expertise on various forms of violent Christian and Islamic extremism) were demonstrated in a number of subsequent cases confronted by the Department of Justice/FBI.[35]

In many contexts, such as in the UK Cabinet Office, the role of chief scientist involves not only directly advising strategic government leaders, but also the enactment of critical knowledge brokerage functions.[36] Knowledge networks developed for purposes other than crisis management (such as networks developed to conduct risk and vulnerability analyses) can also be tremendous assets in crises.

Communicating expertise across disciplines and professional sub-cultures

Communicating expertise across disciplines and professional sub-cultures is a significant challenge. Crisis conditions make risk communication particularly difficult, not only to the general public, but also to others in government who may lack the technical background to appreciate warnings/risk assessments if they are not "translated" effectively. Different professions speak very different languages and professional jargon may be a significant barrier to communication across professional boundaries.

Furthermore, different professions and subcultures may have very different frames of reference with regards to threats, risk, and hazards. The same information may provoke very different reactions. For example, the statement: "influenza claimed twenty thousand lives last year", may be shocking to the general public. However, to medical professionals who are familiar with the toll regularly taken by influenza among risk groups such as the elderly and other immune system compromised individuals, the figure may seem ordinary and no cause for alarm.

Experts must be trained or assisted in formulating messages that can be appropriately digested by decision-makers working under pressure. The ability of experts and crisis support staff in cabinet offices and other organisations to positively influence decision makers depends not only on the technical quality of analysis and data presented, but also on the way in which the information is packaged, presented, and timed.

Integrating expertise and information into strategic crisis decision-making.

Expert advice and information must be provided to strategic decision-makers in a form that they can use and that will neither distract them nor add unnecessarily to the stress levels associated with high pressure and difficult situations. Historical experience and best practice based on the literature strongly suggests that once expertise is found and

translated into a potentially understandable form, it must be brought into the decision-making process in a balanced, measured, appropriate and timely way.

Under crisis conditions, confident and strategically placed experts may exert tremendous influence over policy processes. It has even been noted that in a crisis there is a tendency for experts to assume de facto decision-making roles (Rosenthal and Hart, 1991). The risk is particularly great if only one expert/expert view is brought to the attention of policy-makers. Many crises defy conventional wisdom, which creates uncertainty, and emerge at the limits of scientific knowledge where there is considerable scientific contention. Under such circumstances, generalist leaders are often very reliant on the chosen expert and may struggle to regain their autonomy and distinguish between established or consensual views and idiosyncratic opinions.

There are a number of potential solutions to this problem. One is to have individual or collective gatekeepers who seek to ensure that the most appropriate and qualified experts/opinions are brought to the strategic decision-makers. When executed competently and in good faith, this can be helpful, even essential.[37] The risk, however, is that gatekeepers may exclude unwelcome experts/opinions/information in ways that skew the sense-making process and undermine the basis for effective executive/collective decision-making (George, 1980).

An alternative approach emphasises bringing competing views to the attention of top leadership. There are various institutional approaches to harnessing divergent views in the service of effective crisis sense- and decision-making. These include "devil's advocacy", expert advocacy and multiple advocacy. Devil's advocacy is the simplest approach and generally involves assigning an advisor the role of taking a contrarian view and aggressively probing dominant conceptions of the situation/courses of action. "Devil's advocates" may find themselves arguing positions that they do not genuinely prefer. This is a difficult role to sustain and other participants are liable to tire of a persistent devil's advocate and discount dissenting argumentation coming from such a source.

Expert advocacy is more complex and involves bringing in several credible experts with potentially diverging views to make their best case. This procedure tends to reveal areas of expert consensus and contestation and enable generalists to better navigate areas of technical complexity. Where such a procedure reveals a high level of scientific or other professional differences of opinion (and seemingly equally plausible expert arguments can justify different crisis/policy diagnoses or courses of action), generalists can more comfortably make judgment calls based on broader political/administrative reasoning (Janis, 1982). 2

Multiple advocacy (George and Stern, 2002) is the most elaborate way of harnessing divergent views. It is loosely based on a courtroom model and consists of several roles that can be used to promote constructive competitive interaction among expert/policy advocates, namely the executive, the process manager, and several advocates. The executive corresponds to the judge in a legal courtroom setting and will make the final judgment call and issue a verdict. The process manager serves as benevolent gatekeeper and is tasked with ensuring that sufficient diversity of views and key information are shared, a level playing field exists in terms of access and resources, and that communicative rules of fair play are in place and respected. The advocates correspond to the lawyers (e.g. the prosecutor and defence attorney) in a legal proceeding and are expected to make an effective case for their preferred views and probe the arguments of their competitors to provide (hopefully constructive) criticism (George and Stern, 2002). Policy arrangements inspired by (or more or less corresponding to) multiple advocacy

have been applied in various policy settings. A key factor impacting on success is thought to be the extent to which the process manager can maintain neutrality and avoid the temptation of drifting into advocacy, thereby setting the system out of balance and forfeiting the trust of the other players.

Recommendations for improved crisis sense-making

The crises of today and tomorrow will continue to challenge the capacity of states in detection and sense-making. Familiar and novel crises arise in dynamic environments and are characterised by social, political, administrative, economic and technological change. These changes complicate the pattern of threats and risks faced by OECD societies and their governments, but also provide new possibilities for gathering, processing and sharing information. Only by innovating and adopting/adapting best practices for early warning and crisis management can states effectively and proactively navigate the issues of crisis management. The experience of many recent crises identifies that effective sense-making efforts before (e.g. early warning processes) and during crises require collaboration across professions and disciplines. Significant subcultural, linguistic, knowledge and trust gaps need to be bridged for such collaboration to occur in a timely, efficient and legitimate fashion. To this end, the following actions should be considered:

- **Designing and calibrating all-hazards and threats early warning systems**. Systems must be designed and calibrated in ways that balance the twin risks of over-reaction and under-reaction. It is generally necessary to accept costs associated with false alarms if catastrophic under-reactions are to be avoided. Systems set with a low warning threshold may be prone to warning fatigue due to repetitive false/minor alarms. Leaders who wish to be informed at an early stage and be positioned for crisis prevention, mitigation, and proactive management, may encourage staff to raise preparedness levels.
- **Establishing information sharing processes, practices, and infrastructures across the whole-of-government and beyond** to inform crisis sense-making. These processes, practices and infrastructures must be designed and developed to promote appropriate flows, analysis, and the refinement of information conducive to effective sense-making before and during crises. They should complement and supplement the existing trend towards organisational consolidation.
- **Identifying and accessing relevant and trustworthy expertise in advance and during crises**. Familiar contingencies and post-crisis lessons learned provide opportunities to identify experts in advance and integrate them into "communities of practice". This can be very helpful in making sure that appropriate expertise is available for early warning and crisis sense-making efforts. Identifying potential knowledge brokers, persons or organisations that are strategically positioned and have a broad overview and diverse expert networks can be invaluable for identifying and filling knowledge needs when novel crises occur.
- **Integrating expertise and knowledge into sense- and decision-making**. This generally entails cross-professional communication whereby specialists must translate expert assessments into terms that a leader can understand and use. To avoid the emergence of expert monopolies and to take better account of the uncertainties associated with novel crises, decision-makers may be better served by using competitive arrangements with multiple experts.

- **Adapting sense-making processes and infrastructure to strategic leaders**. Strategic leaders vary greatly in terms of their personalities and their cognitive and management styles. Effective sense-making is facilitated when warners/briefers present information and structure deliberative and decision making processes in ways that fit leaders and that compensate for rather than exacerbate weaknesses and frailties. It is also important to focus information provision on strategic questions, rather than tempting senior leaders to stray into operational matters.
- **Adapting sense-making processes to crisis conditions**. Normal modes of deliberation and decision-making are easily overwhelmed by the stress of trying to make sense of a crisis. Information overload can be avoided to limit distress and distraction by establishing routines for coping with the volume of information generated in crisis situation. A variety of crisis staffing arrangements can help to facilitate the effective screening, distribution, and synthesis of intelligence, while providing sense makers with time for reflection and deliberation.
- **Establishing arrangements for shared sense-making across boundaries**. International co-operation is essential for improving preparedness before and achieving reliable, effective and legitimate responses during crises. Prompt, proactive information sharing about potential and escalating threats is critical. Co-ordinated development of crisis policy can improve policy output and outcomes across the OECD and other collaborating countries.
- **Training and exercising**. In the realm of sense-making, experience is a key asset and officials must have opportunities to practice sense-making and warning skills through drills and strategic crisis management exercises.

Notes

[1] "FEMA Administrator Craig Fugate Urges State Emergency Managers to Prepare for the Worst and Consider the Entire Community while Planning for Disaster," press release, Federal Emergency Management Agency, http://www.ready.gov/press-release/release-101020 (accessed October 25, 2012).

[2] The case also revealed vulnerabilities in planning assumptions regarding sea walls and evacuation zones in relation to the magnitude of the Great Tohuko Tsunami (Tossini, 2012: 259-261)

[3] For a critical discussion of the relative importance of these criteria, see Hermann and Dayton (2009)

[4] Grönvall (2001) and Olsson (2005).

[5] Compare Weick, 1995:61. See also Weick 1988 and 1993 and Nathan (2004).

[6] Thomas and Thomas, 1928; Weick, 1995:66; Stern, 1999.

[7] This section draws heavily on Parker and Stern (2005).

[8] This has been the case with major industrial/technological accidents as well, such as the crash of the space shuttle Challenger in 1986, in which the problem of the vulnerable O-rings was known and brought to the attention of management, but was not addressed prior to the tragic accident (Vaughn, 1997).

[9] Stern and Hansen (2001: 167).

[10] Snyder, Bruck, and Sapin (1963: 92-99).

[11] Hermann (1963) and 't Hart, Rosenthal, and Kouzmin (1993).

[12] Rosenthal et al (1989: 437)

[13] Vertzberger, 1990

[14] See also Rosenthal, 't Hart and Charles eds. (1989).

[15] Janis (1982); 't Hart (1994); 't Hart, Stern and Sundelius eds. (1997); Shafer and Chrichlow (2010)

[16] Weick (1995).

[17] Bruner (1957); Jervis (1976: 203-205); Kahneman (2011).

[18] Nisbett and Ross (1980: 15-16); Hamilton, Devine and Ostrom (1994: 3-4).

[19] Higgens and Bargh (1987); Khong (1992: 28); Larson (2001).

[20] Janis and Mann (1977: 15).

[21] Jervis (1976); Lebow (1981: 101-119); Vandenbroucke (1993: 164-166); David (1993: 23); Lebow and Stein (1993: 115-117); Parker and Stern (2005).

[22] This sub-section draws heavily on Stern (2013).

[23] See the section on information and communications technology below for examples of the application of emerging technology and pedagogics to crisis management exercising.

[24] This section builds upon and reports preliminary research associated with the EU FP7 ATHENA Project on Social Media and Personal Communications Technology. For more information, see http://cordis.europa.eu/projects/rcn/111205_en.html.

[25] See e.g. SOU (2005) Sverige *och Tsunamin—Gransking och Foerslag*. Stockholm: Fritzes.

[26] See Slater et al (2012)) for an analysis of the role of social media in the aftermath of the Great Tohuko/Fukushima disaster.

[27] The platform is called MMOWGLI (Massive Multi-Player Online Wargame Leveraging the Internet) and has been deployed to examine difficult policy problems such as combating piracy in Somalia. (www.onr.navy.mil/en/Science-Technology/Directorates/office-innovation/mmowgli-internet-war-game.aspx).

[28] www.crs4.it/vic/cgi-bin/project-page.cgi?acronym='INDIGO'.

[29] https://dhs-summit.us/.

[30] Daztbaz Dazpan et al. (2013).

[31] Craig and George (1995) *Force and Statecraft*.

[32] This section draws upon on Koraeus and Stern (2013).

[33] See Kamien (2012) especially Chapter Ten.

[34] In fact, these very same organisational learning theories form the foundation for the post-crisis learning perspectives, which are increasingly prominent in the field of crisis management (CM). See e.g. Stern (1997), Lagadec (1997) , Boin et al (2005), and Deverell and Hansen eds. (2009) special issue of the Journal of Contingencies and Crisis Management on *Learning from Crisis*.

[35] See also Weizman (2013) See also S.P. Weizman (2013) "Religious Studies and the FBI: Adventures in Academic Interventionism" Journal of the American Academy of Religion. Published online Aug 14, 2013.

[36] For more information on science advising in the UK Cabinet Office, see the presentation of the Scientific Advisory Group for Emergencies (SAGE) at www.gov.uk/government/publications/scientific-advisory-group-for-emergencies-sage.

[37] This function tends to be viewed positively in the knowledge management literature as a key facilitator of knowledge work, and with some cynicism in the foreign policy analysis/crisis management literatures (Koraeus and Stern, 2013).

References

Agrell, W. (2013), *The Black Swan and Its Adversaries: Early Warning Aspects of the Oslo and Utoeya Attacks of the 22nd of July, 2011* (author's translation of title), Swedish National Defense College (Center for Asymmetric Threat Studies), Stockholm.

Akghar, B. and S. Yates (eds.) (2013), *Strategic Intelligence Management*, Butterworth Heinemann, Elsevier, Oxford.

Betts, R. (1982) *Surprise Attack: Lessons for Defense Planning*, Brookings Institution Press, Washington, D.C.

Boin, A., P. 't Hart, E. Stern and B. Sundelius (2005), *The Politics of Crisis Management*, Cambridge University Press, New York.

Boin, A., M. Ekengren and M. Rhinard (2013), *The European Union as Crisis Manager*, Cambridge University Press, New York.

Boin, A. and C. Renaud (2013), "Orchestrating Joint-Sensemaking Across Government Levels", in *Journal of Leadership Studies*, Vol. 7/3, pp. 41-45.

Brändström, A., F. Bynander and P. 't Hart (2004), "Governing by looking back: Historical analogies in crisis management", in *Public Administration*, Vol. 82, pp. 191-210.

Brändström, A. S. Kuipers, and P. Daleus (2008) "The Politics of Tsunami Response" in Boin et al *Governing after* Crisis pp. 118-147*,* Cambridge University Press, New York.

Bruner, J.S. (1957), "On Perceptual Readiness", *Psychological Review*, Vol. 64, pp. 123-152.

Buzan, B., O. Waever and J. de Wilde (1998), *Security: A New Framework of Analysis*. Lynne Rienner, Boulder, Co.

Craig, G. and George, A.L. (1995), *Force and Statecraft*, 3rd edition, Oxford University Press, New York.

David, C.P. (1993), *Foreign Policy Failure in the White House*, The University Press of America, Washington, D.C.

Daleus, P. and D. Hansen (2011), "Inherant Ethical Challenges in Bureaucratic Crisis Management: The Swedish Experience with the 2004 Tsunami Disaster", in L. Svedin (ed.) *Ethics and Crisis Management*, pp. 21-36, IAP, Charlotte, N.C.

Daleus, P. (2005) *Flodvågskatastrofen: Massmediers and myndigheters framställningar av hanteringen (The Tsunami Catastrophe: Mass Media and Authorities' Portrayals of the Management, expert report to the Hirschfeld Commission, SOU 2005:104)*,

www.regeringen.se/contentassets/8627d9339e414175b0cef6b33eea2a64/sverige-och-tsunamin---granskning-och-forslag-expertrapporter, (Accessed October 22, 2015).

Daztbaz, M. et al. (2013), "Emerging Technologies and the Human Rights Challenge of Rapidly Expanding State Surveillance Capacities", in Akhgar and Yates (eds.) *Strategic Intelligence Management*, Butterworth-Heinemann, Elsevier, London.

Deverell, E. and Hansen, D. (2009), (eds.) "Learning from Crisis" (special issue), in *Journal of Contingencies and Crisis Management*, Vol. 17/3.

Eriksson, J. (2001) *Threat Politics: New Perspectives on Security, Risk and Crisis Management*, Ashgate, Aldershot.

Farazmand, A. (2007), "Learning from the Katrina Crisis: A Global and International Perspective with Implications for Future Crisis Management", in *Public Administration Review* (December), pp. 149-159.

Farnham, B. (1997), *Roosevelt and the Munich Crisis: A Study of Political Decision-Making*, Princeton University Press, Princeton.

Flin, R. (1996), *Sitting in the Hot Seat: Leaders and Teams for Critical Incident Management*, John Wiley and Sons, New York.

George, A.L. (1980), *Presidential Decisionmaking in Foreign Policy: The Effective Use of Information and Advice*, Westview Press, Boulder.

George, A.L. and E.K. Stern (2002), "Harnessing conflict in foreign policy making: From devil's to multiple advocacy," in *Presidential Studies Quarterly*, Vol. 32, pp. 484-508.

Golnaraghi, M. (ed.) (2012), *Institutional Partnerships in Multi-Hazard Early Warning Systems*, Springer, Berlin.

Gronvall, J. (2001), "The Mad Cow Crisis" in Rosenthal, Boin, and Comfort (eds.) *Managing Crises: Threats, Dilemmas, Opportunities*, Charles Thomas, Springfield.

Hansen, D. and Hagstrom, A. (2004), *I krisen proevas ordningsmakten (Crisis Tests Law Enforcement),* Jure, Stockholm.

Hamilton, D., P. Devine and T. Oström (1994), "Social Cognition and Classic Issues in Social Psychology", in Devine, Hamilton, och Ostrom (eds.) *Social Cognition: Impact on Social Psychology*, pp. 2-13, Academic Press, New York.

't Hart, P., U. Rosenthal and A. Kouzmin (1993), "Crisis decision making: The centralization thesis revisited" in *Administration and Society*, Vol. 25, pp. 12-45.

't Hart, P. (1994) *Groupthink in Government*, Johns Hopkins University Press, Baltimore.

't Hart, P., E. Stern and B. Sundelius (eds.) (1997), *Beyond Groupthink: Political Group Dynamics and Foreign Policymaking*, The University of Michigan Press, Ann Arbor.

Heaton, B. (2013), *How Emergency Managers Can Benefit from Big Data*, www.emergencymgmt.com/disaster/Emergency-Managers-Big-Data.html, accessed Oct. 21, 2013.

Hermann, C.F. (1963), "Some Consequences of Crisis Which Limit the Viability of Organizations" in *Administrative Science Quarterly*, Vol. 8, pp. 61-82.

Hermann, M.G. (1979), "Indicators of Stress in Policymakers During Foreign Policy Crises" in *Political Psychology*, Vol 1/1, pp. 27-46.

Hermann, M.G. and B. Dayton (2009) "Transboundary Crisis Through the Eyes of Policy Makers: Sense Making and Crisis Management" in *Journal of Contingencies and Crisis Management*, Vol. 17/4, pp. 233-241.

Higgens, E.T. J. and Bargh (1987), "Social Cognition and Social Perception" in *Annual Review of Psychology*, Vol. 38, pp. 369-425.

Hughes, A. and P. Palen (2009), "Twitter Adoption and Use During Mass Convergence and Emergency Events" in *International Journal of Emergency Management*, Vol. 9/3, pp. 24-260.

Janis, I.L. (1982), *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*, second edition, Houghton Mifflin, Boston.

Janis, I.L. and L. Mann (1977), *Decision Making: A Psychological Analysis of Conflict, Choice, and Commitment*, Free Press, New York.

Jervis, R. (1976), *Perceptions and Misperceptions in International Politics*, Princeton University Press, Princeton.

Kahneman, D. (2011), *Thinking, Fast and Slow*, Farrar, Straus, and Giroux, New York.

Kam, E. (1988) *Surprise Attack*, Harvard University Press Cambridge.

Kamien, D. (ed.) (2012), *The McGraw-Hill Homeland Security Handbook*, McGraw Hill, New York.

Keen, J. (2003), "Strain of Iraq War Showing on Bush…" *USA Today,* 2 April 2003. http://usatoday30.usatoday.com/news/washington/2003-04-01-bush-cover_x.htm (accessed Oct. 21, 2015).

Keeney, R. (1992), *Value Focused Thinking*, Harvard University Press, Cambridge.

Khong, Y.F. (1992), *Analogies at War*, Princeton University Press, Princeton.

Kingdon, J. (1995) Agendas, Alternatives, and Public Policy 2nd edition, Harper-Collins, New York.

Kingston, J. (ed.) (2012), *Natural Disaster and Nuclear Crisis in Japan*, Routledge, London.

Klein, G. (2001), *Sources of Power: How people make decisions*, 7th edition, The MIT Press, London.

Koraeus, M. (2008) Who Knows? *The Use of Knowledge Management in Crisis* CRISMART vol.36, Swedish National Defense College, Stockholm. Available online at: http://www.fhs.se/Documents/Externwebben/forskning/centrumbildningar/Crismart/Publikationer/Publikationsserier/Crismart36-WhoKnows.pdf.

Koraeus, M. and E. Stern (2013), "Exploring the Crisis Management/ Knowledge Management Nexus" in Akghar and Yates (eds.) *Strategic Intelligence Management*, pp. 134-149, Butterworth-Heinemann, Elsevier, Oxford.

Lagadec, P. (1997) "Learning Processes for Complex Organizations" *Journal of Contingencies and Crisis Management* 5:24-31.

Laporte, T. (1996) "High Reliability Organisations: Unlikely, Demanding, and At Risk" *Journal of Contingencies and Crisis Management* Vol 4:60-71.

Lebow R.N. (1981), *Between Peace and War: The Nature of International Crisis*, John Hopkins University Press, Baltimore.

Lebow, R. and J. Stein (1994), *We All Lost the Cold War*, Princeton University Press, Princeton.

Lebow, R. and J. Stein (1993), "Afghanistan, Carter, and Policy Change: The Limits of Cognitive Models" in Caldwell, D. and T. McKeown (eds.) *Force, Diplomacy, and Leadership*, pp. 95-127, Westview, Boulder.

Levite, A. (1987) *Intelligence and Strategic Surprises*, Columbia University Press, New York.

March, J.G. (2006), "Rationality, Foolishness, and Adaptive Intelligence" in *Strategic Management Journal*, Vol. 27, pp. 201-214.

Mittroff, I. and A. Silver (2009), *Dirty, Rotten, Strategies: How We Trick Ourselves and Others into Solving the Wrong Problems Precisely*, Stanford Business Books, Palo Alto.

Nacos, B.L. (1994), *Terrorism and the Media: From the Iran hostage crisis to the World Trade Center bombing*, Columbia University Press, New York.

Nathan, M (2004), "How Past Becomes Prologue: A Sense-making Interpretation of the Hindsight-Foresight Relationship Given the Circumstance of Crisis" in *Futures*, Vol. 36, pp. 181-199.

Neustadt, R. and E. May (1986), *Thinking in Time: The Uses of History for Decision Makers*, The Free Press, New York.

Nisbett, R. and L. Ross (1980), *Human Inference: Strategies and Shortcomings of Human Judgment*, Prentice Hall, Englewood Cliffs, NJ.

O'Hanlon, M. (2011) *Technological Change and Future of Warfare*, Brookings Institution Press, Washington D.C.

Olsson, E.K. (2005), "The Dioxin Scandal" in Larsson, Olsson and Ramberg, *Crisis Decisionmaking in the European Union*, Swedish National Defense College, Stockholm.

Olsson, E.K and Lan Xue (eds.) (2011) *SARS From East to West*, Lexington Books, Baltimore.

Parker, C. and E.K. Stern (2002), "Blindsided? September 11 and the origins of strategic surprise" in *Political Psychology*, Vol. 23, pp. 601-30.

Parker, C. and E. Stern (2005), "Bolt from the Blue or Avoidable Failure? Revisiting September 11 and the Origins of Strategic Surprise" in *Foreign Policy Analysis*, Vol. 1/3, pp. 301-331.

Parker, C. et al. (2009), "Preventable Catastrophe: Hurricane Katrina Revisited" in *Journal of Contingencies and Crisis Management*, Vol. 17/4, pp. 206-220.

Post, J. (1991), "The Impact of Crisis-Induced Stress on Policy Makers" in George (ed.) *Avoiding War*, Westview Press, Boulder.

Quigley (2005) "Bug Reactions: Considering US Government and UK Government Operations in Light of Media Coverage and Public Opinion Polls" *Health Risk and Society* Vol. 3(3): 267-291.

Rosenthal, U., M. Charles and P. 't Hart eds. (1989) *Coping With Crises: The Management of Disasters, Riots, and Terrorism*, pp.436-472, Charles C. Thomas, Springfield, Illinois.

Rosenthal, U. et al. (1989), "From Case Studies to Theory and Recommendations: A Concluding Analysis" in Rosenthal, Charles and 't Hart *Coping With Crises: The Management of Disasters, Riots, and Terrorism*, pp.436-472, Charles C. Thomas, Springfield, Illinois.

Rosenthal, U. and P. 't Hart (1991) "Experts and Decisionmakers in Crisis Situations" *Knowledge* 12: 350-373.

Rosenthal, U., P. 't Hart, and A. Kouzmin (1991), "The Bureau-politics of Crisis Management" *Public Administration* 69(2):211-233.

Russo, J.E. and Schoemaker, J.H. (1989), *Decision Traps: Ten Barriers to Brilliant Decision-Making and How to Overcome Them*, Doubleday Business.

Sagan, S. (1993), *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*, Princeton University Press, Princeton.

Slater, P. et al (2012) "Social Media in Disaster Japan" in J. Kingston *Natural Disaster and Nuclear Crisis in Japan* pp.94-108, Routledge, New York.

Shafer, M. and S. Critchlow (2010) *Groupthink vs High Quality Decision Making in International Relations.* Columbia University Press, New York.

Snyder, R.C., H. Bruck and B. Sapin, B. (eds.) (1963), *Foreign Policy Decision Making*, The Free Press, New York.

SOU (2005) *Sverige och Tsunamin—Gransking och Foerslag*, *(Sweden and the Tsunami: Assessement and Recommendations)*, Fritzes, Stockholm.

Stern, E. (2013), "Preparing: The Sixth Task of Crisis Leadership" in *Journal of Leadership Studies*, Vol. 7/3, pp. 51-56.

Stern, E. (2011), "What the US Can Learn from the Two-Pronged Attacks in Oslo" in *Emergency Management* (online version), www.emergencymgmt.com/safety/US-Learn-Two-Pronged-Attack-in-Norway.html, accessed Nov. 21, 2013.

Stern, E. (2009), "Crisis Navigation: Lessons of History for the Crisis Manager-in-Chief" Governance, Vol. 22/2, pp. 189-202.

Stern, E.K. (1999), *Crisis Decisionmaking: A Cognitive-Institutional Approach*, Department of Political Science, University of Stockholm, Stockholm.

Stern, E.K. (1997) "Crisis and Learning: A Conceptual Balance Sheet" *Journal of Contingencies and Crisis Management*, Vol. 5(2): 69-86.

Stevens, D. (2013), "Redefining the Emergency Manager: A Proposal for Change", in *Emergency Management* (online version), www.emergencymgmt.com/training/Redefining-the-Emergency-Manager.html, accessed 21 November 2013.

Thomas, W. and D. Thomas (1928), *The Child in America: Behavior problems and program*, A.A. Knopf, New York.

Tierney, K., C. Bevc, and E. Kugliowski (2006), "Metaphors Matter: Disaster Myths, Media Frames, and Their Consequences in Hurricane Katrina" in *The Annals of the American Academy of Political and Social Science*, Vol. 604, pp. 57-81.

Tossani, R. (2012), "Thousand Year Event: Towards Reconstructing Communities" in Kingston, R. (ed.) in *Natural Disaster and Nuclear Crisis in Japan*, pp. 255-276, Routledge, London.

US Senate (2006), *Hurricane Katrina: A Nation Still Unprepared*, Homeland Defense and Governmental Affairs Committee, Washington. D.C.

Vaughn, D. (1997), *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*, University of Chicago Press, Chicago.

Vandenbrouke, L. (1993), *Perilous Options*, Oxford University Press, Oxford.

Vertzberger, Y. (1990), *The World in Their Minds: Information Processing, Cognition,and Perception in Foreign Policy Decisionmaking*, Stanford University Press, Stanford, CA.

von Clausewitz, C. (1976), *On War*, Princeton University Press, Princeton.

Weick, K.E. (1995), *Sense making in Organizations*, Sage Publications, Thousand Oaks, CA.

Weick, K.E. (1993), "The Collapse of Sense-making in Organizations: The Mann Gulch Disaster" in *Administrative Sciences Quarterly*, Vol. 38, pp. 628-652.

Weick, K.E. (1988), "Enacted Sense-making in Crisis Situations" in *Journal of Management Studies*, Vol. 25/4, pp. 305-317.

Weick, K.E. and K.M. Suttcliffe (2002) Managing the Unexpected: Assuring High Performance in and Age of Complexity, Jossey-Bass, San Francisco.

Weizman, SP. (2013) "Religious Studies and the FBI: Adventures in Academic Interventionism" *Journal of the American Academy of Religion*. Published online 14 August 2013.

Welch, D. (1992), "The Organizational Process and Bureaucratic Politics Paradigms: Retrospect and Prospect" in *International Security*, Vol. 17/2, pp. 112-146.

Wohlstetter, R. (1962), *Pearl Harbor: Warning and Decision*, Stanford University Press, Palo Alto.

Chapter 3

The use of social media in crisis communication

This chapter highlights how social media can support the changing landscape of crisis communication. It identifies the challenges that arise from the use of social media and ways of dealing with these challenges. A framework for monitoring the development of social media practices amongst countries for crisis communication is proposed. This includes a three-step process that spans passive to dynamic use of social media. This chapter provides governments with a self-assessment tool that will enable them to monitor and track progress in the effective use of social media by emergency services or crisis managers.

This chapter draws on Wendling, C., J. Radisch and S. Jacobzone (2013), working paper "The Use of Social Media in Risk and Crisis Communication", *OECD Working Papers on Public Governance*, No. 24, OECD Publishing, Paris, http://dx.doi.org/10.1787/5k3v01fskp9s-en.

For a comparative snapshot of social media use in and by OECD governments to deliver more open policy processes in other areas of public policies, the following paper provides an in-depth analysis: Mickoleit, A. (2014), "Social Media Use by Governments: A Policy Primer to Discuss Trends, Identify Policy Opportunities and Guide Decision Makers", *OECD Working Papers on Public Governance*, No. 26, OECD Publishing, Paris http://dx.doi.org/10.1787/5jxrcmghmk0s-en.

An updated analysis of the use of social media by government is also available here: http://oecdinsights.org/2015/08/21/reaching-maturity-in-government-use-of-social-media/.

Key Messages

1. Social media are revolutionising communication. They have great potential to support two-way crisis communication at a low cost and with high efficacy, and can maintain trust in government by developing a direct relationship with citizens at a time when expectations are high.
2. There are three main ways to use social media in crisis management: 1) bottom-up as a situation awareness tool; 2) top-down as a state communication tool; and 3) multi-ways as a platform for dynamic interaction.
3. The challenges of using social media in crisis communication include: the multiplicity of players, the amount of information generated, the question of open data, privacy and confidentiality, the question of liability, the expectation of the population, and the issue of security.
4. Governments should develop social media strategies to support their crisis communication strategies before, during, and after a crisis. Guidelines can encourage the use of social media by emergency managers and should address the implications of an increased use of social media (resources, reliability, information overload etc.).
5. Governments should foster citizen-led social media use and enable communities and individuals to self-initiate and volunteer in emergency efforts through the development of technological platform and tools
6. Governments should maintain traditional media in their crisis communication strategies to ensure the inclusion of all segments of the population.

Crisis communication strategies and policies underpin an organisation's overall risk management strategy. It is essential to identify effective risk communication strategies for informing both the public and professionals. As communication technology diversifies and proliferates, social media (Facebook, Twitter, etc.) are increasingly used to convey information during crises to send warnings, conduct situational awareness, and even to catalyse action and sustain dialogue and feedback loops among public authorities, volunteer groups, the business sector and citizens. Despite their usefulness, governments often view social media with some caution due to potential costs of trying to keep pace with growing citizen expectations. The reliability of social media content is sometimes questioned, although filtering tools have been developed that may be used to reduce time spent reading irrelevant messages and untrustworthy sources. Risk management policies should take into account these recent technological changes if policy makers are to keep pace with sociological changes among their end users.

This chapter offers a typology of social media uses to reflect a range of practices in countries and the strategic approaches that governments and other organisations could adopt to go beyond an ad hoc use of these tools and achieve better outcomes, especially for emergency services. The intention of this chapter therefore is to address the conditions under which risk and crisis communication strategies can be adapted to be successful in this new environment.

Risk and crisis communication strategies are evolving with the emergence of social media

Risk and crisis communication strategies began to develop in the 1960s-1970s with the contribution of research from cognitive and social psychology experts. This research concluded that people use cognitive shortcuts to process information and that perceptions could diverge greatly due to expectations, leading to overreactions, mistrust, etc. Risk and crisis communication was developed as a strategy to make people's behaviour more "rational" so that they could make informed decision.

In the 1990s, this unidirectional model of risk and crisis communication was criticised as leading to one-way communication from the expert to the lay public, which did not give enough place for dialogue and feedback. The idea emerged to create platforms for discussion where people could discuss and exchange opinions and information about risks. The focus was on consensus building and conflict resolution. It became key to gather multiple viewpoints. Collective models of decision-making were put in place, together with new participatory approaches for communication. Risk and crisis communication research became multidisciplinary: in addition to psychology, communication science, sociology, and political science also came to play. Organisations dealing with risks and crises were set up and employed social scientists in their communication departments to develop new ways to interact with the public.

The emergence of social media

Since the late 1990s, new social media have not only changed the perception of risks and crises, but also citizens' expectations towards emergency response officials, the private sector, volunteer organisations, etc. Platforms such as Twitter, Facebook and Ushahidi (an open crowdsourcing crisis information platform) have been widely used to communicate about risks and crisis situations (e.g. 2010 Haiti earthquake, 2011 Fukushima nuclear accident). This change is linked to the rapid development of the Web 2.0 and its applications. The United Nations (UN) says that Internet traffic is expected to

grow 25-30% between 2011 and 2015 in North America, Western Europe and Japan, and to reach or surpass 50% in Latin America, the Middle East and Africa (United Nations Global Pulse, 2012). However, the use of social media, such as Facebook and Twitter, is growing even more rapidly. In Senegal, for example, Facebook receives about 100 000 new users per month.

Technological innovation spurs social and institutional change (IRGC, 2012). Best practices are slowly emerging and driving broader changes, such as refining linguistic and other behavioural norms in the use of social media for risk and crisis communication. In many countries, public expectations and roles are changing in terms of the desire for increased transparency of information in the spirit of open government, and participation in information gathering, sharing and verification. Trust in established experts, public officials and numerous bloggers has changed: the public is no longer content to receive official recommendations and advice in a passive way. People are gradually shifting from a situation where the information was pushed on them and made available by authorities, to a situation where the information can also be pulled. For example, followers can register to Really Simple Syndication (RSS) feeds that gather the fragmented information they want and filter the data they access according to their own interests. Social media have also created new arenas of information exchange where dynamic and interactive flows of data are in the hands of millions of individuals who seek a more evidence-based participatory form of risk and crisis communication. New services exist to deal with online communication among official emergency responders. Advanced tools can help map crisis communications on the web in real time.

Social media can be used to enhance risk and crisis communication in several ways: 1) they are collaborative and participatory, online discussions can improve situation awareness; 2) they are decentralised, the information can circulate very quickly among actors, thanks to RSS feeds or tweets that are immediately available online to multiple organisations; 3) social media are popular and accessible, emergency services can extend their reach when sending information or warning; and 4) social media can provide data that are geographically or temporally traceable, digitally generated content allows for the monitoring of the geographical and time development of a crisis.

Different types of social media used in risk and crisis management

Five types of social media can be identified (see Table 3.1.). **Social networking** media, such as Facebook and Myspace, bring groups of people together because they share common interests. **Content sharing media**, such as YouTube and Flickr, allow anyone to upload content such as videos or pictures to be shared with everyone or with a restrictive community of users. **Collaborating knowledge sharing media**, such as Wikis and podcasts, enable participants to ask questions and wait for answers from different users. **Blogging social media** are used to share facts and values, emotions and expectations. Finally, **volunteer technology communities** (VTC), such as Ushahidi and Sahana, are social media platforms or modules created especially for risk and crisis communication.

Different types of social media can be complementary in risk and crisis management. Social networking media can help enhance co-ordination among volunteers and emergency services. Content sharing media can help conduct situational awareness by identifying images or videos of how a crisis is evolving in real time. Collaborative knowledge sharing media can help develop dialogues between different stakeholders in a risk or crisis management situation. Blogging or micro blogging tools, such as Twitter,

can be used to share facts in real time, but also to convey recommendations and warnings very rapidly. Social media platforms or modules like Ushahidi create a synthesis of various social media content to help emergency managers and volunteers become more efficient in their activities.

Table 3.1. The different types of social media used in risk and crisis management

Type of social media	Examples	Use for risk and crisis communication
Social networking	Facebook Myspace Friendster	Enhance co-ordination among volunteers and emergency services. Allow to share information inside a community. Provide swift update on emergency situation.
Content sharing	YouTube Flickr Vimeo	Enhance situational awareness in real time through exchange of pictures and videos. Allow emergency services to easily launch viral campaigns about risks. Help identify missing individuals, victims.
Collaborating knowledge sharing social media	Wikis Forums Message boards Podcasts	Enhance dialogue between victims and emergency services.
Blogging and microblogging	Blogger Wordpress Tumblr Twitter	Convey recommendations and warnings. Share facts. Twitter enables immediate information sharing with a wide reach and feedback possibilities.
Specialised crisis management platform managed by volunteer technology communities (VTCs)	-MAPPING COLLABORATION OpenStreetMap Crisis mappers Google map maker -ONLINE AND ONSITE CONTRIBUTION Ushahidi Crisis commons Sahana foundation Geeks without bounds -PUBLIC-PRIVATE-PEOPLE PARTNERSHIP Random Hacks of Kindness (with Google, Microsoft, Yahoo, NASA, World Bank)	Mapping of emergencies. Community Emergency response team facilitator.

Note: For a description of each social media, please refer to Annex 1.

Using communities like Ushahidi, volunteers have already responded to major disasters, such as earthquakes in Haiti and Chile and flooding in Pakistan. Volunteers created detailed maps, processed imagery, and geo-located posts made –with their geographical information attached - by the affected population to a broad number of social media channels. Some tools developed by these volunteers have already been deployed under the United Nations Disaster Assessment and Coordination (UNDAC); others provided support to the European Union (EU), the United States and across the globe, making their supercomputers and large storage arrays available for managing translation workflows, and serving large data sets.

Finally, Geotagging and Volunteered Graphic Information (VGI) can also play a role in crisis management. Geotagging is the process of adding location information to social media posts, videos, or photos. When the public uploads any of these media to the Internet they may have the ability to add a geotag to their post. Emergency managers, especially at the state or regional level, can obtain a picture of the destruction occurring in an area through these posts. Through the use of internal geographic information systems (GIS) or free online sources (such as Google Earth) these posts can be plotted on a map and will give a high angle view of what is occurring in the community. Many social networks, like Facebook, Twitter, and Flickr, are making their services compatible with geotagging, which can most easily be accomplished when updating social media through a smartphone.

Is there a need for increased use of social media in risk and crisis communication?

The uptake and deployment of social media in emergency services entails development, training and operations costs. The technical and social knowledge to work with social media may represent a steep learning curve for risk and crisis managers who are used to working with traditional media. Senior level management is often not among the primary community of social media users and may be less exposed to the social changes brought about by Facebook and Twitter than younger generations. However, they are exposed to politicians who often pick up on such changes quickly as a way of remaining connected to voters.

There is a tendency among experts and public officials to fear that too much reliance on social media could give rise to new public expectations that would be hard to meet by the authorities in charge. As a result, many organisations still consider that traditional media should be the primary channel to inform the public in risk and crisis communication and still operate by relying on daily news conferences and public briefings. They do not see the need for a constant update in real time and many do not monitor social media networks to conduct their situation awareness or to communicate with the public. Often they do not have the communication infrastructure to make appropriate use of social media in risk and crisis management.

Nevertheless, social media have the potential to bring beneficial changes in risk and crisis communication. Recent studies show that behavioural changes are more easily achieved through personalised communication (Thaler and Sunstein, 2008). Social media can be powerful tools for encouraging resilient behaviour in a community. Messages sent out can be adapted to different categories of the targeted population.

A recent study of the American Red Cross shows that expectations are changing (American Red Cross, 2011). Nearly half of respondents would sign up for Short Message Service (SMS), RSS or other electronic types of alerts that provide safety information; this percentage is growing year after year. One in seven general public respondents experienced an emergency or witnessed a newsworthy event and posted information or photos about that event to a social media site. Facebook is the most popular way to do so, followed by Twitter and Flickr. If unable to reach emergency services with traditional means, one in five of the general public would turn to online channels to request help. Nearly a fourth of the general public and a third of the online population would definitely use social media to let loved ones know they are safe. The public is demanding constant updates: it will accept that a situation evolves but will not tolerate being kept in the dark.

Recent studies show that seniors are also now using social media (Pew Research Center, 2015). This evolution means that the scope of population that can be targeted through social media becomes bigger by the day. New organisational structures exist that go beyond the traditional government centric approach towards a "whole of community" approach to risk and crisis management. According to a recent study conducted for the World Bank, the rise of the volunteer technology communities like Ushahidi has brought a new set of organisational designs to problems that have often become snagged in bureaucracy (See Box 3.1.). VTCs rely on flattened, decentralised structures with decision-making and conflict resolution mechanisms that were adapted from online communities like Wikipedia and open source software projects. As a result, they have moved far faster than larger players in nearly all circumstances - and perhaps faster than established protocols would allow.

New forms of risk and crisis communication are emerging as a result. Social media can be used in major catastrophic events and in steady state situations to enhance both risk and crisis communication. A study by the University of Copenhagen that analysed the motivation to use social media showed that the use of these technologies by emergency services is tied to individuals pushing their organisations to change (Latonero, M. and I. Shklovski, 2011). Part of the impetus to interact more with citizens directly derives from the dissatisfaction of organisations with traditional media. The officers interviewed felt they would be better served if they could interact directly online with the citizens rather than through the media. The study showed that the emergency services users of the social media during a crisis do not only listen to tweets, but also encourage reporting and reward them. To validate the information they read on social media, they try to interact with the persons to verify and ensure they can trust the facts. Their experience of the use of social media helps them know better which tweet to trust, and thus reinforces their motivation to continue using social media, even if they do not necessary receive further organisational support.

What worked well

Several examples illustrate what works well when using social media in crisis communication. The following boxes provide examples of such practices from OECD countries.

Box 3.1. The EU MASSCRISCOM research project in crisis communication

In most EU countries, risk and crisis communication mostly focuses on radio and television. Sirens are used to a considerable degree in some areas to warn the public directly. A major problem is to reach the public in innovative ways, while making it possible for people to provide information when catastrophic events occur. The Masscriscom project explains the added value of using new media such as RSS feed, YouTube, Twitter or Facebook. It gives the example of so called Crisis Communication Centre (CCC), which can rely on a multiplicity of risk, and crisis communication channels coupled with geographical information systems to be as precise as possible in the warning messages and situational awareness. The CCC is thought as a two-way communication cell where information can both be sent to the public and received from it. The CCC is also connected to the EU 112 emergency call number cell. To ensure interoperability and facilitate the distribution on all kinds of communication channels, the CCC relies on a standard format or template, the common alerting protocol. The CCC consists of three main components namely the operators, the monitoring and alarm function and the editorial office. The operators respond to the demand of the public on the different types of communication channels and transmit the information to the authorities.

Box 3.1. The EU MASSCRISCOM research project in crisis communication (continued)

The monitoring and alarm function detects and follows events. It has the capability to detect anomalies that may indicate that something has happened or is happening. The editorial office assists the authorities in elaborating and updating the basis for the FAQ for an event, preparing the information to the different groups and in different languages. It conducts quality assurance of the messages. The office is responsible for the communication on the web and for the traditional media contact. To sum up, the CCC serves as contact point for the public in order to reduce the burden on the 112 emergency call number. It provides the opportunity for supplying the public quickly with information. It also provides a channel for compiled and co-ordinated information from the authorities to the public.

Source: Webpage of the EU MASSCRISCOM project: www.masscriscom.eu/default.aspx

Box 3.2. Community Emergency Response Team (CERT) and the Sahana module

A series of storms flooded Chicago's south west side. The temperature was supposed to get very cold and a lot of households were without power. Chicago's police and fire departments on site were overwhelmed by the number of people needing assistance. The Chicago Office of Emergency Management and Communications (OEMC) was asked to find more volunteers, and the office looks to the Community Emergency Response Team (CERT), which uses the so called Sahana module. This social media platform dedicated to emergency situation offers the possibility to create an event to mobilise volunteers, both medically trained and not. The system sends out the deployment requests and processes the replies. Each volunteer willing to be deployed is automatically sent details on where to go and to whom to report. The general deployment volunteers report to the OEMC Incident Commander while the medical deployment is sent to the on-scene Medical Director.

Source: http://sahanafoundation.org/

Box 3.3. Ushahidi interactive mapping

The Ushahidi platform helped to crowd source information during Haiti's earthquake in January 2010. It aggregated data coming from different social media into an interactive mapping. When telephone lines are not working, people turned to the social media. The fact that they can see their input on the interactive mapping motivates them to continue to contribute. The Haiti Ushahidi map, backed up by a volunteer network that included Haitian-Americans translating text messages from Creole, was used by search and rescue teams to find survivors. It enhanced both the situational awareness and the crisis response provided on site. Since then, Ushahidi interactive mapping has been used to map the impact on communities of the BP oil spill and the consequences of Japan's earthquake and Tsunami in 2011.

Source: http://www.ushahidi.com/

Box 3.4. The Australian Alert SA web portal: social media messages in an emergency in one place

The Alert SA website brings together social media messages from South Australia's emergency services via Twitter, Facebook and RSS in one place, so that all the users of the portal can have a comprehensive pictures of what is shared on social media. http://www.alert.sa.gov.au/ brings together the Facebook page of the police and of the firemen services, the Twitter page of the state emergency services, the RSS feed of the Bureau of meteorology, and so on. It also provides all the emergency contacts (phone numbers, bureau, etc.).

Source: Webpage Alert SA in use in Australia: www.alert.sa.gov.au/

Box 3.5. The X 24 international crisis exercises

The exercises X 24 (http://24.inrelief.org/) are virtual, open-invitation, humanitarian assistance and disaster relief (HADR) exercises with real-world functional components that are hosted every year by San Diego State University's "Immersive Visualization Center" (VizCenter). On 24-25 September 2010, the VizCenter hosted the first virtual HADR event called "Exercise X24". X24 involved over 12500 people from 79 nations and 90 US government, non-government organizations, and public/private partners in a collaborative environment using crowd sourcing, social media, and cloud computing applications. A second exercise, X24 Europe, was held from March 28-31, 2011. X24 Europe transcended formed a collaborative bridge between individuals, communities, and nations with over 49000 participants from 92 nations that included two ambassadors, a US major general, as well as representatives from US European Command (EUCOM), US Northern Command, US Transportation Command, Office of Navy Research, STAR-TIDES at the Center for Technology and National Security Policy from National Defense University, and many others. The focus area for the scenario was the Balkans region with a seismic event that generated a tsunami in the Adriatic Sea followed by aftershock damage inland. 78% of participants were from Croatia, Macedonia, and Bosnia and Herzegovina.

The emergency managers and military officers say the idea was to tap the potential of social media to create video and text channels of communication that offer more immediacy and flexibility than the standard command-and-control operation anchored in a government war room. This new model for emergency response relies on volunteer technical communities of software developers, social media monitors and field volunteers during the crisis management. According to an article published in *USA today* following this exercise, working online from locations around the globe they meet via video, audio and text on Skype, in what they call "virtual emergency operations centres" and carry out countless tasks critical to the rescue and response effort.

Source: Webpage on the X24 exercise: http://vizcenter.net/x24/more.html

What has not worked well

The utilisation of social media can generate issues in time of crisis that can diminish the efficiency of emergency preparedness and response operations. This is exemplified in the cases explored below.

Criticism on the blogosphere

The risk of not including those who feel concerned by a disaster is that they may turn to the blogosphere if they feel they have not been heard. This happened in November 2007 in the United States when the heavy fuel oil of the Cosco Busan container ship spilled into San Francisco bay. The California governor declared a state of emergency and state personnel, funding and equipment were made available to assess and clean the environmental damage. However, no clear guidelines existed on how to include the help volunteers wanted to provide on the spot, so volunteers turned to the blogosphere. The coast guards and other emergency services were so much involved in the crisis response that they did not monitor or counterbalance the communication of potential volunteers who, as they could not be involved, criticised their actions. This is a challenge for organisations as it is very hard to deal with image and reputation issues on the Internet while dealing with a crisis.

Information that comes from sources other than emergency services

A study by the University of Georgia showed that on 22 may 2011, during the Joplin tornado, a Facebook employee started to create a dedicated Facebook page from her iPhone called *Joplin tornado info* (Wiliam, William, Burton, 2012). It was launched less than two hours after the event and quickly received 44 000 followers. This meant that those searching for information on the situation were relying on her and other volunteers instead of on the direct official services of FEMA, who felt they could have done a better job. This example raises the question of the sources that should prevail for social media crisis communication: is it better to develop government led social media risk and crisis communication or to enhance citizen-led social media use during crises to develop resilient communities?

The overload of information

The large volume of tweets and Facebook pages as a result of Hurricane Irene in 2011 meant that it was very difficult to pull meaning out of the flow of information. As a result, FEMA identified a need for new tools to conduct situational awareness through social media.

Good practice examples of using social media in risk and crisis communication

This section illustrates the increasing potential for the use of new social media for risk and crisis communication through 12 examples of practice. When an organisation starts to use social media it is important to decide what goals are identified as a priority. Is the objective to be more visible? To enhance recovery management? To improve situational awareness? Depending on the goals, the audience, content and tools to be used will differ, as explored below.

Raising public awareness about risks and crises

The "Hurricane tip of the week" and e-cards from the US Center for Disease Control and Prevention

Since the 9/11 terrorist attacks in the United States, the Center for Disease Control and Prevention (CDC) has developed innovative strategies to raise awareness through social media of potential risks and crises. For example, the "Hurricane tip of the week" is

a CDC initiative that relies on social media to post a tip per week. The weekly tip, which has more than 1 600 Twitter followers and 34 000 email subscribers, is also available as a widget (a small programme that users can download onto their computers or embed in their social media profiles or blogs). Widgets have also been used for product recall, for example there were more than 15.5 million page views of the salmonella peanut product recall widget, which included a searchable database of recalled products. CDC has also used e-cards to encourage disaster preparedness. During national hurricane week, a dozen e-cards, including a mobile friendly version, were launched. More than 100 000 people opened these e-cards. CDC also makes public service announcements available as podcasts on the web.

The "get prepared" portal of Public Safety Canada

Public Safety Canada's "get prepared" portal is available online and has a mobile friendly site. The general public can stay connected and receive regular updates via Twitter, RSS feeds, email, among others. There is an emergency preparedness week every May that aims for people to understand the risks in their region. It is run in partnership with the Red Cross, the Salvation Army, the Canadian association of fire chiefs, among others. The idea is to work closely with provinces and territories, as well as with non-governmental organisations (NGOs). The tweets sent during emergency preparedness week are approved by Public Safety Canada and then retweeted by the partners.

Recommendations

It is important to use social media as an awareness raising strategy prior to crises so that people can become accustomed to referring to official sources on social media portals. Using social media to raise public risk and crisis awareness allows emergency services to increase their access to audiences of different types, such as younger audiences who rely less on traditional media. The use of social media to raise risk and crisis awareness also helps to reduce the dependence on traditional media channels and to develop new types of campaign that use more personalised tones and creative digital tools to enhance behavioural change. Using social media can also lead to viral dissemination through communities.

Surveillance, monitoring, situation awareness and early warning systems

Social media can help to understand more accurately what is happening during a crisis. Because of the broad flow of information, two options for monitoring information are currently used by organisations: technical and volunteer.

The technical option

The technical option relies on the technology of crowdsourcing. Computer programmes can be used to synthesise what type of content is shared and to provide meaning. Pilot projects exist in various universities to develop such tools. The Empowering the Public with Information in Crisis (EPIC) project tries to understand how to create situational awareness from Twitter during crises. Within EPIC the "Tweak the tweet" tool is looking at recent events and how to extract more useful information from Twitter in times of crises, especially if tweets can be geo-located. Similarly the Twitcident project from the Delft University of technology in the Netherlands filters

Twitter to obtain real time intelligence. The researchers introduced a web-based system for filtering, searching and analysing information about incidents or crises.

For US FEMA, geospatial data and mapping applications are central. One new FEMA application maps emergency declarations, earthquakes, models of building failures, status and location of relief facilities, and the progression of search operations. This application integrates with Microsoft's Bing search to provide a birds-eye view of maps. Disaster relief workers can send SMS updates that are integrated with the maps from the field. Similarly in Japan, in the aftermath of the March 2011 earthquake and tsunami, Georepublic Japan and OpenStreetMap Foundation Japan launched a crisis map that provided and visualised real-time information on news and official reports, as well as information provided by the crisis-affected community (via SMS/text and internet platforms) on evacuation centres, damages, and requests for help.

Google Flu Trends uses aggregated Google search data to estimate current flu activity around the world in near real-time. Emergency services can use automated data extraction and analysis methods. Different approaches already exist to extract and analyse data from Twitter. Many crisis mapping application techniques can visualise crisis developments in real time. Emergency services can also rely on content analysis tools, such as these provided by Google. In addition, emergency services can use network analysis to visualise who retweets what in order to monitor rumours.

The volunteer option

The second option is to rely on volunteers. For instance, 67 volunteers were trained to support media monitoring for the United Nations humanitarian response to the Libyan civil war in 2011. The US meteorological services also relies on people taking pictures or videos of tornadoes using Global Positioning System GPS locators and text messaging to provide real time situational awareness.

Recommendations

The combination of technological and volunteer options can lead to very innovative practices, such as volunteer technology communities. Learning about the different options available and following innovations taking place in the field of crisis situational awareness is important for getting the best meaning out of the overload of information and for having a clearer picture of how to respond to a crisis. According to a study of the ETH Zurich on crisis mapping, volunteer technology communities, mainly managed by non-state actors, can provide states with a low cost way of analysing the terrain in an emergency situation (Cavelty and Giroux, 2011). This phenomenon could develop because the mapping applications are increasingly known and because teams of volunteers can get organised across the globe to initiate and manage the maps when a crisis strikes.

Improving preparedness through social media

Examples from the health field

During the 2009 influenza pandemic, tweets and SMS were used to indicate where vaccination against H1N1 influenza was available. Social media were used to encourage the population to vaccinate and to indicate where the nearest place was to do so. In Kenya, which has a population of 33 million, there are 11.3 million mobile phone subscribers but only 264 000 landline and 3 million Internet users. An opt-in system for

blood donors enables people to receive text messages or email reminders stating when they are eligible to donate again, but also sends messages calling for donors of specific blood types during shortages or crises. This reflects the potential for M-Government (Mobile Government) in developing and emerging economies (OECD, 2011).

The World Health Organisation (WHO) uses social media in its Strategic Health Operations Centres (SHOC), which operate 24-7. Thanks to TweetDeck, they conduct searches by selected keywords on Twitter. WHO now has two full-time social media staff and receives nearly 6 000 new followers on Twitter per week, and about the same number on Facebook per month. These numbers are growing, which helps WHO to both monitor health crises and provide good advice to followers. During the Fukushima events, WHO observed via TweetDeck that some people were telling their friends to drink wound cleaners, which contain iodine, because they thought this would help their body be prepared for nuclear radiation. Via Twitter and Facebook, the WHO social media team warned people not to do this as it could be harmful. The same day, WHO noticed people rushing to take iodine pills and tweeted: "Consult your doctor before taking iodine pills. Do not self-medicate!"

Social media use for natural disasters

Social media can also be used to raise awareness of the risks related to the geographical area where the follower is located and provide recommendations if needed (e.g. what to do in case of major storms or earthquakes). They differ from other channels of communication because the style of communication can be more informal and conversational, which can have an impact on audiences that are not receptive to very official information messages.

Recommendations

Social media can improve preparedness through diversifying the type of approach an emergency service can take. It can be a way to go beyond the command and control position towards more varied tones and styles of information exchange, according to a recent study conducted by Booz Allen Hamilton with the American Public Health Association (Tinker and Fouse, 2009)). The fact that communication can be more individual can have a greater impact on behavioural changes. Social media can also be used to prevent false medical advice from circulating, to clarify rumours and to disseminate tips on crisis preparedness.

Providing information and warning

Provision of information and instruction

Social media, like blogs, can be used to provide advice by posting information such as emergency phone numbers, location of hospitals requiring blood donations and evacuation routes. In its disaster recovery scenario, FEMA can ask retailers which of their stores are closed, then overlay that information on a map to provide food aid to areas where it is needed. During the earthquake in Indonesia in April 2012, a tweet from the US Geo service 15 to 20 minutes after the earthquake said that a tsunami was not likely, which was crucial information for the public and emergency services. This shows that real time communication via social media can change the way crises are managed and experienced by the population.

Real time alert and warning

Social media represent one more channel for emergency services to send alerts and warnings during natural disasters, such as storms or tornadoes. The use of the Twitter sign-off "Please RT" (retweet) and the target of influential online individuals enable an increase in the diffusion of warning messages. Many emergencies require an early warning that reaches many people as quickly as possible. Twitter and Facebook can help because most of users will receive the notification instantly and spread it in their network. During the Iceland volcano eruption, people turned to Facebook and Twitter to know if they could fly and to get information on alternative travel plans in real time. Travellers asked for accommodation and it was offered by others.

Recommendations

Experienced users of social media for emergency warning recommend sticking to facts and being as objective as possible. There is a need to focus not only on communicating to the affected persons but also on understanding that even the unaffected can be worried and in need of information. These unaffected persons can be included in the communication strategy to enhance resilience in the long run, to improve their knowledge of crises, and to enable their mobilisation. Preparation is also important, and many services use pre-messaging where tweets or email alerts are ready and validated to be adapted to the circumstances at the last minute and used very quickly. Crisis communication is increasingly integrated into crisis management as crisis communicators and managers are working hand in hand. This creates a dynamic context where it is important to use the opportunities for information to flow both ways. For instance, travellers during the volcano eruption in Iceland were helping each other find alternative travel plans or accommodation.

Improving crisis response through mobilising volunteers

Social media can be used to mobilise volunteers both during and after a crisis:

Mobilising volunteers

Social media can be used to indicate willingness to help in the event of an emergency. Indicating in the "status" of a social media such as Facebook availability and skills for both professionals and volunteers could be a way for public authorities to know in real time who to mobilise in a given area of disaster.

Social media can also help to direct and target volunteer efforts. During the Deepwater horizon oil spill in the Gulf of Mexico, pictures of birds covered in oil were sent via text message to a volunteer organisation called the Louisiana Bucket Brigade, who then contributed to mapping the most affected areas where efforts should be concentrated. During the earthquake in Christchurch, New Zealand, a large group of volunteers, gathered via a Facebook campaign organised by students called "supporting Christchurch earthquake 22-02-2011", worked closely with the civil defence units.

Mobilising online volunteers far from the crisis epicentre

Online volunteers can be used to relay information provided by emergency services and can also be mobilised to improve situation awareness. The Red Cross trained 150 public affairs volunteers on how to use social media. These volunteers can now upload content onto a website and Red Cross personnel screen. Red Cross platforms include a

wordpress blog, a Facebook page, and an online disaster newsroom that includes shelter locations, numbers of meals served, and other information the media may want to use. The Red Cross Twitter account has 10 000 followers. Tweets cover topics such as shelter, preparedness information and on the ground situational awareness. They can be retweeted by volunteers.

Recommendations

Social media can change risk and crisis communication through empowering and connecting large numbers of volunteers. Governments can no longer focus their risk and crisis communication solely on how much to share and how to package information. Instead, they face a large number of citizens, volunteers and professionals who can exchange critical information between themselves and respond both locally or through remote action. Government officers need to take into account this major change in their risk and communication strategy, and become a steering force for this powerful source of help, information and energy.

Identifying survivors and victims

Identify as "safe and sound" to inform loved ones

Social media can provide a way of checking that family and friends are safe. Applications like safeandwell.org from the American Red Cross allow people to register if they are safe in an area of disaster. Concerned family and friends can search the list of those who have registered themselves as "safe and well" by clicking on the "search registrants" button. The results of a successful search will display a loved one's first name, last name and a brief message. In Japan, during the 2011 earthquake and tsunami, people turned to Google person finder and 320 000 posts were made in one week. People also published photos of the lists of people in evacuation centres on the image web platform of image *Picasa*.

Report as a victim and request assistance

Social media, combined with the use of mobile phones, can help to precisely report an accident and to send requests for assistance. In Korea, 25 000 reports from citizens via an application were processed by public authorities. Korea emergency services and police now promote two-way information sharing by using geographic information systems combined with new technologies.

Recommendations

The use of the social media to identify survivors and victims has proved successful. However, the use of social media to request assistance remains limited to a few examples, such as in Korea. The question is to identify if social media can help avoid crowded emergency phone lines or if there are too many risks of false online declarations to rely on them to request and send assistance. Another issue lies with providing the names of victims. During attacks on campus in the United States, the government had asked for no communication of names online. However, these names were available on Wikipedia.

Managing reputational effects

Using social media for risk and crisis communication can help to counter inaccurate press coverage or to counterbalance rumours.

Counterbalancing damaging rumours

If an organisation is not present in the social media arena, someone else may speak for it and damage its reputation. This can be dangerous if the organisation is not present to counterbalance the information provided. This situation was experienced by Nestlé in the case of an anti-Kit Kat campaign where Greenpeace used social media to accuse the group of using palm oil for its chocolate bars. The company now monitors and uses social media to prevent the reoccurrence of situations that can damage the brand.

Communicating about the organisation's actions

The general public is not always aware of the effort given by emergency organisations. Using social media to communicate about what an organisation is doing can help change the public's perception of the actions taken to respond to an emergency.

Recommendations

It is important to be open to complaints and critics and to respond to them in an appropriate manner. It is important to invest in social media presence to avoid letting bad situations get out of control, which can happen quickly. Social media should be used not only to communicate but also to listen.

Providing incentives to collect funding and support

Encouraging donations

Social media can be used to solicit donations when major catastrophes occur. People can indicate on their Facebook page that they have contributed to funding an NGO for crisis response and hence encourage their friends, families and networks to do the same. The Red Cross is using social media to encourage collective action towards more funding during emergencies.

Facilitating the supply of support

During an emergency, people who want to help by providing blankets or a safe place to stay for victims of a disaster often do not know where to turn. By indicating precisely on social media what type of contribution could be needed, emergency services can avoid flows of unnecessary materials and develop synergies in the communities.

Recommendations

It is important to be specific about what precisely is needed during a crisis and to be aware that fundraising tweets account for a minor percentage of messages during the crisis phase. According to a study conducted by Queensland University of Technology and the University of New South Wales in Australia during the 2011 South East Queensland Floods, fundraising tweets are more efficient in the post crisis phase when people turn to recovery (Bruns, 2012). It is also important to take into account that there may be a gap between the expressed intention and the ultimate decision to donate.

Learning from crises

Social media can be used after a crisis to facilitate the lessons learnt processes and as useful material for risk and crisis researchers.

Facilitating the lessons learnt processes

Social media provide content associated with a date of post, which can help emergency managers keep a very detailed report of what happened hour by hour. Tweets and photographs linked to maps and a time line can help build a comprehensive story of what happened and identify the main vulnerabilities.

Developing skills and knowledge on risks and crises

The content of social media during a crisis can be rich material for social scientists to analyse in order to have a better knowledge of risks and crises. In the United Kingdom, emergency and health services work with behavioural scientists and communication specialists to conduct audience research and track feedback during risk and crisis communication campaigns, such as the 2009 influenza pandemic.

Recommendations

Some websites can help keep records and archives of tweets, or create a timeline that shows a visual mapping of the crisis enfolding and ending. Many applications for mapping or placing tweets on timelines are available for free, which can be an incentive for a greater number of researchers to use these materials. Social scientists could be mobilised in multidisciplinary expert groups to learn from past crises and develop new ways of engaging with the public through tailored risk and crisis communication.

Improving partnerships and co-operation

International co-operation and public-private partnerships in the field of social media in risk and crisis communication are identified as a way forward.

The ICT4Peace Crisis Information Management Advisory Group initiative

Innovative initiatives are taking place, such as the pioneering ICT4Peace initiative based in Geneva and operated through a partnership called the Crisis Information Management Advisory Group (CIMAG). This partnership includes the United Nations Department for Peacekeeping Operation, the United Nations Department of Political affairs, the United Nations Office for Coordination of Humanitarian Affairs (OCHA), the World Food Programme, the United Nations Development Programme, the United Nations Children's Fund (UNICEF) and the United Nations Refugees Agency (UNHACR) The partners work together towards enhancing crisis portals such as OCHA's OneResponse, and also work on bringing together practitioners, developers and policy-makers to develop crisis mapping and address emerging needs in crisis communication.

Build partnerships to enhance the use of digital media

The study of the United Kingdom's response to the 2009 influenza pandemic stresses that health departments should seek to further explore the use of social media, using independent partners such as the Science Media Centre (Hine, 2010). The study underlines that the development of such a partnership will help to engage the wider independent scientific community and the media.

The UN Global pulse initiative

A UN white paper, published in May 2012, states that the purpose of the UN Global pulse is to detect "digital smoke signals", protect the vulnerable and strengthen resilience

to global shocks. It uses real times analytics to turn imperfect, unstructured, and complex information available on the web into actionable information for officials in charge (United Nations Global Pulse, 2012). The programme brings together expertise from UN agencies, governments, academia, and the private sector to research, develop, test and share tools and approaches. This co-operation will lead to the development of free and open source software tools to help governments and organisations make evidence based decisions with limited resources.

Recommendations

Partnerships for using social media in the area of emergency management and communication exist, but they come with difficulties. Not all players have the same interests or the same background. Some are from the humanitarian sector, others are technologists who can build new platforms for imagery and mapping, etc. Traditional players of emergency management teams and new players coming from social media need to make sure they are have a similar outlook, speak the same language, and can learn from each other. Technologists have a tendency to focus their energy on crisis communication, while emergency services need better risk communication in the long run. The question of the financing and sustainability of the co-operation is crucial. Most of the current volunteer technology communities rely on small resources and the public sector may or may not have the means to contribute to greater investment in risk and crisis communication in the future. Public authorities could collaborate with Twitter and Facebook to facilitate a quicker response if the account of an official emergency service gets highjacked.

Building trust

Ensuring an organisation is trusted online

The use of social media could improve transparency and trust in public authorities. Government authorities, and more broadly experts, are no longer easily trusted in crisis situations after cases of misinformation. They are under pressure to respond within tighter time frames as soon as an event occurs. With reliable and updated public safety and emergency notification via Twitter or RSS feeds they could work on enhancing the level of transparency. Developing a community of followers for the communication of hard facts and timely information on disasters could help public authorities benefit from and adapt to the breaking news effect, capitalising trust over time.

Knowing which online sources to trust

It is important to know which types of Facebook pages, tweets or blogs can be trusted or not. Lessons must be learnt from each crisis to identify those that can and can’t be relied upon

Recommendations

Studies show that the more citizens can engage with their government online, the more they develop trust (Mickoleit, 2014). Public authorities in charge need to be aware of this when deciding how to engage with their citizens.

Enhancing recovery management

Social media can be used to enhance recovery management in two ways: through the sending of information on reconstruction and recovery, and through the provision of stress management.

Sending information on reconstruction and recovery

In post crisis phases, social media can be used to send information about recovery and reconstruction. Social media can be used to communicate the recovery of infrastructure (bridges, routes, water supply) and to identify areas that are in most need of recovery. Site clearance can also be co-ordinated.

Planning stress management

Social media can help to identify where stress management is most needed in the recovery phase and to offer tools for managing stress through interactive platforms. Research conducted after Hurricane Katrina shows that interactive information is preferred to static: those who were affected turned to interactive social media forums to share their thoughts and feelings rather than static traditional media. The sense of belonging to and sharing emotions with an online community can help in the post crisis phase.

Recommendations

Social media can play a role after a crisis to enhance recovery and reconstruction. Communication plans must be structured according to the phase of the crisis. As it is difficult to "turn off" social media, ensuring continuity in the use of social media over the risk management cycle is crucial.

Challenges of using social media

The challenges in the use of social media in risk and crisis communication must be taken into account when developing social media strategies. Social media use in risk and crisis communication is complex and must be handled with care. Financial issues, legal issues, political issues and security issues are at stake when deciding to develop the use of Facebook or Twitter in the case of emergencies. For each challenge, solutions and remedial strategies are presented below.

Multiple players and communication channels

The first challenge that emergency officers face is the multiplicity of players and communication channels that exist during a crisis situation. These can be national, regional or local players; officials or volunteers; and they can use traditional media or social media. This can blur the picture and provoke an information overload.

There are three approaches to managing social media information: subsidiarity, multichannel and centralised. Some countries have opted for a subsidiarity principle, where the level of government closest to the community concerned is responsible for communication. Others use a multi-channel approach so that people can rely on different sources of information, some more factual some more subjective. Other countries favour a centralised use of social media to eliminate multiple communication strategies from multiple departments. The challenge is for an organisation to decide how best to deal with

the broad range of players and channels that could potentially be part of their risk and communication strategies. They must see which approach best suits their organisational and national culture and the choice must be clearly stated.

It is important to have guidelines and a comprehensive strategy for risk and crisis management that gives precise rules and recommendations on how to engage with social media. On a day-to-day basis it is possible to have an online and social media division in the risk and crisis communication department. This unit plans the social media strategy on a weekly basis with all the relevant services.

There could also be social media roundups with a daily or weekly presentation of situation awareness through crowdsourcing of social media content. It is important during inter-services meetings to validate pre-messaging strategies for crises. The experience of Eurocontrol during the volcanic ash cloud over European airspace shows the importance of an integrated approach: Eurocontrol had established its Twitter account few months before the crisis, this account became the most active crisis communication tool utilised by passengers blocked in airports throughout Europe. The member of staff responsible for monitoring and using social media had to integrate this information into briefings with the crisis manager and with staff who handled traditional media. The use of social media needs structure the services in charge of its use must be aware of what information is delivered and what tone is preferred for different social media platforms, etc.

Transparency and reliability

The content of social media does not follow a process of validation to indicate its truthfulness. Therefore, there is a risk of propagating rumours and misinformation. Retweeting can make a rumour spread very quickly and get out of control. This could lead to panic in a population that would not be justified by facts, but only spread through misinformation. As traditional media often quotes online interaction it can relay false social media information without the reader/watcher noticing.

Social media information from official channels should be clearly labelled as such. In March 2011, researchers from Kobe City University of Foreign Studies surveyed Twitter users and tracked updates from earthquake victims in Tohoku, Japan. This survey shows that in order to increase the validity of tweets during an emergency, management officials could announce them with an official "hashtag" (topics labelled with the "#" symbol) via multiple social media platforms (Acar and Muraki, 2011). Establishing official accounts that can be retweeted increase the validity and reliability of using Twitter as a tool during a disaster event. The official tweets should be clearly labelled. In Japan during the 2011 earthquake and tsunami, each official service had an icon to indicate from which official sources the tweets were coming. In addition, it is crucial to educate people to the use and risks of social media. Communication campaigns, school programmes, and other initiatives could be developed to explain the risks of misinformation and rumours.

Mobile wireless devices (e.g. smartphones) are often equipped with advanced sensor technology, GPS, accelerometer and a digital compass. They offer the potential for remote sensing and information fusion in an emergency. Sensor measurements could ensure information integrity and avoid misinformation being spread too easily. Combining sensor measurements with the information shared online via social media could be a way to limit misinformation.

Regulation is another way of approaching the problem of misinformation. In Mexico in 2012, Twitter has more than 4 million users, 98% of citizens have a Facebook profile

and 30 million people are able to access the Internet. As these figures keep on increasing a bill has been passed called the Veracruz Law. This law prohibits citizens from spreading false rumours and information that may trigger panic. The difficulty lies in the definition of the false rumours. A risk is to use these types of legislation or regulation to censor social media.

To avoid panic it is possible to rely on the geographical precision of the communication tool used. In certain cases, social media offers the possibility to see the localisation of the account holder. In these cases, to avoid the unwanted movement of people who may block escape routes or cause unnecessary panic, it is possible to target only the persons positioned in a limited geographical area, instead of addressing everyone as with mass traditional media.

Reputation damage

The Japanese authorities used social media during the 2011 earthquake and tsunamis. On 13 March 2011 they started a Twitter page in Japanese, and on 16 March 2011 a Twitter page in English. On 23 March 2011 they started to use Facebook, and the number of followers increased rapidly. However the Facebook and Twitter pages were also used to attack Japan's image, even about unrelated topics such as anti-government messages protesting against the killing of whales, as well as against the use of nuclear power plants. This practice is known as trolling.

It is important to understand that social media cannot be controlled. Social media allow for responding to criticism and attacks as quickly as possible, and the respectful correction of inaccurate information can stop the spreading of rumours.

Keeping in touch

The elderly, the disabled and people who do not speak the local language may not be able to access the data provided by social media. A solution is to use various types of warnings and alerts. In Japan during the 2011 earthquake and tsunami, emergency responders used both tweets and traditional public display and wallpapers at the same time. The important aspect is to be consistent in the communication strategy throughout different channels. By multiplying the types of channels, it is possible to increase the probability that crucial information will be received by the targeted public. A technical solution is to use different social media in aggregated ways through websites such as Hootsuite and Tweetdeck. A user can type content into one webpage and it will be sent through multiple social media channels. This solution can help save precious time in an emergency situation. Prior to Facebook and Twitter, public communication officers had to organise press conferences and press releases during a crisis situation. Now they can also use social media, which the press can access directly.

Avoiding information overload

During a crisis, the number of information exchanges through social media can be so high that it becomes impossible to have a clear picture of what is happening. Bloggers or Facebook users can also publish false information or their perception of reality might be biased during a crisis, which makes it difficult for the emergency manager to get the right picture of the situation. The overload of true and false information can even go as far as blocking the whole telecommunication system and raising the question of the allocation of the bandwidth, like in Japan during the 2011 earthquake and tsunami.

A solution is trending or data mining. Starting with the right question and following the right data with the right metrics, a clearer picture can emerge from the intense flow of information exchange. Using services such as Trendistics or Google analytics, it is possible to see if there are trends in what people are exchanging. However, caution must be exercised to avoid inaccurately interpreting social media data. For instance, emergency services must take into account the sampling selection bias as social media users are not always representative groups of the larger population affected by a disaster. An "Information and Communication Technologies for Development" blogger from the University of London expressed his doubts on the use of Ushahidi during the Haiti earthquake. Ushahidi staff found correlation between the building damage and the SMS streams, however, after controlling for the presence of any buildings (damaged or undamaged), the text message stream had a weak negative correlation with the presence of damaged buildings. This example shows that caution and learning from past experiences are crucial when using crowdsourcing and data mining based on new media.

To avoid jamming the system with too many exchanges of information, public authorities can ban the use of certain media during a major emergency. For example, in Japan during the earthquake and tsunami the government decided to give priority to exchanges of emails in some affected areas.

Promoting open data while protecting privacy and confidentiality

Maintaining open data is important for social media to be able to crowdsource data easily. Although most social media do not have the in-house capacity to develop specific products for emergency managers, the platform is kept open and adaptable so that third-party developers can build customised tools to carry out crisis situational awareness. However, a risk could arise from this openness as the level of confidentiality of data provided by users on their social media pages could be endangered. It is not clear whether bloggers or Facebook and Twitter users consent to the analysis of their data. According to a study of the ICT4Peace Foundation on the potential and challenges of open data for crisis informatics management, there is still a long way to go before all actors are convinced of the benefits of openness (Stauffacher et al., 2012).

Overcoming the challenges of open data requires working on several fronts. Legal experts can be mobilised to address confidentiality issues. For instance, there is a need to make a distinction between the monitoring of one personal page and of a large number of pages. In the Netherlands, the law authorised the analysis of a flow of data coming from social media platforms, but banned the monitoring of individual social media use. Legal experts can also be mobilised to deal with proprietary technologies. A clear line must be found to protect commercial interests and to save lives. Law, policies and guidelines should be developed to ensure the use of social media in a crisis situation does not become out of control; but without regulations and laws restraining too strongly the innovative processes taking place.

Who is liable for what?

Risk managers have expressed fears that people could believe they should receive assistance if they have indicated via a social media platform that they are in need of help. There is a risk that emergency services could be held liable if they don't answer to an online request. Going one step further, could they be liable for providing incorrect or unclear information?

The Web 2.0 and use of social media in risk and crisis management may require adapting laws and public policies. More importantly, the emergency services and authorities in charge must have a clear process of internal validation of what can and cannot be put on social media. However, this process must not to include too many layers of validation, as this would hinder the provision of a swift social media response.

Managing public expectations

The use of social media in emergency management can create new expectations in the population at a time when human and material resources may be scarce. For instance, according to the social media emergency management camp organised in 2011 (Wardell and San Su, 2011), the use of 24/7 social media by the Los Angeles Fire Department (LAFD) means that three LAFD officers are committed to providing support over a 24-hour period through engaging in information dissemination and discussion across their Twitter profiles: @LAFD and @LAFDtalk. On a steady state basis, the officers use the tools to monitor user-provided information and look for emergency reports and opportunities to clarify information for citizens with questions or concerns. Not all emergency services can dedicate as much time and resources to the use of social media.

It does not require a large resource commitment to begin using social media within an emergency organisation; creating a Facebook page or a Twitter account is not very time consuming. The questions are how far to go and what is the objective. Once these are decided, it is important to make clear what the organisation can and cannot do with social media.

During emergencies, social media can play an important back-up role in disseminating warning and response information if traditional services are overwhelmed by demand. For example, during the 2011 floods in Queensland, Australia, Facebook was used to share warning information when official emergency services websites failed to cope with the heavy traffic. The use of social media can also be a way of avoiding an overload of information coming from phone calls. In the case of the volcano eruption in Iceland, the use of Facebook and Twitter helped with the shortage of resources to deal with phone calls and incoming emails.

Addressing security issues and avoiding potential misuse

With social media, one message intended for a target audience can be read by others who may not share the same culture or intention. This situation can create misunderstandings and, as it is not possible to know who is reading the information, offer opportunities for terrorists or criminals to use catastrophes to their own advantages and plan deadly attacks. Social media do not guarantee security in the authentication, which leads to questions concerning the potential dangers of an overly transparent exchange of information during a disaster.

There is a need to clearly define, at a high level, what information can and what should not be made available online. Rules can be discussed in advance, for instance, a decision could be made not to communicate names of victims or give information that could be used to endanger parts of the population.

Impact of social media

There is limited evidence on the impact of social media in crisis communication and management. People have diverse reasons for using social media during an emergency

situation: helping victims, being anxious, trying to find out if it is possible to return to the affected area, supporting emergency services, mourning, exploiting the situation, or being curious. These are all very different incentives for using social media and they lead to different strategies for the officials in charge.

It is difficult to precisely evaluate the costs and benefits of using social media in risk and crisis communication. Metrics such as Google analytics can be used to assess how many followers exist for a given social media, but they do not provide information on the extent to which people's practices are affected by their use of social media pages in times of crisis. It is also very difficult to know how much of the information conveyed by social media is reliable, and how much it could enhance effectiveness or create additional difficulties. According to a study conducted by Booz Allen Hamilton and the American Public Health Association (Tinker and Fouse, 2009), most emergency services use a combination of metrics, online comments and surveys to evaluate their use of social media in times of crisis. However, as the crowdsourced use of social media is rather recent, it is difficult to have enough data available to evaluate the impact of social media in risk and crisis management.

Crisis information systems and analytics aim to bridge the gaps across social sciences to analyse the non-routine use of social media (i.e. use in times of crisis) and how it can differ from regular use. Further surveys and research are necessary to obtain a fuller assessment.

Developing strategies for the dynamic use of social media

Social media are a knowledge-gathering tool to ascertain public sentiment or disseminate a message to the public in times of crisis. They also allow for a dialogue with the public, and for the public to interact with services about an event without the intermediation of public authorities. Searching for a dynamic use of social media requires multistep strategies. Large discrepancies exist between different emergency services and different countries, etc. This section presents an analysis of how countries and organisations can go beyond an ad hoc approach to social media towards a more strategic and empowered approach. This should help emergency services to review their current social media use and develop more comprehensive and flexible communication strategies.

Bottom up: Situation awareness tool to identify "digital smoke signals"

When the use of social media is coupled with the possession of smartphones, everyone can send information from the site of an accident or catastrophe. From the emergency services' perspective, receiving this real time information (pictures, videos etc.) can help them to react accordingly. The measurement of trends on Twitter or other social media, carried out electronically or with the help of volunteers, can help conduct situational awareness in real time. Early detection of digital anomalies in how the population suddenly tweet can enable faster responses in times of crisis if they are interpreted correctly and timely as "digital smoke signals". The social media manager can provide daily social media updates on ongoing crises or risks, or conduct a weekly analysis of trends. Table 3.2. provides a self-assessment checklist for organisations on the use of social media to conduct bottom-up situation awareness.

Table 3.2. Checklist for situational awareness use of social media

	Yes	No
Do you have a list of blogs, Facebook pages, and Twitter accounts of people who follow risks and crisis and who could help you gather information from the communities? Do you follow specific hashtags?		
Does your organisation regularly monitor social media for situational awareness? (Every hour? Day? Week?)		
Do you use metrics to monitor the number of visits on emergency services web pages and social media pages in order to identify a trend towards one particular focus of a given risk or crisis?		
Do you build methodology or tools to monitor the flow of information exchanged via social media on the Internet?		
Do you encourage citizens to report during crisis using a social media (Twitter, blog)?		
Do you train your staff to use of social media as a situational awareness tool?		
Does your organisation have the necessary human skills to use social media to conduct situational awareness?		
Do you integrate social media in emergency exercises?		
Do you use crisis mapping based on crowdsourced social media data?		
Do you have a partnership agreement with a volunteer technology community in case of a major emergency?		

There are technical challenges in accessing and analysing data streams to conduct situational awareness. Ensuring the interoperability of systems can be challenging when monitoring various social media platforms and tools. What could appear as an anomaly in the flow of information and be interpreted as a digital smoke signal, can in fact be a false alarm due to sample bias or misinterpretation of the data. Nevertheless, innovative initiatives such as the creation of virtual platforms combining different social media analytical tools, are under way that could change the way emergency services conduct situational awareness in the near future (Smith, 2011). The technological innovations could be complementary to traditional tools of situational awareness.

In a February 2012 presentation on the topic of "Real-Time Awareness", Craig Fugate, Administrator of FEMA, explained what it means for his agency to become a "sophisticated user of information". In 2011, during a series of devastating tornadoes in the American mid-west, FEMA monitored Twitter and noticed an unusual number of different geographical locations being mentioned for tornado damage. Mr Fugate proposed immediately dispatching relief supplies to the long list of locations, but his team thought that they did not yet have an accurate estimate of the damage level to send assistance. His challenge was to get staff to understand that the priority should be one of changing outcomes, meaning that even if half of the supplies dispatched were never used and sent back later, unless trucks were sent immediately there would be no chance of reaching communities in need if they were suffering tornado damage already.

Mr Fugate explains: "If you're waiting to react to the aftermath of an event until you have a formal assessment, you're going to lose 12 to 24 hours…Perhaps we shouldn't be waiting for that. Perhaps we should make the assumption that if something bad happens, it's bad. Speed in response is the most perishable commodity you have…We looked at social media as the public telling us enough information to suggest this was worse than we thought and to make decisions to spend [taxpayer] money to get moving without waiting for formal request, without waiting for assessments, without waiting to know how bad because we needed to change that outcome." Fugate also stressed that using social

media to conduct situational awareness is not a precise science and the response is not going to be precise either. "Disasters are like horseshoes, hand grenades and thermal nuclear devices; you just need to be close— preferably more than less."

Top down: Using social media to communicate with the population

Social media allow for warnings to be sent to a broad group of people while at the same time precisely targeting individual information sending, according to the type of target groups identified by the communication managers. Table 3.3. shows the most common steps in top down use of social media.

Table 3.3. Checklist for top down communication use of social media

Checklist questions	Yes	No
Does your organisation have guidelines on the use of social media for the communication team? For the employees?		
Does your organisation have an RSS system on its webpage for people to follow it?		
Does your organisation have a Twitter account?		
Does your organisation have a Facebook page?		
Does your organisation have a blog?		
Does your organisation have hidden web/Twitter/Facebook pages that are prepared to be launched in case of crises?		
Does the head of your organisation have a Twitter account? A Facebook page? A blog?		
Does your organisation use social media to redirect people to its official website?		
Does your organisation use a variety of formats (pictures, videos, etc.) to communicate on social media?		
Does your organisation regularly update its posts?		
Does your organisation regularly archive its social media messages?		
Does your organisation have a team dedicated to social media communication?		
Does your organisation outsource its social media communication?		
Does your organisation have a fast track clearance approval process in place for social media strategy in times of crisis?		
Does your organisation have a list of your followers on the web and their profiles? Are you trying to build a subscriber base to extend your outreach via social media? Do you know who the key influencers are?		
Do you publicise your social media presence in press releases and place links towards your social media pages on your website?		
Do you have a strategy so that your social media network can grow? What are your objectives in terms of growth in scope (increase the age/ethnicity/gender/geographical range of Facebook fans, Twitter followers, etc.)?		
Has your organisation tried to use social media to raise risk awareness by sending tips of the week, what to do in case of an emergency on Twitter, or planned a viral campaign on YouTube?		
Does your organisation monitor, in real time, the evolution of its social media communication and its audience profile?		
Does your organisation alter its communication according to the different social media formats (Facebook, Twitter, etc.)?		
Does your organisation have co-ordination mechanisms with other emergency or government services to ensure that consistent information is widely spread?		
Does your organisation share content from other services on its pages?		

Caution must be exercised when using social media to communicate on risk and crisis. First, it is crucial to ensure the security of sensitive information; and second, a

validation process of information accuracy must be followed and if false information is posted by mistake a very swift correction must be put in place. Most government agencies using social media have clear guidelines on how to communicate. When their social media communication is not mature and well developed, they only provide basic information, such as weather warnings or real time information about an ongoing emergency.

Using social media for two-way communication and as a platform for dynamic interaction

Social media can be used as dynamic interaction platforms that are mobilised for two-way communication during a crisis situation. Crises lead to an urgent need for the public to receive information, but they also give rise to a strong wish to supply information to the authorities in charge. Using social media offers the possibility of including two-way communication options and of reacting to the demands of the public. Using two-way communication tools means that it is possible to know whether or not the message has reached and been understood by the recipient.

Table 3.4. Checklist for two-way use of social media

Checklist questions	Yes	No
Can your organisation receive and react to public input via social media?		
Does your organisation update regularly the question and answer page of your website?		
Do you have a forum where you can exchange in real time with the population in case of emergency?		
Do you initiate online conversation and exchange with your audience through social media?		
Do you encourage feedback through your social media communication?		
Does your organisation participate in other people/organisation's social media to encourage exchanges? Does your organisation join in relevant online conversations?		
Can people use social media to identify as a survivor?		
Can people use social media to request assistance?		
Do you use GIS as a dialogue tool to enhance the mapping of a disaster?		
Do you implement online interactive risk awareness campaigns (interactive games, etc.)		
Do you integrate the different social media platforms you use with each other?		
Do you have partnerships for sharing methods of two-way communication (with private sectors, etc.)?		

The tables above provide guidance on a selection of the most common existing communication strategies that rely on social media. Each emergency service can then explore the available options to see how to adapt their communication strategies. The technical systems available are changing very quickly, which means that a permanent scanning of new technologies must be done to keep aware of the last available solution. Social media strategies must be updated on a regular basis as the social media landscape is continually changing.

How to draft social media guidelines for risk and crisis communication

Several countries (e.g. United Kingdom, Australia, New Zealand), regions (e.g. Catalonia), cities (e.g. Seattle, New York) and agencies (e.g. US environmental protection agency) have already developed social media guidelines, but only a few, for example the American Red Cross and FEMA, have specific documents for the use of social media in risk and crisis communication. These guidelines exist in various forms: high level guidance exists for managers and decision makers to decide if their organisation should use social media or not; codes of conduct explain to the employees how to use social media, what the risks are and how to prevent them; and social media training can be offered to public sector employees and managers. Failure and success cases of social media use should be studied to learn from existing practices.

Major issues to be included in social media guidelines and training are highlighted in Table 3.5.

Table 3.5. How to draft social media guidelines

A social media glossary	Explain the wording used in social media and the technical terms related to social media platforms (e.g. crowdsourcing, data-mining, etc.)
A rule for private and public use of social media	Provide fundamental norms about how to communicate at work, but also in the private sphere about work.
A social media philosophy/strategy	Explain the objectives of the organisation when using social media to communicate. The goals are clearly stated (listen to public expectations, communicate about what the organisation does, enhance the reputation of the organisation, build a community, inspire volunteers, etc.). In addition it explains the resources available for social media communication and the main steps to follow to reach the desired outcome.
A social media tactics	Explain how different social media will be used (Twitter, Facebook, etc.), how the content will be developed and validated, how often the social media pages will be updated, what type of links or retweet practices your organisation will have with partnering organisations, what type of content is to be solicited from followers, etc.
A "what to do in case of…"	Explain what to do in case of problems such as spams, negative comments, provision of false information by mistake and jamming.

Key recommendations for social media use in risk and crisis communication

The use of social media in risk and crisis communication remains in its infancy. Tools are emerging to aggregate more and more data so that meaning can be drawn from the flow of information exchange via the Web 2.0 during a crisis. Technological innovations allow for risk and crisis relevant information to be crowdsourced from social media streams, which can be very valuable for emergency services and authorities in charge.

An increasing number of emergency officers and volunteer organisations use online activity to enhance the resilience of their communities during a disaster. Social media has enabled informal partnerships that enhance dialogue capacity among various stakeholders, although there are major challenges with this approach.

Emergency services must clearly tell their audience what they can expect to receive through social media in terms of risk and crisis communication. To make the best use of social media in risk and crisis communication, the following actions should be considered:

Governments should develop public policies to support the development of social media use in risk and crisis communication. These should include policies to sustain and implement open data strategies, to regulate the spreading of dangerous rumours, to assess the impact of social media, and to enable systematic national infrastructure to have the long-term storage capacity to incrementally learn from past crises.

Governments should foster citizen-led social media use through volunteer technology communities. Social media have been used spontaneously by citizens to enhance resilience and solidarity in affected communities. There is therefore an opportunity to accompany the current citizen-led initiatives to enhance collective intelligence in disasters and make sure that information provided is as reliable as possible. Different tools can be used, including: publishing rules and guidelines on the use of social media during a crisis and producing leaflets and education materials. Developing government-led social media strategies for use during a crisis requires introducing codes of practice at government level and training officials in charge.

Governments should develop social media strategies to support crisis communication strategies before, during, and after a crisis. Before a crisis, the capacity to filter social media for monitoring and situation awareness, grasping trends and early warning signals should be considered. Developing social media strategies requires organising crisis communication staff, establishing clear validation procedures, pre-messaging, and preventing crises by performing risk awareness social media campaigns. Organisations should position themselves as trusted sources and identify other trusted sources. In crisis phase, organisations need to provide real time objective facts so that the public are not kept the dark or forced to use other non-reliable sources. IT volunteers can be mobilised via online technology communities to improve crisis mapping and situational awareness. Rumours and misinformation must be mitigated as quickly as possible to avoid negative retweets and help set priorities for which audiences to target, depending on available resources. In post crisis phase, social media can be used to communicate about recovery and reconstruction, improve stress management and contribute to lessons learned.

Governments should consider the implications of a greater use of social media in terms of working practices and changes in organisational culture and organisational structure, etc. The use of social media can alter a user's perception of barriers that exist between persons, functions and organisations; and impart a false sense of access that raises expectations. This needs to be taken into account when deciding how to use social media in risk and crisis communication. Practices need to meet expectations that are reasonable for the organisation to handle. Change management may be needed to develop the use of social media.

Governments should draft guidelines for the use of social media in risk and crisis communication by public agencies. Given the large number of stakeholders that can be involved in crisis management, guidelines can be an efficient way to harmonise practices across government agencies, share lessons from good practice, and foster the development of social media strategies in each organisation.

Governments should maintain traditional media in their crisis communication strategy. Traditional media, such as sirens, wallpapers, radio and television, should be maintained and their interaction with social media considered.

Annex 1

While the list below is not comprehensive, it provides an overview of the social media platforms most used for risk and crisis communication.

Social media type	Short description
Facebook	A social utility that connects people with friends and others who work, study or live around them. People use it to keep in touch with friends and colleagues. There were 901 million monthly active users reported at the end of March 2012.
Myspace	An online community that allows users to connect, interact and exchange information with those who have the same interests. It is often used to discover new artists and watch videos online. Myspace had over 262 million users in 2012.
Friendster	A social gaming site launched in 2002. The service allows users to communicate with each other, share online content, etc. The site, at its peak, reached tens of millions of registered users; however, it has since declined in popularity.
YouTube	A user generated site that allows people to share videos and view and comment on the uploaded videos of others.
Flickr	A user generated site that allows people to share pictures and view pictures of others.
Vimeo	A user generated site that allows people to share videos and view and comment on the uploaded videos of others.
Wikis	A website that everyone can update to share and manage content with others.
Forums and Message boards	Online internet sites where people can hold a conversation through posting and responding to messages.
Chats	Online internet applications to hold conversations through real time instant text messages.
Podcasts	Web based audio and video content made available to download to a personal audio or video player.
Blogs on Blogger, WordPress, Tumblr	IA personal website that is updated frequently. It contains regular entries of commentary, pictures, and other materials.
Microblogs on Twitter	With 140 million users, Twitter is a platform for people who register to post and receive short messages to a network of followers. Top five countries in terms of Twitter accounts are the United States, Brazil, Japan, the United Kingdom and Indonesia (according to a study conducted by Semiocast in 2012)
-MAPPING COLLABORATION Crisis mappers OpenStreetMap Google map maker	Crisis mapping collaborative social media exist under various forms. Crisis Mappers leverage mobile and web-based applications, participatory maps and crowd sourced event data, aerial and satellite imagery, geospatial platforms, advanced visualisation, live simulation, and computational and statistical models to power effective early warning for rapid response to complex humanitarian emergencies. OpenStreetMap provides free geographical data and mapping. Google map makers can be used to access and improve maps according to various needs.
-ONLINE AND ONSITE CRISIS CONTRIBUTION SOCIAL MEDIA Ushahidi Crisis commons Sahana foundation tools Geeks without bounds	Ushahidi is an open crowdsourcing crisis information platform that is easily deployable to meet local needs. Crisis commons is an international network of professionals that aggregate during crisis camps and work collaboratively online to enhance crisis management. Sahana foundation software is dedicated to saving lives by providing information management solutions that often rely on social media. Geeks without bounds are developing applications to enhance the provision of humanitarian aid in disasters.
-PUBLIC-PRIVATE-PEOPLE PARTNERSHIP FOR SOCIAL MEDIA CRISIS COMMUNCATION Random Hacks of Kindness (RHoK) (with Google, Microsoft, Yahoo, NASA, World Bank)	RHoK organises and hosts biannual two-day events where volunteer technology experts develop software solutions for risk and crisis management. They are developing new social media products for the risk and crisis communication of the future.

References

Abel, F., Hauff, C. et al. (2012), "Semantics + Filtering + Search = Twitcident. Exploring Information in Social Web Streams", *Proceedings of International Conference on Hypertext and Social Media (Hypertext)*, Milwaukee, USA.

Acar, A. and Y. Muraki (2011). Twitter for Crisis Communication: Lessons Learnt from Japan's Tsunami Disaster, *International Journal of Web Based Communities.*

American Red Cross (2011), *Social media in disasters and emergencies*, online survey of 1046 respondents, telephone survey of 1011 respondents, Summer 2011, www.redcross.org/www-files/Documents/pdf/SocialMediainDisasters.pdf.

Bertot, J.C, P.T Jaeger and D. Hansen (2012), "The impact of polices on government social media usage: Issues, challenges, and Recommendations", *Government information quarterly,* Vol. 29, Issue 1, January 2012, pp. 30-40.

Bertot, J.C, P.T Jaeger, S. Munson and T. Glaysier (2010), *Engaging the Public in Open Government: Social Media Technology and Policy for Government transparency*, www.tmsp.umd.edu/TMSPreports_files/6.IEEE-Computer-TMSP-Government-Bertot-100817pdf.pdf.

Bruns, A., et al. (2012), *#qldfloods and@QPSMedia: Crisis communication on Twitter in the 2011 South East Queensland Floods*, Brisbane, ARC Centre of Excellence for Creative Industries and Innovation.

Cabinet Office National Resilience Extranet (2012), *Using social media in emergencies, smart practices, DSTL Smart Tips for Category 1 responders using social media in emergency management.*

Carrel, L. F. (2005), *Leadership principles during, after and before a crisis, A Guide*, Swiss Federal Chancellery, 4th edition.

Cavelty, M.D. and J. Giroux (2011), "Crisis mapping, a phenomenon and tool in emergencies", in *CSS analysis in security policy*, ETH Zurich, N°103, November 2011.

CDC (2011), *The health communicator's social media toolkit*, Centre for Disease Control and Prevention, www.cdc.gov/socialmedia/Tools/guidelines/pdf/SocialMediaToolkit_BM.pdf.

Central Office of Information (2012), *Engaging through social media, a guide for civil servants,* http://coi.gov.uk/guidance.php?page=264.

Ganapi, S. (2010), *Using geographic information systems to increase citizen engagement*, IBM centre for business development, Washington DC.

Grimaldi, A. (2010), *Les différents habits de l'« expert profane »,* Les Tribunes de la santé 2/2010 (n° 27), pp. 91-100, www.cairn.info/revue-les-tribunes-de-la-sante-2010-2-page-91.htm.

Hine, D. (2010), *The 2009 influenza pandemic, an independent review of the UK response to the 2009 influenza pandemic*, www.dhsspsni.gov.uk/the2009influenzapandemic_acc.pdf.

Hughes, A. et al. (2008), "'Site-Seeing' in Disaster: An Examination of On-Line Social Convergence", *Proceedings of the 5th International ISCRAM Conference*, Washington, DC.

ICT4Peace foundation (2012), *Activity report 2006-2012*, http://ict4peace.org.

IRGC (2012), *Social media for crisis communication*, Concept Note, International Risk Governance Council, Lausanne.

Latonero, M. and I. Shklovsli (2010), "'Respectfully yours in safety and service': Emergency Management & Social Media Evangelism", *Proceedings of the 7th International ISCRAM Conference*, Seattle, USA.

Latonero, M. and I. Shklovski (2011), Emergency Management, Twitter, and Social Media Evangelism, International Journal of Information Systems for Crisis Response and Management, 3(4), 1-16, October-December 2011.

MASSCRISCOM (2011), *The mass communication with the public project,* masscriscom project results, www.masscriscom.eu/default.aspx.

Mickoleit, A. (2014), "Social Media Use by Governments: A Policy Primer to Discuss Trends, Identify Policy Opportunities and Guide Decision Makers", *OECD Working Papers on Public Governance*, No. 26, OECD Publishing, Paris http://dx.doi.org/10.1787/5jxrcmghmk0s-en.

OECD/ITU (2011), M-Government: Mobile Technologies for Responsive Governments and Connected Societies, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264118706-en.

Palen, L. (2008), "Online social media in crisis events", *Educause quarterly*, Issue 3, http://net.educause.edu/ir/library/pdf/eqm08313.pdf.

Patton, R.M. and T.E. Potok (2008), "Identifying Event Impacts by Monitoring the News Media", *12th International Conference Information Visualization*, IEEE, pp. 333-337.

Pew Research Center (2015), Social Media Usage: 2005 to 2015, http://www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/.

Prentice, S. and E. Huffman (2008), *Social media's new role in emergency management,* Idaho national laboratory, www.inl.gov/technicalpublications/Documents/3931947.pdf.

Smith, A., et al. (2011), *Social media and virtual platforms: the new situational awareness for emergency management professional, A white paper*, Yale New Haven Health Center for emergency preparedness and disaster response.

Stauffacher, D., S. Hattotuwa and B. Weekes (2012), *The potential and challenges of open data for crisis information management and aid efficiency, a preliminary assessment*, ICT4Peace Foundation.

Sutton, J., L. Palen and I. Shklovski (2008), "Back-Channels on the Front Lines: Emerging Use of Social Media in the 2007 Southern California Wildfires" *Proceedings of the 5th International ISCRAM Conference*, Washington DC.

Sutton, J. M. (2009), "Social Media Monitoring and the Democratic National Convention: New Tasks and Emergent Processes", *Journal of Homeland Security and Emergency Management,* Vol. 6, Issue 1.

Thaler, R. and C. R. Sunstein (2008), Nudge, Yale University Press.

Tinker, T. and D. Fouse (eds.) (2009), *Special report – Expert Round Table on Social Media and Risk Communication during Times of Crisis: Strategic challenges and opportunities*.

United Nations Global pulse (2012), *Big data for development, challenges and opportunities*, www.unglobalpulse.org/sites/default/files/BigDataforDevelopment-UNGlobalPulseJune2012.pdf.

Veil, S.R., T. Buehner and M.J. Palenchar (2011), "A work in process literature review: Incorporating social media in risk and crisis communication", *Journal of contingencies and crisis management*, Vol. 19, Issue 2, pp. 110-122, http://onlinelibrary.wiley.com/doi/10.1111/j.1468-5973.2011.00639.x/pdf.

Vieweg, S., L. Palen, S. Liu, A/Hughes and J. Sutton (2008), "Collective Intelligence in Disaster: Examination of the Phenomenon in the Aftermath of the 2007 Virginia Tech Shooting", *Proceedings of the 5th International ISCRAM Conference*, Washington DC.

Wardell, C. and Y. San Su (2011), *2011 social media emergency management camp, Transforming the Response enterprise,* CNA Analysis and Solution, www.scribd.com/doc/72281369/2011-Social-Media-Emergency-Management-Camp-Transforming-the-Response-Enterprise.

Wendling, C. (2012), "What for social scientists in risk expertise?", *Journal of Risk Research*, Vol. 15, No.5.

William, R., G. William and D. Burton (2012), *The use of social media for disaster recovery, Lessons learned while creating and managing "Joplin Tornado Info" (2011) on Facebook and further implemented with "Branson Tornado Info" (2012), Missouri Flood Info (2011-2012) "US Tornado Info (2012) and others,* University of Missouri, http://extension.missouri.edu/greene/documents/PlansReports/using%20social%20media%20in%20disasters.pdf.

World Bank (2012), *Volunteer Technology Communities: Open development,* Global facility for disaster reduction and recovery, World Bank, www.gfdrr.org/gfdrr/sites/gfdrr.org/files/documents/Volunteer%20Technology%20Communities%20-%20Open%20Development.pdf.

World Meteorological Organisation (2012), *Guidelines on Strategies for use of Social Media by National Meteorological and Hydrological Services*, N°1086, www.wmo.int/pages/prog/amp/pwsp/documents/1086_PWS-24_NMHSs_report_en.pdf.

Additional online sources

Webpage on the X24 exercise: http://vizcenter.net/x24/more.html

Webpage Alert SA in use in Australia: www.alert.sa.gov.au/

Webpage of Public Safety Canada: www.publicsafety.gc.ca/index-eng.aspx

Webpage of US FEMA: www.fema.gov/

Webpage of the US Red Cross Safe and well: https://safeandwell.communityos.org/cms/index.php

Webpage of Twitcident: http://twitcident.com/

Webpage of the Swiss Federal office of civil protection: www.bevoelkerungsschutz.admin.ch/internet/bs/fr/home/partner/zivilschutz.html

Webpage of the EU MASSCRISCOM project: www.masscriscom.eu/default.aspx

Chapter 4

Strategic crisis management exercises: Challenges and design tools

This chapter discusses the challenges involved in designing crisis management exercises for strategic leaders. It offers a source of reference for countries and collaborating organisations and can be seen as a "toolkit" intended to facilitate reflective and effective future crisis management exercise designs in the future. This chapter first discusses the rationale, types and purposes of strategic crisis management exercises as part of building the right skill set for strategic crisis management. It highlights the main challenges of involving leadership, engaging partners from the private sector, and developing international crisis management exercises. Finally, it presents the parameters and options for scenario development, including case-based scenarios and options for involving and working with leaders.

Key messages

1. Developing the skills and capacities to manage and prepare for complex crises, as well as for unknown and "black swan" events, is key to effectively fulfilling leadership functions.
2. Strategic crisis management exercises are essential for developing and "stress-testing" the capacity of leaders to cope with novel crises and large-scale emergencies.
3. Engaging leaders in strategic crisis management exercises requires the design of dedicated exercises and for a convincing case to be made.
4. Exercise formats, designs and techniques should be adapted to the goals and purposes of a given exercise.
5. Good exercises should appear to be simple, while masking their complexity. There should be a theoretical underpinning and elements of surprise included.
6. Joint crisis management exercises can contribute to building efficiencies and trust between governments and the private sector, which is essential in many complex crises. Incentives and a good understanding of private sector constraints can facilitate private sector engagement.
7. Developing further international crisis management exercises is necessary for improving capacities to cope with the cross-border effects of complex and large-scale crises.

Over the last decade, OECD countries have experienced many highly stressful crises that have tested the abilities of societies and their leaders to withstand shocks. These events have revealed fragilities and vulnerabilities not only in the prevailing institutional frameworks, but also sometimes in the ability of strategic leaders to work effectively with their staff and organisations in fulfilling the tasks of crisis leadership. Such events serve as extreme tests of the ability of societies and communities to absorb and recover from shocks. Crises force strategic level decision makers to make some of the most consequential decisions in public life under the most difficult of circumstances. In order to rise to such challenges, leaders, their teams, organisations and key partners must be prepared to cope with the rigours and trials of contemporary crisis management.

Fundamentals of strategic crisis management exercises

Training professionals and leaders

It is increasingly recognised in many OECD and other countries that crisis/emergency/disaster management represents a field of specialised expertise. One approach to developing competence is to emphasise the need to educate and develop a cadre of professionals who are equipped to manage or facilitate the management of crises and emergencies (Stevens, 2013). Such a profession could depart from military, medical, legal, or other professional models. Professionalisation entails the identification of a body of knowledge, core skills, and standards, including a code of ethics. This can be helpful, but care must be taken to prevent the emergence of a static orthodoxy and excessive homogeneity. However, professionalisation is only a partial solution to a rather more complex challenge.

When facing major crises, partnerships between political leaders and professionals is essential. This means that political leaders who are not professionals must also be educated as to the nature of crisis management, informed of what is required of them in a crisis, familiarised with crisis planning and organisation, and equipped to engage in meaningful communicative interaction with others inside and outside of their organisations. Individual and collective crisis management skills are best acquired and honed through hands-on practice. While there is no substitute for real life experience, well designed and executed exercises allow leaders to hone their skills, familiarise themselves with (and identify gaps in) crisis planning, and make mistakes (and hopefully learn from them) when lives, legitimacy, and societal welfare are not on the line.

As noted in the UK Cabinet Office Guidance for Emergency Planning and Preparedness Exercises:

> *Planning for emergencies cannot be considered reliable until it is exercised and has proved to be workable, especially since false confidence may be placed in the integrity of a written plan. Generally, participants in exercises should have an awareness of their roles and be reasonably comfortable with them, before they are subject to the stresses of an exercise. Exercising is not to catch people out. It tests procedures, not people. If staff are under-prepared, they may blame the plan, when they should blame their lack of preparation and training. An important aim of an exercise should be to make people feel more comfortable in their roles and to build morale (UK Government, 2014).*

This chapter will explore the wide variety of powerful exercise designs and techniques (both traditional and technology enhanced) that are suitable for practicing and

developing strategic crisis management skills and stress-testing individuals and organisations.

Evolving exercise practice over time

Recognition of the need to practice and rehearse national and local level responses to rapidly emerging threats has a long history among the OECD and other countries. During the Cold War, preparations for military and civil defence/civil protection were conducted on both a unilateral and a multi-lateral basis (e.g. under North Atlantic Treaty Organisation [NATO] auspices). Over time, such exercises have evolved in keeping with the evolving risk, security, and European institutional landscapes. They have taken a variety of forms and developed in different ways in different countries. Much of the emphasis has often been on developing capability and practicing the skills, processes and procedures associated with operational/tactical level crisis management. As a result of these efforts, a body of knowledge and a community of practice have emerged.

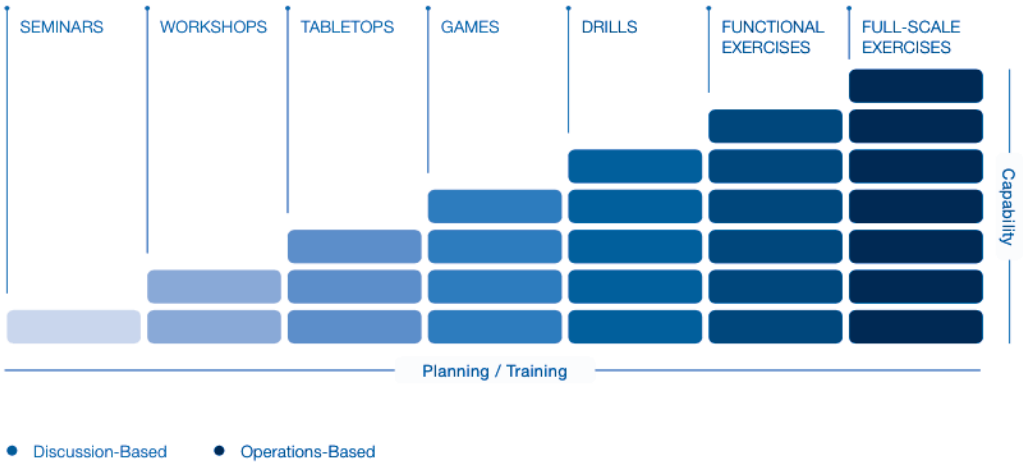
Significant attention has been devoted to developing techniques and designs for operational training and exercises in the public sector in both civilian (e.g. first responder) and military organisations (Crego, 1996; Crichton et al., 2000; Crichton, 2009). However, less attention has been devoted to the problems involved in designing crisis management training and exercises for strategic level leaders in governmental organisations; and existing practice varies in terms of quality and effectiveness (Borodzizc and Van Haparen, 2002). Furthermore, while small and relatively closed communities of experts in various countries have developed know-how in this specialised area, relatively little exchange of knowledge and good practice tends to take place as the topic is seen as sensitive and governments may be reluctant to share information about their actions and developments. Experts may regard their knowledge as best passed on through mentor-mentee communication and informal apprenticeships; and see their designs as proprietary trade secrets that are best left undocumented and un-diffused.

The first step in approaching and structuring this fragmented body of knowledge and experience in order to improve strategic crisis management exercises is to specify the exercise concept and a core skill set for strategic crisis managers.

Types and purposes of crisis management exercises

There are different ways to conceptualise crisis management exercises. The UK Cabinet Office defines these exercises as simulations of an emergency (or crisis) situation that have three main purposes: to validate plans (validation); to develop staff competencies and give them practice in carrying out their roles in the plans (training); and to test well-established procedures (testing). The multiple purposes of exercises will be further explored below.

Figure 4.1. Different types of crisis exercise



Source: adapted from Callahan et al (2008), p.52 http://www.businessofgovernment.org/pdfs/OBrienReport.pdf.

Figure 4.1.[1] depicts a ladder of different types of crisis management exercises at different levels of scale and complexity. Moving from left to right on the figure shows the shifting emphasis from classroom or seminar discussion about crisis management towards increasingly elaborate role-playing with emphasis on practicing/rehearsing procedures, processes and functions etc. While this figure emphasises operations, strategic elements exist for virtually all of the exercise variants mentioned. The most ambitious types of exercise design (termed full-scale exercises in the figure) may entail attempts to combine relatively realistic ("high fidelity") exercises at multiple levels up to and including the strategic level.[2]

The strategic crisis management skill set

Decades of research and close examination of hundreds of crises have helped identify the core crisis management tasks that tend to be associated with successful crisis management efforts (Boin et al, 2005). These are: sense-making, decision-making and co-ordination, meaning-making (strategic crisis communication), accounting, and learning.

Sense-making in a crisis refers to the challenging task of developing an adequate interpretation of what are often complex, dynamic, and ambiguous situations (Weick; 1988; Stern, 2014). This entails developing not only a picture of what is happening, but also an understanding of the implications of the situation from an organisation's vantage point and the vantage point of other salient stakeholders. According to Alberts and Hayes (2003: 102): "Sense-making is much more than sharing information and identifying patterns. It goes beyond what is happening and what may happen to what can be done about it." Prior to a crisis, sense-making is difficult due to attention scarcity, weak and conflicting signals regarding mounting threats, and a high degree of uncertainty. Once it is clear that a crisis has occurred, a combination of information overload and uncertainty/scarcity regarding key parameters is common.

Decision-making and co-ordination refers to the fact that crises tend to be experienced by crisis managers, first responders, and citizens as a series of "what do we do now" problems triggered by the flow of events. These occasions for decision emerge simultaneously or in succession over the course of the crisis (Stern, 1999; Stern et al., 2014). Protecting communities often requires an interdependent series of crucial decisions to be taken in a timely fashion under very difficult conditions. It is increasingly recognised that public sector resources (and traditional command and control capacities) are unlikely to suffice when dealing with larger scale, more complex and challenging contingencies. Recent experience of crises clearly demonstrates the power of social media and personal communications-based information to empower and potentially improve decision-making, and to enable more agile, flexible and decentralised forms of co-ordination. (See Chapter 3 for examples.) This is critical both for leveraging the potential of community-based responses via self-organising, and for managing interfaces between the public-sector, private sector and non-profit sector components of a whole-of-community/society response.

Meaning-making (crisis communication) refers to how crisis managers must provide relevant information in a timely fashion; attending not only to the operational challenges associated with a contingency, but also to the ways in which it is perceived and understood by various stakeholders and constituencies. Because of the emotional aspects associated with disruptive events, followers look to leaders to help them understand the meaning of what has happened and place it a broader perspective. By their words and deeds, leaders can convey images of competence, control, stability, sincerity, decisiveness, and vision - or their opposites. Social media channels - including direct social media based communication by leaders on platforms such as Twitter - have become key arena where information is exchanged and competing risk and situational assessments compete. A sound understanding of the discursive backdrop of citizens and opinion leaders' frames of reference is essential for formulating and implementing effective strategies for crisis communication.

Being accountable (Boin et al., 2005, 2008) refers to the demands placed on crisis actors to justify their actions prior to, during, and in the aftermath of major crises and emergencies. The following example questions are likely to be posed in a range of forums where accountability is discussed:

- Why was it not possible to prevent the crisis from occurring or more effectively mitigate the damage?
- Why was the organisation/society not better prepared?
- Why did delays, misunderstandings, mis-coordination, mis-communication occur?
- Why was the response not more effective, fair and legitimate?

Leaders and their staff need to be prepared and equipped to answer such questions in an effective and legitimate fashion if they are to avoid becoming victims of "blame games", which are increasingly common during and after crises (Boin et al, 2008).

Effective learning requires an active, critical process that recreates, analyses, and evaluates key processes, tactics, techniques, and procedures in order to enhance performance, safety and capability etc. The learning process begins with the production of a "lessons learned document". In order to bring the learning process to fruition, change management/implementation must take place in a way that leaves the organisation with

improved prospects for future success (Boin et al., 2005; Stern, 1997; Deverell and Olsson, 2009). Leaders and organisations must cultivate the capacity to learn from experience so that they can formulate and then implement effective reform strategies and programmes.

Exercises can be specifically designed to cultivate and practice the skills associated with each of the above crisis leadership tasks, drawing on both traditional and state of the art interactive instructional designs. Sense-making exercises - such as the Swiss Federal Chancellery's Rapid Reflection Exercises, and the case-based low-medium fidelity exercises developed by the Swedish National Center for Crisis Management Research and Training (CRISMART) - can be very useful to cultivate crisis "diagnostic" and strategic problem solving skills associated with sensemaking.[3] Other exercises can be designed to elicit decisions and present leaders with crisis co-ordination problems to be solved. Crisis communication exercises can provide opportunities for leaders to practice motivational and emotional forms of leadership, show empathy, and practice rituals of contrition, mourning, or remembrance against the backdrop of social media and the increasingly globalised 24-hour news cycle. Exercises can be crafted to help leaders prepare for the rigours of post-crisis accountability forums (legislative, judicial, or other) or to better equip leaders and their organisations to extract and implement lessons learned from crisis experiences.

Training challenges associated with the new crisis landscape

In this section, three types of challenges associated with strategic crisis management exercises will be discussed: 1) working with strategic level leaders; 2) conducting exercises across sectoral boundaries, emphasising potential obstacles to be overcome from bringing in private sector actors; and 3) conducting international exercises.

Involving Leadership

Leaders have an indispensable role to play in strategic crisis management and must be prepared for leadership tasks such as sense-making, strategic decision-making and meaning-making. Effective performance under the extreme conditions associated with a crisis requires leaders and their advisors to function well individually and together. However, strategic level leaders (those working at the top level of their government or other organisations) are a particularly challenging target group to engage in crisis management exercises, as explored below.

Today's leaders face tremendous demands and often keep challenging schedules. Their time and attention are scarce resources and competition for them is fierce. Time spent preparing for future crises is time not spent on current challenges and proactive policy making. Leaders (or those who manage their schedules) may feel that they are too busy to participate in crisis management training and exercises. They may not be aware of, or choose to disregard, the immense cost of being unprepared when a crisis occurs.

Leaders, or those that help prioritise their agenda, may be overconfident regarding the ability of leaders and their staff to cope with future crises. Some leaders may not wish to participate in simulations/exercises for fear of setting expectations and precedents through choices made or priorities revealed in scenario exercises. However, this fear is often exaggerated as the alternative option - leaving others in persistent uncertainty about the likely direction of normative leadership from strategic leadership - is likely to have far worse consequences for preparedness.

Other leaders may be insecure about their ability to perform under the pressure of a crisis and will avoid the "hot seat" in exercises in the hope that a crisis will be manageable if it should arrive in reality. However, a better coping strategy would be for leaders to seek to equip themselves for future challenges by embracing crisis management training and opportunities to practice under "safe" conditions.

Leaders may choose to opt out of exercise programmes entirely as a result of their fears and insecurities. This may have serious consequences as gaps may emerge between the frames of reference of key subordinate actors (who have actively familiarized themselves with and practiced using. the crisis management arrangements) and senior leaders (who have not). Understandably, leaders unfamiliar with existing, sound, arrangements for crisis management may be inclined to deviate from them when they are needed most.

When leaders do participate in exercises, their high position in the hierarchy may cause other difficulties. Other players, some of who may not be used to working with strategic leaders on an everyday basis, may be inhibited by the fact that powerful leaders are present and may be reluctant to express opinions on controversial issues. Various conformity dynamics documented in the literature (e.g. compliance and anticipatory compliance behaviours, 't Hart, 1994; 't Hart et al., 1997) may emerge in exercise environments. If detected and brought to the attention of participants this can pose a learning opportunity. However, if not addressed it may undermine the process and outcomes by reinforcing bad habits and tendencies towards "yea-saying".

Facilitators and evaluators during training exercises may also need to present criticism to strategic leaders and their powerful aides/advisors, which can be difficult and personally risky. Not all facilitators and evaluators will feel comfortable speaking truthfully, which could mean that, potentially improvable individual or collective deficiencies in preparedness for crisis management may go unremarked and uncorrected, with potentially devastating future consequences for real events.

Leaders vary in terms of their willingness to hear, absorb and act upon constructive criticism. Those who are intolerant of criticism and dissent and surround themselves with "yes" men and women are less likely to get candid feedback in training and exercise sessions. Those who encourage and reward candour - protecting rather than shooting messengers bearing reports of vulnerability and areas with room for improvement - will get more honest and actionable feedback and tend to have better prospects for future success.

It is not uncommon for training and exercise efforts to develop in a bottom up way: starting with operationally challenging events and then progressing to involve strategic leaders. Furthermore, because operational level emergency/crisis management training tends to be better established, scenarios and designs may be optimised for operational leaders. In such cases, strategic leaders may not be presented with problems that challenge and engage them, which turns them into spectators rather than active partners in integrated strategic/operational crisis management. Such experiences may make leaders disinclined to participate in future exercises and may lead them to misunderstand and underestimate the role that they may be called upon to play in future major events.

Involving the Private Sector[4]

It is increasingly recognised (OECD, 2014) that a whole-of-government approach to crisis management and disaster response is insufficient. Responding to highly complex,

large scale crises (especially the "maximum of maximum" scenarios), as well as smaller events with trans-sectoral impacts, is likely to require the mobilisation of whole-of-society efforts for response and recovery. Active private sector participation in the management of such crises is essential.

Following the public administration reforms and privatisation trends that have taken place in OECD countries in recent decades, governments tend to have fewer ways of directly managing a crisis than they did in the past. Governments now need now to work in partnership with the private sector to respond to crises; in particular with the operators of critical infrastructures, the transportation industry and providers of critical emergency supplies. For such partnerships to work well in times of crisis, it is essential for both sides to get to know each other and learn how to communicate in order to solve problems together.

Involving the private sector poses significant challenges to designers and organisers of strategic crisis management exercises. For example, how can governments motivate (and create incentive structures) for private sector actors to invest time and resources in government-driven preparedness processes and exercises? While regulatory obligations may be a possibility in some contexts, participation will often rest on corporate social responsibility and the government's ability make a "business case" for participation.

Selecting corporate partners for exercises may also be difficult. Who should participate and what mix should there be among large, medium, and small enterprises? There may also be fairness concerns. For the purposes of the exercise it may only be necessary or advisable to have a small number of representatives from a given industry, or even the private sector as a whole. Competitors or other organisations not included may feel that they have been left out or that those participating are receiving unfair advantages.

When corporations are willing to participate, securing the participation of persons at the right level or with the right background may be difficult. As with public sector leaders, top corporate leaders have overloaded schedules and many competing demands for their attention.

Corporations may be reluctant to participate in exercises if participation could require or pressure them to reveal information about vulnerabilities or internal processes that they would prefer to keep confidential. Similarly, there may be concerns that participation could lead to unflattering portrayals of the firm and involve a risk of damaging the brand, reputation and valuation etc.

Other potential concerns include:

- Secrecy and classification rules (from a public sector perspective).
- Risks of disclosure of proprietary information (from the corporate perspective).
- Differing levels of corporate commitment and competence with regard to intra- and inter-organisational exercising.
- Barriers to communication deriving from language and professional terminology/jargon/acronyms.
- Trust deficits in relation to the public sector in some countries/industries.
- Sensitivities related to the relationship between regulators and the regulated (or the tax collectors and the taxed).

- Potential legal risks and liabilities associated with the identification of vulnerabilities, preparedness gaps and involvement in multi-sector crisis responses etc.

Despite these obstacles, which can be and regularly are overcome, the active participation of the private sector in strategic crisis management exercises is extremely important.

Involving international partners: Bi-multi-lateral exercises[5]

As many crises do not recognise national borders, international co-operation in crisis management is imperative. Working across national boundaries in bi-or multi-lateral configurations requires getting to know other actors and finding opportunities to practice and test preparedness and collaborative ability. Exercises take place regularly under the auspices of organisations such as NATO and the European Union, and other regional or global international organisations. International exercises targeted at the strategic level may be particularly difficult to design, arrange, and implement.

There are various obstacles and challenges to be overcome regarding international exercises. For example, participants in international exercises are likely to exhibit particularly pronounced differences in various respects that can impact on strategic crisis management exercises. They are also likely to differ in terms of their perception of the most important threats and risks: a scenario or issues within a scenario that are highly relevant and salient for one country may be of little interest to another, which greatly complicates scenario selection and development. Participants may have very different levels of prior preparation, skill, and experience.

Another challenge in preparing exercises is that countries have very different institutional arrangements for crisis management in terms of governmental structure; the division of responsibility; labour; and resources among public, private and non-profit sectors. Understanding who should be included and the appropriate national focal points for participation can be demanding, particularly for novel crisis scenarios where such issues may not have been adequately considered within and across countries. Exercise development may be challenged by issues of organisational or technical inter-operability and information sharing among nations. However, conducting training exercises provides valuable opportunities to identify and overcome these challenges.

Other important challenges and obstacles include:

- Political sensitivities related to real world interests and conflicts among actors.
- Political sensitivities related to scenario roles (victim of or responsible party for an attack), accident or disaster recipient (e.g. host country) or helper (provider of assistance).
- Secrecy and classification rules.
- Building trust.
- Barriers to communication deriving from language and professional terminology/jargon/acronyms.
- Participants may be from different levels and organisations in their respective countries.

- Different levels of prior knowledge, skills, preparedness in general and with regard to specific contingencies.
- Different cultural and historical frames of reference, and different cultures with regard to participation in exercises and evaluation.

Exercise design and scenario development

Key parameters associated with exercise design and scenario development are identified and explained in this section. Good practice associated with involving leadership and the potential of technology for overcoming challenges and improving scenario quality and efficiency of development is discussed.

Exercise and scenario design parameters

This section presents some key parameters of exercise design and highlights good practice for coping with some of the challenges of developing training exercises for different purposes. These design parameters are summarised in and explained Table 4.1. and explicated below.

Table 4.1. Exercise and scenario design parameters

Purpose	Learning	Testing
Group	Homogeneous	Heterogeneous
Constellation	Leader solo or with advisory group	Leader and additional levels of the organisations
Fidelity	Low	Medium or High
Player/group interactivity	Low	High
Technology	Low	High
Scenario openness	Open	Closed
	Simple	Complex
Relationship to scenarios	Analysis and discussion	Role play and practice of tasks/skills.
Player roles	Uniform	Differentiated
	Stipulated	Natural
Context and setting	Hypothetical/masked	Natural
Exercise time	Real time	Game time

Purpose: refers to the purpose of the exercise. Broadly speaking, purpose can be divided into two categories: learning and testing exercises. Learning exercises are intended to raise awareness of issues; improve knowledge of the crisis organisation, plans, procedures, protocols etc.; and develop/maintain crisis leadership skills. Testing exercises are designed to probe individual, group, and organisational preparedness and identify areas of strength and vulnerability that can be addressed by remedial actions.

Group: refers to the composition of the group participating in an exercise. Homogeneous groups are composed of participants with similar roles/functions, levels of seniority or organisational affiliations. Heterogeneous groups are composed of participants with different roles/functions, levels of seniority and organisational affiliations. Hybrid compositions are common, for example, a cabinet level exercise focusing on principals (cabinet secretaries or ministers) would be relatively homogenous with regard to level of seniority, but heterogeneous with regard to participation from

multiple departments or ministries. Both homogeneity and heterogeneity have advantages and disadvantages with regard to the exercise experience. Design choices should be linked to the purpose of the exercise.

Constellation: refers to the selection of participants. For example, exercises focused on developing the crisis management capacity of strategic level leaders could involve scenario-based dialogue between the leader and one or more instructors or "coaches", or the leader with a small group of key officials. Alternatively, the top-level leader or leadership group can participate as part of a broader effort that involves a much larger body of participants.

Fidelity: refers to the degree of detail and realism associated with a scenario exercise. Low fidelity exercises involve relatively brief, abstract, and general descriptions of a scenario. These exercises are often used to generate discussion and experience sharing among experienced, qualified practitioners who have a solid frame of reference and can "go beyond the information given" in useful ways. High fidelity exercises involve the production of detailed, highly realistic, often case or risk analysis based scenarios grounded in deep contextual knowledge about the organisation(s) in question and the threats, risks, and hazards they face. High fidelity exercise scenarios often involve the creation of a relatively realistic (and fragmented) information flow involving government, stakeholders, and media-generated communications and documents. Medium fidelity exercises fall somewhere in between low and high fidelity exercises.

Player/group interactivity: refers to the extent to which players and groups interact with each other and through player/team initiatives to request information during game play. In low interactivity designs, player interaction is primarily in the form of discussion of a scenario. In high interactivity designs there is more role- and/or team-based interaction among players within or between groups. In high interactivity designs, game play and dynamic interaction progress through the revealing of pre-prepared elements that portray an unfolding situation, persuasion attempts, bargaining, and other forms of public or behind the scenes communication. More interactive designs often work well with less elaborate (e.g. medium fidelity) scenarios as the players themselves provide much of the mutual stimulation in the exercise.

Technology: strategic crisis management exercises vary greatly in terms of how much they depend upon and exploit the potential of technology. Well-designed (low tech) exercises with compelling scenarios may be delivered using paper handouts, PowerPoint, or email. These relatively simple and inexpensive means can provide a valuable exercise experience for participants, however, where resourcing permits, technology has the potential to enhance the effectiveness, efficiency, accessibility, pedagogical potential, documentary record and emotional impact of exercises. For example, exercise management software platforms may be used to choreograph and manage the delivery of elements in high fidelity designs for large numbers of players. Technology may also be used to enable players to participate in activities at a distance or to participate individually at a time of their choosing.

Technology can help to overcome conformity pressures (such as fears of antagonising peers or superiors) by enabling anonymous suggestions regarding problem diagnosis, strategy and tactics. It can also enable more candid communication about individual or collective performance and lessons learned etc. Multi-media techniques, such as still images, audio and video, can enhance the exercise experience and complement text based information. For example, simulated traditional media broadcasts (e.g. from television and radio) and web-based social media can enhance the realism and facilitate emotional

and professional engagement in an exercise. However, these measures also increase costs. Modelling, simulation, and visualisation technologies may be used for decision support in scenario development and presentation and to provide real time or post-exercise feedback regarding the implications of actions taken or not taken at various points in the exercise.

Scenario openness: scenarios can be open or closed. The scenario trajectory and outcome of closed scenarios are pre-determined, meaning that the course of events in the exercise cannot be changed by player deliberations or actions (this is often not apparent to the players if the scenario is skilfully constructed and presented). In open designs, multiple trajectories and outcomes are possible. These may consist of a limited number of predetermined outcomes (e.g. branches in a decision tree) or, in very open designs, scenario trajectories may arise in an unconstrained fashion from the creative problem solving, bargaining and other interactions among players and teams. More open designs tend to require considerable pre-exercise research and/or well developed "exercise "control cells" staffed by subject matter experts or access to stand-by networks that enable game controllers to access expertise in real time to credibly cope with unanticipated initiatives and information requests from players.

Relationship to the scenario and player roles: some exercises are designed to stimulate analysis and discussion of a contingency or specific scenario. In such exercises, players tend to relate to the scenario from an "intellectual distance" and discussions are likely to involve consideration of implications and problems, division of responsibility and labour, and organisational processes. Participants will talk about rather than practice crisis management. In other exercise designs, players will engage with the scenario through a given set of roles (either actual ["natural"] organisational roles or hypothetical roles stipulated in the exercise) and tasks. This gives players the opportunity to practice crisis management skills, processes, procedures and problem solving. This may be done in real time or under time pressure in order to simulate the pressures associates with real world crisis management. Stipulated roles in an exercise can either be general and uniform (all players play the same broadly defined role such as "advisor to the Prime Minister" or "member of a senior inter-agency working group") or highly differentiated. In the latter case, participants may be assigned roles associated with different countries, organisations, or functions within an organisation. Manipulation of role descriptions, contextual information and information provided during the exercise can then be used to create incentives for co-operative and competitive/conflicting behaviour in the exercise.

Context and setting: crisis management exercises may take place either in hypothetical, masked, or natural settings. Hypothetical or masked settings may be helpful for sidestepping sensitive political or jurisdictional issues and creating a level playing field. For example, in an international exercise it may be convenient to set a simulated crisis in a fictitious country/region rather than privileging (or disparaging) a particular set of participating countries. Setting an exercise in a hypothetical context and setting also provides exercise designers and scenario writers with a certain freedom regarding their control of the behaviour of non-player actors, natural or anthropogenic events, and political/organisational contexts. Working in hypothetical settings can help to focus player attention on problem solving and skill development and help prevent them from getting bogged down in distracting discussions regarding details of the legal framework, rules or procedures that may not be relevant to the primary purposes of the exercise.

Masked scenarios are closely related to hypothetical settings (they are often the direct or indirect inspiration for hypothetical settings). Masked scenarios (or teaching cases) generally depict contexts and situations derived from current or past historical settings,

but with the names or other identifiers changed. Depending on the purposes and circumstances of the scenario, masking may be light, where the source of inspiration is relatively easy to identify, or heavy, where it is difficult to identify the original cases, actors and events that inspired the scenario. For some exercises, the mask may be maintained during the exercise but unmasked during a debriefing session in order to contrast the behaviour of the participants in the exercise with the choices and outcomes associated with the case or cases that inspired the scenario. For example, during the June 2014 OECD Swiss Federal Government Workshop on Strategic Crisis Management Exercises in Geneva, a demonstration scenario involving the escalation of a regional conflict and cascading effects for critical energy and transportation (primarily aviation) security was presented. The research-based scenario was inspired by a number of real world cases as well as contemporary risk and vulnerability analyses from different countries.

Exercise time: exercises may be played in real time or game time. An advantage of playing in real time is that it is possible to practice crisis analysis and skills while working under realistic time pressures. However, in an exercise lasting hours or days it may be difficult to get an overview of the entire trajectory of a crisis. Some exercise and scenario designs involve time compression or the ability to fast-forward through the development of a crisis to examine a situation through its various phases of escalation and de-escalation. Thus game time may be set to elapse either faster or slower than equivalent events in real time. Hybrid designs exist whereby some phases of the crisis are played in compressed game time and certain role-playing activities and tasks are rehearsed in real time.

Case-based scenario development

A common problem in many OECD (and other countries) is that participants in training and exercise events often "fight" the scenario and question the realism and relevance of the hypothetical events and problems presented. This may be due to enduring psychological, organisational or political defence mechanisms, or to an imperfect understanding of the methodologies used and the purposes of training events and exercises. It may also derive from the use of sub-optimal scenario development techniques.

Certain types of "attacks" on scenarios can be prevented or countered by using modelling and simulation to help formulate the contingencies presented to participants; thus demonstrating that the scenario rests on a systematic, state of the art scientific foundation. Modelling and simulation-based scenarios have clear advantages in terms of boosting scientific credibility and can greatly contribute to improving training, exercise and decision-support tools. However there may still be challenges in terms of the plausibility of the assumptions underlying the models and their applicability to various real world contexts. Reconstructing historical and contemporary cases using state of the art qualitative case research methodologies, such as process tracing and structured, focused comparison, has the potential to further improve scenario quality and relevance. The concepts of quality and relevance are explored below:

- **Quality**: using hazard/threat development trajectories and impacts based upon real cases has the advantage of relatively high external validity. In other words, the point of departure (or in some circumstances the complementary source of inspiration) for developing the scenario is an event that has occurred at a real place at a particular point of time and for which credible documentation exists. As

a result, when players become defensive and question the scenario's plausibility scenario there is proof that the problem is realistic and based on real, historical/contemporary events. This is extremely effective in countering attacks on the scenario and can increase the engagement of participants and enable them to refocus on the main purposes of the training/exercise.

- **Relevance**: a common problem in creating training and exercises for strategic leaders is developing scenarios that they will find fresh, interesting, challenging, and relevant to their roles and needs. This may be because exercise scenarios are often developed by people with operational or technical backgrounds and orientations who may have a limited insight into the worldviews, frames of reference and concerns of strategic leaders. Scenarios may also be developed with both strategic and operational levels in mind. However, even extremely challenging operational scenarios may be of little direct interest to strategic decision-makers, for example, when the obvious course of action is straightforward delegation to the operational level.

The research strategy deployed at the Swedish National Center for Crisis Management Research and Training (CRISMART) has explicitly focused on strategic crisis management (and the interplay between strategic and operational levels) in international, national, regional, and local contexts. The research effort, which includes extensive interviewing, observation and debriefing of leaders and advisors in crisis situations/simulations, is geared towards identifying and reconstructing decision problems faced by leaders in actual crises (Stern and Sundelius, 2001; Stern et al, 2014). As such, the case bank (and parallel work in the crisis studies literature) provides real world problems and challenges that strategic crisis managers have faced in the past. Furthermore, the focus of the effort has been to capture experience not only from high profile events (e.g. 9/11, the 7/7 Bombings and Hurricane Katrina, Norway 2011 terrorist attacks) from the United States and United Kingdom, but also from many lesser known cases taking place in Australia and New Zealand and smaller countries from across Europe, Asia and the Americas. As a result, many of these cases - though characterised by considerable problem complexity, diversity, and drama - may be relatively unfamiliar to participants in training and exercise events and thus easily masked. At appropriate points, it becomes possible to compare the strategies and solutions adopted by players (and the anticipated consequences/outcomes) to those revealed in the underlying real world cases. Use of this development strategy has an excellent track record of producing scenarios easily accepted and appreciated by strategic level leaders. [6]

Case-based scenario generation facilitates the rapid development of high quality scenarios at a relatively low cost. This is particularly the case when ongoing research efforts can be harvested for a variety of research and (applied) educational purposes, including the development of training and exercise tools. Although older (and relatively forgotten) cases can be very useful in scenario development, it is essential to continue documenting experiences in contemporary socio-technical and political contexts. While many crisis management challenges derive from enduring aspects of the human condition, others are driven by evolving threats and vulnerabilities and changing governmental/governance/community and socio-technical contexts. It is critical for researchers, as well as designers and developers of crisis management, to incorporate these developments into their work.

Involving and working with leaders

Emphasise the difficulty of the crisis management task

Strategic crisis management under contemporary political, organisational, and societal conditions has many challenges. Although strategic leaders often bring great ability, talent, skills, and experience, crisis management involves strong competing opinions and difficult decisions in extreme circumstances. Performing well under the stress of crisis conditions is facilitated by cultivating crisis leadership skills and regular practice in real and/or simulated events (Boin et al., 2005: 153-154). Crisis decision makers and communicators can hone their skills through coaching, feedback, and reflection upon their performance in practice and competition (Russo and Shoemaker, 1990; Stern, 2013).

The need for a tailored approach

Success in this area requires a rich set of tools and design templates. Crisis management training and exercises for strategic leaders should be consciously and explicitly designed and adapted to the specific purpose, target, and time (including leaders' availability) and resources available for the effort.

Exercises may be designed primarily to explore a theme and familiarise leaders with parameters, actors and stakeholders, distributions of responsibilities, and capabilities associated with a particular issue or threat. They may be designed to test a particular crisis plan in order to identify gaps, faulty assumptions, and areas for further development. They may also be used to help develop skills and/or fluency with particular processes, protocols, or systems. These different purposes are often best served by different exercise designs and formats.

Exercise designs (and associated briefings and educational activities) should be adapted to the leader or group's experience and skill levels. Approaches appropriate for a new leader with little past crisis management experience may not work as well for a veteran leader with a wealth of experience and a well-developed crisis management skill set. The US Department of Homeland Security's Mobile Exercise Team (MET) executive education format is a good example of a discussion-based design that has been well received by many newly elected mayors and governors, their staff, and other collaborating officials over the life of the programme.[7]

Training and exercise designs for strategic leaders should take into account leader personality, learning and management styles. The literature on presidents and prime ministers (Daleus, 2012; Preston, 2001; George and Stern, 1998) demonstrates that leaders may have very different cognitive, learning and policy-making styles. Choices regarding how much information to include in crisis management exercises and in what way the information should be provided may depend in part upon these factors. Some leaders may respond best to written information while others may prefer oral briefings or videos. Strategic leaders may vary in terms of their comfort level regarding technology: some may enjoy technology and want to see and use it themselves; others may be better served by hiding the technology "back stage".

The availability of leaders in terms of time and geography can impact on training and exercise design. Shorter windows of leader/senior official availability often suggest using simpler, lower fidelity designs. Bigger windows of time enable the use of more elaborate medium or high fidelity designs that more realistically simulate intra-and inter-

organisational processes and involve greater numbers of supporting functions. If it is difficult to gather leaders in one place or at one time, the introduction of technology for distance participation and/or asynchronous game design (explored below) may be indicated.

Societal, organisational, training and exercise-specific cultures impact on training and exercise design choices. For example, organisations vary in terms of the extent to which senior officials are willing and expected to be subjected to evaluation and criticism. For some organisations, exercises aimed at testing preparedness or capability may be unheard of. Whereas other organisations (e.g. the military in many countries) train regularly and see it as an integral part of readiness for leaders and operational staff alike. For some militaries, particularly in periods of relative peace, real action may be rare and exercise settings a key source of leadership experience. By contrast, first responder organisations may see smaller scale action on a daily basis and train/exercise far less often, although even in these organisations major novel crises that fully challenge the coping capacity of strategic leaders are rare. "High reliability" organisations known for their vigilance, adaptability, and safety culture (LaPorte and Consolini, 1991) tend to value and prioritize rigorous training and exercise, evaluate performance at all levels (including that of strategic level leaders), and take prompt, proactive remedial action on the basis of training and exercise results.

Feedback and follow up

Well-designed and implemented exercises, and associated educational activities, can generate valuable information regarding preparedness gaps and vulnerabilities. This information should be documented, analysed, and used as the basis for remedial measures and/or organisational reforms. Lessons identified in crisis training and exercise sessions should be lead to enhanced individual and collective preparedness. Leaders run the risk of serious failures in future real crises if identifiable issues are not addressed, however, there may be significant legal and political obstacles and disincentives for strategic leaders to fully benefit from feedback.

There needs to be further exploration of measures for assuring confidentiality and legal protection of such information, while still allowing information to circulate to those with a legitimate need to know. Efforts are underway in many countries to improve learning from both real and simulated events,[8] but, as noted above, crisis management exercises for strategic leaders are particularly challenging in this regard.

Box 4.1. Providing feedback through a self-critique questionnaire

Providing feedback to strategic leaders is a sensitive, difficult, and potentially risky task. Organisational cultures in which strategic leaders are expected to participate and receive feedback should be cultivated. Leaders who do not want honest feedback (and who punish those giving it) are not likely to receive feedback. Good practice is often to start with self-critique, where facilitators ask participants questions such as:

- What went well today and what went less well?
- What was most challenging?
- What was most surprising to you?
- What would you do differently next time?
- Which tasks associated with the exercise do you feel most comfortable with and which were most challenging?

Such questions can open the way for a critical discussion of performance, general preparedness and preparedness gaps, and areas where additional practice and skill building might be appropriate.

When feasible and appropriate, feedback from the participants themselves can be complemented with feedback from peers and/or expert evaluators. Finding peers of strategic level leaders (particularly top national leaders) is likely to be difficult and may be prevented by a variety of political or organisational rivalries and sensitivities. In some cases, recently retired officials or others with insight into the office in question may be appropriate sources of peer feedback.

For strategic leaders willing to receive feedback, it is important to carefully choose timing, venue, and the mix of positive and negative feedback. In some cases it may be best to provide feedback immediately following an exercise. Immediate feedback may be the only opportunity if there are likely to be difficulties in getting the leader's attention at a later date. However, if the exercise has been dramatic and emotionally or physically draining it may be that more sensitive or critical feedback is better given later, after participants have had time to process and recover from the experience Critical feedback may be best undertaken privately, when possible, or with just a few trusted advisors present. Feedback can also be presented in writing, although sensitivities and the need for secrecy may prevent that possibility.

It is important to try to balance positive and negative feedback carefully. A series of negative criticism is likely to provoke defensive reactions, while a balanced treatment which gives due credit for things that went well tends to help participants absorb feedback about areas in which there may be room for improvement. This may entail prioritising and focusing on the most important areas, and other less significant critical observations may have to wait for another opportunity.

The use of technology in training exercises

Significant obstacles must be overcome if training and exercises for strategic leaders are to take place and be a meaningful and constructive experience for leaders, their advisers and their organisations. Making use of current and emerging technology has great potential to help overcome many of these obstacles.

Gathering leaders and scheduling exercises

Getting firm commitment from a single leader to participate in exercises is often difficult, and getting an entire leadership team in one place may be particularly challenging. Technology enhanced training and exercise techniques enable participation by individuals who may be geographically dispersed. For example, US FEMA's Emergency Management Institute has successfully deployed communications technology to enable remote participation in table-top exercises. The STANCE concept, developed by the US Naval Post Graduate School at the Center for Homeland Defence and Security, allows participants to take part in policy simulation exercises from diverse geographic locations at a time of their own convenience. This possibility is a function of STANCE's asynchronic design and could potentially be incorporated into other forms of training and exercise. This development could enable participation in exercises that take place over extended periods (weeks or months rather than hours or days), which would not usually be feasible for strategic leaders and others with very heavy time constraints.

Overcoming hierarchy and constraints on candid communication and integrating feedback

Giving honest feedback to those in power may be challenging for subordinates and for those tasked with debriefing an exercise or formally evaluating the results. Technology can provide a means of facilitating open, candid conversations. For example, the Massive Multi-Player Online Wargame Leveraging the Internet (MMOWGLI) platform, developed by the US Office of Naval Research and Naval Post Graduate School, enables broad based participation in policy games in which the use of anonymous participation enables players to freely express opinions without fear of sanctions. This approach would be well suited for use in larger exercises and a good way of accomplishing the "360 degree" evaluation of leadership that should take place at all levels of an organisation, including the strategic level (Maxwell, 2006; Marcus, Dorn and Henderson, 2006). MMOWGLI can aggregate, weigh, and integrate the perspectives expressed by a substantial number of players and/or observers of exercises.[9]

Improving scenario quality, impact and development efficiency

Modelling, simulation, and geo-spatial visualisation technologies, such as those demonstrated in the US Standard Unified Modelling and Simulation Toolkit (SUMMIT) Project[10] and the European Union FP7 INDIGO,[11] provide enhanced opportunities to develop and present scenarios in a more rigorous, visually compelling and plausible way. Drawing upon state-of-the-art hazard models (hurricanes, floods, earthquakes), SUMMIT provides an excellent point of departure for scenario development and is a good complement to scenarios based on real life crisis cases. Using tools such as SUMMIT is a good way of bringing science into the exercise development process and can greatly enhance the credibility of scenarios for operational and strategic leaders.

The use of geo-spatial visualisation technology, such as that used in the SUMMIT and INDIGO platforms, can help to accurately convey complex situational information in a visually compelling way. However, the information needs of strategic leaders is often different from those of operational decision-makers, and care should be taken to deploy technologies in ways that will facilitate strategic crisis management and not tempt strategic leaders into operational territory. Integrated modelling and simulation technology, such as the SUMMIT portal and model bank, can help to bring down costs

and reduce the need for specific hazard subject matter expertise in scenario development and exercise control.

Providing feedback on alternative crisis development and response/recovery trajectories

Real-time modelling, simulation and visualisation technologies help to provide enhanced scenario flexibility, interactivity and impact in preparation and delivery. For example, they allow for hazards to be modelled at various levels of severity (e.g. hurricanes of different wind speed categories) and geographic trajectories (e.g. alternative storm surge patterns). It also becomes possible to vividly demonstrate the consequences of proactive versus reactive strategies for interventions. For example, in a public health emergency event, it is possible to show the consequences of the different timing and scope (e.g. narrow definition of risk groups, broad definition of risk groups, whole population) of vaccination strategies or other medical countermeasures (e.g. social distancing). This can be a powerful pedagogical tool in crisis management training and exercises for strategic leaders.

Designing exercises and exercise programmes for strategic leaders

There are a variety of ways to engage strategic leaders and their staff in crisis management, training and exercises. The following questions can inform exercise design.

- **Who is the target group for strategic crisis management exercises?** Those responsible for crisis management should be as well equipped as possible for the challenge. Leaders must be convinced to take the time to prepare and practice for crisis management, and they must be provided with state of the art training and exercise experiences that are well adapted to their needs. However, this approach should be complemented with a broader, longer term strategy that also emphasises reaching those who support and advise leaders. Efforts should be made to reach not only today's strategic leaders, but also those who are making good progress in their government (or other relevant sector) careers and may be in strategic leadership positions in the future.
- **Should training be delivered in house or offsite?** There are advantages to both training taking place in the locales where strategic leaders generally work (in situ), and to removing leaders from their everyday environment. Conducting activities in situ tends to enhance realism and provide broader access to the supporting context and infrastructure that are most likely to be used in a crisis. Leaders, and many other key players, will already be in place and special travel arrangements will not be necessary. However, it may be more difficult to maintain focus on training or exercises if the leader is an environment where he or she can easily be interrupted by subordinates with questions relating to on-going matters. Holding the activity offsite in an educational institution or conference facility (especially one with limited cell phone access) may help organisers maintain relatively undivided attention. In some cases it may be advantageous to hold an activity in a location that hosts a particular training/exercise infrastructure or that is convenient for instructors/exercise facilitators (thus reducing their travel costs). It may sometimes be possible to hold events in places that have a symbolic significance or other positive quality (e.g. natural or architectural beauty, post event recreational potential), which may make it easier to attract and retain participants.

- **How should participants be selected and grouped?** Working in an intra-organisational way and grouping leaders with advisers, aides, and other subordinates has advantages as they are groups that are likely to engage in future crisis management. The US DHS/Naval Post Graduate School METS (Mobile Executive Training Seminar) programme for governors and mayors uses this approach with the training and scenario exercises delivered in state capitals and other major cities in the United States.12 However, such groups can be very hierarchical and may be inhibited by conformity or conflicts brought with the participants. An alternative approach is to work in homogenous groups of peers across agencies or organisations, for example principals from various departments or press secretaries from all of the ministries. Such groups often gather individuals of similar professional backgrounds and formal seniority and face similar challenges. These groups are often very good for identifying current problems and identifying/exchanging good practice. They may take place within or help to develop networks and familiarity (personal and organisational) across agencies. Network building is often a valuable secondary benefit of training and exercise activities. A third approach to training group selection is to work with heterogeneous and diverse groups with individuals drawn from various organisations (e.g. public, private, non-profit, federal, state, local government) and functions. Optimising training and exercises for highly diverse groups is often challenging, but the benefit of bringing eclectic groups together is that they represent a cross-section of society and may lead to valuable enhanced awareness of other levels and sectors.
- **Should educational (training and exercise) efforts be short term and ad hoc (e.g. one off events) or longer term, programmed, and cumulative?** Accessing strategic leaders is difficult and even brief and isolated engagements can be very valuable. However, there are significant benefits from sustained efforts to widen and deepen competence in preparedness for leadership tasks to cope with various types of contingencies. At the opposite end of the spectrum from single training sessions are degree-granting programmes (such as those offered by the Swedish National Defence College and the Naval Post-Graduate School), which enable sustained cumulative interaction. While such programmes are generally too time consuming to be feasible for top-level national government leadership, they can attract rising mid-level officials and those participating in strategic leadership groups at other levels of government. In between one day training and degree programmes are options such as multi-day or multi-week courses, and other forms of shorter, regularly scheduled sessions on a monthly, quarterly, or yearly basis.
- **What types of teaching and learning strategies are likely to be most effective?** Multiple strategies and tools for training strategic leaders should be deployed. Traditional briefings, lectures, and "war stories" by other strategic leaders, followed by question and answer sessions, can be very helpful. However, these approaches should be complemented by various forms of active instructional designs including teaching cases, role playing, low to medium fidelity scenario exercises, various forms of high fidelity simulations and "command post"/strategic leadership exercises. In the field of crisis management, learning by doing is the most effective way of improving competence.

Instructional design needs to fit the purpose and skill set that is to be developed or practiced. Costly and elaborate instructional/exercise designs and formats may be preferable for certain purposes, while simpler and more economical approaches may be

optimal for others. As noted above, strategic leaders vary greatly in their cognitive/learning styles (George and Stern, 19988; Preston, 2001; Daleus, 2012), so it is important to adapt training and exercise formats to reach and engage specific leaders.

Key recommendations for designing and developing strategic crisis management exercises

This chapter has discussed the advantages and challenges in setting up strategic crisis management exercises for country leaders in order to strengthen preparedness and improve the capacity to successfully address major adverse events and crises. To help governments design and develop strategic management exercises, the following actions should be considered:

- **Establish strategic crisis management exercise programmes for leaders and high-level public officials** to train them in the leadership roles they are expected to play during crises and to confront them with the new realm of complex crisis management. Exercises should be adapted for individuals, groups, and organisations and take into account their prior frames of reference, previous experience, and levels of proficiency.
- **Clarify early on the objectives of strategic crisis management exercises and make this goal clear to participants**. Exercises can test and stress different functions, abilities and capacities. They can be used for multiple purposes, such as familiarisation, skill-building and preparedness testing. Exercise formats, designs and techniques should be consciously and explicitly adapted to the goals and purposes of a given exercise. One size (and one instructional design) does not and cannot fit all.
- **Develop the right incentives for the private sector to develop their crisis management skills** in partnership with government, including at the leadership level. The scale and complexity of major crises requires whole-of-society co-operation under difficult conditions. Engaging the private sector, although potentially difficult, is essential.
- **Engage across borders in international crisis management exercises, including among leaders**. Many of the most significant threats and hazards do not respect national boundaries. Conducting exercises is essential for developing, testing, and improving the ability of nations to co-operate effectively under adverse condition. International exercises, although challenging to arrange, design, develop, and implement, can play a key role in improving preparedness.

Notes

[1] This figure is reproduced from *Hong Kong Efficiency Unit (2009)*

[2] See below for an explanation of the notion of exercise *fidelity*.

[3] For more information regarding the rapid reflection force concept, see http://www.patricklagadec.net/fr/pdf/Implementing_Rapid_Reflection_Forces.pdf. For more information regarding CRISMART exercise methodology, see Stern ed (2014) and https://www.fhs.se/en/research/research-centres-and-programmes/crismart/services/#content.

[4] This section draws heavily upon the discussion at the OECD/Swiss Federal Government workshop held in Geneva in June of 2014.

[5] This section draws heavily upon the discussion at the OECD/Swiss Federal Government workshop on *Strategic Crisis Management Exercises* held in Geneva in June of 2014.

[6] For more information, see www.crismart.org. See also, Stern, ed. 2014.

[7] http://www.chds.us/?met. See also Woodbury (2014).

[8] This was a major topic of discussion at the Oslo workshop organized by OECD and Norwegian DSB in September 2014. http://www.oecd.org/gov/risk/agenda.pdf.

[9] The MMOWGLI platform (Massive Multi-Player Online Wargame Leveraging the Internet) and has been deployed to examine wicked problems such as combating piracy in Somalia and developing a sustainable energy policy for the future. (http://www.onr.navy.mil/en/Science-Technology/Directorates/office-innovation/mmowgli-internet-war-game.aspx)

[10] https://dhs-summit.us/.

[11] http://www.crs4.it/vic/cgi-bin/project-page.cgi?acronym='INDIGO'.

[12] http://www.chds.us/?met (Accessed November 26, 2014).

References

Alberts, D. S. and R.E Hayes (2003), *Power to the Edge*, Command and Control Research Program, Washington, DC.

Boin, A., A. McConnell and P. 't Hart (eds.) (2008), *Governing after Crisis*, Cambridge University Press, New York, NY.

Boin, A., P. 't Hart, E. Stern and B. Sundelius (2005), *The Politics of Crisis Management: Public Leadership Under Pressure*, Cambridge University Press, Cambridge, UK.

Borodzicz , E. and K. Van Haparen (2002), "Individual and Group Learning in Crisis Simulations", *Journal of Contingencies and Crisis Management*, Vol. 10/3, pp. 139-147.

Crego, J. (1996) *Critical Incident Management: Engendering Experience Through Simulation* Dissertation, University of Salford, Manchester.

Crichton, M.T. (2009) "Improving Team Effectiveness Using Tactical Decision Games" *Safety Science* Vol.47 (3):330-336.

Crichton, M.T., R. Flin, and W.A. Rattray (2002) "Training Decision Makers: Tactical Decision Games" *Journal of Contingencies and Crisis Management* Vol 8(4): 208-217.

Daleus, P. (2012) *Politisk Ledarskapsstil (Political Leadership Style)*, Dissertation, Stockholm University Department of Political Science, Stockholm.

Deverell, E. and E.K. Olsson (2009), "Learning from crisis: A framework of management, learning, and implementation in response to crises", *Journal of Homeland Security and Emergency Management*, Vol. 6/1, http://dx.doi.org/10.2202/1547-7355.1574.

George, A. and E. Stern (1998), "Presidential Management Styles and Organizational Models", in George and George, *Presidential Personality and Politics*, Westview, Boulder.

't Hart, P. (1994) *Groupthink in Government*, Johns Hopkins University Press, Baltimore.

't Hart, P., E. Stern and B. Sundelius (eds.) (1997), *Beyond Groupthink: Political Group Dynamics and Foreign Policymaking*, The University of Michigan Press, Ann Arbor.

Hong Kong Efficiency Unit (2009), *Crisis Management: An International Overview*, http://www.eu.gov.hk/en/reference/publications/crisis_management.pdf, accessed Nov 26, 2014.

Keeney (1992), *Value-Focused Thinking*, Harvard University Press, Cambridge.

Kendra, J.M. and T. Wachtendorf (2003), "Elements of resilience in the World Trade Center disaster: Reconstituting the EOC", *Disasters*, Vol. 27, pp. 37–53.

Laporte, T. and Consolini (1991), "Working in Practice But Not in Theory: Theoretical Challenges of High Reliability Organizations", *Journal of Public Administration Research and Theory*, Vol. 1/1, pp. 19-48.

Mittroff, I. and A. Silver (2009), *Dirty, Rotten, Strategies: How We Trick Ourselves and Others into Solving the Wrong Problems Precisely*, Stanford Business Books, Palo Alto.

Marcus, L, B. Dorn and J. Henderson (2006), "Meta-Leadership and National Emergency Preparedness", *Bio-Security and Bio-Terrorism*, Vol. 4/1, pp. 128-135.

Maxwell, J. (2006), *The 360 Degree Leader*, Thomas Nelson, Nashville, TN.

Preston, J. (2001), *The Inner Circle*, Columbia University Press, New York.

Russo, J. E. and P. Shoemaker (1990), *Decision Traps*, Fireside Publishing.

Stern, E. (ed.) (2014) *Designing Crisis Management Training and Exercises for Strategic Leaders: A U.S.-Swedish Collaborative Project*, Swedish National Defense College, Stockholm.

Stern, E. (2013), "Preparing: The Sixth Task of Crisis Leadership", *Journal of Leadership Studies*, Vol. 7/3, pp. 51–56.

Stern, E. (1999), *Crisis decision-making: A cognitive institutional approach*, Swedish National Defense College, Stockholm.

Stern, E. (1997), "Crisis and learning: A conceptual balance sheet", *Journal of Contingencies and Crisis Management*, Vol. 5, pp. 69–86.

Stern, E. et al (2014) "Post-Mortem Crisis Analysis: Dissecting the London Bombings of July 2005" *Journal of Organizational Effectiveness* Vol.1(4):402-422.

Stern, E. and B. Sundelius (2002), "Crisis management Europe: A regional research and training program", *International Studies Perspectives*, Vol. 3, pp. 71–88.

Stevens, D. (2013), *Redefining the emergency manager: A proposal for change*, http://www.emergencymgmt.com/training/Redefining-the-Emergency-Manager.html, accessed 23 September 2015.

Swedish Civil Contingencies Agency [MSB] (2009) *Exercise Evaluation Handbook available online at* https://www.msb.se/RibData/Filer/pdf/25885.pdf (Accessed Oct 22, 2015).

HSEEP (2013), US DHS Homeland Security Exercise Evaluation Program, www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf, (accessed 26 November 2014).

UK Government (2014) "Emergency Planning and Preparedness: Training and Exercises" https://www.gov.uk/guidance/emergency-planning-and-preparedness-exercises-and-training (accessed October 21, 2015).

Weick, K.E. (1988), "Enacted sense-making in crisis situations", *Journal of Management Studies*, Vol. 25, pp. 305–317.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where governments work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Union takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

OECD PUBLISHING, 2, rue André-Pascal, 75775 PARIS CEDEX 16
(42 2015 24 1 P) ISBN 978-92-64-24903-5 – 2015-18

OECD Reviews of Risk Management Policies

The Changing Face of Strategic Crisis Management

Contents

Consult this publication on line at ***http://dx.doi.org/10.1787/9789264249127-en.***

This work is published on the OECD iLibrary, which gathers all OECD books, periodicals and statistical databases.
Visit ***www.oecd-ilibrary.org*** for more information.

OECD*publishing*
www.oecd.org/publishing

ISBN 978-92-64-24903-5
42 2015 24 1 P