enisa

European Union Agency for Network and Information Security

Report on Cyber Crisis Cooperation and Management

Comparative study on the cyber crisis management and the general crisis management

November 2014

enisa.europa.eu

Report on Cyber Crisis Cooperation and Management

Authors

Panagiotis Trimintzios, Roger Holfeldt, Mats Koraeus, Baris Uckan, Razvan Gavrila and Georgios Makrodimitris.

Acknowledgements

ENISA would like to thank with Secana and Crismart who helped co-authoring this report and extend its deepest gratitude to the experts and researchers who were willing to participate in the interviews held for this study (full is available in Section 6.1 p.53).

Contact

For information regarding this report please contact the Cyber Crisis Cooperation and Exercises (C3E) team at: **c3e@enisa.europa.eu**

For media enquires about this paper, please use **press@enisa.europa.eu.**

About ENISA

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

Follow ENISA on

Facebook Twitter LinkedIn YouTube and RSS feeds

Contact details

For contacting ENISA or for general enquiries on Privacy please use the following details:

Email: sta@enisa.europa.eu

Internet: http://www.enisa.europa.eu

ISBN: 978-92-9204-100-7 - DOI: 10.2824/34669 - Catalogue Number: TP-05-14-030-EN-N

Executive Summary

The goal of this study is to provide an analysis of cyber crisis management by identifying relations between this emerging field and the better established subject of general crisis management. This includes terminology and key concepts in these fields. This study further seeks to gain knowledge and understanding of the involved actors' perspectives on the challenges for Cyber Crisis management within the European context.

AThe purpose of the study is twofold: to compare concepts from the general crisis management systems with the corresponding systems related to cyber crisis management, and to conduct a conceptual analysis of the language and terminology within these two fields. The primary aim is to analyse the similarities and differences between general and cyber crisis management, employing examples from countries and organizations within the EU.

Based on interviews with members of key national and EU institutions, and on an analysis of the differences between their practitioner perspectives and the theories of general crisis management, the study arrives at six key areas of recommendations for future activities in the cyber security realm:

1. **Develop a common Cyber Crisis Management glossary**

   As a first step towards a common terminology in a European context, we recommend that a cyber crisis management glossary be drafted and published. To ensure a strong European commitment, we further recommend that an EU organization such as ENISA should be responsible for drafting the glossary.

2. **Gain further knowledge regarding Cyber Crisis Management**

   We recommend that a series of studies covering the topic of cyber crisis management should be initiated, especially in a European context. Further studies could for example focus on:

   - Comparisons of the cyber crisis mechanisms of Member States;
   - Roles and interaction between technical levels and decision-makers;
   - Deeper studies on the role and function of cyber centres in crisis management.

   The responsibility for producing international studies could be with ENISA or other EU institutions, depending on the focus of the study.

3. **Initiate activities for enhancing the knowledge on Cyber Crisis Management**

   More concretely, we recommend the implementation of knowledge creation activities such as education programmes, seminars or workshops for targeted audiences, with themes such as:

   - Cyber crisis from a technical perspective;
   - Cyber crisis from a decision-making perspective;
   - Understanding the processes of cyber crisis management;
   - Cyber risks, vulnerabilities and threats, and their possible consequences.

   This should be the responsibility of the cyber security community in general, with initiatives taken by national organizations.

4. **Support training and exercises in the field of cyber crisis management**

   Targeted exercises for certain functions and sectors are encouraged. Exercises in cyber crisis management for vital societal functions and critical infrastructure should also be carried out, perhaps regularly.

   We recommend training and exercise activities of a wide range in terms of scope:

   - National and international;
   - Inter-sectorial and cross-sectorial;
   - Specific to various technical and/or political levels.

   The training and exercise activities are the responsibility of national governments and appropriate public organisations and agencies, as well as of larger private companies. We would also encourage central EU organizations such as ENISA to provide inputs and thoughts on cyber crisis management exercises.

5. **Support development and sharing of strategic cyber crisis management procedures**

   We recommend a concerted effort to create national and EU-level plans using a shared terminology and giving due attention to the complex and interconnected nature of the management and escalation of cyber crises and incidents in a European context. Further to the development of procedures one should pay attention to sharing them in the community together with other related good practices.

   The supporting responsibility therefore lies with ENISA and the appropriate cyber crisis organisations at a national level to assist in the development of these kinds of procedures or plans.

   We also recommend that ENISA, together with appropriate organisations within Member States, should not only encourage the sharing of well-tested best practices, but also provide support in the process of developing new best practices through training and exercises, or to test practices for analysis and evaluation.

6. **Enhance information sharing and collaboration between private and public organizations**

   Methods for information sharing in both preventive and handling purposes are crucial. Operational information sharing with information flows that can be interpreted by both private and public organizations are encouraged.

   More specifically, we recommend that measures be taken to develop methodologies for operational cyber crisis management information sharing in order to increase exchange of knowledge for cyber crisis preventive and handling purposes.

   This is not only the responsibility of central EU institutions, but of the cyber crisis management community as a whole together with appropriate Member State agencies.

Contents

Executive Summary 4

1 Introduction 8
1.1 Aims and objectives 9
1.2 Target audience 10
1.3 Structure of this document 11

2 Characteristics of Crisis Management 12
2.1 Most prominent key factors in crisis management 13
2.2 Crisis management tasks 15
2.3 Crisis management challenges 18
2.4 Crisis communication 20

3 Discussion on Terminology 24
3.1 Key concepts and terminology 25
3.1.1 General crisis management 26
3.1.2 Cyber Crisis Management 28
3.2 Terminology issues 30
3.3 The theory-practice terminology gap 31

4 Cyber Crisis Cooperation and Management 32
4.1 Cyber Crisis sense-making 35
4.1.1 Early warning 35
4.1.2 Political sense-making 36
4.1.3 Scope of the crisis 36
4.2 Cyber Crisis meaning-making 37
4.2.1 Sharing and understanding dependencies 38
4.2.2 The speed and obstacle of technical jargon 39
4.3 Cyber Crisis decision-making 39
4.3.1 Availability of competence and expertise 40
4.3.2 Cross-sector co-ordination 41
4.4 Cyber Crisis termination 42
4.4.1 What was the problem? 43

4.5 Cyber Crisis learning & reform 44
4.5.1 Slowing factors in the learning and reform process 45
4.5.2 Lessons learned and reform information-exchange 45
4.5.3 Learning from exercises 46
4.6 Cyber Crisis communication 47

5 Recommendations 48
5.1 Create common cyber crisis management terminology and enhanced knowledge 49
5.2 Information campaigns for an increased understanding of cyber crisis management 49
5.3 Support activities for enhanced sharing of information, best practices and the development of cyber crisis management procedures 50

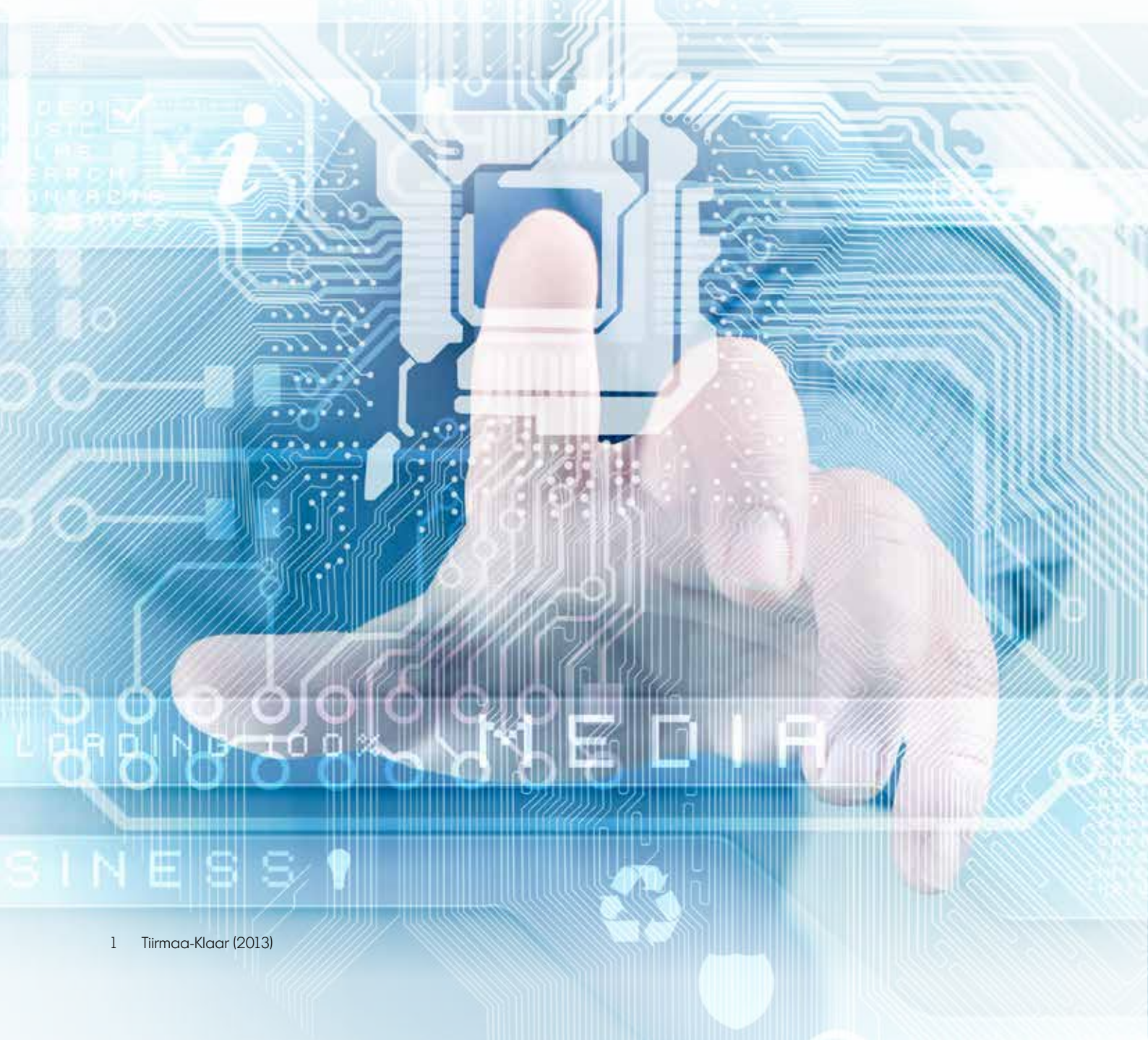
6 References 52
6.1 Interview subjects 53
6.2 Literature 53
6.3 Policy 54
6.4 Strategy 54
6.5 Web 55

Table of figures

Figure 1: The intensity pattern of a crisis 13
Figure 2: Characteristics of crises vs. normal decision-making 14
Figure 3: Timing and intensity of crisis management tasks 18
Figure 4: Crisis information flows 20
Figure 5: Practical crisis management activities 31
Figure 6: Cyber Crisis management challenges 33
Figure 7: The intensity pattern of a cyber crisis 34
Figure 8: Crisis escalations in the EU 40

1. Introduction

The societal developments of the last decade have made ICT systems a crucial part of our daily lives. The last decade has brought about new possibilities and produced unprecedented developments within the areas of communication and information sharing. However, these developments have at the same time brought with them new risks and threats, such as the 2013 Distributed Denial of Service (DDoS) attacks on the Dutch banking system, which resulted in thousands of people being unable to access their accounts online or use mobile payment systems.[1] Another example is the hacking of Indian government officials' e-mail accounts, 12,000 of which were penetrated in 2012.



1 Tiirmaa-Klaar (2013)

Today, European societies require functioning ICT infrastructures and services. Reliance on ICT and cyberspace have been increasing and continues to grow rapidly in many other critical sectors, such as Energy. This entails that vulnerabilities in the systems can have great consequences, both for individuals as well for societies at large. Cyber related crime [hereafter cybercrime], identity fraud, cyber-attacks or other harmful activities in cyber space are seldom limited to a local geographical area or restricted to one organization. These threats hence require broad cooperation of governmental and non-governmental bodies at the national as well as international level.

From a crisis management perspective, there have been significant achievements both within EU Member States and in organizations at the EU-level. The principles of crisis management have been reflected in national strategies and policy documents, focusing on crisis prevention, preparation, response and recovery. Education, training and exercises in cooperative mechanisms for cross-border and sector dependent crisis management have also taken place. To what extent have these achievements and knowledge been transferred to cyber-related crisis management? What characteristics can be identified within Cyber Crisis management that bring to light similarities or differences with the more well-known general crisis management? To what extent do the cooperation mechanisms resemble cooperation within crisis management?

This study seeks to explore and analyse cyber crisis cooperation and management at the national and multinational (e.g., EU) levels by identifying relationships with general crisis management. It furthermore presents an overview of the general crisis management systems, covering for example their structures, scopes and actions. The study will therefore focus on analysing how these issues are applicable in the area of cyber (ICT systems).

1.1 Aims and objectives

The purpose of this study is twofold: to compare and contrast general crisis management systems with the corresponding systems related to Cyber Crisis management, and to conduct a conceptual analysis of the language and terminology within these two fields. This report tries to analyse the differences and compatibilities between general and Cyber Crisis management, with examples from countries and organizations within the EU. This goal is further reinforced by the conceptual analysis, which aims to highlight and clarify any similarities and differences that simply derive from different terminology being used in the different fields. The goal of this study is to provide an analysis of cyber crisis cooperation and management at national and European levels by identifying relationships with general crisis management, including terminology and key concepts in these fields. This study further seeks to gain knowledge and understanding of the involved actors' perspectives on the challenges of Cyber Crisis management within the European context.

This report does not aim to provide a full reflection of the cyber crisis management and cooperation status at national or cross country levels in the EU. It tries to cover the topic from an analytical and research point of view paving the way for additional research and formalism in this area.

The research questions that will drive this study are the following:

1. What is the scope of and methodologies for responding to a Cyber Crisis?
2. How does decision-making take place?
3. How do the scope and methodologies differ from the scope and methodologies in general crisis management?
4. What methodologies are there for cooperation and information sharing amongst stakeholders?
5. Do current Cyber Crisis management practices include learning processes and capacity building in a similar fashion to those that exist within general crisis management?
6. What similarities and differences between general and cyber crisis management activities can be observed? Are there any issues in one field that cannot be mapped onto the other field, or do the differences largely amount to a simple variation in terminology?

1.2 Target audience

This study is addressed to organizations, institutions, political entities and individuals that are either active within the fields being researched, or are interested in gaining further knowledge on the topic Cyber Crisis management and cooperation and its relation to general crisis management. This study is the first of its kind and is thus explorative in nature.

The methodology used for this study is a combination of literature review and semi-structured interviews with experts and academics from the fields being researched. The literature review focused on classic aspects of crisis management and its terminology, while the interviews with experts and academics focused on cyber crisis management and the experiences, knowledge and perceptions of the experts in the field. The interviews are the core of this study, as they provide the necessary insight and knowledge that actually represent the many perspectives on cyber crisis management and cooperation.

The interview process- from identifying experts and researchers, to scheduling and finally conducting the interviews- is time-consuming in nature. Since the bulk of the analysis was based on the interview responses, an analytical structure is required. The structure of the interviews therefore builds on the key research questions and on the theoretical framework of this study.

1.3 Structure of this document

The remainder of this report is structured as follows. Chapter two covers the characteristics of general crisis management. It also contains definitions and terminology, as well as a presentation of some of the general key concepts.

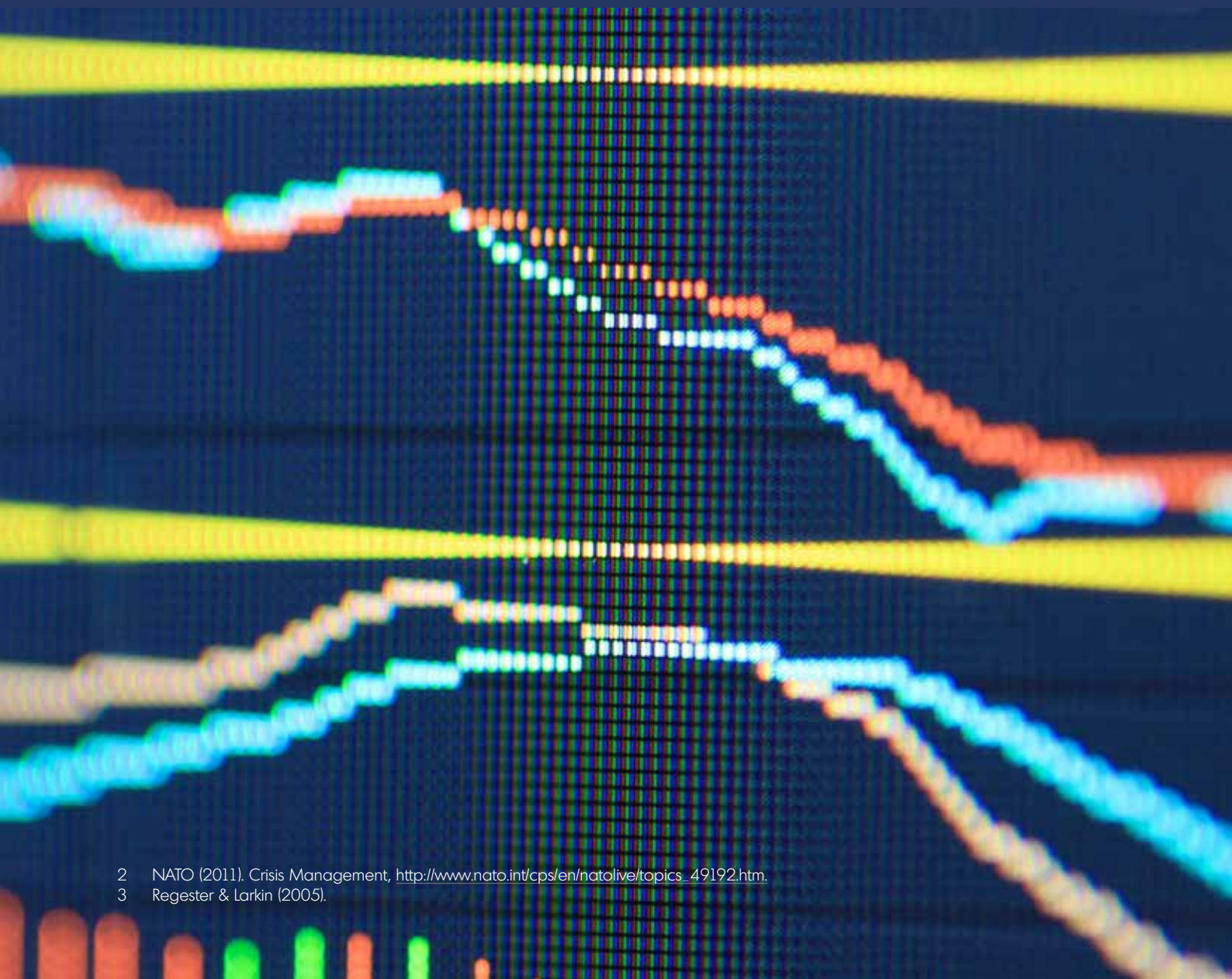
The third chapter presents various perceptions and understandings of the key terminology in the field of crisis management, both within and outside cyberspace. It focuses on illustrating the differences and scope of definitions commonly used within general and cyber crisis management. Furthermore, the chapter highlights how definitions have changed when moving from the general perspective to the cyber domain.

The fourth chapter consists of the results of the interviews, with a cyber-security in focus. It presents some similarities and differences between general crisis management and crisis management in cyber-related areas.

The final chapter consists of recommendations for further actions and commitments within this field based on the results of this study, entailing both operational commitments as well as those related to further theoretical analysis and research.

2. Characteristics of Crisis Management

The concept of "crisis management" can at times be very ambiguous. It is a term that has been appropriated in a number of different research fields and practices, each with its own interpretation of what it entails. At one end of the spectrum, there is the military notion of crisis management, which deals with keeping conflict escalation in check. NATO, for instance, often describes itself as a crisis management organisation[2]. This can be contrasted against the business management notion of crisis management, which sometimes morphs into the closely related concept of issues management, and which deals primarily with solving public relations problems. Here, the question is rather how a business keeps customers, regulators, investors, and the market happy when something goes terribly wrong on the operational side[3]. This study deals with yet another type of crisis management, which is the more general political-institutional view: crisis management as a process of institutional and organisational design, and of the role and actions of decision-makers within this larger construct. Crisis management is also dealt with from a preventive perspective and assists in determining measure to be taken, in regards to Business Continuity Management (BCM).



2 NATO (2011). Crisis Management, http://www.nato.int/cps/en/natolive/topics_49192.htm.
3 Regester & Larkin (2005).

2.1 Most prominent key factors in crisis management

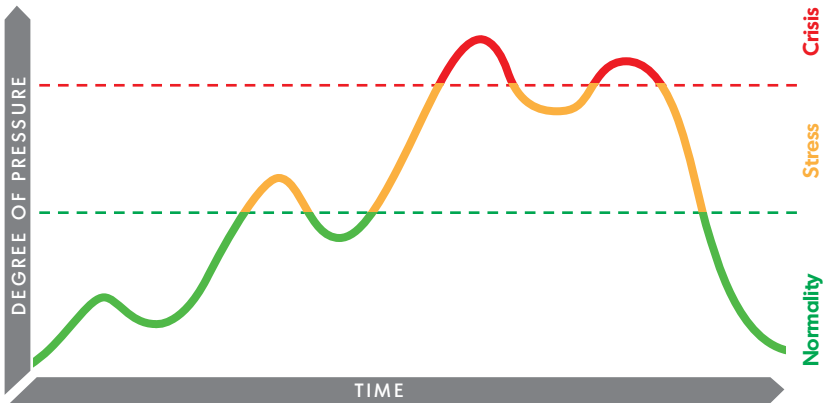
In general terms, the literature on general crisis management defines crisis management as making and effecting difficult decisions under difficult circumstances[4]. There is a basic divide between an objective and a subjective school of thought as to what actually counts as "difficult circumstances". The more objective- often mathematic-analytical and risk-based- point of view loosely defines crises as events where sufficiently high values are at stake. The cognitive-institutional approach offers a more subjective viewpoint, where perceptions and political and organisational constraints are what "creates" a crisis: it exists as an interpretation of the state of affairs rather than as a numerical truth. The advantage of the latter perspective is that it allows for a more inclusive and nuanced picture of different actors in different situations, all dealing with the same event. What one actor perceives as a serious crisis will be almost daily routine for another. Hence a subjective approach lets us deal with both viewpoints, and analyse and explain the decisions made and the mechanisms involved in reaching a final decision.

Boin et al. (2005) offer a subjective definition of a crisis as an event that a) creates a high degree of uncertainty or ambiguity, b) evokes a sense of great urgency, and c) puts high and often conflicting values at stake. The exact characteristics of these individual attributes can vary wildly: it can be uncertainty over what is actually happening, but can also be uncertainty over the outcomes of some proposed set of actions. Urgency can be anything from having to make acute triage decisions to save certain lives while considering others a lost cause, to having to implement immediate large-scale policy changes that will have consequences 10 years down the line. The values at stake can include not only human lives or material assets, but also more intangible values such as trust, approval, reputation or clout.

As the degrees of uncertainty, urgency and values at stake shift over time, both upwards and downwards, an event can drift in and out of a "proper" crisis state, meaning there will be lulls or calm moments in the storm. But perhaps more importantly, they will drift closer or farther away from some semblance of normalcy, and things can become very hectic indeed without tipping over into a full crisis.

Figure 1 illustrates how such a pattern can look over a period of time. Note that this illustration would indicate two separate instances of an event being what might be seen as a full-on crisis–the rest of the time, the pressure is at a level that could conceivably be handled using normal means. There is a baseline of normality, a threshold for a crisis, and some degrees of system stress between the two.

Figure 1: **The intensity pattern of a crisis**



While these various degrees of intensity may come under different names–special events, incidents, accidents and so on–there is often a vague general sense that if they can be handled using every-day means and methods, they do not really qualify as anything as extraordinary as a crisis. Indeed, some institutions manage

4 Boin et al. (2005); Boin, McConnel & 't Hart (2008); Bovens & 't Hart (1996); Rosenthal, Boin & Comfort (2001).

incidents as their every-day job, so if anything, a lack of such events would be considered extraordinary. Nonetheless, the distinction is broadly made between crises and non-crises, with some grey area of increased pressure separating the two states. This distinction then becomes the guiding principle between two distinct scopes and contexts of decision-making, with crises often providing some special emergency measures and with decision-making powers that exceed what is normally afforded the agency or actor in question.

This divergence from what is ordinarily available thus becomes a perverse incentive to keep the crisis going a little longer than might be strictly necessary. It should therefore be noted that there is a distinction to be made between the intensity and the explicit crisis state: the latter is a subjective (and even slightly intentional) interpretation of the former. In a case that would create a pattern that matches Figure 1, it would most likely be considered as a single crisis state rather than two separate crises with a dip in the middle. Unless we are talking about very slow-moving crises, the time it takes to positively identify the downward trend from the first peak would be long enough for the second peak to occur, and the state of emergency would never be lifted between the two.

The trick to "solving" a crisis, rather than just let it run its course, is to remove or resolve one of the three conflicting issues–after all, if one is resolved, the remaining two others become far more manageable. A situation of absolute certainty is not hindered by urgency or conflicting values; the best course of action is already obvious. A situation without urgency likewise offers ample time to untangle any uncertainties and value conflicts, and a situation without any values at stake means that even a 'best-guess' or an instant 'knee-jerk' decision will do because even if it is wrong, nothing is really lost in the process. As Figure 2 demonstrates, this issue and the way to resolve it closely mirrors George's (1993) triangle of dilemmas for evaluating decisions in a policy environment[5]. He describes the inherent conflict in political decision-making where trade-offs have to be made between the quality of a decision and prudent use of resources; between the prudent use of resources and the need for acceptability and support; and between the need for acceptability and the quality of the decision. Here too, if one of these is rendered a non-issue, the remaining problems are easily resolved as well.

The crucial thing to note about both these models is that they assume that decision-making does not take place in a vacuum. There are all kinds of constraints that need to be taken into account, which hampers attempts at unilaterally solving an issue. Someone's course of action may be incomprehensible to those they are supposed to co-operate with; the values they are trying to preserve will come at the expense of values someone else considers critical; and their urgent needs can come into conflict with the speed of response capabilities of other actors.

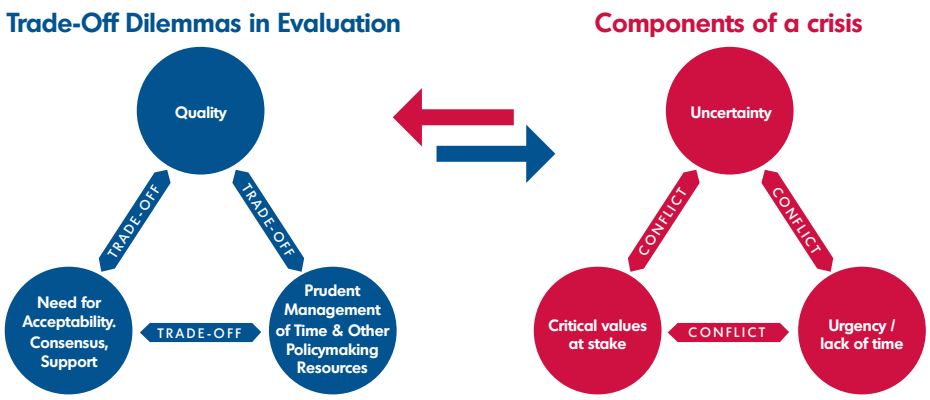


Figure 2: **Characteristics of crises vs. normal decision-making.**

5 Koraeus (2015). Figure is a composite of two illustrations found in the publication.

2.2 Crisis management tasks

Boin et al. (2005) define five key tasks or challenges that are involved in resolving these kinds of crisis situations. The tasks are, in rough chronological order: sense-making, meaning-making, decision-making, termination, and learning. These tasks can be (unevenly) separated into a loose before–during–after categorisation, where the bulk of the actual crisis management obviously happens during the actual crisis. The five tasks should not be seen as distinct events. Rather, they overlap and flow into each other. As a crisis evolves, new sense-making and immediate decision-making might be needed, even though the managers of the crisis are in the middle of trying to explain what it all means.

Sense-making involves finding out what is going on and why. Sense-making straddles the boundary of "before" and "during" the crisis and should not be confused with early warning and detection. Rather, early warning and detection are activities that trigger the sense-making phase. The better those activities are handled, the easier the sense-making tends to be. This is where the uncertainty of the crisis is at its peak: something has happened, but the exact causal chain that led to the contingent event, and the consequences of the crisis, are as of yet unclear. Figuring out exactly what needs to be done to deal with the issue at hand, and not being distracted by ancillary events is of critical importance. Determining the actual crux of the matter is what allows crisis managers to move forward in a decisive and constructive manner. A common trait of modern crises is a massive information overflow, but an acute lack of information value. Much of the sense-making process is about evaluating which information is germane to the core of the crisis, and to avoid getting stuck in the nitty-gritty (or outright irrelevant) details.

Once some sense can be made of what is going on, **meaning-making** becomes the new problem. The understanding of the situation must now be conveyed to others in order to make them realise why this is a crisis and why certain actions need to be taken. This involves all kinds of issue framing and symbolic messaging with the purpose of building or maintaining trust and credibility. This can be particularly problematic when dealing with a highly technical issue or when dealing with events that could conceivably have been foreseen. For instance, how is it that an Icelandic volcano has made it impossible to find an available train ticket or rental car to get home? How is it that a nuclear power plant north of the Black Sea has made it inadvisable to go on a hunting trip anywhere in northern Europe? There is often also a strong symbolic component that has to be handled, such as being able to answer why a country has been targeted for terrorism, or explaining how societal strength can be drawn from catastrophe.

Meaning-making is important because it builds a foundation of consensus and understanding for the next task.[6] **Decision-making** entails actually taking action to resolve the situation given the available resources, logistical and time constraints, and the legal and democratic constraints. It also involves making the ultimate goals of managing the crisis at hand guide every action, from top-level strategic planning down to ground-level operational actions. It is essentially about making the entire crisis management machinery work, which is not a small task. Here too, the threat looms of becoming too detail-oriented and ending up with strategic planners trying to micro-manage field work rather than delegating to lower levels and staying focused on the goal of formulating a good long-term strategy. The decision-making phase lasts until there are no more decisions to be handed down through the system, and when operational matters start to return to normal. Hence the responsibility for future operational decisions can at that point be handed back to the regular, every-day authorities.

The **termination** task is perhaps the most distinct of the five tasks but, at the same time, the one where the handling of the other tasks becomes the most critical. This is where decision makers decide that the crisis is finally over and that the crisis management organisation can be disbanded (for now). This does not necessarily mean that every last detail of the crisis has been fully resolved, but rather that what remains can be handled using normal, non-crisis means and methods. It is a return to normalcy rather than a declaration that there is nothing left to do. But here is where the subjective crisis conception really comes to the fore: it is quite likely that not everyone will agree with the assessment that the crisis is over. If meaning-making is not properly managed, divergence in opinion can be vast. For some, the crisis may have only just started. For others, it was over long ago, if it even started at all. In a political environment, this is often where things become calm enough for recrimination and blame-games to begin: Who was responsible for the event? Why were there not more precautions taken, and if they were, why did they not work? Why did it take so long to act decisively, or why did the decision-makers jump the gun and overreact? Again, the subjective nature of crises makes it entirely possible that both of the last two questions will be asked simultaneously.

Another quirk in the termination task is that ending a crisis is not always what a decision-maker might actually want to do. In many systems, the crisis itself confers special powers and/or allocates emergency resources to those in charge, and there is a clear temptation to make good use of these extra assets while they are still available. Even long after operational crisis management has come to a close, the political or symbolical management could benefit from additional strong actions to prepare for the next phase. Even the operative level can benefit from this extension. During the crisis, quick and direct routes of communication may have become established between policy makers and those doing the hands-on work. So as long as the crisis carries on, there is an opportunity to influence those policy-makers regarding what reforms might be needed when the crisis ends, or even demonstrate that some of the crisis measures might be useful on a day-to-day basis.

At the same time, the termination task presents a conundrum for decision-makers. On the one hand, they are struggling to explain that it is time to return to a state of normality, but on the other hand, the crisis demonstrates that the normality that existed before the crisis was unsuited for preventing these kinds of events. So is it really worth returning to the pre-crisis status quo? It is this balancing act that is situated at the centre of the termination task and, if badly handled, can even trigger a crisis of its own. The crisis management literature is rife with examples of lingering crises that refused to end, or that spawned a seemingly never-ending chain of new crises as a result of mishandled termination.[7]

6 It should be noted that Boin et al. lists decision-making before meaning-making, but in looking at the ingredients and prerequisites for the former, the question arises of whether or not the chronology of the two happens in the reverse order: i.e. meaning-making taking place first to build that foundation of credibility that lets the decision-making happen unopposed. The order chosen by the authors makes sense in that the two are closely interlinked and the meaning of meaning-making easier to convey if decision-making has already been explained to the reader.

7 Cf. Boin et al. (2007); Rosenthal et al. (2001); Bovens & 't Hart (1996).

Learning and reform is, at least rhetorically, the way out of the termination conundrum. By promising an investigation and changes in policy and practice, a temporary return to things as they were can be made much more palatable. However, beyond being a symbolic gesture, the learning and reform task serves a functional purpose. It offers the opportunity to effect genuine improvements and to fix the bugs in the system that were exposed by the crisis. Historically, crises have shown to be a great catalyst for much-needed systemic changes, to the point where some policy theories are now entirely centred on the idea that crises are almost natural occurrences in a system. Without these events that shatter the equilibrium, the system risks stagnating and becoming cumbersome and overburdened with minutiae. The crisis shakes up the system and forces a fresh look at what works and what does not; it is a test of the improvements made since last time[8].

Learning thus closes the loop in anticipation of the next crisis. It generates the early-warning and detection mechanisms that feed into making sense of new events; it preserves experiences that offer a basis for, not just decision-making, but also for future meaning-making efforts in which historical analogies help others understand new threats that appear.

Figure 3 provides a rough illustration of how the different tasks vary in intensity over the course of a crisis.[9] It should be noted that while the decision-making and meaning-making phases naturally end as the crisis comes to a close, they do not start when the crisis starts, but rather during its ramp-up. As it becomes increasingly obvious that something has gone awry, decisions are already being made and justified to some given target audience. The best-case scenario is one where the early sense-making and subsequent decision-making and meaning-making processes are accurate and effective enough to actually stop the escalation and prevent the incident from ever reaching the state of a full-blown crisis.

Another thing to note is that, as previously mentioned, concepts such as "early warning", "prevention" and "preparedness" fall somewhat outside of the five tasks. The early warning process is what detects unusual increases in pressure on the system, and thus (hopefully) triggers the first sense-making efforts. At this stage, it is also conceivably possible to prevent the crisis from ever erupting. Similarly, the preparedness process is what initiates the meaning-making and decision-making processes in that this is where the key decision-makers are contacted, and the first attempts at formulating a message to describe the crisis are made. The differentiation between "prevention" and "preparedness" is of particular note since, even outside of the purely analytical realm, there is some confusion between the two terms. Here, as in most instances of structured crisis planning, the notion of preparedness does not include any kind of pre-planning or general mental preparation for some potential event in the future. It rather signifies the specific activity of gearing up for the active management of a crisis that seems very likely to occur in the immediate future. This means activating emergency measures, calling in the relevant decision-makers, clearing schedules for everyone involved, and so on.

8 Cf. Kingdon (1995); True et al. (2007); Birkland (2006).
9 Koraeus (2008).

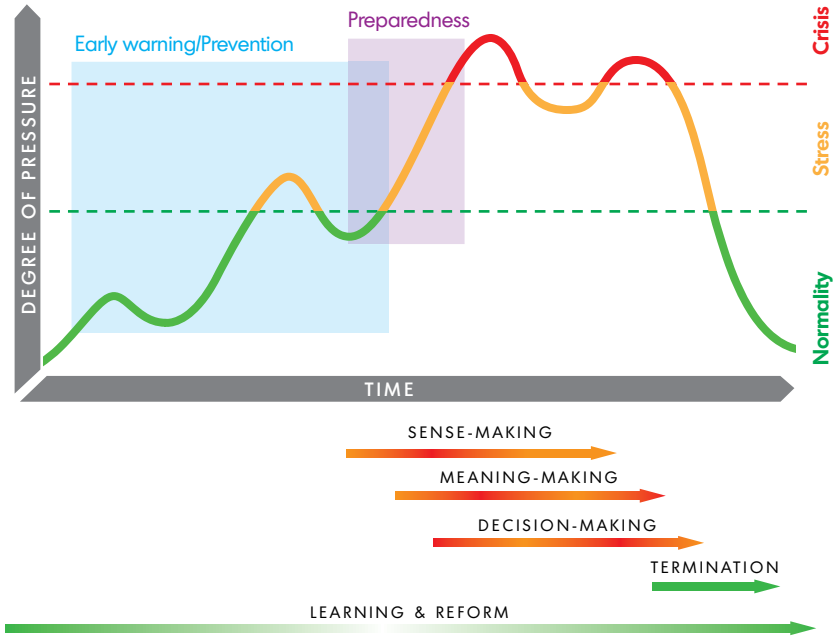


Figure 3: **Timing and intensity of crisis management tasks**

Finally, it should be noted that this is indeed just a simplified and even optimistic illustration of the many ups and downs of a crisis, especially as far as their placement over time. There are ample historical cases where the learning and reform process never happens at all, or the termination phase dragged on for years or even decades. Nevertheless, the fact that three of the five crisis management tasks operate in parallel at the height of the crisis is at the same time both obvious and noteworthy: with that much to do at once, no wonder that crisis management is stressful.

2.3 Crisis management challenges

The categorisation of crisis management as five key tasks is not only an analytical convenience, but also provides a laundry list of critical issues that will face the crisis management practitioner. The literature on the subject is massive and to go into every detail is beyond the scope of this inquiry. However, some general patterns can be discerned for the five tasks. Each task sets up a number of key challenges for the crisis management organisation, which will ideally guide the design of the crisis management system. For instance, many–but not all–of the sense-making challenges belong to some kind of analytical function within the organisation or with the policies that guide the work of that function.

The challenges straddle the gap between theoretical-analytical questions of the inner workings of crisis management, and more practically oriented best practices for organisational design. Without needlessly reiterating the tasks themselves, the key challenges in the five crisis management tasks are, in order:

Sense-making challenges:

- First and foremost, is the organisation set up to collect and respond to early-warning signals?
- Does the organisation accept that crises can actually happen, or does it suffer from a form of "it will never happen here" exceptionalism?
- How is the issue verified? Just because a problem has been detected and classified does not mean that it has been properly identified.
- If a problem is not known or familiar beforehand, it becomes much harder to detect, much less to properly identify it.
- What kinds of crises are actually allowed to be detected? Political constraints may render some issues unacceptable–the detection of such issues have the added obstacle of overcoming institutional ideology and inertia.

Meaning-making challenges:

- How is the issue framed? A simple difference in the choice of words can alter the perception of an event. Labelling the same event as an accident generates a different response than if it were called a tragedy. What, then, is the desired response?
- Is messaging surrounding the crisis tailored for its audience? Making the public understand an issue is often a very different matter than making experienced practitioners understand what the chosen course of action and the reasons for doing so.
- How credible is the message? It is very easy to degrade one's freedom to make decisions by repeatedly overpromising and under-delivering, or by overstating the degree of certainty behind a decision. Such mistakes erode trust and make it less likely that other parties will support the next critical decision.
- Is symbolic communication being used? By their very nature, crises stir up emotions, and it is important to actually take the time to acknowledge this. A failure to perform the rituals of shared shock and grief, for instance, means that every message only manages to further convey an air of indifference and callousness, which once again quickly erodes trust in, and support for, the crisis management efforts one might want to attempt.

Decision-making challenges:

- How are ambiguities and uncertainties resolved? Is the organisation able to retain previous hypotheses about the situation and act on them if it turns out that the initial interpretation was incorrect?
- Non-decisions are also decisions. It is often convenient and comforting to take a "wait and see" approach, but are such decision analysed and treated like any other course of action?
- How much actual decision-making takes place? It is very easy for plans to become scripts, removing the agility, adaptability, and improvisation that is needed to handle a crisis.
- How does the coordination work? Are the strategic goals and operational efforts in line with each other, or do they end up working at cross-purposes?
- At the same time, are the different levels of decision-making properly separated or does, for instance, the strategic level become distracted by trying to micro-manage operative matters?

Termination challenges:

- How does one determine that the crisis is really over? Mirroring the problems involved with sense-making, it can hard to state with any certainty that things are now back to normal.
- Terminating the crisis too late is just as bad as ending it too soon. Calling an end to crisis management only to have the crisis flare up again proves beyond any doubt that the crisis manager is not–and perhaps never was–in control of the situation. On the other hand, dragging the crisis out just gives the impression that the decision-makers are trying to profiteer on the emergency efforts and/or that the crisis is largely artificial.
- The accountability trap: the same decision-makers that were responsible for "letting the crisis happen" are now trying to take charge and say that the crisis is over. Yet how can they be trusted to make that kind of judgement call given the error in judgement just witnessed by all?
- Blame games often ensue as one party or another tries to pin responsibility on someone else in order to score political points, to further some agenda, or to shift responsibility away from themselves in an attempt to avoid the accountability trap.

Learning and reform challenges:

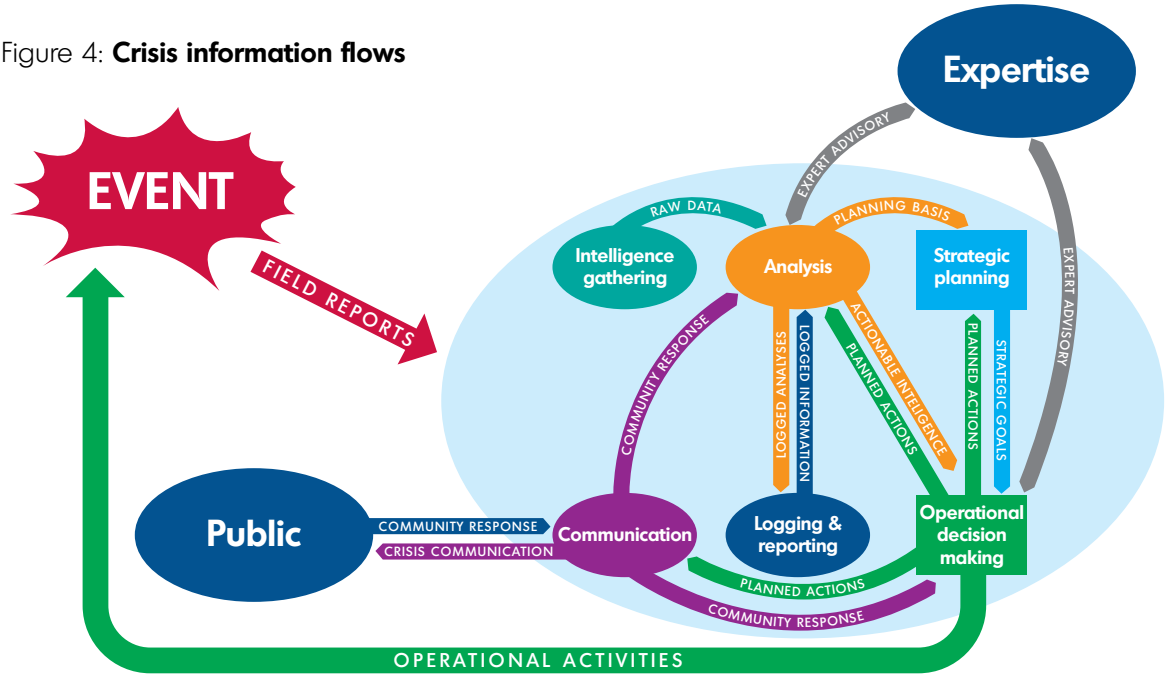
- Return of the accountability trap: how does one argue for reform when the same party was, just recently, intent on returning to a state of normality that permitted the crisis to occur?
- How much of the learning actually results in tangible improvements? Many times, the supposed learning is purely a paper product: an unrealistic document that claims that lessons have been drawn and changes made, but in practical terms, everything just goes back to the way it was before the crisis.
- At the same time, learning is not the same thing as change! While there is often a strongly felt need for change, it is equally important to recognise mechanisms that worked perfectly well, and which should therefore not be needlessly swept away by reform.
- What is the lesson that actually needs to be learned? There may be nothing wrong with the procedures and mechanisms involved, but rather with the fundamental assumptions about what kind of problems the crisis management system is meant to solve. So it is the perception of the problem that needs to be reassessed rather than the methods used in dealing with whatever problem might arise.

There is a recurring trend in all these challenges; namely that a huge portion of crisis management comes down to communication. Detection, verification, hypothesising, coordination, framing, messaging, et cetera–these are all aspects of communicating a perceived image of a situation, as well as ideas on how to best manage it, between different stakeholders.

2.4 Crisis communication

The fundamental problem of crisis management, then, is one of communicating needs and proposed solutions to the necessary parties. While research on the topic often focuses on decision-making, that decision is based on what information is at the disposal of decision-makers. Hence what stimulates the interest of the researcher is exactly how the information is being interpreted and used to promote a given course of action. The literature on the exact methods of crisis communication is vast, and it is beyond the scope of this study to provide a complete overview. Rather, it is important to gain a general understanding of the key issues involved that make crisis communication so difficult.

Figure 4: **Crisis information flows**



First of all, it is important to note that crisis communication is not just a matter of sending out information, but also of receiving it. There are numerous design features in a crisis organisation that may help or hinder communication in either direction. Even though the literature on the topic is vast, the principles of good crisis organisational design can roughly be summed up as an attempt to create distinct nodes of information management: a data gathering function; a function for refining that data into useful information; an operative decision-making function that turns the information into action; a strategic planning function that takes the long view, perhaps even with its own separate analysis function; and a communication function that presents a single point of contact to the outside world.

From an external perspective, this may seem like a fairly simple procedure: impressions of what is going on go at one end, and activities and communication comes out at the other. Under the surface, however, communication between these separate functions is necessarily intense. As shown in Figure 4, experience shows that the single output node is not always the best idea. If several different actors have to co-operate, it may actually be better to establish additional direct lines of communication between similar functions, rather than to overload the supposed "communication" node with all the details each cell in the organisation needs. The figure, busy as it is, also only shows a small select portion of the tangled mess of communication that goes on within this black box.

Beyond the actual design of the crisis management system, features inherent in how decision-making groups operate are at play, and those group dynamics can make or break any and all communication efforts. Perhaps the most well-known of these is the phenomenon of mind-guards and gatekeepers, as described in Janis' (1982) work on groupthink.[10] Essentially, these are individuals in a decision-making group or organisation that–almost entirely unwittingly–work towards maintaining a supposed consensus view on a topic, and who therefore tend to suppress or dismiss information that does not fit that view. Janis proposes a solution in the form of having deliberate "devil's advocates" in the group whose job it is to explicitly and persistently bring up alternate points of view and other interpretations of the facts.

On the macro level, both of these functions are necessary for a crisis management organisation. Even gatekeeping, which is generally thought of as something of a group-behaviour pathology, serves an important role: namely to keep unimportant information off the table. The pathological aspect only becomes an issue when actually important information is being excluded as well. The issue is that, contrary to how it often feels in a crisis situation, information is not actually scarce. Rather, a common problem for crisis decision makers is a massive information overflow that makes the situation impossible to grasp. What is lacking is relevant information or, put another way, the signal-to-noise ratio is very low. It feels like there is no relevant information because, out of ten pieces analysed and considered, only one actually has any bearing on the crisis. With proper filtering, that ratio could easily be inversed. It is rarely the case that the required information is impossible to find, but rather that it is being drowned out by irrelevancies.

This concept holds true for outgoing information as well: it is very easy to want to say too much, and to go off message in such a way that the key points are lost. In particular, there is often a need to tailor the message to the recipient: the general public needs to have certain points stressed that are of little to no relevance to technical experts, and vice versa. Technologically complex issues almost universally need to be "translated" into a more easily understood language or terminology. Even such a common tool as statistics is often poorly understood outside of expert groups, and could similarly benefit from translation into practical terms. If concentrations of harmful chemicals after a hazmat accident "doubles" the chances of long-term adverse health effects, does that mean that everyone will be affected (because the incidence doubles from 50% to 100%), or that almost no-one will (because the incidence doubles from one to two in a million)? Technical jargon can also evoke a very different response in the uninitiated than it does in the experts who write the incident reports. The word "incident" itself may be situated at the very lowest end of the disaster

10 Janis (1982)

spectrum, but to the untrained ear, it may instead evoke images of such "incidents" of near-cataclysmic proportions as the 1966 Palomares plane crash in Spain, where two hydrogen bombs broke apart and irradiated a large area, and a third bomb was lost at sea for months.[11]

The need for translation of technical information is often necessary in the other direction as well: the general crisis manager or decision-maker will perhaps have his or her own field of expertise, but outside of that, s/he is as unfamiliar with these terms as the general public. The aforementioned filtering process that provides the decision-maker with relevant information therefore also needs to ensure that it is relevant *and possible to understand*. Incomprehensible information might just as well be noise, even if it is actually relevant to the decisions being made.

The point where all of this becomes really problematic is when many different target audiences exist, each with their own wants and needs, and with different missions and competencies. Unfortunately, coordination is also at the very heart of crisis management, so that point is soon reached as an issue starts to escalate out of control. Good communication becomes crucial at this stage. Even in today's IT-saturated society, it is not a matter of technical solutions but of competent people using good procedures. The right competencies need to exist at the connection nodes between different organisations–people who can speak the languages of both parties and act as trustworthy translators between the two. Trust further becomes an issue the instant sensitive or confidential information enters the picture, either because the crisis is of such a nature that affects national security or because the information is proprietary to the parties being affected. The legal issues alone–what can be shared with whom in such a situation–are a field of expertise of their own, which place yet another demand on the communicators that are involved in the information-sharing.

While there certainly are procedural solutions that will greatly increase the chances of making it all work, such as the SECI process of knowledge exchange[12], the nature of crises almost ensures that anything more detailed than a general strategy is likely to break down very quickly. The literature on the topics of knowledge management and crisis communication procedures is truly vast and beyond the scope of this

11 Palomares Summary Report (1975)
12 Socialisation/Externalisation/Combination/Internalisation; cf. Koraeus (2008), McNabb (2007), Nonaka & Takeuchi (1995).

study. The main conclusion is that while competent individuals can make due with bad processes, good procedures will only rarely save inept communicators except in the most trivial of situations, and in the former case it is more due to the improvisational ability of the communicator to work around the processes in place.

If coordination and cooperation issues become a recurring theme between two organisations, a mutual exchange of liaisons is one way of formalising communication routes. However, such a solution relies on problems being known before the fact, and as previously discussed, a key aspect of crises is that they often present completely new and unforeseen problems: the crisis exists exactly because the issue was not known beforehand. In such cases, the established routes of communication might not–and in fact, most likely will not–be sufficient. Instead, what is needed is a broad knowledge network and, once again, skilled personnel that know how to find experts that can provide the right answers, even though the actual question is not even clearly understood yet. This entails being able to communicate not just the facts of the crisis, but also the perception of it–be it a common operational picture or just the hypotheses and working assumptions about how the facts of the matter are being interpreted. Proper communication of the perception of the crisis allows the responding expert to calibrate not just their answer, but also the initial question. If the expert understands the logic behind how the crisis is being perceived, he or she can respond by giving a more relevant answer than what the question is actually asking for. Before the Boxing Day tsunami in 2004, for instance, the effects of earthquakes under water were not nearly as widely known as they are today. As a result, in the immediate aftermath of the earthquake in the Indian Ocean, decision-makers across the globe tried to quickly query experts about what happens during an earthquake. Finding an answer to this question was not hard; what proved difficult was finding an expert that was able to say, "it is not the earthquake that is the problem, but the tsunami it will create."[13]

There is a flip side to all this information filtration: no matter how well-targeted and precise, there is always a want for more. An almost universal characteristic in crises is that, when asked, the general public will always say that they did not get enough information. The reasons for this are many. One is that, as already mentioned, information needs to be targeted to its audience, but the public is not really a single audience–rather it consists of a myriad of interests and needs, and many of those will not be satisfied by a single broad message. In particular, the issue of selecting the right language can become an issue: "the public" is a very disparate group that can hold any level of expertise, from complete ignorance to amateur interest to complete insight. Communicating too simplistic a message to accommodate the first group will often make the latter two ignore it because it does not contain enough actionable details to catch their interest.

Another reason why people end up uninformed is an almost mythical fear of spreading panic: the notion that, if given full disclosure about what is going on, people will start behaving irrationally and generate a further loss of control of the situation. This is a particularly die-hard myth, but is nonetheless exactly that: a myth. Research has shown that the panicking public has next to no factual basis and that, in some cases, the victims would probably have benefitted if they panicked slightly more than they actually did.[14]

A third reason is that the system that is doing the communicating is not aware of how outsiders will interact with that system. Put another way, just because a crisis management system has established very clear responsibilities for who communicates what, it does not mean that the general public is aware of this distribution and will know where to look for answers. Rather, they will use their normal channels and whatever else that immediately comes to mind, none of which necessarily includes the information nodes set up by the crisis management system. Even if the system is set up so as to "speak with one voice" from a central position, the public may not be aware of that either, and will still use its accustomed information channels. Therefore distributing information about where to get information is just as important as spreading the actual information about the crisis itself.

13 Koraeus (2015).
14 Clark (2002).

3. Discussion on Terminology

Understanding the terminology used within the field of crisis management and cooperation, general as well as in cyber space, is crucial. Perceptions on key terminology can and do differ between organizations, nations, fields and academia. It is therefore important to analyse the variations of terminology used for certain key concepts that are of particular importance, especially when exploring how general crisis management might comprehend a concept compared to how the concept is perceived in the cyber context. To further understand how various key concepts are comprehended in the fields of general crisis management and Cyber Crisis management, there is a need to consider diverse definitions of key concepts, and how they are interpreted or treated at different levels.

This study also represents a first attempt at illustrating and comparing the complex nature of the terminology and key concepts within the fields of general crisis management and cyber crisis management. This segment is not all-encompassing, nor does it aim to settle which definitions are the correct ones. It is merely a pre-study of the topic, and further research focused on similar terminology issues is recommended.

In order to systematically identify the various definitions and concepts, the definitions have here been generally systemized into four different categories: national, EU, academia and best practice. These categories allow for a wide illustration of the general understanding of these critical concepts, and contributes to a discussion on communication. The different categories entail the following:

The national and the EU categories include definitions from national strategies, actions plans and other official documents issued by government bodies in regards to crisis management or cyber-security related documentation. The category further refers to definitions used in European contexts, such as directives and communications. The academia section focuses on definitions and perceptions from areas of study, with examples drawn from e.g., published books, articles and presentations from well-known publishers and journals. The best practice segment includes definitions that are either widely recognized or embedded such as definitions used in standards (ISO/TC) or in guidelines/guidebooks and handbooks. The best practice segment might entail the same definitions as in other levels or sections since chances are they are the most recognized.

3.1 Key concepts and terminology

The following tables illustrate how key concepts and terminology can be defined depending on context, e.g., national or academia, as well as on how the concept and terminology have been transferred to the cyber domain.

3.1.1 General crisis management

The understanding of various key concept and terminology will differ not only between the general crisis management structure and Cyber Crisis structures or arrangements, but also within the structure depending on context.

	EU and national	Academia	Best practice
Crisis	An event that affects many people and large parts of society and threatens fundamental values and functions. Crisis is a condition that cannot be handled with ordinary resources and organization. A crisis is unexpected, far removed from the ordinary and mundane. Resolving the crisis requires coordinated action from several players/actors.[15]	A serious threat to the basic structures or the fundamental values and norms of a system, which, under time pressure and highly uncertain circumstances, necessitate making vital decisions.[16]	An extraordinary event that differs from the normal and involves serious disturbance or risk for disturbance of vital societal functions.[17]
Incident	An occurrence or event, natural or human-caused, that requires an emergency response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wild-land and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.[18]	All temporary and from the normal diverging events that result or could result in damaging consequences for security, health and/or environment.[19]	Unplanned interruption to a service, a reduction in the quality of a service or an event that has not yet impacted the service to the customer.[20]
Incident Management	Activities that address the short-term, direct effects of a natural or human-caused event and require an emergency response to protect life or property.[21]	Incident Management provides the capability to anticipate and plan for unexpected large-scale crisis events that require prompt and effective response.[22]	The objective of Incident Management is to restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price.[23]

15 MSB (2011) Guidance for risk and vulnerability assessment https://www.msb.se/RibData/Filer/pdf/25893.pdf.
16 Boin, 't Hart, Stern & Sundelius. (2005).
17 Säkerhetspolitik.se (2013). http://www.sakerhetspolitik.se/krisberedskap/Vad-ar-en-kris/
18 NRC (2005) Incident Response Plan. http://www.nrc.gov/about-nrc/emerg-preparedness/respond-to-emerg/incident-response.pdf.
19 MSB (2012) On learning big from small incidents https://www.msb.se/RibData/Filer/pdf/26272.pdf
20 ISO 2000 (2011).
21 NRC. (2014) Incident Response. http://www.nrc.gov/reading-rm/basic-ref/glossary/incident-response-ir.html.
22 Paton (2005)
23 ITIL http://itlibrary.org/index.php?page=Incident_Management.

	EU and national	Academia	Best practice
Critical Infrastructure	Critical infrastructures are organizations or institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences. At the federal level, the following areas have been identified: Energy, Information technology and telecommunication, Transport, Health, Water, Food, Finance and insurance sector, State and administration and Media and culture.[24]	An asset, system or part thereof located in Member States that is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact on a Member State as a result of the failure to maintain those functions.[25]	The systems, services, networks and infrastructures that form a vital part of a nation's economy and society, providing essential goods and services. Their disruption or destruction would have a serious impact on vital societal functions.[26]
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.[27]	Information security is the protection of information and minimises the risk of exposing information to unauthorised parties.[28]	Preservation of confidentiality, integrity and availability of information. NOTE: In addition, other properties, such as authenticity, accountability, non-repudiation), and reliability can also be involved.[29]

24 Germany Cyber Security Strategy.
25 EC (2008) Council Directive. 114/EC.
26 ENSIA (2012) National Cyber Security Strategies - Practical Guide on Development and Execution.
27 CNSS (2010).
28 Venter & Eloff (2003).
29 ISO/IEC 27000 (2009).

3.1.2 Cyber Crisis Management

It is often the case that popular definitions frequently referred to within the field of general crisis management have simply been transferred to the field of Cyber Crisis management, i.e. the same definition of crisis is applied to contingencies in cyber space.

	EU and national	Academia	Best practice
Cyber-incident	A (cyber) incident is a disruption of IT services where the expected availability of the service disappears completely or in part. It can also be the unlawful publication, obtaining and/or modification of information stored on IT services.[30]	Violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.[31]	A malicious act or suspicious event that: • Compromises, or was an attempt to compromise, the Electronic Security Perimeter or Physical Security Perimeter or, • Disrupts, or was an attempt to disrupt, the operation of a Cyber System.[32]
Cyber Crisis	An abnormal and unstable situation that threatens an organisation's strategic objectives, reputation or viability. An event that strikes at the heart of the organization.[33]	A serious threat to the basic structures or the fundamental values and norms of a system (in cyber space), which, under time pressure and highly uncertain circumstances, necessitates making vital decisions.[34]	Situation where the equilibrium among the basic components of the system on the one hand, and approach of the environment on the other hand, is disrupted in a serious way.[35]
Cyber Space	Cyber space is the virtual space of all IT systems interconnected at data level on a global scale. The basis for cyber space is the Internet as a universal and publicly accessible connection and transport network, which may be supplemented and expanded through other data networks. In common parlance, cyber space also refers to the global network of different independent ICT infrastructures, telecommunication networks and computer systems. In the social sphere the use of this global network allows individuals to interact, exchange ideas, disseminate information, give social support, engage in business, control action, create art and media works, play games, participate in political discussions and a lot more. Cyber space has become an umbrella term for all things related to the Internet and for different Internet cultures. Many countries regard networked ICT and independent networks operating through this medium as components of their "national critical infrastructures".[36]		The complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form.[37]

30 Netherlands. Cyber Security Assessment.
31 Wilshusen (2014).
32 NERC (2014).
33 Snowdon (2014) Managing a Cyber Crisis. http://www.regesterlarkin.com/news/managing-a-Cyber Crisis-what-is-the-most-effective-way-to-prepare-leadership-teams-for-a-high-tech-threat/.
34 Boin, 't Hart, Stern & Sundelius (2005).
35 Jirásek, Novák & Požár (2013).
36 Austria Cyber Security Strategy.

	EU and national	Academia	Best practice
Cyber Infrastructure	Includes electronic information and communications systems and services and the information contained therein. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example, computer systems; control systems (e.g., Supervisory Control and Data Acquisition); networks, such as the Internet; and cyber-services (e.g., managed security services) are part of cyber infrastructure.[38]		
Cyber Security	Cyber security describes the protection of a key legal asset through constitutional means against actor-related, technical, organisational and natural dangers posing a risk to the security of cyber space (including infrastructure and data security) as well as the security of the users in cyber space. Cyber security helps to identify, assess and follow up on threats as well as to strengthen the ability to cope with interferences in or from cyber space, to minimise the effects as well as to restore the capacity to act and functional capabilities of the respective stakeholders, infrastructures and services.[39]	The most widespread is the notion according to which cyber-security is identified with information security, which refers to protection of information and information systems against being broken into, used, spread, or subjected to service interruptions, unauthorized changes, or destruction, with the aim of guaranteeing their confidentiality, integrity, and availability. The emphasis in information security is put on preventing unauthorized access to information systems. From this standpoint, confidentiality of information is the main consideration.[40]	Preservation of confidentiality, integrity and availability of information in the Cyberspace.[41]

37 ISO/IEC 27032. (2012).
38 NIPP (2009). Partnering to enhance protection and resiliency.
39 Austria Cyber Security Strategy.
40 Putnik (2013).
41 ISO/IEC 27032 (2012).

3.2 Terminology issues

The area of cyber security has developed rapidly, causing a terminological explosion accompanied by a multiplicity of names for the same phenomena - even in English, which is the dominant language of the subject. The terminology commonly used in the field of crisis management and Cyber Crisis management tends to be broad in nature but with a widespread possibility of interpretation. Crossing over from general crisis management to Cyber Crisis management with terminology in tow can thus generate misinterpretations.

While some key concepts and terminology carry a basic definition and are understood similarly by most expert observers, they can also cause misunderstandings among the general public, which lacks the insight of practitioners. For example, defining a Cyber Crisis as a threat to a certain IT-system or to an organization's reputation undermines the possible comprehension of a Cyber Crisis as an event that strikes a nation such as in the case of Estonia, or as e.g., a cross-sectorial attack that threatens the critical infrastructure of an entire society. The key insight here is that the crisis itself is not a threat but rather, as mentioned in the previous chapter, the result of a threat to any number of critical values. These values often go beyond just the technical operation of a handful of IT systems. For instance, even if the system is restored relatively quickly, the actual crisis might remain since the value at stake was, and still is, the public faith in the reliability of the system.

Since an increasing number of employees and managers with different levels of knowledge and expertise need to be able to communicate precisely and effectively about crises, there is a need for codification of the means of communication in this area. However, this clashes with the fact that users of language can be sensitive and critical over the creation of jargon and new meanings of words.[42]

42 Jirásek, Novák & Požár (2013).

3.3 The theory-practice terminology gap

Beyond the differences in terminology in different fields, there is also a fundamental gap between how crisis management is discussed in theory and in practice. This difference also needs to be addressed. Chapter 2 approached the subject from an entirely theoretical perspective, but the terms used there bear little to no resemblance to what is commonly found in crisis planning documents.

Concepts such as "sense-making", "decision-making", and "termination" offer handy analytical tools, but in practice these tasks are almost universally broken down into activities such as "alerting" or "implementation" or "recovery". There is certainly some overlap, and the practical and theoretical realm both make reference to the same terms in different contexts. It is, however, important to highlight that there is a fundamental difference in what they entail.

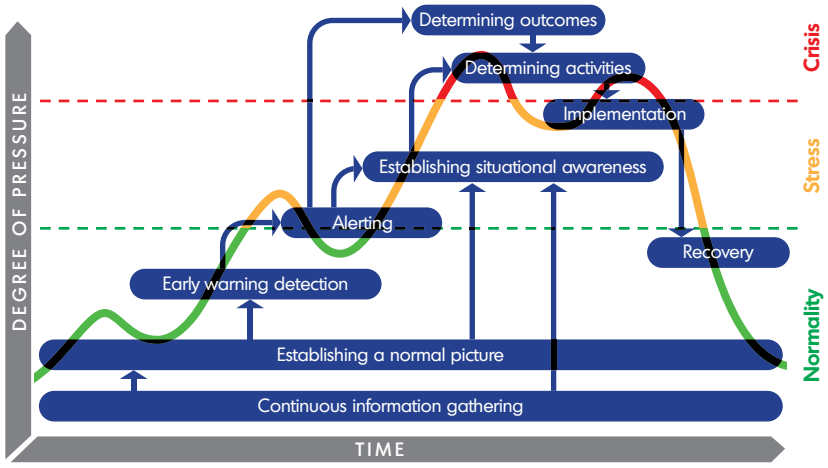


Figure 5: **Practical crisis management activities**

Plotting some common practical tasks over time as in Figure 5 provides something that shows hints of the general structure shown in Figure 3 and, indeed, some of the terms used there make an appearance here as well. While it is possible, at least intuitively, to roughly map some of these activities to the five tasks presented in Boin et al, that intuition is not all that accurate.

As already mentioned, early warning and alerting fall outside of the easy label of sense-making; the activity of establishing a common operational picture straddles the two tasks of sense-making and meaning-making, as does the activity of determining outcomes. Decision-making also includes portions of determining outcomes, and includes having to determine various activities and seeing to their implementation as well. The "recovery" activity in Figure 5 might seem like it should be part of the termination task, but is, if anything, an extension of decision-making–termination deals more with political outcomes and maintaining (or re-establishing) trust and confidence in the system.

In short, while it is certainly tempting to try to map practically-oriented activities to the five analytical tasks, doing so would do both the analytical tools and the activities injustice. The activities in Figure 5 can overlap any number of the analytical tasks and, conversely, each of the five theoretical tasks can contain a wide variety of these practical activities. As such, the analytical realm offers yet another source of terminological confusion, and any mixing of analytical and practical terms should be done with some care.

4. Cyber Crisis Cooperation and Management

This chapter is entirely based on interviews with experts and researchers that are active in the field of cyber crisis management, or have extensive knowledge about the topic. The analysis is based on the responses from the interviews, and the contrasts that can be seen between the actual practices in use and the more theoretically based descriptions and assumptions made in earlier chapters.

Discussing with experts the topics of general crisis management and crisis management in the cyber domain highlighted some of the major differences and similarities between the two. It also illuminated what types of arrangements are being implemented in the European context, as well as on the EU level. There is no silver bullet for how to manage a Cyber Crisis, or on how stakeholders in the public and private spheres can implement collaborative arrangements for addressing incidents or crises in the cyber domain. Nor do there exist arrangements without faults. Discussing these topics also illustrated the on-going developments and the continual process of improving and increasing the capacity of organizations to handle cyber-related incidents.

The interviews indicated that, to a large extent, many of the cooperation mechanisms are based on the fundamental processes used in general crisis management arrangements. This means that IT-incidents, while not serious enough to reach the level of a full-blown Cyber Crisis, are still mainly managed in accordance with the collaborative processes specified in the existing crisis management or response plans, especially on a strategic level. The outcome of this is that, on a strategic level, issues concerning cyber-related threats or vulnerabilities are not treated as long as a crisis is not imminent. Incidents per se are common in the cyber domain, and even recurring or sequential incidents are not unusual. Incidents reaching crisis levels are however rare, although the potential consequences can be substantial. Therefore, not treating incidents as potential crises can be detrimental to cyber security. Also, if a crisis would become a concern at a strategic level, it would mean a shift of mandates and resources across sectors and borders. From a contingency planning perspective–especially in a European context–cross-border and multi-sector cooperation is already crucial, and doubly so in cyber crisis management. The interviewees stress that, since cyber crises by their very nature are not geographically bound or based on sector, cooperation across borders and sectors becomes an absolute necessity in this field. This means that the shifts in mandates become that much more important to assess, clarify and understand for all parties involved.

The five key stages of crisis management discussed in section 2.2 provide an analytical framework for Cyber Crisis management and cooperation, as they illuminate critical issues of crisis management in general. Other aspects that have been taken into account are crisis communication, including terminology issues, as well as response and learning. Figure 6 below highlights some of the most prominent challenges of cyber crisis management based on the analytical framework.

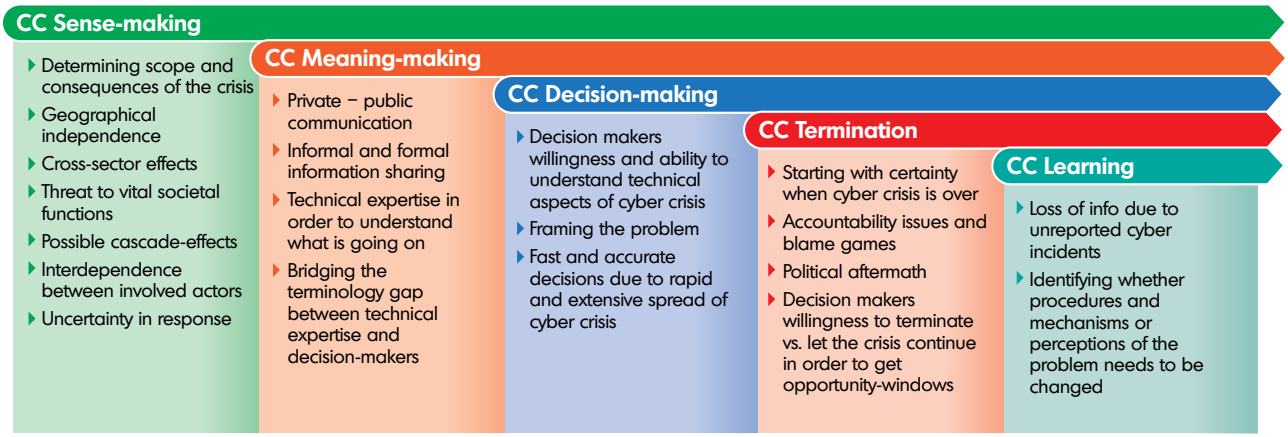


Figure 6: **Cyber Crisis management challenges**

Beyond the added tasks listed here, the way incidents are treated is one of the key differences identified between general and cyber-crises. Whereas general crisis management only really separates matters into crises and non-crises, as discussed in section 2.1 and as illustrated in Figure 1, in Cyber Crisis management, the grey area between the two is, almost universally, clearly categorised as under the reasonably well-defined heading of "incidents". The more general figure can thus be modified to better illustrate how cyber crises are handled, as shown in Figure 7, to include not just this clearer distinction between the different degrees of intensity, but also the added workload generated by the specific challenges of cyber crisis management as listed in Figure 6.

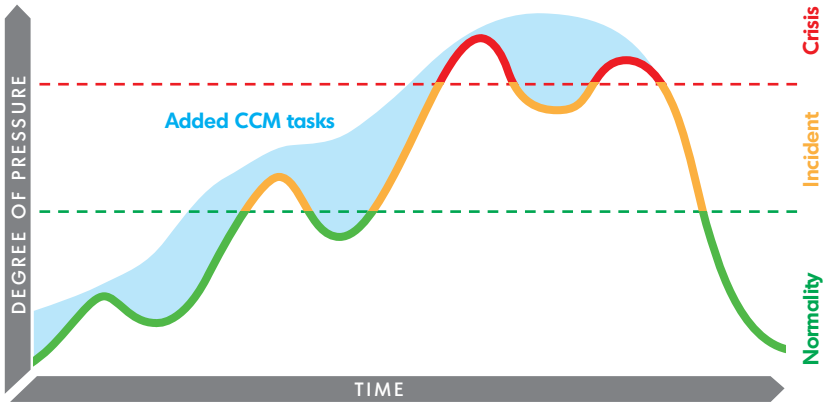


Figure 7: **The intensity pattern of a cyber crisis**

The additional workload created by the cyber crisis challenges means that the dynamic of the crisis could be drastically different than what would have been the case without the cyber aspect. In this figure, the imagined crisis changes from having ups and downs to presenting a slow but steady increase in intensity as the incident grows larger. Once it tips over into a full crisis, that crisis is not just more intense, but also prolonged and continuous, with a heavy workload occurring where there was previously a brief lull in activities. As we will discuss in the section on cyber crisis decision-making, this might entail a situation where the management of the crisis has to be lifted to the highest political level, and previously dormant procedures–or even entire organisations–then have to be activated to deal with the crisis.

What the interviewees point out is therefore an interesting phenomenon, where many institutions never, or only rarely, face any real crises in the system they operate within. Instead, everything stays at an "incident" level of pressure and is handled by managers of subsidiary systems. At this lower level, it may reach crisis proportions, but not for the system as a whole.

Another key difference is that, since there is a distinct "incident" level of activity rather than a swathe of issues that are handled using normal means, the threshold for when matters go beyond what might be considered "normality" is significantly lowered. There is no longer a hard-to-define grey area between the normal and the critical, and an escalation to extra-normal management happens sooner. While there are some intuitive benefits to this, it also has a couple of downsides as will be discussed in the section on learning.

4.1 Cyber Crisis sense-making

The majority of the experts stressed that an incident or crisis within the cyber domain differs from those we are accustomed to in the more general sense, first and foremost from a sense-making perspective. An event in the cyber domain does not become apparent in the same way as a general crisis. A Cyber Crisis can be on-going for an extended period of time before being discovered or causing a large enough impact that the consequences become evident. Hence sense-making processes can be qualitatively different than those during other types of crises. A wide range of activities have thus been initiated, such as a series of workshops and exercises focusing on components and frameworks for modern crisis sense-making and possibilities for further adapting general crisis management structures to more rapidly detect and make sense of cyber-related incidents or crises.

4.1.1 Early warning

The interviewees argue that established early-warning sensors usually only work with already identified threats. They are thus of limited utility in the cyber domain, as threats that cannot be monitored require high quality sense-making when and if they become cyber-crises.

Many national Cyber Security Authorities (and/or CERTs) have established incident detection sensors for early warning signals. Other detection and early warning arrangements include monitoring open sources and media coverage, and information exchange between actors. This exchange could for example take place within a critical infrastructure information exchange forum, which in some cases could include large private companies. In all cases the interviewees report that there are multiple channels for detection, early warning and intelligence gathering.

The detection mechanisms most often consist of:

1. Threshold systems that alert when breached;
2. Ticketing systems for monitoring abnormalities;
3. Developed systems for detection;
4. Network sensors;
5. Surveillance;
6. Open-source intelligence;
7. Reports from private companies;
8. Reports from other countries;
9. Media coverage.

Even though sensor systems and other detection arrangements or mechanisms are crucial for sense-making, the interpretation and analysis conducted by experts is equally important. As reported, any system is rendered useless if the information from that system cannot be interpreted correctly and appropriately translated for decision-makers or emergency services.

In additional interviews, it was explained that detection and reporting is supposed to be carried out by the affected organization, and that it is proximity to the contingency that determines who and how detection is carried out and analysed.

It is also necessary to separate what is an actual threat and what is merely a vulnerability. This is necessary because of several factors:

- Undetected vulnerabilities are immediate threats if they are discovered and become real-time actions.
- Vulnerabilities are not threats when undetected.
- Vulnerabilities can be a known problem.
- Threats are often targeted.

New vulnerabilities are constantly emerging from all directions and in all varieties, due to the complexity of the cyber domain. New vulnerabilities can for example be a result of regular IT-maintenance, a bad patch or update. The differences between a threat and a vulnerability is the fact that a threat does not really exist without an intent or an active agency behind it.

4.1.2 Political sense-making

The interviews suggest that in some cases the crisis sense-making processes determine the involvement from the strategic level. This entails the process going from detection to sense-making, when it becomes determined whether or not the incident is severe enough to be regarded as a crisis, and furthermore if a crisis management group or committee is necessary. If the crisis management group or committee is deemed necessary, the political policy level will be informed, meaning that a large number of detected incidents are never treated at a political level.

Interviews regarding crisis management on a political EU-level suggest that Cyber Crisis sense-making does not differ from general crisis management mechanisms, such as the integrated political crisis response arrangement (IPCR), which cover socio-economic factors and critical infrastructure. However, the lack of experience from past events on cyber-crises that have triggered the crisis management mechanisms on the EU policy level makes it difficult to determine what factors would in fact trigger this mechanism on a policy level. The mechanisms would, if triggered, call for round table meetings with cyber-experts and representatives from all member states in order to activate decision-making processes. The mechanisms require that the threat is imminent, but in some cases, cyber-related incidents or crises do not immediately reveal themselves as such. These mechanisms rely heavily on the member states to alert political bodies on cyber-crises, and provide input on whether or not the issue should be raised to the level of political consideration.

According to the interviews, the political agenda - especially on the EU policy level – to some extent neglects vulnerabilities and incidents, as the focus is on crisis and crisis management, meaning that many types of incidents can occur without triggering political action.

4.1.3 Scope of the crisis

When it comes to cyber crises, one challenge that became apparent in the interviews was the difficulty in determining the scope of the crisis and its possible consequences. The interviewees highlighted the fact that, when comparing general crisis management to Cyber Crisis management, there are several important and special factors inherent to the domain that need to be considered.

One such factor is the geographical cross-boundary nature of cyber crises. General crises have a determined geographical position, and are thus contained within both national borders and sectorial boundaries, which facilitates identifying the proper mandate and response. Of course, there are examples of general crises that have a cross-border and cross-sectorial impact, but the nature of Cyber Crisis inherently exceeds

real-world geographical and political boundaries. Furthermore the cross-sectorial effects of cyber crises threaten critical societal functions to a larger extent than a general crisis, as the escalating effects are more palpable in cyber-incidents or crises. Also the interdependencies between actors within borders and sectors cause uncertainty in the response to a Cyber Crisis. Determining what will be the cause or effect of an Internet service provider "pulling the plug" on their services is complex. Will the effect be that communication fails at another critical service, such as hospitals? There also cases where pulling the plug is not an option, and the crisis must thus be dealt with by other means.

Other factors repeated in the interviews were the challenges in predicting the consequences of cyber-crises, and in some cases even understand the consequences at hand. The combination of escalating factors and the trans-boundary nature of a Cyber Crisis makes it challenging to identify, make sense of, and predict.

4.2 Cyber Crisis meaning-making

Cyber Crisis management is often embedded in general crisis management arrangements, even at the EU-level. However, the interviewees argue that awareness and interest in Cyber Crisis and Cyber Crisis management – as a separate field from general crisis management - is increasing.

It was pointed out in the interviews that some crisis management systems do not label specific types of crisis, but instead focus on the severity and amount of damage for society caused by the crisis in framing the situation.

Some actors handling Cyber Crisis issues strive for solutions that will apply not only in crisis but in everyday working life and in standard operating procedures.

Interviews further show that crises in cyberspace can be especially difficult to detect, both nationally and at the EU-level.

4.2.1 Sharing and understanding dependencies

Many of the experts point out the need to bridge the gap between technical and societal terminology and between different perspectives on cyber-related issues. Some have not been fully confronted with the issue of technical jargon in Cyber Crisis management, but still see a challenge when it comes to making the technical terminology comprehensible for non-technical audiences. This also applies at the EU-level. In crises with a highly technical component, it is difficult for decision-makers to comprehend the full scope of the crisis and its possible consequences. Moreover, it is not always obvious that there is a threat, as there seems to be some reluctance to report cyber-incidents.

What is evident is that when Cyber Crisis management arrangements are separate from the general crisis management system, language barriers will exist and present a substantial challenge. Cyber-security arrangements do not themselves have an issue with technical language. However, if the cyber function has been separated from general crisis management or from the BCM function, the result is a need to tailor incoming information from the technical cyber-security function before it reaches the crisis management structure and decision makers.

Another aspect is the willingness to learn. Crisis management in its basic format is well-known. The Icelandic ash cloud crisis (2011)[43], for example, was easy to understand both in term of its origin and its consequences, especially when compared to cyber crises such as the Estonia attacks in 2007 [44] or Stuxnet [45]. To completely understand these cyber-crises there must be a willingness to learn, since cyber-related issues are heavily reliant on technical knowledge. This to some extent differs from general crisis management, where e.g., manpower can be a part of a solution. In cyber security cases, technical knowledge is the critical currency.

Because of the technical aspect of Cyber Crisis, the experts argue, meaning-making becomes a greater challenge than in general crisis management. It is naturally much harder for both the public sector and for decision-makers to understand cyber-crises due to their complex and technical nature. Technical translation issues have to be dealt with if Cyber Crisis management is to work effectively. Mutual understanding between actors in the Cyber Crisis realm is crucial for improving coordination and cooperation in Cyber Crisis management. Otherwise information sharing in Cyber Crisis management needs to be tailored depending on who the message is for.

The interviews suggest solutions such as having a team translating technical terminology and complex information for external/public communication as well as for political authorities and decision-makers.

National and international networks of experts and practitioners, for example between the national CERTs, seems to be important in increasing the knowledge and understanding of cyber related issues.

Information exchange at the EU-level on cyber-security issues is extensive, with annual seminars, meetings, training and exercises on the topic being arranged to increase understanding.

43 ECC-Net Air Passenger Rights Report 2011
44 Herzog et al (2011)
45 Stuxnet Under the Microscope: Mircosoft

4.2.2 The speed and obstacle of technical jargon

The interviewees stress the importance of responsible actors being prepared and able to handle cyber-crises. If not, they risk losing the trust of citizens. In order for responsible actors to be prepared, they identify a need for a national Cyber Crisis management plan. This due to the special demands of Cyber Crisis management in terms of technical expertise, and because cyber-crises tend to be hard to detect in time, expand rapidly, and can create major cascade effects in society.

4.3 Cyber Crisis decision-making

Cyber Crisis management is often integrated in the general crisis management structures, policies and plans - both nationally and internationally. There could according to interviewees be several processes for Cyber Crisis decision-making, such as establishing common operational pictures, situational awareness reports, analysis, response, recovery, etc. The common operational picture processes is crucial for both the meaning-making and termination processes. The common operational picture as well as situational awareness lay the ground for decision-makers.

Interviewees further elaborate that one way of handling Cyber Crisis is to have a Cyber Crisis management function, separate from the general crisis management structure. This function could coordinate cyber-incidents with the private and public spheres, as well as provide the general crisis management system with information and expertise for decision-making. Some have a crisis committee that meets with representatives from the organizations involved, where decision-making takes place.

Another way is to instead give responsibility for decision-making and crisis management to the people/organization/institution that normally has responsibility for that area/function. Instead of being coordinated from some Cyber Crisis management group, they need to cooperate in order to coordinate and manage the crisis.

In some cases, the responsibility for decision-making depends on the severity of a crisis. On a national level, the government is responsible for the overall management of cyber-crises. Regarding more specified cyber-threats, responsibility falls to the department in question.

In the EU, the question of who is responsible for decision-making depends on where the Cyber Crisis took place, regarding both geography and sector. Cyber Crisis at the member state-level will involve a less direct decision-making process at the EU level due to the principle of subsidiarity. It would instead provide the member states with support and for example organize meetings for the member states in order to manage Cyber Crisis decision-making. Cyber Crisis targeted toward EU-institutions will however be handled by the CERT of the EU Institutions (CERT-EU), with decision-making taking place after a roundtable meeting with specialists and experts.

Figure 8: **Crisis escalations in the EU**

The many levels, actors and institutions involved, as well as the subsidiarity principles that exist both within the EU and in individual nations, mean that the same event will be classified and handled very differently depending on where in the overall European system one looks. Events that are considered a crisis on a national level might only raise an incident flag on the EU level, and be handled without any involvement from the EU political level. Likewise, a Cyber Crisis within a handful of individual organisations–perhaps a small group of companies–will most likely not reach the EU level at all, but rather at most be handled in some national institution for incident coordination. Minor crises within each arena might not even be escalated to the political or strategic level, but rather be handled by some operational body using inter-organisational or international fora as an initial escalation step.

The interviewees also brought up the real-time aspect, i.e. the rapidness of a Cyber Crisis and its cascading effects. This entails that incidents developing towards full-blown crises can undergo a large number of variations such as the rapid developed from an incident; several incidents leading up to a crisis; or a hidden crisis becoming visible. As mentioned in the introduction of this section, this is a key difference between cyber crises and general crises: that incidents constitute their own, well-defined category of events that are managed in their own specific institutional structures and which often keep events from being escalated all the way to a "full crisis" where a strategic decision-making level needs to get involved.

4.3.1 Availability of competence and expertise

In general crisis management, the effectiveness of handling a crisis can be increased by calling in more manpower, for example fire fighters to put out a fire. By contrast, in order to manage a Cyber Crisis, the interviewees point out that it is crucial that the right people with the necessary competence are involved - both in order to make sense of the crisis itself, and to understand the technical language and communicate the proper information to decision-makers. Even if governments consider Cyber Crisis management and general crisis management as one cell, the differences are substantial. In cyberspace, technical expertise is more important than sheer manpower, both from an analytical (meaning- and sense-making) as well as from a response/solution finding point of view. This is not to dismiss that in some scenarios, manpower can also be a contributing factor.

4.3.2 Cross-sector co-ordination

The new cross-sector crisis landscape means that multiple actors in different sectors need to cooperate and share information. Many see the need to improve Cyber Crisis management, communication and coordination between important functions in society. According to experts, cooperation and information sharing between the private and public spheres is especially important in order to handle cyber-crises.

The interviews indicate that information on cyber-related issues is not generally shared between public and private actors because private actors tend to be reluctant to share sensitive information for competitive reasons. However, examples such as the attacks on the Dutch banking system[46] suggest otherwise for certain cases, and informal information-sharing arrangements seem to be quite common both on national and international levels. Some interviewees even contend that the latter are more effective than formal arrangements.

In some interviews it was pointed out that it is hard to coordinate information regarding Cyber Crisis management. Different groups need to be addressed at different levels, and the information needs to be compiled in different ways. A problematic aspect of information-sharing between public and private actors is that it requires a high level of trust. Privacy and compliance is therefore something that could be a serious issue in Cyber Crisis management. It is also challenging to bring together key actors from different sectors for exercises.

According to the experts, formal and informal CERT-networks are used extensively and are generally considered important sources of crisis management support, discussion and information sharing internationally. In case of a serious Cyber Crisis at the EU-level, it is networks for dealing with big crises that apply. However, many of the networks for cooperation during cyber-crises are also used during normal conditions, that is, platforms that are used for other issues could also be used for cyber-security issues.

46 Tiirmaa-Klaar (2013)

4.4 Cyber Crisis termination

When discussing some of the most prominent differences between traditional crisis management and cyber crisis management, the interviewees illustrated several factors regarding the termination of cyber-crises:

- The challenge of really knowing whether or not the Cyber Crisis is over.
- The political aftermath of Cyber Crisis.
- Accountability issues.

The concerns raised by the experts stem from the crisis management challenge of determining when a crisis is terminated. The argument is that the challenges from meaning- and sense-making in the cyber domain adds to the challenge of Cyber Crisis termination. The complex nature of cyber- incidents or crises complicates the termination process to a greater degree than with traditional crisis management.

There are also the political aspects of cyber termination. Some cyber-crises have simply not become a political issue. However, there have been cyber-crises of a more political nature, such as Flame and Prism, where political bodies have become involved and discussions have been raised. Neither of these two, however, resulted in the activation of political crisis management mechanisms such as the IPCR. Furthermore, determining whether or not to terminate a Cyber Crisis can include a political agenda, for example prolonging a crisis for the sake of maintaining a political discussion.

There were reports of cyber crises as acts of one state against another. In these cases there can be a discussion surrounding the definition of such types of contingencies: Is it warfare? Is it a "normal" crisis? Is it espionage? Or is it something completely different?

Some of the interviews also echo the notion presented in chapter 2, that being in a crisis can actually be beneficial, and that it would almost be a wasted opportunity if it ended too soon. A crisis is an excellent

opportunity to raise awareness of an entire issue complex and demonstrate the need for certain solutions. Far from being crass or cynical, it can be something as simple as illustrating the value of regular contacts and more engaged information sharing. The whole issue bleeds into the question of learning and reform, but that is also why it is of such importance: because proper reform requires a properly terminated crisis, that is to say, a termination that takes into account the many different aspects of the crisis and its management.

4.4.1 What was the problem?

Perhaps the primary question that needs to be asked is what the actual problem was. Without this piece of information, it is next to impossible to provide a plausible argument that the crisis is actually over. One detail in cyber crises that complicates matters is that such a definitive answer can be very difficult to get. Just because a system has been restored to working order does not mean that the vulnerabilities are gone and the threats neutralized. As long as those remain, the crisis is merely dormant. The distinction between these two states–dormant and definitively "over"–can also be difficult to describe to the less technologically savvy decision-maker, mirroring the exact same language issues that exist at the beginning of a crisis.

To complicate matters even further, the actual problem might not have been within the (technical) system to begin with, but with the social system surrounding it. In other words, the detection and early warning systems all operated properly, but organizational issues kept the information from escalating the perception of the event to the level of a crisis. Once again, the communication has failed, which is as much a part of the Information Technology system as the hardware and software that one usually associates with the term with. So while it may be easy to say that the crisis was allowed to escalate through a failed early-warning system, no amount of patches and updates may fix the actual seed of that escalation: a lack of knowledge on how to read the signs and/or how to escalate the issue to receive the right level of action.

On a related note, another human factor that needs to be remembered in the midst of all the technical trouble-shooting is that a technical failure may spark a failure of trust. The system has demonstrably been proven to be unreliable, so why should the users come back to it once everything is up and running again? Again, properly identifying and acknowledging the actual problem, and demonstrating that forceful and effective measures have been put into place to keep it from happening again are needed to maintain trust in the system. Should that failure prove to be of a non-technical nature, such measures are if anything even more necessary, since it is now the entire socio-technical construct - the organization, system, individual and all - that has lost the user's faith.

Some classes of problems are of course next to impossible to put an end to. Mistakes will happen, cables will be broken, and software will contain bugs that affect operation, and so on. All of these factors are also embedded in the meaning-making process that extends into the termination phase: explaining why, in spite of all actions taken, we will see similar problems occur in the future. In a sense, this is another case where trust needs to be maintained or rebuilt before the crisis is fully over: even if there is no longer anything technically wrong with the system, it might as well still be completely inoperative if no one deems it worth using.

In short, the actual technical aspects of ending a Cyber Crisis are only a small facet of the crisis termination. As illustrated in earlier chapters, this part of Cyber Crisis management does not differ all that much from general crisis management other than the, by now standard, complication of a jargon barrier, and the added issue of not knowing whether the exposed vulnerability has been fully addressed. Therefore, Cyber Crisis termination is just as rife with "people problems" that have to be solved before the crisis can be declared over as any other type of crisis.

4.5 Cyber Crisis learning & reform

As mentioned in the previous section, learning and reform after cyber-crises often at present suffer from a curious duality in how these crises are handled. On the one hand, some of our interview participants note, a crisis is an attention-grabbing event that demonstrates the need for change. But on the other hand, once the crisis is over, the will for reform quickly fades. At the same time, reform cannot really occur while the crisis remains, or at best it will be very slow or delayed. A few of the interviewees speak of the need for an issue to gain momentum at the very tail end of a crisis in order to keep it on the agenda long enough to implement large-scale change.

During the crisis, specific organisations or actors may have emergency mandates that could conceivably allow them to implement new policies. Those powers however are stripped once the crisis is deemed to be over, so that someone else will have to carry the question of reform. In practice, this rarely happens.

On a more positive note, cyber-crises at the very least act as focusing events and demonstrate the complexities of the field. They illuminate the need for preparedness and - increasingly often as more and more systems become integrated or at least intertwined - a need for co-operation in solving what might look like a local problem. More actors get involved, which also raises the issue of having everyone act in a cohesive manner that does not hinder more than it helps. This is an area, in particular, where the interviews provided many examples of how constant learning and the guidance of newcomers is needed to facilitate their interaction with established actors.

4.5.1 Slowing factors in the learning and reform process

When change is required as a response to a Cyber Crisis on the national or international level, it is both a question of the particular political level figuring out what went wrong, and of considering the legislative issues that need to be resolved. Cyber Crisis involves additional levels and challenges compared to general crisis management, including the technical aspects, the fact that Cyber Crisis can be hard to detect in time, and the possible cascade effects. To a much greater degree than in cases of general crisis management, there is a vast amount of information that needs to be grasped and coordinated during instances of Cyber Crisis management. Furthermore, due to the complex nature of cyber crisis, learning and reform is difficult to implement.

Some experts would like to see Cyber Crisis management developed separately from general crisis management, while others state that they would rather have Cyber Crisis as an integrated aspect of general crisis management.

Even though smaller companies and organisations have started building their own CERT-like capabilities, and are becoming increasingly competent to deal with Cyber Crisis management, some companies instead request help from third party service providers. The interviewees argue that this could make the learning process slower in the case of a Cyber Crisis. The more they start handling incidents in-house, the less of an incentive there is to share knowledge and crisis management operations with other actors. Since these types of problems can soon involve sensitive company information, the willingness to share is reduced even further, even in instances where it would be obvious that other parties are being affected by the same problem. As a consequence, the willingness to expose those vulnerabilities and share experiences, be it in open seminars or in joint exercises, can easily evaporate and consequently create fertile ground for poor, or at least ill-prepared, crisis management at a later date.

This also ties in with the previous observation that many would-be crises in the cyber realm only reach an "incident" level of pressure for the system, which drastically reduces the incentives and perceptions of need for initiating any kind of large-scale reform. Again, it is the lower level, where matters might actually escalate to a crisis level, that the learning has any chance of taking place, yet that impetus for reform does not really "leak" out into the larger crisis management system.

4.5.2 Lessons learned and reform information-exchange

The interviews suggest that there is a cultural change going at the EU-level regarding sharing information about lessons learned and reform. Actors used to hold on to information rather than share it. However, since closer cooperation and sharing is regarded as critical in order to deal with cyber-crises, tradition is changing. There are however many different sectors, intents and methodologies that would need to be aligned in the EU if there were ever to be a single standard. This process of increased information sharing will take time.

Some of the interview subjects mentioned that in order to improve Cyber Crisis knowledge and management, one could draw from experience and copy the most common best practices from other systems. CERT-communities reportedly play an important role for this kind of information sharing. Somewhat curiously, there was little mention of any of the more public events, such as security conferences and scientific research communities. The question of what constitutes a best practice thus becomes a bit confounding, as there does not seem to be any coherent effort to actually collect, compare, and contrast such practices within a larger pool of examples. No doubt, good practices can be extracted from a smaller community of participants as well, but it is equally certain that it could be further improved and facilitated by increasing the pool.

4.5.3 Learning from exercises

Interviewees state that exercises are important learning tools to draw experience from when no Cyber Crisis has yet happened. Exercises raise awareness and are an important part of communication between the technical and non-technical parts of Cyber Crisis management. Yet there are often small incidents for individual actors to learn from. Direct experience obviously yields a stronger response, while exercises mostly serve as a means for building awareness. Since attacks are becoming more severe, perhaps not in number but in their precision and in the actual damage they cause, a different focus has evolved. The experience of a cyber-attack jolts and motivates the political-legal system to implement new processes.

Creating exercises at the correct level for improving Cyber Crisis management is often seen as quite resource intensive. Moreover, many cyber-incidents are handled internally, within a nation or a company. Some experts suggest that the high number of unreported cyber incidents indicate that a change in approach to Cyber Crisis management is necessary. This suggests that perhaps the exercise tool is not always used appropriately. Instead of smaller, more frequent exercises to keep up-to-date with a highly dynamic problem field, the matter is allowed to "boil over". It is left alone until it becomes absolutely untenable to not address it immediately, which invariably means pushing the entire organisation through some kind of exercise as soon as possible at great expense.

These large-scale and intensive exercises also entail that they cannot be tailored for different needs: all are tested at once in a single scenario that fits everyone, rather than practitioners being trained in specific issues of more critical need. The upper management level might need an exercise that entirely focuses on collaboration with different actors and meaning-making in relation to the general public. The technical level might need an exercise that focuses on explaining to upper management what the problem is. Key points of contact in two different organisations might need to train crisis communication and co-ordination. Each exercise on its own does not need to be all that complicated; complexity arises if and when one tries to fit all those requirements into a single massive session.

More fundamentally, though, and far from being a unique problem with Cyber Crisis learning, is that research shows that a large portion of organisations need to exercise simply to learn how to do exercises. In the field of organisational learning, there is the concept of "learning how to learn"–that is, learning how to draw good lessons from an experience and to adjust processes accordingly. This is a skill that is often lacking at all levels. As a result, ambitious exercises are being set up solely on the principle that exercises are inherently good. Yet the ability to actually benefit from them turns out to be lacking, and very little of consequence is actually learned. So with Cyber Crisis learning, as with any learning, there is a widespread need to start doing more modest exercises that, while they can certainly still touch on topics related to cyber-crises, are more aimed at teaching the participants how to draw substantial and actionable knowledge from their own training sessions.

4.6 Cyber Crisis communication

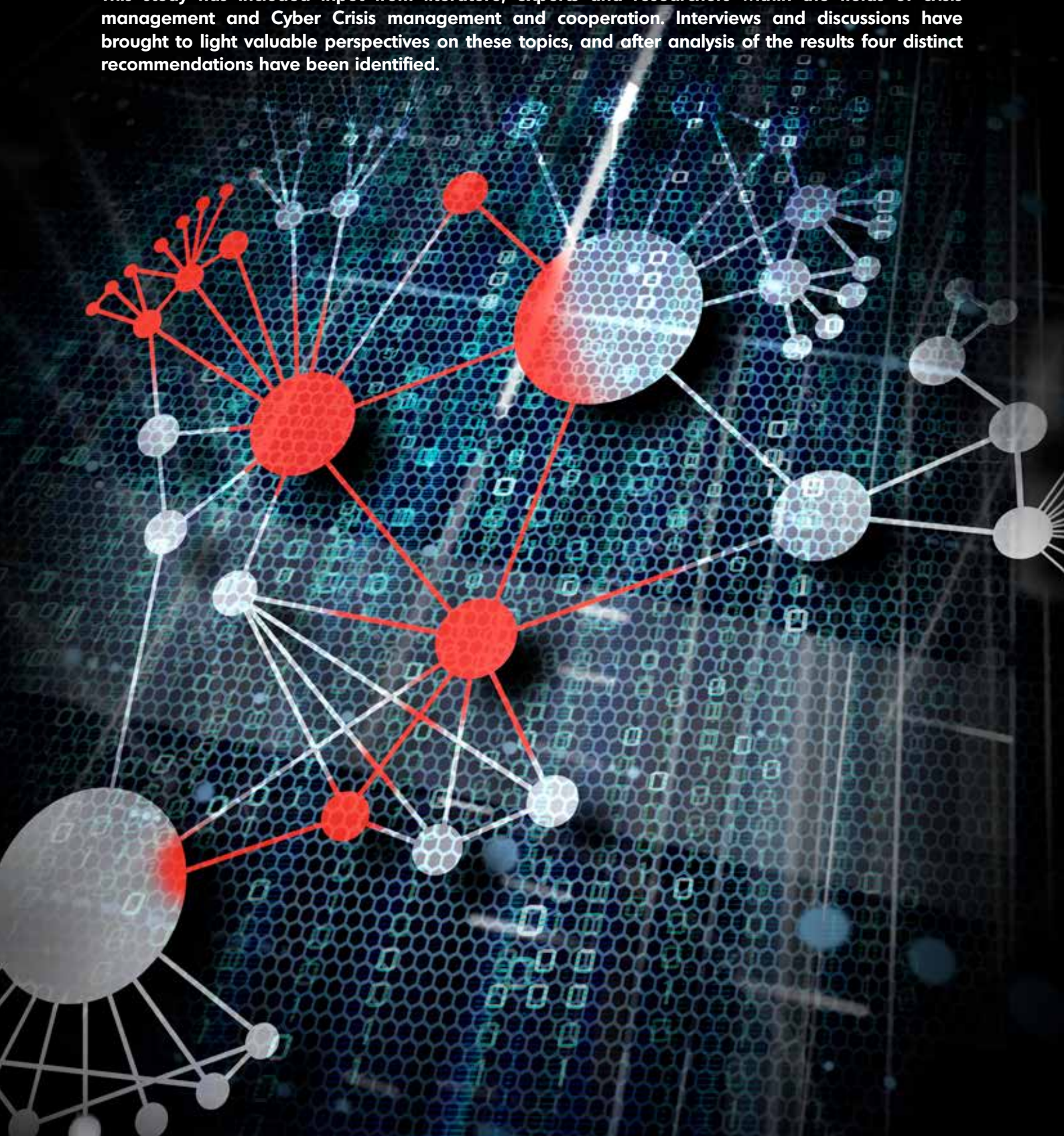
For effective crisis management, information is critical. Crisis managers depend on reliable information, yet the availability of robust infrastructure for gathering information, analysis and dissemination is not always available. Crisis communication is thus critical in order to support decision making activities.

As touched upon earlier, Cyber Crisis communication faces challenges due to the language barriers caused by technical jargon that is often not understood by decision makers. Interviewees explain that in some cases cyber centres have to act as liaisons between decision makers, media, the general public and the technical staff. There have been examples where it was necessary to separate the technical divisions from the other departments in order to minimize the possibility of misinterpretations. There have also been cases where the media reported misleading information due to their own misinterpretation of technical information.

The challenge is not only the language barrier itself but that there are few people that have both the technical expertise and the appropriate policy knowledge necessary on the policy level. This suggests that there is need for a liaison as an extra knowledge broker in the cyber crisis-management process.

5. Recommendations

This study has included input from literature, experts and researchers within the fields of crisis management and Cyber Crisis management and cooperation. Interviews and discussions have brought to light valuable perspectives on these topics, and after analysis of the results four distinct recommendations have been identified.



5.1 Create common cyber crisis management terminology and enhanced knowledge

It became evident that a European-wide glossary covering the terminology and definitions commonly used within field of cyber security, including crisis management, would prove beneficial from several perspectives, such as communication between experts and the public. This glossary would then serve as the key reference for e.g., strategies, standards and guidelines.

The field of cyber crisis management has barely been researched, and the feedback from interviews suggested that further studies are both encouraged and necessary.

1) Develop a comprehensive Cyber Crisis Management Glossary

The first steps towards establishing a common understanding of cyber crisis management terminology is to draft a glossary covering the terminology and definitions commonly used within the field of cyber security, including crisis management.

Specifically, as a first step towards a common terminology in a European context, we recommend that a Cyber Crisis management glossary be drafted and published. Furthermore, to ensure a strong European commitment, an EU organization such as ENISA should be responsible for the development of the glossary.

2) Gain further knowledge regarding Cyber Crisis Management

We recommend that a series of studies covering the topic of Cyber Crisis management should be initiated, especially in a European context. Further studies can for example focus on:

- Mapping of the cyber crisis structures in the EU;
- Roles and interaction between technical levels and decision-makers;
- Deeper studies on the role and function of cyber security centres in crisis management.

The responsibility for international studies could be with ENISA or other EU institutions depending on the focus of the study.

5.2 Information campaigns for an increased understanding of cyber crisis management

Supporting knowledge raising activities should be implemented to a larger extent, since cyber crisis management is generally complex and even personnel active in the field lack knowledge on areas other than their own.

3) Initiate informative awareness-raising activities

More concretely, we recommend the implementation of knowledge creation activities such as education programmes, seminars or workshops/conferences for targeted audiences, with themes such as:

- Cyber crisis from a technical perspective;
- Cyber crisis from a decision-making perspective;
- Understanding the processes of cyber crisis management;
- Cyber risk, vulnerabilities, threats, and their possible consequences.

This should be the cyber security community's responsibility in general, with initiatives taken by appropriate Member States agencies and/or EU-institutions.

4) Support training and exercise in the field of cyber crisis management

Targeted exercises for certain functions and sectors are encouraged. Vital societal functions and critical infrastructures as well as private sector stakeholders should also be exercised in cyber crisis management, perhaps regularly.

We recommend training and exercise activities of any scope:

- National and international;
- Inter-sectorial and cross-sectorial;
- Specific to the technical or strategic level.

The training and exercise activities are the responsibility of national governmental agencies within and public organizations. We would also encourage central EU organizations such as ENISA to provide expertise and guidance on cyber crisis management exercises.

5.3 Support activities for enhanced sharing of information, best practices and the development of cyber crisis management procedures

It is recommended that activities that encourage exchange of knowledge and experiences are supported. We also recommend supporting new initiatives for sharing best practices or the development of well-tested methodologies and best practices.

5) Support the development and sharing of strategic cyber crisis management practices and procedures

The development of cyber crisis management response plans, action plans, information sharing procedures and tools, other strategic documents such as guidelines, handbooks and procedures should be encouraged and supported, since these increase capacity for dealing with cyber crisis. It is in everyone's interest that activities concerning prevention and preparedness, such as the development of action plans, receive support, especially from institutions with knowledge and insight into cyber crisis management.

The arenas or platforms should encourage activity under normal conditions as well as during situations of stress. For example, prevention tasks like establishing situational awareness by mapping the normal situations and practices should be supported in order to detect abnormalities at an early stage and to improve sense-making.

We recommend a concerted effort to create national and EU-level plans using a shared terminology and giving due attention to the complex and interconnected nature of the management and escalation of cyber crises and incidents in a European context. The supporting responsibility therefore lies with ENISA together with appropriate cyber crisis organisations within Member States to assist in the development of these kinds of procedures or plans.

Also, we recommend that ENISA together with appropriate organisations within the Member States not only encourage the sharing of well-tested best practices and tools, but also support in the process of developing new best practices through training and exercise, or to test practices for analysis and evaluation.

6) Enhance information sharing and collaboration between private and public organizations

Methods for information sharing in both preventive and handling purposes are crucial. Operational information sharing with information flows that can be interpreted by both private and public organizations are encouraged. Normative guidance, including developing generic templates and models for Cyber Crisis management, should be instituted. The analysis suggested that important information is being kept secret by larger private entities and other actors. Establishing mechanisms for sharing such information without jeopardizing that sensitive information is leaked or be exposed is therefore of great importance.

More specifically, we recommend that measures be taken to develop methodologies for operational cyber crisis management information sharing in order to increase exchange of knowledge for cyber crisis preventive and handling purposes.

This is not only the responsibility of central EU institutions, but of the cyber crisis management community as a whole together with appropriate Member State agencies.

6. References

6.1 Interview subjects

The following individuals were interviewed for this study. Their specific contributions have intentionally been anonymised and specific statements left unreferenced.

1. Helena Andersson, MSB, Sweden
2. Hans Oude Alink, NCSC, The Netherlands
3. Charles Baubion, OECD
4. Johannes Clos, BSI, Germany
5. Marika Ericsson, Uppsala University, Sweden
6. Arya Honarmand, Director General European Commission
7. Uwe Jendricke, BSI, Germany
8. Michalis Ketselidis, European Commission
9. Lauri Luht, RIA, Estonia
10. Tarik Meziani, Council of the European Union
11. Timo Mischitz, BKA, Austria
12. Adrien Ogee, ANSSI, France
13. Andreas Reichard, BKA, Austria
14. Urmo Sutermäe, RIA, Estonia

6.2 Literature

1. Bird, L. (2011). *Dictionary of Business Continuity Management Terms.* Business Continuity Institute [http://www.thebci.org/glossary.pdf]
2. Birkland, T. A. (2006) *Lessons of Disaster: Policy Change After Catastrophic Events.* Washington, D.C: Georgetown University Press.
3. Boin, A., 't Hart, P., Stern, E. & Sundelius, B (2005). *The politics of crisis management: public leadership under pressure.* Cambridge: Cambridge University Press
4. Boin, A., McConnel, A. & 't Hart, P. eds. (2007) *Governing after Crisis – The Politics of Investigation, Accountability and Learning.* Cambridge: Cambridge University Press
5. Bovens, M. & 't Hart, P. (1996) *Understanding Policy Fiascoes. N.J.: Transaction Publishers* EC. (2008). COUNCIL DIRECTIVE 2008/114/EC. Official Journal of the European Union.
6. Clarke, L. (2002). *"Panic: myth or reality?"* Contexts, 1(3), 21-26.
7. George, A. (1993) *Bridging the gap: Theory and practice in foreign policy. Washington, D.C.: United States Institute of Peace Press*
8. Herzog, S. (2011) *"Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses."* Journal of Strategic Security 4, no. 2, 49-60
9. Janis, I. (1982) *Groupthink,* 2. ed., rev. and enl. Boston: Houghton Mifflin
10. Jirásek, P. Novák, L. and Požár, J. (2013) Cyber Security Glossary. National Cyber Security Center of the Czech Republic and the National Security Authority of the Czech Republic. Prague.
11. Kingdon, J. (1995) *Agendas, alternatives, and public policies.* 2. ed. New York: HarperCollins College Publishers
12. Koraeus, M. (2008) Who Knows? – *The Use of Knowledge Management in Crisis.* Crisis Management Research Program vol. 36. Stockholm: CRISMART, National Defence College
13. Koraeus, M. (2015) *Stressing Knowledge – Modelling outside pressure on organisational knowledge* (title tentative). Nijmegen: Radboud Universiteit. Forthcoming.
14. McCullar, S. (2013). *Decision-making.* In K. Penuel, M. Statler, & R. Hagen (Eds.), Encyclopedia of crisis management. (pp. 245-247). Thousands Oaks, CA: Sage Publications, Inc.
15. McNabb, D. (2007) *Knowledge Management in the Public Sector – A Blueprint for Innovation in Government.* Armonk, NY and London, England: M. E. Sharpe.

16. Nonaka, I. and Takeuchi H. (1995) *The Knowledge-Creating Company: How Japanese Companies Create the Dynamics of Innovation*. Oxford, England: Oxford UP.

17. Nthakomwa, M. (2013). *Response/Countermeasure*. In K. Penuel, M. Statler, & R. Hagen (Eds.), Encyclopedia of crisis management. (pp. 820-828). Thousand Oaks, CA: SAGE Publications, Inc.

18. Paton, D. (2013). *Incident management*. In K. Penuel, M. Statler, & R. Hagen (Eds.), Encyclopedia of crisis management. (pp. 503-507). Thousand Oaks, CA: SAGE Publications

19. Putnik, Ž. (2013). *Cyber security*. In K. Penuel, M. Statler, & R. Hagen (Eds.), Encyclopedia of crisis management. (pp. 218-220). Thousand Oaks, CA: SAGE Publications, Inc.

20. Regester, M & Larkin, J (2008). *Risk issues and crisis management in public relations: a casebook of best practice*. 4th ed. London: Kogan Page

21. Rosenthal, U., Boin, A. & Comfort, L. eds. (2001) *Managing Crises – Threats, Dilemmas, Opportunities*. Springfield, Ill: Charles C Thomas

22. True, Jones & Baumgartner (2007) *Punctuated Equilibrium Theory: Explaining Stability and Change in Public Policymaking*. In P. Sabatier, (Ed.) Theories of the Policy Process, 2nd ed. Boulder, Colorado: Westview Press, pp. 155-187.

23. Heli Tiirmaa-Klaar, 2014. *Botnets (Springerbriefs in Cybersecurity)*. Springer London,

24. Venter, H. S., & Eloff, J. H. P. (2003). *A taxonomy for information security technologies*. Computers & Security, 22(4), 299–307.

25. Wilshusen, G. C. (2014). *INFORMATION SECURITY: Agencies Need to Improve Cyber Incident Response Practices*. GAO Reports, pp. 1-50

26. Yumagulova, L. (2013). *Interdependence*. In K. Penuel, M. Statler, & R. Hagen (Eds.), Encyclopedia of crisis management. (pp. 534-537). Thousand Oaks, CA: SAGE Publications, Inc.

6.3 Policy

27. NSPD. *White House Cyberspace Policy Review*. 54/Homeland Security Presidential. [http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf]

28. EC. (2008). COUNCIL DIRECTIVE 2008/114/EC. Official Journal of the European Union.

6.4 Strategy

29. NRF. (2008). *National Response Framework*. Homeland Security. [http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf]

30. MSB. (2011). *Handlings Serious IT-Incidents*. MSB339. [http://www.qcert.org/sites/default/files/public/documents/SE-PL-Handling%20Serious%20IT%20Incidents-Eng-2011.pdf]

31. MSB. (2011) *Handling Serious IT-incidents: national response plan, interim version*. MSB339. [https://www.msb.se/RibData/Filer/pdf/26085.pdf]

32. Committee on National Security Systems. (2010). *National Information Assurance (IA) Glossary*, CNSS Instruction No. 4009. [http://www.ncix.gov/publications/policy/docs/CNSSI_4009.pdf]

33. Austria. *Cyber Security Strategy*.

34. Germany. *Cyber Security Strategy*.

35. Netherlands. *Cyber Security Assessment*.

6.5 Web

36. 2014-09-09. ENISA Web (2014). *What is CSIRT?* [https://www.enisa.europa.eu/activities/cert/support/guide2/introduction/what-is-csirt]

37. 2014-09-09. Dickinson, I. (2013). *National Resilience Extranet Common Operating Picture*. NW/Pj/ResComms/4902. [https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/79250/National_Resilience_Extranet_Common_Operating_Picture_v1_1_report_0.pdf]

38. EHSC (2008). *Environment, Health and Safety Committee Note on: Environmental Risk Assessment.* [http://www.irl.ethz.ch/plus/education/BSc_level/102-0516-01L_alt/RSC_EnvironmentalRiskAssessment.pdf]

39. ECC-Net Air Passenger Rights Report (2011). [http://ec.europa.eu/consumers/ecc/docs/ecc_net_air_passenger_report_2011.pdf]

40. Jacobsson, A. (2012). *Att lära stort från små incidenter – en handledning med fokus på att utvärdera effektiviteten i lärandet*. MSB430. [https://www.msb.se/RibData/Filer/pdf/26272.pdf]

41. Lavoix, H. (2014). *Developing an Early Warning System for Crises.* [http://eeas.europa.eu/ifs/publications/articles/book2/book%20vol2_part4_chapter47_developing%20an%20early%20warning%20system%20for%20crises_helene%20lavoix%20and%20ifri.pdf]

42. IIEP. (2006). *Capacity Building. Guidebook for Education in Emergencies and Reconstruction.* UNESCO. [http://www.iiep.unesco.org/fileadmin/user_upload/Research_Highlights_Emergencies/chapter3.pdf]

43. NCIRP. (2010). *National Cyber-incident Response Plan.* Homeland Security. [http://www.federalnewsradio.com/pdfs/NCIRP_Interim_Version_September_2010.pdf]

44. NERC. (2014). *Glossary of Terms Used in NERC Reliability Standards.* [http://www.nerc.com/files/glossary_of_terms.pdf]

45. Booz Allen Hamilton. (2011). *Resilience in the Cyber Era – Building an Infrastructure that Secures and Protects.* [http://www.boozallen.com/media/file/resilience-in-the-cyber-era.pdf]

46. Palomares Summary Report (1975). [http://www.dod.gov/pubs/foi/International_security_affairs/spain/844.pdf]

47. Stuxnet Under the Microscope [http://www.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf]

48. 2014-09-08. NATO. (2011). *Crisis Management.* [http://www.nato.int/cps/en/natolive/topics_49192.htm]

49. MSB. (2011). *Guidance for risk and vulnerability assessment* [https://www.msb.se/RibData/Filer/pdf/25893.pdf]

50. 2014-09-09. NRC. (2014). *Incident response.* [http://www.nrc.gov/reading-rm/basic-ref/glossary/incident-response-ir.html]

51. NRC. (2005). *NRC Incident Response Plan: Revision 4.* [http://www.nrc.gov/about-nrc/emerg-preparedness/respond-to-emerg/incident-response.pdf]

Annex A: Methodology for this study

This study had a two-fold approach, the first being a pure literature study where general crisis management systems and terminology in the field of crisis management were reviewed. The second approach was focused on the cyber security sphere. This field was studied mainly through interviews. The cyber security field has been important for some years now, yet the number of studies in the field of Cyber Crisis cooperation management are scarce. Hence the interview approach. Meanwhile the field of crisis management is far more studied both on the national level as well as on the EU level.

The analysis in this study was based on the responses from the interviews and the analytical framework. The theoretical framework allowed the study to analyse the interview responses and systematically answer the research questions.

A.1 Interviews

This study employed a semi-structured interview method. This approach was suitable as it maintained some level of control while still being flexible enough for the interviewee to provide information beyond the set interview guideline. This approach allowed the interviewer to ask open ended questions that allowed the interviewee to guide the information flow if necessary.

The requirements of the interviewees were that they were either experts in cyber related issues or academics conducting research within the field of cyber security.

Since the study is a synthesis of the state of a number of countries and EU institutions, the specific contributions of each interviewee are intentionally left unmentioned, and the individuals are not directly quoted or linked to any given statement.

A.2 Comparative approach

In order to compare and contrast general crisis management systems with the corresponding systems related to Cyber Crisis management, a comparative approach was selected. This approach allows the literature study of general crisis management to be compared to the interview results focusing on cyber-security. This approach allows the study to analyse the differences and compatibilities between general and Cyber Crisis management with examples from Member States and organizations within the EU. This aim is further reinforced by the conceptual analysis, which aimed to highlight and clarify any similarities and differences that purely come down to different terminology being used in the different fields.

A.3 Delimitations

This study did not include all of the European Union's Member States since the aim was to explore and lay the ground for possible future research. This study did however include examples from Member States. These Member States were chosen on both the basis of availability and by their track record of making substantial efforts in the cyber sphere.

Annex B: Definitions and Abbreviations

B.1 Definitions

Alarm — Notification of a present or imminent danger.

Alert — A formal notification that an incident has occurred which might develop into a Business Continuity Management or Crisis Management invocation.[47]

All-Hazard — An "all-hazards perspective" covers adaptive, proactive and reactive strategies before, during and after a disruptive incident.[48]

Asset — Anything that has value to the organization.[49]

Capacity Building — Capacity building is the process by which individuals, groups, organizations, institutions and societies increase their abilities to: 1. Perform core functions, solve problems, define and achieve objectives: and 2. Understand and deal with their development needs in a broad context and in a sustainable manner.[50]

Counter Measures — Response refers to the activities undertaken to counteract the further escalation of a set of events that potentially leads to crisis or disaster. The single most important issue at this point in time ceases to be about planning for some once-distant and unknown disaster; instead, the focus at this stage is to ameliorate the worst effects of an emergency crisis or disaster situation. For this reason, response will comprise activities, often attempts or interventions, aimed at changing the trajectory of a worsening situation.[51]

Consequence Assessment — Estimation of the probability of the consequences. There are three components to this, the presence of the hazard, the probability of the receptors being exposed to the hazard and the probability of harm resulting from exposure to the hazard.[52]

Common Operational Picture — A continuously updated overview of an incident compiled throughout an incident's lifecycle from data shared between integrated systems for communication, information management, and intelligence and Information sharing. The common operational picture allows Incident Managers at all levels to make effective, consistent, and timely decisions.

The common operational picture also helps ensure consistency at all levels of incident management across jurisdictions, as well as between Various governmental jurisdictions and private sector and non-governmental entities that are engaged.[53]

47 Bird (2011).
48 ISO/TC 223.
49 ISO/IEC 27000:2009.
50 IIEP (2006).
51 Nthakomwa (2013).
52 EHSC (2008).
53 NCIRP (2010).

Situational Awareness	The knowledge and understanding of the current operational status, risk posture, and threats to the cyber environment gained through instrumentation, reporting, assessments, research, investigation, and analysis, which are used to enable well-informed decisions and timely actions to pre-empt, deter, defend, defeat, or otherwise mitigate against those threats and vulnerabilities.[54]
Status Report	Report based on verified information and explicit details (who, what, when, where and how) related to the incident/crisis. Status reports can be or contribute to warnings for the wider public thus providing emergency information.[55]
Decision-Making	Decision-making refers to the process a person goes through in order to make the choices necessary during a crisis. During a crisis this skill is critical for a leader. During a crisis the stress level rises and the ability to make decisions becomes harder as a result of the added burdens.[56]
Dependencies	Dependencies refers to the complex, interconnected and interdependent atmosphere that today's society demands. For example the global economy is increasingly dependent on interconnected networks of infrastructures that are spread across multiple temporal and spatial scales and serves as the critical lifelines to the functioning of the modern society. In short, there are few occasions where a crisis only affects one actor or unit alone. Dependencies also refers to an organizations reliance on other organizations or actors for their existence.[57]
Early Warning	A system that enables preventative measure due to detailed diagnosis for decision-making in order to intervene, plan and implement a response to a crisis or incident.[58]
Service	Critical infrastructures or societal services are organization and institutions with major importance for the public good, whose failure or damage would lead to sustainable supply bottlenecks, considerable disturbance of public security or other dramatic consequences. At federal level, the following areas have been identified: Energy, information technology and telecommunication, transport, health, water, food, finance and insurance sector, state and administration, media and culture.[59]

54 CNCI (2009). Partnering to enhance protection and resiliency.
55 NRF (2008). National Response Framework.
56 McCullar (2013).
57 Yumagulova (2013).
58 Lavoix (2014).
59 Cyber Security Strategy, Germany

European Union Agency for Network and Information Security

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias Str.
ENISA building
Marousi 151 24, Athens, Greece

enisa.europa.eu

Catalogue Number: TP-05-14-030-EN-N