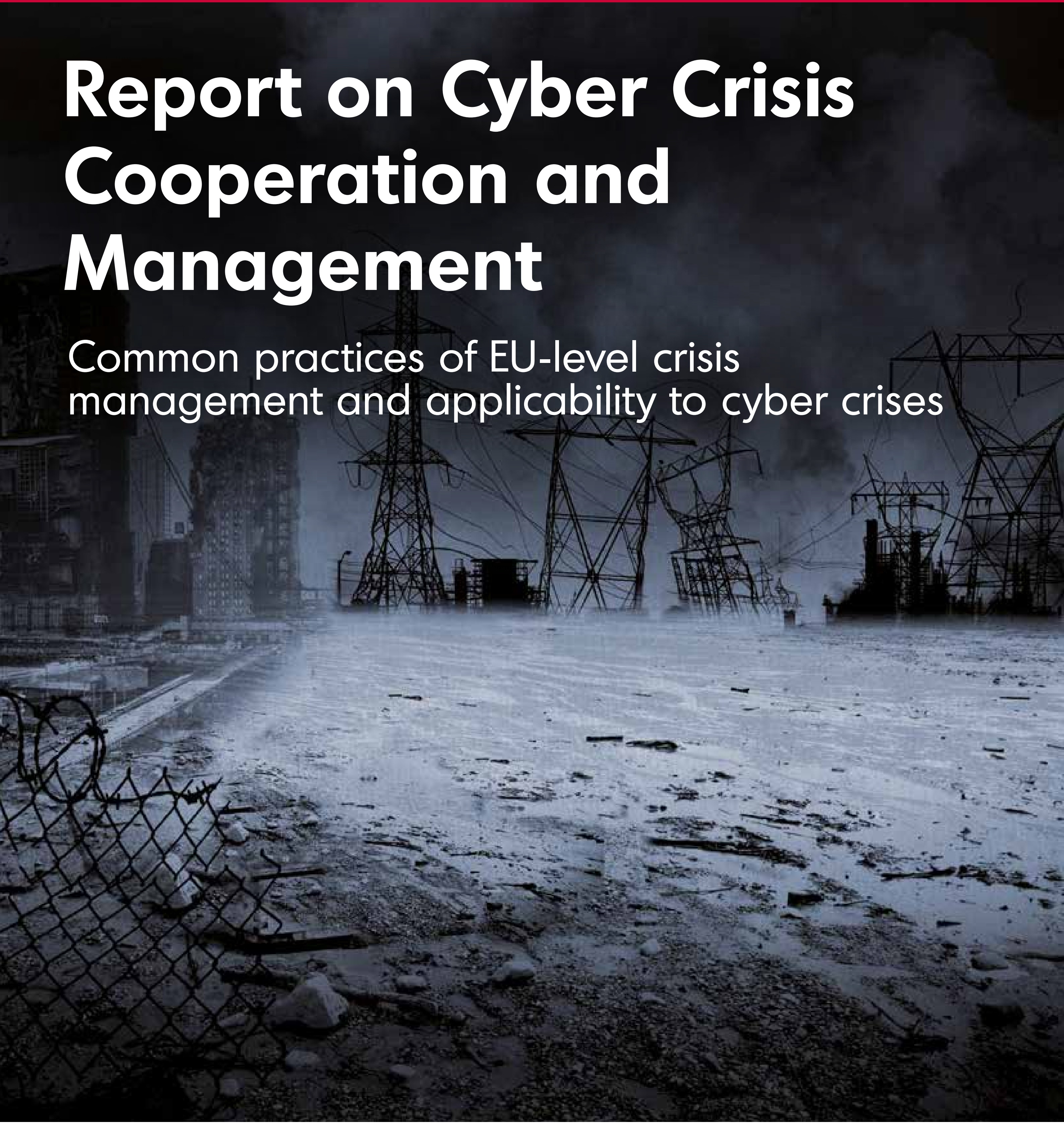
European Union Agency for Network and Information Security

Report on Cyber Crisis Cooperation and Management



Common practices of EU-level crisis management and applicability to cyber crises

December 2015

enisa.europa.eu

Common practices of EU-level crisis management and applicability to cyber crises

Authors

Panagiotis Trimintzios, Adrien Ogee, Razvan Gavrila and Alexandros Zacharis.

Contact

To contact the authors please use c3@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to thank Deloitte Belgium, notably Dan Cimpean, Anna Lauridsen, Stine Werbrouck, Patrick Kozakiewicz and Alexander Cespedes Arkush who helped co-author this report and extend its deepest gratitude to the experts who took the time to be interviewed and whose expertise and views have informed many of the findings and suggestions of this study (full list available in Annex C).

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

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

This publication is intended for information purposes only. It must be accessible free of charge. Neither

ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ISBN: 978-92-9204-165-6 – DOI: 10.2824/948513 - Catalogue Number: TP-01-15-966-EN-N

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.

Executive Summary

Despite a number of initiatives within the European Network and Information Security community to establish frameworks and standard operating procedures, the **EU-level response to cyber incidents** and in particular those which lead to responding to crisis situations, **lack consistency**. Today, should a crisis arise from a large-scale cyber incident, Member States would need a harmonised framework to effectively respond to the challenges posed by such an incident.

Based on a detailed analysis of five different EU-level crisis management frameworks, this report **highlights lessons learnt** from years of crisis management in five different sectors, which would be applicable to the cyber domain, and **provides a series of key recommendations** regarding EU-level priorities to alter the outcome of the next cyber crisis.

In recent years, the need for a robust EU-level response mechanism to manage cross-border threats has become overwhelmingly apparent within several sectors. The challenges faced by the EU in coordinating a common response have been highlighted following a number of crises, notably the **volcanic ash cloud** over Iceland in 2010 [1], **pandemics** such as the influenza virus in 2009 [2], and, with increasing frequency, **terrorist attacks** on European soil [3]. These crises have all sparked EU-level action, and indeed prompted the emergence of common legal and operational frameworks.

EU-level crisis situations originating in one or more cyber incidents are not commonplace: so far only the 2007 crisis in Estonia was ever called a "cyber crisis" [4]. This single event sparked, just like the volcanic ash cloud or the influenza virus, various initiatives at European level to improve the response against such incidents. The 2009 CIIP Communication [5], the Telecom Package [6], the EU Cybersecurity Strategy [7], the Digital Agenda for Europe [8] and the Cyber Europe exercise series [9]: all followed this event. Yet as the latter has shown repeatedly [10], crisis management at EU-level still lacks the proper mechanisms to support effectively the EU-wide cybersecurity community in the event of another cyber crisis.

At present, EU decision-makers are in the privileged position to take action before a major cyber crisis occurs.

Although more abstract in nature, the cyber domain would indeed benefit from a stronger crisis management framework, and in that regard, learning from other more mature sectors is invaluable. The sectors within the scope of the study are aviation, border control, civil protection, counter terrorism and disease control. For each of these sectors, the legal and operational frameworks underpinning the crisis management work at the EU-level were analysed. The findings in terms of good practices and challenges encountered within the sectors in scope can be summarised as follows.

The promulgation of a legal framework with regards to EU-level crisis management has drastically increased the efficiency of the European response to crises in all sectors analysed. Clearly defining the roles and responsibilities of the key actors may speed up the response time considerably when faced with a crisis situation. Conversely, the lack of it was seen as an impediment for the relevant bodies to operate effectively as they lacked a common strategy and were not legally mandated to do so. Lastly, in areas related to sovereignty, it was recognised that the currently observed lack of **trust** has been a significant issue which legislation can help improve.

The main difficulty associated with the field of cyber crisis management, and hence with the development of an appropriate legal framework, lies in the fact that in the common language, **the severity of a crisis tends to be measured by the severity of its impacts**. In this light, a severe cyber incident might lead to a crisis in the telecom sector, in the energy sector, in the industrial sector, but never to a cyber crisis provided that there is no "cyber" sector per se. The term "cyber crisis" is still relevant, provided that there is an essential distinction to be made in the field of crisis management between the mitigation of the impacts and the causes of the crisis. Despite this inherent distinction, traditionally, there is legitimate emphasis and priority given to impacts. Nevertheless, **the effective mitigation of any sectorial crisis induced by severe cyber incidents, will depend on the effective mitigation of the causes of the incidents**. This is a clear paradigm shift from traditional crisis management, from managing impacts only, to a combined management of impacts and causes, which is currently not yet reflected in the EU legislation, although the proposed NIS Directive takes a step in this direction.

In order the support the above, ENISA recommends that the Commission, together with the Member States *revise the current EU legislation with regards to crisis management to better reflect upon the* ***separation of causes, impacts and leverage on the development of the field of cyber crisis management*** *as an essential tool in the mitigation of crises induced by cyber incidents* (recommendation 1).

Looking at governance issues under the operational framework, **it was clear that there was significant added value for EU Member States when EU Agencies acted as a facilitator** for information sharing and resource pooling. Crisis management should remain in the hands of Member States, but crisis coordination at EU-level is naturally best handled by EU bodies. One of the main challenges identified was the occasional lack of consideration for the capabilities of the EU-level body, and the fact that multinational crisis management was not always a priority for individual Member States.

Within the NIS community, numerous informal and voluntary initiatives were launched over the last ten years: the development of Standard Operating Procedures, the foundations of a crisis plan and a prototype cooperation platform. The pending NIS Directive is supposed to formalize many of these initiatives, and could certainly bring about the encompassing framework which is currently missing. Independently from the entering into force of the Directive, ENISA strongly recommends that the EU Member States ***develop and formally adopt an EU-level crisis management plan specific to crises induced by cybersecurity incidents*** (recommendation 2).

In terms of structures, good practices pointed as a first step towards those sectors in which **an EU hub coordinates a pool of voluntary Member States experts**, hereby sharing expertise and further developing trust. Some of these hubs, like the ERCC[1], provide continuous support to Member States, in this case monitoring disasters and hazards. The EACCC[2] in the Aviation sector operates as a "cold cell" which is permanent but can be further manned in the event of a crisis. FRONTEX[3] builds upon resources from the Member States to coordinate Joint Operations to address common issues such as the refugee crisis. Such set-ups minimise resource constraints at the most critical times, while providing an additional level of support to Member States.

[1] The Emergency Response Coordination Centre, part of DG ECHO, is a civil protection 'hub' for monitoring disasters and enhancing preparedness and resilience of disaster-prone countries.

[2] Established by the European Commission and hosted by EUROCONTROL, the European Aviation Crisis Coordination Cell supports coordination of the response to network crisis situations impacting adversely on aviation, in close cooperation with corresponding structures in States.

[3] FRONTEX is an agency of the European Union established in 2004 to manage the cooperation between national border guards securing its external borders.

With regards to cybersecurity, it would be advisable at an early stage to build upon these lessons and for the Commission and the EU Member States to attempt ***to create an EU-level pool of cyber crisis experts*** (recommendation 3), whose role would be first and foremost to exchange information and best practices in the event of cyber incidents and related crises. The CSIRT Network foreseen by the pending NIS Directive could certainly form the foundation of this pool, which would need to be coordinated by a small core capability at EU-Level. Considering its longstanding experience and outreach in the European cybersecurity community, its work in cyber crisis management and also its expected role in the network of national Computer Security Incident Response Teams (CSIRTs), **ENISA would be a valid candidate for integrating such a pool of experts.**

An EU-level entity is singularly positioned to provide a complete and consistent picture across all borders and domains in addition to operating as a focal point for information-sharing, assuming the pre-existence of cooperation procedures between all stakeholders. This type of EU-level entity, such as the EUROCONTROL Network Manager Operations Centre, has the advantage of collecting information from multiple sources in order to form a common situational awareness and coordination, which it provides back to its stakeholders. In terms of preparedness, another key ingredient to successful crisis management was exercises undertaken in between periods of crises. Again, the EU Civil Protection Mechanism serves as a good practice example as it continuously provides training opportunities to participating countries.

Still on processes, the aviation and health sectors both exhibited the value of procedures for crisis communication, including clear delineation of responsibility for communication and the need for a common narrative at the EU-level. A challenge by several entities studied was the absence of lesson learning processes.

Many of these findings are somewhat reflected in the informal European Union Standard Operating Procedures developed jointly by the Member States and ENISA. However, these procedures have never been formally adopted, or used in a real situation. ENISA simply recommends, in the perspective of the latter, that the Member States ***develop and formally adopt EU-level Cyber Standard Operating Procedures*** (recommendation 4).

Lastly the most effective tools and platforms were those which provided both the means for the EU Member States **to share information and to contribute to a common understanding of the operational landscape, both in crisis and non-crisis times**. Indeed, the fact that a platform is only used for crises creates a need for frequent trainings and certainly limits its effectiveness in times of crisis.

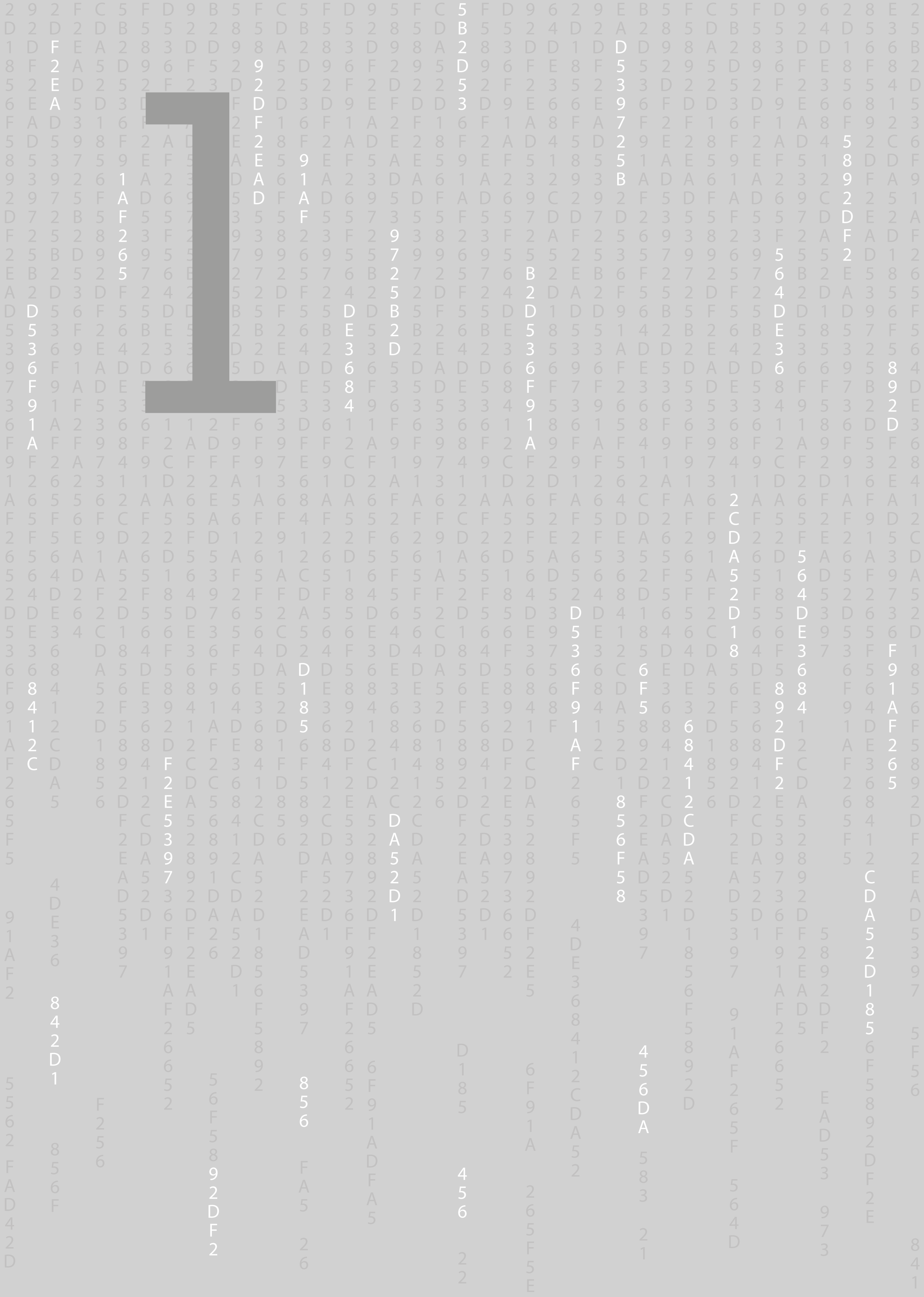
Challenges in this domain also included the lack of integration between various platforms, the output of which often serves as input to each other. The lack of standardised formats to exchange information, all-the-more relevant in cybersecurity where machine-readable formats are as critical as heterogeneous, was also perceived as an impediment to effective crisis management.

With this in mind, the development of a platform to support crisis management in cybersecurity should build upon the tools used by the CSIRTs on a daily basis, and should easily integrate with other crisis management tools at strategic level. The ongoing project led by the European Commission on the development of a CSIRT Platform, supporting incident information exchange, could fill this gap. ENISA, which is involved in this process, recommends that the Commission funds an effort ***to design and develop an EU-level Cyber Crisis Cooperation platform*** *to offer support to cyber crisis management cooperation activities to Member States, in conjunction with the Core Service Platform of the Cyber Security Digital Services infrastructure of* *the Connecting Europe Facility funding program, seeking stronger integration of the tools used by both the CSIRT community and the EU-level crisis management community* (recommendation 5).

Within its policy area, ENISA has been supporting the field of European cyber crisis management for several years, with activities ranging from crisis simulations to trainings, support to Member States in developing their crisis plans and structures, international conferences and reports such as this one. The contents of this document do not only build upon interviews and desk research, but also very much upon the expertise from ENISA authors, countless discussions on the topic with key experts in the EU Member States and numerous exchanges with crisis practitioners across Europe. Although this report reflects only the view of the authors, ENISA trusts that **implementing the abovementioned recommendations would significantly improve the mitigation of any crisis at European level triggered by a cyber incident**. ENISA is fully committed to support the European Commission and the Member States in implementing these recommendations.

Contents

1



1. Information about this study

In 2014, ENISA published a first report defining the field of cyber crisis management [11], in an effort to provide European Union (EU) Member States and cyber crisis managers in particular, with a common understanding of this area.

This report is the continuation of this effort and the result of a study carried out in 2015 with the objective to raise the maturity of the field of EU-level cyber crisis management, by identifying good practices and challenges in other sectors and discuss their applicability to the cyber domain.

The key objectives of this study are to:

- Identify good practices and challenges from the EU-level crisis management legal and operational frameworks in different sectors.
- Draw parallels between the abovementioned findings and cybersecurity to issue key recommendations on how to better prepare the EU to handle crises with a cyber component.

The sectors studied during the course of this study are the following:

- Aviation
- Border control
- Civil protection
- Counter-terrorism
- Health/disease control

1.1 Target audience

The report is targeted at managerial staff, senior experts in Network and Information Security (NIS) and competent authorities in the EU Member States, as well as senior EU level officials and the European NIS community at large.

1.2 Structure of the report

The remainder of this report consists of two chapters. **Chapter 2** provides a brief outline of the current stay of play of EU-level strategic crisis management, along with in-depth analyses of the lessons learnt and challenges of the legal and operational frameworks of crisis management in the sectors abovementioned. **Chapter 3** provides key recommendations on how to raise maturity in EU-level cyber crisis management by drawing parallels between the findings of chapter 2 and the cyber domain.

2

2. EU-level crisis management: challenges and good practices

A crisis is an event that is unexpected and far removed from the ordinary and mundane, affecting many people and large parts of society while threatening fundamental values and functions that cannot be handled with ordinary resources and organisation, and that requires coordinated action from several actors [11]. In recent years, **the need for a robust EU-level response mechanism to manage cross-border threats has become overwhelmingly apparent** within several sectors. The challenges faced by the EU and the Member States in coordinating a common response have been highlighted as a result of a number of crises, in particular, the volcanic ash cloud over Iceland, pandemic diseases, terrorist attacks and the migrant crisis.

In the aftermath of the terrorist attacks in Madrid (2004) and London (2005) [3], the tsunami in the Pacific and the Indian Ocean (2004) [12], the EU set up its Emergency and Crisis Coordination Arrangements (CCA), to enable the Institutions and its Member States to provide a strategic and political response to crises in a coordinated manner. In 2013, the Council approved the EU Integrated Political Crisis Response (IPCR) [13], the update to the CCA following the Lisbon Treaty and in particular **the Solidarity Clause**. The latter treaty stipulates that the role of the EU is to **facilitate cooperation** between Member States, complementing national policies especially to cover monitoring, early warning and combating serious cross-border threats. In this regard, the IPCR can be seen as the EU's ambition to have a coherent response during crises, avoiding unnecessary duplication of efforts. As of then, in the event of a crisis, the Council Presidency, possibly at the request of the affected EU Member State(s), activates the IPCR. The Presidency further gathers advice and support to develop proposals for action to be presented to the Committee of the Permanent Representatives of the Governments of the Member States (COREPER)/the Council of Ministers and even the European Council [9].

In parallel, the European Commission developed a **procedure to produce Integrated Situational Awareness and Analysis (ISAA)** reports [14] that can support decision making at the highest level, based on inputs from the Member States but also very much from the Institutions services, Directorate Generals and Agencies. Depending on the sectors affected, legal and operational frameworks in place between Member States and these services allow for information exchange and crisis coordination at operational level, before strategic discussions take place in the IPCR process.

Cyber incidents are commonplace [15] and the likelihood for a crisis to be caused by one or more of these incidents increases every day. The EU counter-terrorism coordinator, Gilles de Kerchove, was interviewed for the purposes of this report: he argues that "there is a distinct possibility that Daesh[4] will try to launch a cyber-attack against the control system of an electrical grid or of a nuclear plant".

Because of the borderless nature of cyber incidents, their mitigation requires multinational cooperation; the EU is ideally placed to foster cooperation between Member States in that regard. This is notably demonstrated by the numerous crisis management frameworks in place at EU level which structure such coordination in their respective sectors. Unfortunately, because of their sectorial limitations, none of them fully absorb the cross-sectorial nature of the threat posed by cyber incidents.

[4] Daesh or Da'ish refers to a jihadist group present in Syria and Iraq. Daesh is an acronym formed from the initial letters of the Arabic sentence "al-Dawla al-Islamiya fil Iraq wa al-Sham". The group is also known as the Islamic State (IS), the Islamic State in Irak and Syria (ISIS) and the Islamic State in Iraq and al-Sham (ISIL). The group itself has not used the name Daesh since June 2014 when it declared the creation a caliphate and shortened its name to IS to reflect its expansionist ambitions [27].

2.1 EU-level legal frameworks for crisis management

This section covers the good practices and challenges of five EU-level crisis management legal frameworks identified during the course of this study. Special attention is given to practices and challenges that can be relevant or applicable to cyber crisis management.

The good practices identified for the EU-level crisis management legal frameworks are the following:

G1 Research carried out during this study clearly suggests **that the establishment of a legal framework is a prerequisite to effective EU-level crisis coordination**. Mitigating a crisis cannot just be achieved without clearly delineated mandates and responsibilities: if everyone is responsible, at the end nobody feels the need to accomplish the task.

G2 A probing example of this statement can be found in the aviation sector: despite several decades of existence, EUROCONTROL had no role whatsoever in terms of crisis management until the 2010 ash cloud crisis - which highlighted the difficulties to manage such crisis without EU-level coordination. The fact that EUROCONTROL was legally mandated [16] **to deal with crisis coordination at such level, was a direct consequence of this event**.

G3 Another prime example of EU legislation providing a sound foundation for crisis management is the Union Civil Protection Mechanism. Created in 2001 it fosters cooperation among national civil protection authorities across Europe and enables coordinated assistance from the patriating states to victims of natural and man-made disasters in Europe and elsewhere [17] [18]. This mechanism was updated in 2014 [19] to create the European Emergency Response Capacity (EERC). It also laid the foundation for voluntary pooling of knowledge and skills from several EU countries allowing for an immediate deployment of experts. In the refugee crisis the EU is currently facing, the role and capabilities of the EERC are proving essential. Such capacity could not have been created prior to the Union Civil Protection Mechanism.

G4 Other sectors, such as health and disease, have also benefitted from EU legislation to improve crisis management. The legislation on communicable diseases established in 1998 a network for the epidemiological surveillance and control [20]. Further complementing the latter, the EU legislation on cross border health crisis enacted in 2013 strengthened EU level planning and coordination response capabilities [21]. Both legislations proved key instruments in supporting the pan-European management of diseases likely to transcend internal borders.

G5 The development of sector specific regulations, adopted and monitored at the EU level, as in the aviation industry, created consistently understood parameters for safety and security as well as baseline capabilities against which the maturity of the sector can now be benchmarked. In this regard, the regulatory efforts in cybersecurity with the NIS Directive are likely to have a similarly positive effect.

G6 Where an issue transcended a number of different sectors, it was arguably more applicable to underpin those legislative measures with a common set of principles. This is exemplified in the case of counter terrorism, where legislative acts adopted at the EU level were supported by the acknowledgement of a common set of principles agreed following the numerous terrorist attacks in the Western world between 2001 and 2005 [22]. The establishment of these principles created consistency of approach and harmonisation of definitions, which in turn contributed to achieving a higher level of preparedness.

The challenges identified for the EU-level crisis management legal frameworks are the following:

C1 The first challenge to the setting up of an effective legal framework addressing an EU-level crisis was reported to be **the sensitivity of most crisis management activities** and the limited trust between Member States with regards to **sovereign issues**. In terms of facilitating this process from an EU perspective, this was perhaps most effectively managed when a common strategy and set of principles was first established, in close collaboration between the EU Commission and the Member States, paving the way for more concrete decisions pertaining to the areas genuinely requiring collaborative effort. **Achieving EU-level crisis coordination without a commonly shared vision is certainly a major challenge.**

C2 Secondly, as the example of EUROCONTROL and the volcanic ash crisis highlighted, pre-existing competence at EU-level, within the relevant DG and/or Agencies, is required before formalising a clear mandate for crisis management. Nevertheless, the absence of such clear mandate **limits the development of such capabilities**, which benefits hence cannot be perceived in the event of a crisis, **and which ultimately further justifies the limitations imposed to their development**. This is a difficult conundrum which solution lies in courageous policy making.

C3 However, while a common legislation can greatly enhance crisis management, **quick access to critical information is essential and relies upon one essential element that no legislation can enforce: trust**. In more established crisis management frameworks, trust is institutionalized via generic services and platforms, leaving the human element aside. In this regard, much effort needs to be consented by crisis management actors in building trust via regular exercises and trainings, which can prove costly.

2.2 EU-level operational frameworks for crisis management

This section covers the good practices and challenges of EU-level operational frameworks for crisis management, in particular governance models, structures and setup, processes and lastly tools and platforms. Special attention is given to practices and challenges that can be relevant or applicable to cyber crisis management.

2.2.1 Governance

The good practices identified for the EU-level operational crisis management governance frameworks are the following:

G7 There is significant added value for Member States when an EU body or Agency with EU-wide competence acts as a facilitator of information sharing and resource pooling in the case of a multinational crisis. Interviewed experts summarized this simply: *"There is a clear division of labour: crisis management is in the hand of the MS and coordination of the European Commission with support by the Agencies"*. All interviewees agreed that not only is information sharing more consistent, but the overall management of the multinational crisis was more effective as opposed to situations where the Member States dealt with it separately.

In the case of the ash cloud crisis, there were at the time no procedures to manage cross-company and national border disruptions, and no support mechanism for the exchange of information. The resultant decision-making process was thus lacking in accurate information and the response centred purely on the Member States' singular purpose of repatriating those citizens stranded abroad, with some, limited, bilateral cooperation. Following the Commission proposals to improve crisis preparedness through EUROCONTROL and the greater level of engagement with the airlines, there have been major improvements in information gathering, sharing and dissemination.

Similarly, in the case of the migrant crisis in the Mediterranean, the historical challenges of the years between 2005 and 2007, when the Member States had different standards and procedures, presented significant issues when trans-border issues needed to be managed by more than one Member States. These challenges were, if not fully addressed, significantly tackled by FRONTEX which created standard procedures related to joint maritime operations and joint land/air operations.

G8 In parallel to capability development at EU-Level, as in the case of the crisis responsibilities of EUROCONTROL or the HSC, **a clear definition of the mandate and responsibilities of all parties** has helped significantly to improve shared crisis coordination processes. In the context of cybersecurity, the attacks against Estonia in 2007 highlighted the lack of such harmonised approach and led to several policy initiatives, though insufficient with regards to crisis management. Today, **there is still no clear mandate nor explicit responsibilities for any entity**, neither at national nor EU-level, **for multinational crisis management in the field of cybersecurity**.

The challenges identified for the EU-level operational crisis management governance frameworks are the following:

C4 One of the greatest challenges in the governance mechanism was the occasional **lack of consideration for the capabilities of the EU-level body or Agency on the part of the Member States**. Interviewees indicated that this is mostly due to the idea that expertise lies in the hands of Member States, although most admitted that EU-level bodies or agencies were in a better position to handle cross-border crises, provided that developing capabilities **supporting multinational crisis management was not a priority for individual Member State**.

C5 Respondents also claimed that **information collection capabilities vary from one Member State to another, and information is not always shared or trusted amongst them as national interests prevail**. In the case of public health, a common consensus remains that MS consider the well-being and protection of their own populations before that of other Member States.

2.1.2 Structure and setup

The good practices identified for the EU-level operational crisis management structures and setup are the following:

G9 In terms of EU-level structures for crisis management, there are different operational models across the sectors examined from which lessons can be drawn. One effective means of supporting Member States was the creation of the ERCC [23] as the operational hub of the EU Civil Protection Mechanism for humanitarian crises and for civil protection. This is a prime example of an effort to **strengthen inter-sectoral communication** and, as a result, **making information from one sector available to other sectors**.

G10 Cybersecurity being also a cross-sector problem, the example of the ERCC is particularly relevant. **It continuously collects information on disasters and monitors hazards**, prepares plans for resource deployment (experts, teams and equipment), cooperates with EU Member States and coordinates the EU's disaster response attempts. Importantly, **it has direct connections** to civil protection authorities in **Member States**, ensuring a consistent European response to disasters. Through its pre-positioned and autonomous civil protection modules, the ERCC teams are ready to intervene at short notice both within and outside the EU. They can undertake specialised tasks, such as search and rescue, aerial forest fire fighting, advanced medical posts and more. Undisputedly, the ERCC acts **as a key coordination and support platform**.

G11 Another good practice example is found within the aviation sector. The European Aviation Crisis Coordination Cell (EACCC) was established as a direct consequence of the 2010 volcanic ash cloud crisis. Created by the Commission, it is hosted by the Network Manager for aviation (EUROCONTROL). The EACCC is permanent in nature, which facilitates the possibility for an effective response in the event of a disruption, and allows for better preparedness. It operates as a 'cold' cell with minimum staff and is only activated fully by the Network Manager during a crisis. In particular, it acquires and shares information with the aviation community, including decision makers, airspace users and service providers, in a timely manner. **This set-up minimises resource constraints at the most critical times, while providing an additional level of support to Member States.**

The challenge identified for the EU-level operational crisis management structures and setup is the following:

C6 There were some potential and perceived challenges, for example, in the case of the border agency, FRONTEX, in terms of cooperation with the national competent authorities. For instance, there is no coast guard at EU level on stand 24/7 though FRONTEX can only perform its duties with the resources offered by the Member States, which can be limited by operational or political constraints. The voluntary nature of such operations and the way equipment is procured during a crisis was a key challenge according to one respondent, who also stated that a solution to this problem would be to make the support obligatory and for the Agency to have its own equipment.

2.1.3 Processes

The good practices identified for the EU-level operational crisis management processes are the following:

G12 Almost all EU-level bodies offer some form of common situational awareness which was largely regarded as beneficial, as an enhancement of the existing information individual Member States can obtain and process. Especially, in identifying emergent crises, **an EU-level entity is singularly positioned to provide a complete and consistent picture across all borders and domains in addition to operating as a focal point for information-sharing**. For example, EUROCONTROL focuses on the integration of horizon-scanning mechanisms at the crisis management planning stages.

G13 Recent disasters in the aviation sector have shown that the difficulties in handling major disruptions and crises are linked to an inadequate level of preparedness and cooperation between the actors involved, which has resulted in the creation of inefficient crisis management mechanisms, insufficient institutional coordination at the EU level, and inefficient information management [24]. Preparedness for a crisis plays a key role in protecting Member States against the negative impact of a major disruption, and in particular, **having a process for sectorial public private cooperation at the EU level was considered advantageous when dealing with a crisis**. In that regard, the European Commission has proposed that certain operators that play a crucial role in cross-border transport are obliged to adopt contingency plans. The purpose of the plan is to ensure that when passengers are stranded due to a major disruption, they are provided with adequate information and assistance [24]. In terms of cybersecurity, the European Commission is pursuing a similar objective with the Data Protection regulation and the drafting of the NIS Directive.

G14 There was an almost **unequivocal view on the value of exercises to enhance the ability of EU-level bodies** and agencies and their counterparts to become familiar with, and enhance existing procedures.

G15 Finally, Agencies operating in sectors such as aviation and public health appeared to have more **sophisticated procedures for managing the public affairs dimension of a crisis, with a clear delineation of responsibilities between Member States and the EU level**. In the case of aviation, EUROCONTROL nominates one individual to act as the Communications Focal Point for the crisis and a crisis cell spokesperson. During the interviews for this study, Antonio Nogueras, head of the ATM security unit at EUROCONTROL, indicated a team within the communication cell has been set up following the 2010 volcanic eruption and is **dedicated to social media analysis during a crisis**.

This capability proved so useful that it is now integrated in the crisis detection process, monitoring for instance the number of tweets on specific subjects. There was also a pronounced value in Agencies such as ERCC **acting as a hub for EU Member States and even industry, as in the case of the EACCC, to discuss public affairs strategies**.

The challenges identified for the EU-level operational crisis management processes are the following:

C7 Many of the EU-level bodies and agencies whose staff were interviewed clearly delineated the different phases of the types of crises they face. Few, however, focused on the final phase, namely **identifying lessons learnt and challenges**, and **defining and implementing an action plan**, although recognizing its importance. Similarly, cross-sector lesson learning processes at EU-level might require a shift in the institutional culture and dedicated resources.

C8 Although there was good crisis management training and awareness across most of the agencies, **there was a noticeable lack of rehearsals for public affairs handling**. This was one of the key lessons from crises such as the influenza pandemic and the 2011 E.coli crisis where miscommunication between EU Member States had a severe economic impact first on the Spanish and then European markets.

2.1.4 Tools and platforms

The good practices identified for the EU-level operational crisis management tools and platforms are the following:

G16 The internal crisis management platform of the European Commission (ARGUS), can be used for information exchange only needs (activation at level 1). This allows for **regular usage of the platform**, which reduce the need for training for crisis practitioners and ensures that all functionalities of the platform are used efficiently in times of crisis (activation at level 2).

G17 By far the most effective tools and platforms were those which **provided the means for the EU Member States to share information and to contribute to a common understanding of the operational landscape**.
One tool which proved particularly valuable was EUROCONTROL's **web-based portal which provides real time, constantly validated information using a robust collaboration process**. The Virtualisation Interactive Tool employed by EUROCONTROL provided for the simulation of ash cloud behaviour also emerged as particularly successful in facilitating those in tactical roles to prepare and to take informed decisions.

G18 There were remarkably few multi-sectorial tools and platforms, aside from the IPCR Platform that is, but one that was acknowledged as successful was AIRSAN, which was created as a collaboration between the Aviation and Public Health sectors. One may venture that more such collaborations would be beneficial either for those sectors with common interests (e.g. borders) or where an issue (e.g. cyber) transcends a number of sectors.

The challenges identified for the EU-level operational crisis management tools and platforms are the following:

C9 Several of the sectors examined seemed **to be faced with a plethora of platforms** for monitoring, communication and information sharing during a crisis, depending on the stakeholders or the crisis stages. If the unification of such platforms is illusory, even more within cybersecurity agencies which often rely upon unclassified and classified communication channels, **further integration in terms of input and output products can be sought**.

C10 Despite these platforms, respondents indicated that the EU as a whole faces major challenges in dealing with effective and efficient information exchange between EU institutions, its Agencies and the Member States. **Firstly, there is a lack of standardised formats to exchange information.**

C11 Secondly, Member States have **different priorities** in terms of investing in tools and platforms compared to EU organisations, **which often paralyse their development**. In this regard, the budget attributed to development of a cooperation platform for European cybersecurity agencies by the European Commission, as part of the Connecting Europe Facility mechanism, should prevent the latter challenge from arising.

C12 Funding, hosting and the transmission and storage of classified data, all pose potential challenges to the effective operability of EU-level tools. It is also acknowledged that rapid alert tools are useful only insofar as good quality and current information is shared with them. As such, there is a clear need, for any tool to be deployed at the EU or Member State level, to be supported by a cooperation framework and a culture of information exchange amongst the Member States and Agencies. For instance, the Early Warning Response System, a web-based system linking the Commission, Member State public health authorities and the European Centre for Disease Prevention and Control (ECDC), suffers from slow updates and inadequate exchanges.

C13 Moreover, **some service limitations of the existing tools were highlighted when these were developed for crisis only purposes**. For instance, the online tool for Air Traffic Flow and Capacity Management (EVITA) allows users to visualise the impact of a crisis on air traffic. The tool supports decision-making in times of a crisis, and is hence the most important communication channel for airlines operating in Europe during a major crisis situation. However, the interviews showed that the tool is not suitable for use as an operational tool outside crisis situations. Hence, while EVITA is a key tool during a crisis, **the fact that it is not used otherwise creates a need for frequent trainings and certainly limits its effectiveness in times of crisis**.

3

3. Lessons learned for the EU-level cyber crisis management

This section draws a number of parallels between the sectors analysed in the study and the emerging field of cybersecurity, notably to support the strengthening of the EU-level cyber crisis management framework, taking into account both the best practices and challenges summarized in the previous section.

3.1 Observations on crisis management in the current legal framework

The main difficulty associated with the field of cyber crisis management, and hence with the development of an appropriate legal framework for the conduct of such crisis activities, lies in the fact that in the common language, **the severity of a crisis tends to be measured by the severity of its impacts**. In this light, a severe cyber incident might lead to a crisis in the telecom sector, in the energy sector, in the industrial sector, but never to a cyber crisis provided that there is no "cyber" sector per se. At first glance then, a "cyber crisis" is nothing less than an oxymoron, yet the combination of these terms is quite relevant.

There is an essential distinction to be made in the field of crisis management between the mitigation of the impacts – saving lives, rebuilding villages or sending planes to bring back stranded passengers, and the mitigation of the causes of the crisis. Despite this inherent distinction, there is legitimate emphasis and priority given to impacts, because of their urgency, visibility and the associated public pressure, but also often because the causes cannot be addressed on the short term to put an end to the crisis, or simply because they are deemed impossible to mitigate, as in most natural disasters.

Few modern crises deviate from this statement, only very specific crises do, such as the Boston bombings, the Charlie Hebdo attacks or the 13/11 attacks in Paris, which all led to nation-wide manhunts, where finding the terrorists (causes management) became much more critical than dealing with the short and long term consequences of their attacks (impact management).

Unfortunately, the parallel between the last examples and the virtual world is difficult to draw, provided that finding those responsible for a cyber-attack is difficult when not impossible, time-consuming and often pointless if they operate from certain countries. Nevertheless, the cyber domain offers **plenty of other possibilities to crisis practitioners to manage the causes of crises to speed up overall mitigation, which do not exist in the real world**, such as disrupting the weapons used by the attackers (active defence on the attacking infrastructure), providing targets of attacks with bullet-proof vests within seconds (DDoS counter measures) or injecting a vaccine to a population instantly (over-the-air updates).

This is a clear **paradigm shift** from traditional crisis management which is currently not reflected in the EU legislation, to the grave detriment of **the effective mitigation of "cyber-induced" crises, because the effective mitigation of any sectorial crisis induced by severe cyber incidents, will depend on the effective mitigation of the causes of the attacks**. If such causes are not understood and mitigated, the crisis will continue or start somewhere else.

Too frequently, the impossibility for decision makers to understand the underlying technicalities of cybersecurity incidents – for lack of awareness but also difficulties for technical experts to present the situation in non-expert terms, results in a focus on impact management.

In this regard and as a first step, the current EU legislation should be updated to reflect this concept and better prepare the Union and Member States to mitigate crises induced by severe cyber incidents.

Recommendation 1: ENISA recommends that the European Commission, together with the Member States revise the current EU legislation with regards to crisis management to better reflect upon the separation of causes and impacts and leverage on the development of the field of cyber crisis management as an essential tool in the mitigation of crises induced by cyber incidents.

3.2 Operational framework

3.2.1 Governance

Although the legal framework governing EU-level crisis management activities in cybersecurity is missing, many of the key building blocks allowing for operational-level crisis management have been developed informally already. In terms of governance, the EU Cyber Crisis Coordination Framework (ECCCF), developed by Member States in 2012, attempted to delineate the responsibilities of each stakeholder in this field, from the technical to the strategic level. In terms of processes, the EU-Standard Operating Procedures, developed as from 2011, represent the effort from the cybersecurity community to structure cooperation in the event of a cyber crisis at the operational level. Lastly, ENISA has developed a prototype web-based crisis platform in the attempt to support this cooperation.

All the aforementioned efforts are but **informal and voluntary initiatives**, often led by the Member States, to overcome the shortcomings associated with the absence of an established governance process, the absence of an entity in charge at EU-Level, the lack of formally agreed cooperation procedures and the inexistence of a pan-European platform supporting information exchange and crisis cooperation activities.

Some of these elements are likely to be formalized in the near future. The pending NIS Directive shall include a CSIRT Network for information exchange, supported by ENISA. Such network would naturally become **an ideal candidate for crisis cooperation activities between European CSIRTs**. In this regard, the rules of operation of such network would also be an excellent candidate to **include crisis cooperation procedures** at the operational level. Lastly the CSIRT Platform, currently under development to facilitate the CSIRT Network set by the NIS Directive, shall become **the crisis cooperation platform** for the cybersecurity community in Europe.

Nevertheless, these are but isolated assumptions which might only become meaningful if they are complemented by key missing blocks presented below, and brought together by **an encompassing cyber crisis governance framework, in other words, an EU-level crisis management plan specific to cybersecurity**.

Such a plan should build on previous efforts, such as the ECCCF, and bring it to a mature state, notably in the light of the pending NIS Directive. In fact, the idea of a crisis management plan for cyber crises at the EU level was introduced in the proposed NIS Directive [17] through the 'Union NIS cooperation plan' (article 12). The Union NIS cooperation plan is defined as a "plan establishing the framework for organisational roles, responsibilities and procedures to maintain or restore the operation of networks and information systems, in the event of a risk or an incident affecting them".

Recommendation 2: independently from the entering into force of the proposed NIS Directive ENISA strongly recommends that the Member States develop and formally adopt an EU-level crisis management plan specific to crises induced by cybersecurity incidents.

3.2.2 Structure and set-up

As a first EU-Level capacity in the field of cybersecurity, European policy makers should consider fostering the development of an EU-level pool of cyber crisis experts. This capability should build upon **a pool of voluntary EU Member States experts from national and governmental CSIRTs**: similar to the pooling of experts which is already in place at ERCC, with voluntary resources available to be activated in the event of a crisis. The ultimate objective of such pool of experts would be to provide, just like NATO's Cyber Rapid Reaction Teams do for military purposes, support to EU Member States, including to critical infrastructures operators, in the event of severe cross-border cyber incidents.

By having a pool of experts in place, the EU could ensure a rapid and qualitative EU level response when faced with a cyber-crisis. This means, for instance, that the information collection, analysis and the attainment of the situational awareness following an incident or during a crisis could start immediately instead of time being spent to identify the relevant experts. Additionally, in between crises, this pool of experts could participate in cyber exercises and other preparedness activities, **hereby sharing expertise among EU Member States and further developing trust**.

At EU level, this pool of experts could be **coordinated by a core cyber crisis team** dedicated to monitor alerts from the Member States through direct channels in-country, fostering situational awareness prior and during incidents. Considering its longstanding experience and outreach in the European cybersecurity community, but also in the light of its expected role in the NIS Directive in terms of support to the CISRT Network, **ENISA would be the natural candidate for such role**.

In terms of both crisis preparedness and crisis response, the creation of a pool of cyber crisis experts would be an important step towards **completing the EU level cyber crisis management governance framework aforementioned**.

Recommendation 3: ENISA recommends that the European Commission and the Member States attempt to create an EU-level pool of cyber crisis experts.

3.2.3 Processes

Following Recommendation 3, **working procedures** specifically detailing the cooperation activities of the EU-level pool of experts and the core cyber crisis experts should be developed, building upon the EU-SOPs currently being maintained by the Member States and ENISA, while seeking alignment with the rules of operations of the CSIRT Network likely to be introduced in the proposed NIS Directive. Article 8 of the same Directive argues for a "cooperation network" of the competent authorities from the Member States. These procedures could be formally adopted by this "cooperation network".

Recommendation 4: ENISA recommends that the Member States develop and formally adopt EU-level Cyber Standard Operating Procedures (SOPs).

3.2.4 Tools and platforms

Information management and situational awareness are crucial components to define how to take action during a crisis. A cooperation platform for cyber crisis management would allow the key actors involved in EU-level cyber crisis management activities to have better access to contact details, to interact more effectively, to exchange information, to communicate and coordinate in the case of an EU-level cyber crisis. For this reason, compatibility with other tools and platforms used by the communities involved in cyber crisis management is essential. In particular, **the tools used by CSIRTs on a daily basis should easily communicate with the platform**, notably for the exchange of technical information. Similarly, the tools used by the EU-level crisis management community, such as the IPCR, **should easily integrate output products from the platform**.

The discussion around cyber crisis management tools and platforms cannot be carried out without due consideration for the proposed NIS Directive, which specifically mentions that Member States' competent authorities should be in "permanent communication" to cooperate on "risks and incidents affecting network and information systems, including the use of a common website". With this in mind, the Connecting Europe Facility (CEF), which is a European funding mechanism of more than 1Bn euros supporting the development of trans-European networks and infrastructures in the sectors of transport, telecommunications and energy [26], follows the same logic. In particular, the CEF Cyber Security Digital Service Infrastructure, is currently being used to develop a "core service platform" which ultimately should support "cooperation mechanisms that will enhance the EU-wide capability for preparedness, information sharing, coordination and response to cyber threats".

In anticipation of the set-up of the suggested "core service platform", which is still a few years in the making, one suggestion is to start by building on existing ones, such as the ENISA Cyber Crisis Cooperation Platform which provides some of the required features but so far only for exercises purposes. Considering the involvement of ENISA in the development of the "core service platform" abovementioned, the Cyber Crisis Cooperation platform can be seen as a prelude to the latter.

Recommendation 5: ENISA, which is involved in this process, recommends that the European Commission funds an effort to design and develop an EU-level Cyber Crisis Cooperation platform to offer support to cyber crisis management cooperation activities to Member States, in conjunction with the Core Service Platform of the Cyber Security Digital Services infrastructure of the Connecting Europe Facility funding program, seeking stronger integration of the tools used by both the CSIRT community and the EU-level crisis management community.

Within its policy area, ENISA has been supporting the field of European cyber crisis management for several years, with activities ranging from crisis simulations to trainings, support to Member States in developing their crisis plans and structures, international conferences and reports such as this one. The contents of this document do not only build upon interviews and desk research, but also very much upon the expertise from ENISA authors, countless discussions on the topic with key experts in the Member States and numerous exchanges with crisis practitioners across Europe. Although this report reflects only the view of the authors, ENISA trusts that implementing the abovementioned recommendations would significantly improve the mitigation of any crisis at European level triggered by a cyber incident. ENISA is fully committed to support the European Commission and the Member States in implementing these recommendations.

4

4. References

[1] Eurocontrol, “What has changed for aviation in dealing with volcanic ash since 2010?,” Eurocontrol, 2015. [Online]. Available: http://www.eurocontrol.int/articles/what-has-changed-aviation-dealing-volcanic-ash-2010. [Accessed 8 12 2015].

[2] ECDC, “The 2009 A(H1N1) pandemic in Europe,” Stockholm, 2010.

[3] The Economist, “Terror attacks and arrests in western Europe,” 16 11 2015. [Online]. Available: http://www.economist.com/blogs/graphicdetail/2015/11/daily-chart-10. [Accessed 8 12 2015].

[4] D. E. McNabb, “Vladimir Putin and Russia’s Imperial Revival,” Boca Raton, 2015.

[5] European Commission, “Communication on “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”,” Brussels, 2009.

[6] European Parliament, European Council, “Directive 2009/136/CE du Parlement Européen et du Conseil,” Brussels, 2009.

[7] European Commission, EEAS, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,” Brussels, 2013.

[8] European Commission, “Digital Agenda for Europe,” [Online]. Available: http://ec.europa.eu/digital-agenda. [Accessed 11 23 2015].

[9] ENISA, “Cyber Europe,” 2015. [Online]. Available: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe. [Accessed 23 11 2015].

[10] ENISA, “ENISA Cyber Europe 2014 After Action Report,” Athens, 2015.

[11] ENISA, “Cyber Crisis Cooperation and Management,” European Union Agency for Network and Information Security (ENISA), 2014.

[12] United Nations Environment Programme, “After the tsunami, Rapid Environmental Assessment”.

[13] Council of the European Union, “The EU Integrated Political Crisis Response Arrangements,” 2014. [Online]. Available: http://www.consilium.europa.eu/fr/documents-publications/publications/2014/eu-ipcr. [Accessed 23 11 2015].

[14] European Council, “COUNCIL DECISION of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause,” 24 June 2014. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0415&from=EN. [Accessed 8 12 2015].

[15] ENISA, Threat Landscape report, European Union Agency for Network and Information Security (ENISA), 2014.

[16] European Commission, “Commission Implementing Regulation (EU) No 970/2014,” 12 September 2014. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=celex:32014R0970. [Accessed 23 11 2015].

[17] Council of the European Union, “ Council Decision of 23 October 2001 establishing a Community mechanism to facilitate reinforced cooperation in civil protection assistance interventions,” 23 October 2001. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=celex:32001D0792. [Accessed 23 11 2015].

[18] European Council, “Civil Protection Mechanism,” Brussels, 2007.

[19] European Parliament, Council of the European Union, “Decision laying down rules for the implementation a Union Civil Protection Mechanism,” 16 October 2014. [Online]. Available: http://ec.europa.eu/echo/files/civil_protection/C_2014_7489_EN_ACT.pdf. [Accessed 23 11 2015].

[20] European Commission, “Legislation on Communicable diseases,” [Online]. Available: http://ec.europa.eu/health/communicable_diseases/early_warning/comm_legislation_en.htm. [Accessed 23 1 2015].

[21] EEAS, “Crisis Management,” 2015. [Online]. Available: http://eeas.europa.eu/cfsp/crisis_management/index_en.htm. [Accessed 23 11 2015].

[22] D. O. Bures, EU Counterterrorism Policy: A Paper Tiger?, Farnham: Ashgate Publishing, 2011.

[23] European Commission, “Emergency Response Centre: for a faster and more efficient European response to disasters,” 15 5 2013. [Online]. Available: http://europa.eu/rapid/press-release_IP-13-422_en.pdf. [Accessed 8 12 2015].

[24] European Commission, “Continuity of passenger mobility following disruption of the transport system,” Brussels, 2014.

[25] European Commission, “Proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union,” 2013. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=celex:52013PC0048. [Accessed 23 11 2015].

[26] European Commission, “Connecting Europe Facility,” 04 11 2015. [Online]. Available: http://ec.europa.eu/digital-agenda/en/connecting-europe-facility#cef-as-part-of-the-eus-infrastructure-package. [Accessed 23 11 2015].

[27] BBC, “Isis, Isil, IS or Daesh? One group, many names,” 2 12 2015. [Online]. Available: http://www.bbc.com/news/world-middle-east-27994277. [Accessed 9 12 2015].

A

Annex A. Methodology

The study has been based upon a dual methodological approach, including a desk review of the key legal and policy documents, and a number of interviews with key experts from each sector within scope.

Interviews were conducted either in person or via phone, between the months of April and November 2015. The interviews were pursued in a semi-structured manner allowing for auxiliary questions and for new lines of questioning depending on the responses of the respondents. The complete list of interview questions is available in Annex B while the list of interviewees is available in Annex C.

Both desk research and interviews laid the foundation for the development of in-depth analyses of each of the sectors selected for this report along with one case-study per sector. These analyses in turn allowed for the development of this report.

In order not to overload readers with information non-specific to cybersecurity, the authors have decided not to include the in-depth analyses and the case studies; they are available upon request.

Lastly, a video presenting the report and highlighting some of the key lessons learnt was produced.

Annex B. Interview Questions

#	Domain	Questions
1.	Governance	Please describe the high-level decision-making process for EU-level crisis management in your sector, including: 1) Decision making during crisis 2) Strategic decision making
2.	Governance	Please describe the composition and responsibilities of top management in charge of high-level decision-making related to EU-level crisis management?
3.	Governance	How would you describe the balance of power between the Member States and the European Institutions in crisis management activities in your sector?
4.	Structure and set-up	What challenges did you face in the past in terms of cooperation at EU-level between the Member States and how did you overcome them? Are Member States willing to cooperate on a multilateral basis (EU) or do they prefer bilateral and regional cooperation?
5.	Structure and set-up	Please describe the operational EU-level crisis management framework in place in your sector (including, the roles of all entities involved and the concepts underpinning/driving the crisis management, structures and processes).
6.	Structure and set-up	How did you entice cooperation with and between Member States in all activities related to crisis management on the EU-level (preparedness, response and recovery)?
7.	Structure and set-up	What are the lessons learned from EU-level cooperation in managing crises in your sector? What could be improved and how?
8.	Processes	What are the key steps of the crisis management process in your sector relating to EU-level crises? Please describe the following phases: Preparedness – response – recovery
9.	Processes	Preparedness: What type of trainings are provided to the crisis management team? Are these trainings/exercises carried out at the EU-level with relevant partners? (Examples of trainings: crisis readiness simulations, preparedness exercises, etc.) Is there a clear link between lessons learnt following a crisis managed at the EU-level and the subsequent trainings/exercises?
10.	Processes	Response: What is the activation mechanism (criteria) for a crisis and how does it work in practice? How do you activate the crisis management process?
11.	Processes	Response/recovery: What communication channels do you use with EU-level partners during a crisis? How do you deal with sovereignty and secrecy challenges in your sector? How do you overcome the challenges associated with information exchange?
12.	Processes	Recovery: Following a crisis, how is the review and evaluation conducted? How are lessons learnt communicated and who makes sure the necessary organisational changes are implemented?
13.	Processes	How are you ensuring the timely recovery of an incident? For instance, which specific procedures are in place? These might range from: formal escalating "down" the incident, considering final external communication, to ensuring Recovery Plans are fully implemented, etc. How are people informed to return to normal duties after the incident?
14.	Tools and platforms	What are the main EU-level crisis alert and/or management systems in place in your sector? Please describe their functions, including strengths and weaknesses.
15.	Tools and platforms	To what extent are the crisis management systems and tools standardised (e.g. between different Member States, DGs, agencies, etc.)?
16.	Tools and platforms	How are you monitoring a crisis (on an ongoing basis) and communication updates at the EU-level? Do you use tools to monitor media pressure and social medias?
17.	Tools and platforms	Is there a clear link between lessons learnt following a crisis managed at the EU-level and the systems/tools in place? Have there been fundamental changes to the systems in place following a crisis?

Annex C.
List of interviewed organisations per sector

Aviation

ORGANISATION	NAME	DEPARTMENT/ROLE
Airports Council International (ACI)	David Trembaczowski-Ryder	Head of Aviation Security
Ministry of Infrastructure and the Environment	Marc Van Oudheusden	Senior Policy Analyst/Advisor Crisis Management Directorate for Mobility and Transport Civil Aviation Department Division Safety, Security and Public Order
European Aviation Safety Agency	Rachel Daeschler	Deputy Strategy and Safety Management Director, Head of Safety Intelligence and Performance Department
European Aviation Safety Agency	Cyrille Rosay	Senior Expert Avionics - Cyber Security, Certification Directorate - Large Aeroplanes
EUROCONTROL	Antonio Nogueras	Head of Air Traffic Management security unit
EUROCONTROL	Žarko Sivcev	Advisor to Director of the Network Manager Directorate

Border Control

ORGANISATION	NAME	DEPARTMENT/ROLE
The Directorate-General for Migration and Home Affairs (DG HOME)	Laurent Muschel	Director for Migration and Protection at European Commission
FRONTEX	No name	-

Civil Protection

ORGANISATION	NAME	DEPARTMENT/ROLE
European Commission's Humanitarian Aid and Civil Protection (ECHO)	Dimitrios Pagidas	Emergency Response Unit

EU Crisis Response

ORGANISATION	NAME	DEPARTMENT/ROLE
EEAS – European External Action Service	Luigi Bruno	Planning and methodology – CPCC, Civilian Planning and Conduct Capability
EEAS – European External Action Service	Nicola Delcroix	Head of Division Consular Crisis Management
EEAS – European External Action Service	Kathleen Verstreken	Deputy Head of Division Consular Crisis Management
EEAS – European External Action Service	Giuliano Porcelli	Senior Crisis Management Officer – Office of the Deputy Secretary General for CSDP and Crisis Response

Counter Terrorism

ORGANISATION	NAME	DEPARTMENT/ROLE
EUROPOL – EC3 Division	Bruno Halopeau	Strategic & Crime Prevention Advisor
EUROJUST	Jon Broughton	Head of Information Management
EUROJUST	Pavel Golob	Deputy Head of Corporate Services
EUROJUST	José Eduardo Guerra	Deputy to the National Member for Portugal. Cyber Crime Unit
European Council	Giles de Kerckhove	EU Counter-terrorism Coordinator

Health and disease

ORGANISATION	NAME	DEPARTMENT/ROLE
European Centre for Disease Prevention and Control (ECDC)	No name	-
European Food Safety Authority (EFSA)	No name	-
The Directorate General for Health and Food Safety (DG SANTE)	No name	-

Annex D. Acronyms

ACRONYM	
AIRSAN	Coordinated action in the aviation sector to control public health threats
ARGUS	European rapid alert system
ATM	Air Traffic Management
COREPER	Committee of the Permanent Representatives of the Governments of the Member States to the European Union
CSIRT	Computer Security Response Team
EACCC	European Activation Crisis Coordination Cell
EC	European Commission
ECDC	European Centre for Disease Prevention and Control
EEAS	European External Action Service
EERC	European Emergency Response Capacity
ENISA	European Union Agency for Network and Information Security
ERCC	Emergency Response Coordination Centre
EU-LISA	European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice
EU	European Union
EUROCONTROL	European Organisation for the Safety of Air Navigation
Europol	European Police Office
EVITA	European Crisis Visualisation Interactive Tool
FRONTEX	European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union
HSC	Health Security Committee
IPCR	EU Integrated Political Crisis Response arrangements
ISAA	Integrated Situational Awareness and Analysis
JOs	Joint Operations
NIS	Network and Information Security (term used as equivalent to cybersecurity)
TFEU	Treaty on the Functioning of the European Union
UN	United Nations

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 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

enisa.europa.eu