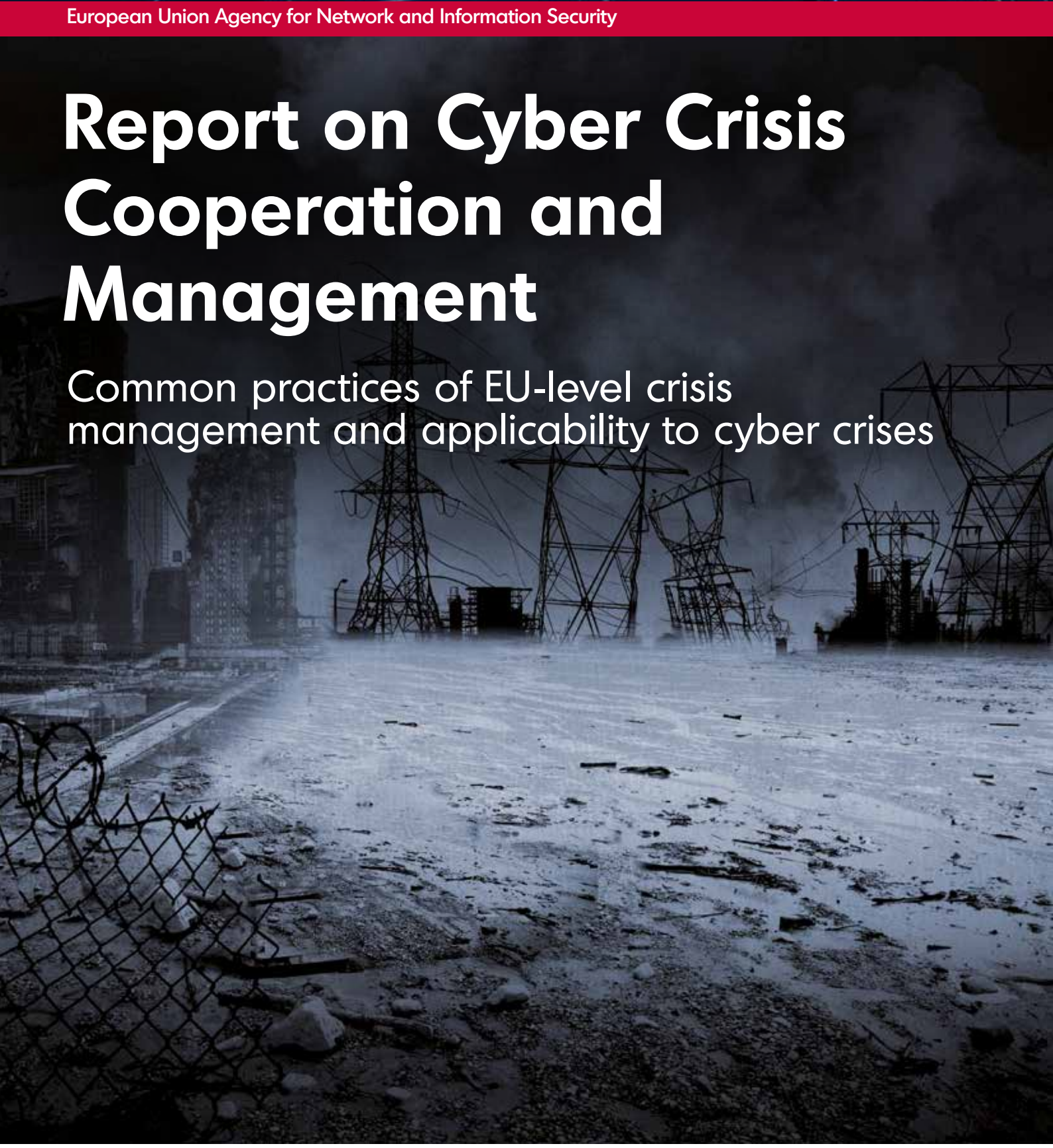
European Union Agency for Network and Information Security

Report on Cyber Crisis Cooperation and Management

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



December 2015

enisa.europa.eu

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.

enisa

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