Report on Cyber Crisis Cooperation and Management - Comparative study on the cyber crisis management and the general crisis management

Executive summary

The goal of this study is to provide an analysis of Cyber Crisis cooperation and 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.

The 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