EU-level Cyber Crisis Management

Prof. Dr. Udo HELMBRECHT

The Executive Director, EU Agency for Network and Information Security (ENISA)

Introduction

The societal developments of the last decade have made Information and Communication Technology (ICT) systems a crucial part of our daily lives. The last decade has brought 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. 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.

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 [1]. Cyber incidents are commonplace [2] and the likelihood for a crisis to be caused by one or more of these incidents increases every day (see incident escalation Figure 2). There is a high possibility that even terrorists may 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 governmental and non-governmental bodies at the national as well as international level 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 absorbs the cross-sectorial nature of the threat posed by cyber incidents.

From a general crisis management perspective, there have been significant achievements both within EU Member States and 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?

EU-level Political Crisis Management

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) [4], 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) [5], 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
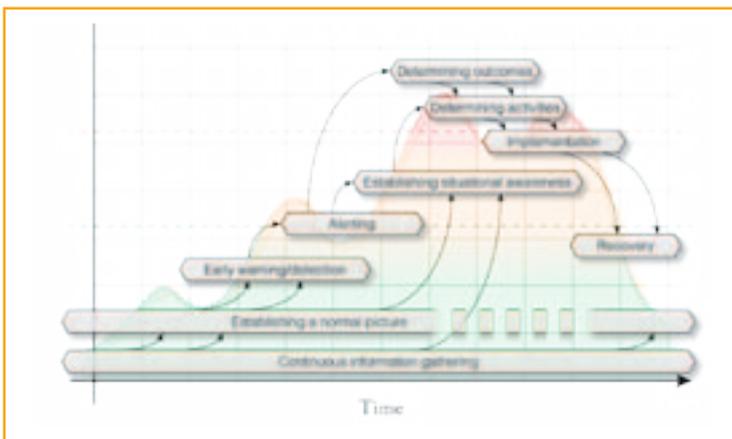

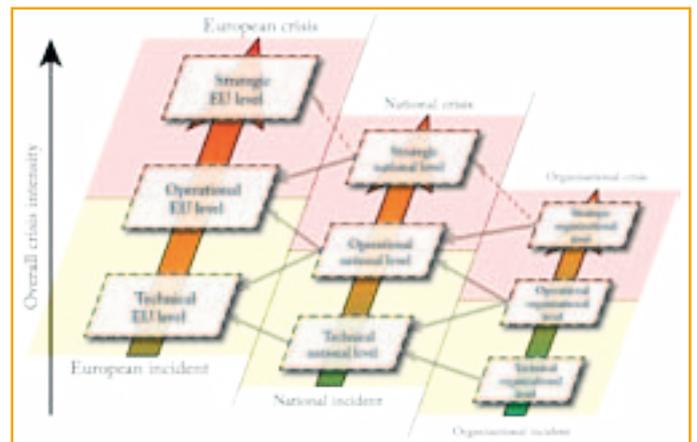*Figure 1: Practical crisis management activities overtime (source ENISA [1])*

Figure 2: Crisis escalation: from organisation to national and EU levels (source ENISA [1])