Strategies for incident response and cyber crisis cooperation

MARCH 2016

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.

Authors

ENISA

Contact

For contacting the authors please use cert-relations@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

Acknowledgement should be given to Jo De Muynck, Silvia Portesi (ENISA), and Bence Birkas as well as to the ENISA colleagues of COD1 (Secure Infrastructure & Services Unit) and COD3 (Operational Security Unit) who provided input and feedback during the compilation of this document

Table of Contents

Executive Summary

This document was prepared for the NIS Platform WG2 members introducing the main functions of CSIRTs from incident handling to crisis coordination – a high-level summary of the basics of incident response based on ENISA's previous work on CSIRTs and resilient European infrastructures.

The Network and Information Security (NIS) Platform[1] was created in 2013 to help European stakeholders carry out appropriate risk management, establish good cyber security policies and processes and further adopt standards and solutions that will improve the ability to create safer market conditions for the EU. All this was brought to life as a contribution to the implementation of the Cyber Security Strategy of the EU[2].

This document is an input for the NIS Platform for the discussion on incident response and cyber crisis coordination.

The document focuses on incident response: it briefly introduces what incident response is, who the main actors are, what baseline capabilities these entities should possess in order to effectively combat cyber-attacks, and what challenges there may be that impede efficiency in incident response. The notion of Computer Security Incident Response Teams (CSIRTs) as key players in incident response is introduced. Descriptions of incident response mechanisms will be elaborated, taking into account national-level cyber security strategies, cyber crisis coordination and management covering both escalation and communication between CSIRTs and government bodies.

The essence of the document was developed based on previous work undertaken by ENISA in the field of CSIRTs and Critical Information Infrastructure Protection (CIIP) and resilience. The main topics used as input for this document cover the following:

- findings and recommendations published under the baseline capabilities of CSIRTs and a brief description of incident response mechanisms;
- work done in the field of national cyber security strategies with special regard to implementation and evaluation of these strategies;
- aspects of cyber crisis cooperation and management focusing on escalation mechanisms and ways of further enhancing crisis cooperation mechanisms, such as mutual aid, training and exercising and Standard Operational Procedures (SOPs).

Some challenges will be raised on the typical issues that slow the incident response mechanisms, and to address these challenges, ways of enhancing incident handling cooperation will be provided.

[1] Information on NIS Platform - https://resilience.enisa.europa.eu/nis-platform
[2] High Representative of the European Union for Foreign Affairs and Security Policy, Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, 07 February 2013 - http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

1. Overview and scope of the document

The Network and Information Security (NIS) Platform[3] was created in 2013 to help European stakeholders carry out appropriate risk management, establish good cyber security policies and processes and further adopt standards and solutions that will improve the ability to create safer market conditions for the EU.

The expert work of the NIS Platform was divided into Working Groups (WGs), all dealing with their special field of expertise in cyber security. The following WGs were established:

1) WG1 on risk management, including information assurance, risks metrics and awareness raising;
2) WG2 on information exchange and incident coordination, including incident reporting and risks metrics for the purpose of information exchange;
3) WG3 on secure ICT research and innovation.

WG2 has been established to promote the sharing of cyber threat information and incident coordination in both the public and private segments of the EU. It aims to identify requirements and issue recommendations on sharing cyber threat information as well as appropriate incident management processes in order to better prevent and best respond to cyber incidents.

WG2 also investigates the feasibility and needs to address the ability of an organisation to share cyber threat information and to utilize a standard incident management process. This covers both public and private organisations, and all industry verticals within the private sector, with special focus on Critical National Infrastructures (CNIs).

The foreseen work by WG2 will be a series of deliverables (Chapters) to be adopted by the NIS Platform, identifying cyber security good practices, as an implementation of the Cyber Security Strategy of the EU published in 2013[4]. Incident response and cyber crisis coordination will be encompassed in Chapter 4 of these deliverables.

The foreseen Chapters by the three WGs are:

- Chapter 1: Organisational structures and requirements;
- Chapter 2: Verification and auditing of requirements;
- Chapter 3: Voluntary information sharing;
- Chapter 4: Incident response (**current document is prepared as an input for this deliverable**);
- Chapter 5: Mandatory incident notification;
- Chapter 6: Data protection;
- Chapter 7: [Optional] Incentives for the uptake of good cyber security practices;
- Chapter 8: [Optional] Recommendations on research challenges and opportunities.

In addition to the Chapter on incident response (Chapter 4), WG2 will also be responsible for delivering the chapters on voluntary information sharing (Chapter 3), mandatory incident notification (Chapter 5) and data protection (Chapter 6).

[3] Information on NIS Platform - https://resilience.enisa.europa.eu/nis-platform

The content of this document, which has been compiled as an input for Chapter 4, was developed based on ENISA's previous work in the field of Computer Security Incident Response Teams (CSIRTs) and the resilience of critical information infrastructures. The notion of CSIRTs will be introduced. Descriptions of incident response mechanisms will be elaborated, taking into account national cyber security strategies, on how incident response is structured in Member States – covering both escalation and communication between CSIRTs and government bodies.

This document focuses on incident response: how main incident response capabilities tie in with incident response mechanisms to potentially cover the cyber security landscape of a Member State.

This document does not go into details on the various aspects mentioned above as it aims to give a compact overview. However, in case of further interest, references to available literature on the aspects are provided in footnotes and in the Appendix.

2. Basics of incident response

An **information security incident** can be defined as a "single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security"[5], while a **cyber security incident** can be defined as "an IT disruption that limits or eliminates the expected availability of services, and/or is the unauthorized publication, acquisition and/or modification of information" [6]. A cyber security incident can involve a real or suspected breach or the unlawful act of exploiting vulnerability. Typical incidents include the introduction of malware into a network, Distributed Denial of Service (DDoS) attacks, unauthorised alteration of software or hardware and identity theft of individuals or institutions. Hacking in general can be considered a security incident unless the perpetrators have been deliberately hired for the specific purpose of testing a computer or network for vulnerabilities.

Incident response and management is the protection of an organisation's information by developing and implementing an incident response infrastructure (e.g. plans, defined roles, training, communications, management oversight) in order to quickly discover an attack and then effectively contain the damage, eradicate the attacker's presence, and restore the integrity of the network and systems.[7]

A **Computer Security Incident Response Team** (CSIRT) is an organisation that receives reports of security breaches, conducts analyses of the reports and responds to the senders.[8] A CSIRT may be an established group or an ad hoc group of experts. Other widely accepted terms exist for CSIRTs, such as CERT (Computer Emergency Response Team), IRT (Incident Response Team), CIRT (Computer Incident Response Team) or SERT (Security Emergency Response Team).[9] For a comprehensive list of CSIRTs in Europe, ENISA regularly updates an inventory of European CSIRTs[10], and Forum of Incident Response and Security Teams (FIRST)[11] and Trusted Introducer (TI)[12] have public links to their global members as well.

There are various types of CSIRTs. Dedicated incident response teams or CSIRTs may operate as part of a parent organisation, such as within a government, a corporation, a university or a research network. National and governmental CSIRTs, for example, oversee incident handling for an entire country or parts of its critical infrastructure. Typically, CSIRTs rely on information coming from within the organisation's information systems and act on an ad hoc basis in the event of a security incident. Business-oriented

---

[5] https://www.iso.org/obp/ui/#iso:std:iso-iec:27035:ed-1:v1:en

[6] Cyber Security Assessment Netherlands, 2014 - https://english.nctv.nl/publications-products/Cyber_Security_Assessment_Netherlands, p. 105. More discussion on the terminology is available in Report on Cyber Crisis Cooperation and Management, ENISA, 2014, p.26 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study

[7] https://www.sans.org/critical-security-controls/control/18

[8] For more information on what a CSIRT is, see also: https://www.enisa.europa.eu/activities/cert/support/guide2/introduction/what-is-csirt

[9] For more information on what a CSIRT is, see also: https://www.enisa.europa.eu/activities/cert/support/guide2/introduction/what-is-csirt

[10] Link to ENISA's CERT inventory - https://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe/at_download/fullReport

[11] Link to the FIRST website - https://www.first.org - Link to FIRST Members - https://www.first.org/members/teams

[12] Link to the TI website - https://www.trusted-introducer.org - Link to TI Directory - https://www.trusted-introducer.org/directory

CSIRTs provide paid services based on service level agreements (SLAs) or on an on-demand basis[13]. Sectoral, national or governmental CSIRTs oversee and act upon network activities of larger sectors or critical infrastructures. The basic types of service covered by a typical CSIRT will be elaborated upon in the 'incident response capabilities' section.

CSIRTs also provide proactive services, such as alerts and warnings or end-user security training, besides responding to incidents.

Regardless of the type of CSIRT, one of the main powers of CSIRTs lies in the fact that they can effectively mitigate incidents on a technical level in a relatively short time. Since attacks on the internet are borderless, the countermeasures involve cross-border cooperation between CSIRTs. To facilitate this cooperation, several international and regional CSIRT communities and initiatives have been formed over the past twenty years. Involvement in the following CSIRT communities is strongly advised for CSIRTs, including national and governmental CSIRTs:

TF-CSIRT (Task Force of Computer Security Incident Response Teams): this provides a forum where members of the CSIRT community can exchange experiences and knowledge in a trusted environment in order to improve cooperation and coordination. It maintains a system for registering and accrediting CSIRTs, as well as certifying service standards. The task force also develops and provides services for CSIRTs, promotes the use of common standards and procedures for handling security incidents, and coordinates joint initiatives where appropriate. This includes the training of CSIRT staff, and assisting in the establishment and development of new CSIRTs. (http://www.terena.nl/tech/task-forces/tf-csirt)

TI (Trusted Introducer): this forms the trusted backbone of infrastructure services and serves as a clearinghouse for all security and incident response teams. It lists well-known teams and performs accreditation and certification of teams according to their demonstrated and checked level of maturity. For a CSIRT to proceed from the status of 'listed' to the status of 'accredited', it needs to go through a formalized accreditation scheme. Once 'accredited', the CSIRT can gain access to the restricted TI repository where details of fellow accredited CSIRTs can be found, along with several value-added services such as readily downloadable contact lists and PGP-Keyrings, secure discussion forum, automatic RIPE Database IRT-object registration and more. (https://www.trusted-introducer.org/)

There is an on-going process to better integrate TF-CSIRT and TI to establish a unified European group with a recognizable membership and to improve coordination and use of staff resources, as well as to establish a more direct relationship between CSIRTs and the TF-CSIRT leadership[14], which will happen under the structure of GÉANT, formerly TERENA (Trans-European Research and Education Networking Association)[15].

FIRST (Forum of Incident Response and Security Teams): this is a premier organisation and a recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents by providing access to best practices, tools, and trusted communication with member teams. (http://www.first.org)

EGC (European Government CERTs group): this is an informal group of several governmental CSIRTs that is developing effective cooperation on incident response matters between its members, building upon the

[13] http://whatis.techtarget.com/definition/Computer-Security-Incident-Response-Team-CSIRT
[14] https://www.terena.org/activities/tf-csirt/publications/restructuring.pdf
[15] TERENA (http://www.terena.org/) and DANTE joined forces in October 2014 to become GÉANT Association. From 1 May 2015, the organisation changed its logo and its name to simply 'GÉANT'. New website - http://www.geant.org/Pages/Home.aspx

similarity in constituencies and problem sets between governmental CSIRTs in Europe. EGC is a closed group of CSIRTs that only allows European governmental CSIRTs among its members on the basis of invitation. (http://www.egc-group.org)

ENISA national and governmental CSIRT network: ENISA formed a network of national and/or governmental CSIRTs in Europe. It reaches out to this network via a mailing list to keep the network up to date on its activities. ENISA relies heavily on the input from this network when it is publishing studies. Many experts from this network have been members of expert groups organised by ENISA, and have been interviewed or have responded to questionnaires. The network is a key input for the work ENISA is doing in this field. (https://www.enisa.europa.eu/activities/cert) ENISA's 'CERTs in Europe' workshops have been organised since 2005 for the national and governmental CSIRTs in Europe as an efficient and indispensable method for ENISA in supporting the teams in improving their capabilities. In 2011, ENISA started to collaborate with Europol to focus on CSIRT cooperation with law enforcement. From 2012, the annual ENISA workshop was split into two parts, one part aimed only at national and governmental CSIRTs and had a technical focus, and the other part aimed at both national and governmental CSIRTs and law enforcement representatives, organised together with Europol. These workshops are particularly important as a forum for information sharing.

In December 2015, the Commission, the Parliament of the EU, and the Council of Ministers reached an agreement on the Network and Information Security (NIS) Directive. This draft Directive still needs to be formally adopted, the final text is expected in spring[16]. In the context of this directive, a CSIRTs network to is expected to be established, also with the support of ENISA, to ensure effective cooperation from all Member States[17].

The term '**constituency**' is used to refer to the customer base or the served group of users of a CSIRT. A single customer is a 'constituent'; a group is called 'constituents'.

2.1 A brief overview of incident response capabilities

ENISA started its stocktaking of CSIRT capabilities in Europe in 2009. The outcome of this activity was the first document on baseline capabilities for national and governmental CSIRTs, focusing on operational aspects[18]. A follow-up to this was a second document on baseline capabilities focusing on policy recommendations in 2010[19]. ENISA updated its considerations for the capabilities of national and governmental CSIRTs in 2012[20]. Although these capabilities are generally valid for all types of CSIRTs, the attention was specifically given to national and governmental CSIRTs in order to align them with the recommendations laid down in the EU Cyber Strategy. The four baseline capabilities were redefined as

[16] For more information see http://www.consilium.europa.eu/en/press/press-releases/2015/12/18-cybersecurity-agreement A link to the preliminary version is also provided.
[17] An informative note on what provisions of the upcoming NIS Directive might mean for CSIRTs has been published by ENISA and available at: https://www.enisa.europa.eu/activities/cert/other-work/nis-directive-and-national-csirts
[18] Baseline capabilities for national/governmental CERTs (Part 1: Operational Aspects), ENISA, 2009 - http://www.enisa.europa.eu/activities/cert/support/files/baseline-capabilities-for-national-governmental-certs/at_download/fullReport
[19] Baseline capabilities for national/governmental CERTs (Part 2: Policy recommendations), ENISA, 2010 - http://www.enisa.europa.eu/activities/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations/at_download/fullReport
[20] Baseline capabilities for national/governmental CERTs (Updated recommendations 2012), ENISA, 2012 - http://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012/at_download/fullReport

'formal capability', 'operational-technical capability', 'operational-organisational capability', and 'cooperational capability'.

2.1.1 Formal capability[21]

This capability should make the official mandate of the national or governmental CSIRT clear. This mandate should assume the CSIRT will be the official national point of contact for incident response issues, or act as the '*CSIRT of last resort*' in case of emergencies. With the designation of national point of contact, the CSIRT should be the national representation at the international CSIRT communities.

This capacity should also provide proof of sustainable financial and other resources. Ideally, an existing cyber security strategy (see later in chapter) should define the roles and responsibilities of the CSIRT, its relationships with other national public and private stakeholders in the national cyber security landscape and Incident Response (IR) practice. Generally, the main role of the national or governmental CSIRT should be supporting the management of security incidents for systems and networks within its state's borders.

2.1.2 Operational-technical capability[22]

The service portfolio of any national or governmental CSIRT should consist of the external services it provides to its constituency and its internal support processes, when the CSIRT is part of a larger host organisation.

There are four **external service** categories that cover the main CSIRT activities. **Internal services** might be, for example, a good situational awareness, technical cyber security training for staff or participation in various cyber security exercises (e.g. Cyber Europe Exercise).

- **Proactive services**, which are aimed at improving the infrastructure and security processes of the constituency before any incident or event occurs or is detected. The main goals are to avoid incidents and reduce their impact and scope when they do occur.
- **Reactive services**, which are aimed at responding to requests for assistance, reports of incidents from the CSIRT constituency, and tackling threats or attacks against the CSIRT's systems.
- **Other security management services**, which are the common services designed to improve the overall security of an organisation.
- **Optional (internal) services**, covering the field of awareness-raising or cyber security training within the host organisation.

In the context of core services for the constituency, a national or governmental CSIRT should provide incident handling and management, be the designated national point of contact, and play a role in the protection of Critical National Infrastructure (CNI). A comprehensive table of potential CSIRT services are include in CERT/CC's incident management guide[23].

---

[21] National/governmental CERTs; ENISA's recommendations on baseline capabilities, ENISA, 2014, p.3 - https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/national-governmental-certs-enisas-recommendations-on-baseline-capabilities/at_download/fullReport

[22] National/governmental CERTs; ENISA's recommendations on baseline capabilities, ENISA, 2014, p.4 - https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/national-governmental-certs-enisas-recommendations-on-baseline-capabilities/at_download/fullReport

[23] http://www.cert.org/incident-management/services.cfm

REACTIVE SERVICES	PROACTIVE SERVICES	SECURITY QUALITY MANAGEMENT SERVICES
Alerts and Warnings Incident Handling ▪ *Incident analysis* ▪ *Incident response on site* ▪ *Incident response support* ▪ *Incident response coordination* Vulnerability Handling ▪ *Vulnerability analysis* ▪ *Vulnerability response* ▪ *Vulnerability response coordination* Artefact Handling ▪ *Artefact analysis* ▪ *Artefact response* ▪ *Artefact response coordination*	Announcements Technology Watch Security Audits or Assessments Configuration and Maintenance of Security Tools, Applications, and Infrastructures Development of Security Tools Intrusion Detection Services Security-Related Information Dissemination	Risk Analysis Business Continuity and Disaster Recovery Planning Security Consulting Awareness Building Education/Training Product Evaluation or Certification

Table 1: List of CSIRT services[24]

2.1.3 Operational-organisational capability[25]

These capabilities cover resources, infrastructure, service delivery and business continuity. There are a number of best practices[26] that deal with organising resources – both human and technical – and processes to effectively comply with the mandate of the CSIRT. Apart from having the appropriate staffing, training and budget, the most important aspects in incident response are being available in 24/7 operating mode (duty officer), and becoming and maintaining a position as a trusted member of the existing CSIRT communities.

The section below on key challenges, however, outlines some of the common problems CSIRTs face in terms of organising their people, processes and technology.

[24] http://www.cert.org/incident-management/services.cfm
[25] National/governmental CERTs; ENISA's recommendations on baseline capabilities, ENISA, 2014, p.5 - https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/national-governmental-certs-enisas-recommendations-on-baseline-capabilities/at_download/fullReport
[26] RFC2350 at http://www.faqs.org/rfcs/rfc2350.html; Introduction to Return on Security Investment, ENISA, 2012 - http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment

2.1.4 Cooperational capability[27]

As threats, vulnerabilities and subsequent incidents in cyberspace affect more than one sector or country, both horizontal and vertical cooperation models need to be in place in incident response. Stakeholders include operators, service providers, hardware and software providers, end-users, public bodies and national governments, as well as peer organisations with similar responsibilities which require cross-border cooperation. Cooperation in each aspect involves a high level of trust between any participating members in a cooperation model.

National or governmental CSIRTs bear the responsibility of incident coordination over (part of) a nation's critical information infrastructure, which requires prompt action against well-defined metrics. Although incident types vary in the response required, service level agreements (SLAs) are a good basis to lay down the expected actions and response times between the CSIRT and its constituents. This should also apply to the national cooperation mechanisms between CSIRTS and local industry stakeholders.

Since cyberspace is borderless, large-scale incidents impact several nations. As covered above, a CSIRT should have enhanced cooperational capability to be able to reach out to peer CSIRTs and act in a coordinated manner. Cooperation in the international arena should also happen based on a voluntary approach, where peer CSIRTs share information and act in coordination based on the trust level they have built.

[27] National/governmental CERTs; ENISA's recommendations on baseline capabilities, ENISA, 2014, p.6 - https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/national-governmental-certs-enisas-recommendations-on-baseline-capabilities/at_download/fullReport

3. Key challenges in incident response

In general, incident response carries the burden of remediating any breaches in IT security at an organisation at micro level, or of a nation at macro level. A number of best practices exist to initiate or safeguard the level of integrity in IT security, but there is always a gap between legislation and practice. The current situation in the EU does not always provide the highest protection against NIS incidents and risks across the EU. Existing NIS capabilities and mechanisms are simply insufficient to keep pace with the fast-changing landscape of threats and to ensure a common high level of protection in all the EU Member States. As a first step in aligning the NIS level Member States, incident response capabilities need to meet a common minimum threshold level.

Many cyber security incidents today are cross border but Member States do not follow a harmonised approach when it comes to incident responses. However, there are challenges that need to be addressed when discussing common incident response mechanisms within the Member States. Having a regulatory framework and the required institutions in place will not automatically resolve the ever growing cyber threats within the EU boundaries. What need to be taken into consideration when assessing the incident response capabilities are, amongst others, the following areas: human resources, processes and procedures, political and legal framework, and technology (tools and data).

3.1 Human resource at CSIRTs

In general, skilled IT security personnel are hard to find. National and governmental CSIRTs will always lag behind in recruiting skilled and dedicated long-term staff members as compared to the private sector.

Defining the right size and composition of an incident response team may also be challenging, especially if the focus tends to fluctuate between deep technical activity and high-level, policy-driven ambitions. So when choosing the right personnel to staff an incident response team, it is important to ensure that these professionals are not only skilled in their own respective fields, but are also capable of making high impact decisions, especially when it comes to escalating an incident to national (or even international) crisis level. Good management oversight and clearly defined roles and responsibilities should help to overcome this challenge.

3.2 Processes and procedures

Another aspect that is strongly connected to the human factor in the course of incident response is the available processes and procedures. A clear, concise, well-documented incident response plan must be in place that complies with the existing policy framework at organisational level as well as national level. Overcomplicated response plans will delay the effectiveness of incident response and escalation procedures. If policies are loose, the incident response team may lack autonomy to act responsibly. It is vital that the personnel are available for the processes and procedures related to incident response. It is just as vital that the constituents of the national and governmental CSIRTs are also aware of their parts in the process of managing an incident.

3.3 Political and legal framework

At a high political level there may be a lack of full awareness of the importance of investing resources in incident response activities or difficulty in investing more resources due to a need to balance different priorities.

In addition, there might be conflicts of responsibilities or challenges in the cooperation between the different actors, e.g. authorities responsible for the public network, governmental network, military networks, classified networks, etc.

An adequate political and legal framework[28] can help to define various roles and responsibilities and enhance the overall cooperation in order to resolve an incident in a timely manner. "Cooperation at [national and] pan-European level is necessary to effectively prepare, but also respond to cyber-attacks. Comprehensive national cyber security strategies are the first step in this direction."[29]

3.4 Technology: tools and data

Incident response activities rely on tools to enable the discovery of information about systems and people involved in an incident. Buying the latest and best equipment will not lead to complete protection against cyber-attacks if used inadequately, unmanaged, untested, not updated, or if the properly trained human resource is absent. Therefore, continuous updates and training are essential for incident response teams. (See section on CSIRT training later.) Whether the decision is self-developed tools or services procured from vendors, the management of pertinent data is always a challenge.

[28] On the topic of legal aspects of information between CSIRTs in Europe, see ENISA, A flair for sharing - encouraging information exchange between CERTs. A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe, 2011 - https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing/legal-information-sharing-1

[29] ENISA, National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace, ENISA, 2012, p. 11 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper. For more information about cyber security strategies, see - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss

4. Incident response mechanisms

The previous sections briefly introduced what incident response is, who the main actors are, what capabilities these entities should possess in order to effectively combat cyber-attacks, and what challenges there may be that impede efficiency in incident response. This section aims to present some nexus between the main elements of incident response, with more emphasis on the daily technical-operational aspects and less focus on the high-level structures of incident response (sections on cyber security strategies and cyber crisis management will deal with these aspects later).

In the course of incident response, CSIRTs have to assess the information that characterises the existing cyber threats and attack vectors and all the data that comes from the logs of the number of electronic information systems under the scope of the CSIRT/incident response team. Also, any activities carried out and shared by peer CSIRTs need to be taken into consideration. The correlation between any of these factors will contribute to mitigating the impact of the incidents.

In general, incident response follows the process below[30]:

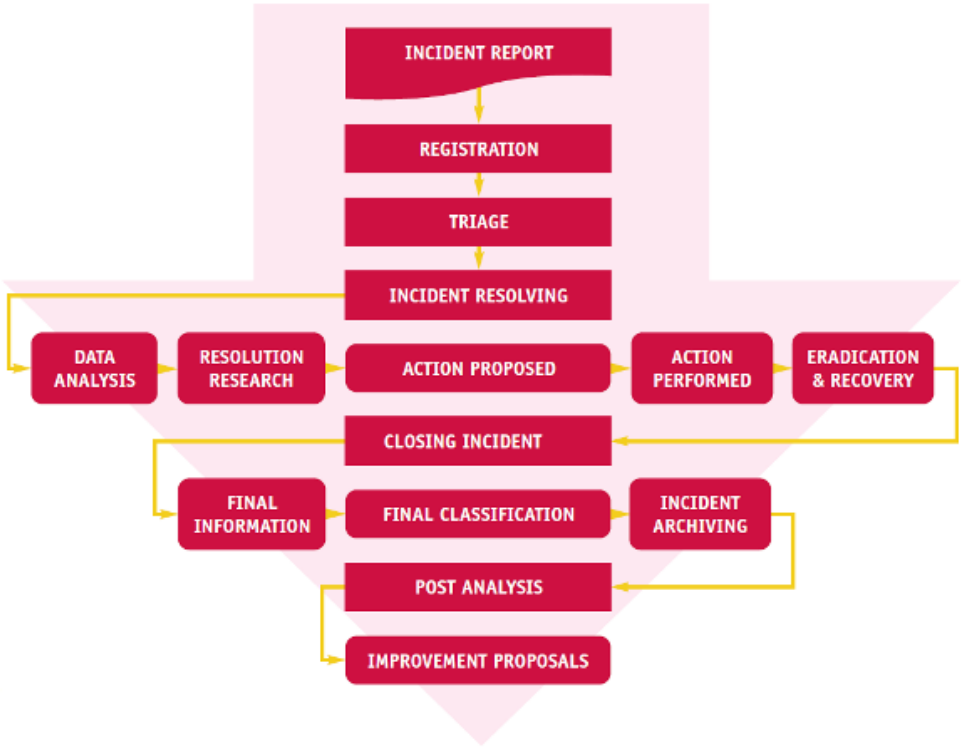

Figure 1: The typical incident response process

[30] More information on the incident handling process - https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process

4.1 Current threats and ways to respond

Based on the recently published ENISA Threat Landscape[31], a comprehensive matrix of current threat ranking and the impacted infrastructures is presented below.

Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Cyber-Physical Systems and CIP	Mobile Computing	Cloud Compu-ting	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtuali-sation
1. Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2. Web-based attacks	↑	↑	↑	↑	→		↑	
3. Web application attacks /Injection attacks	↑	↑	↑	↑	↑		↑	↑
4. Botnets	↓		↑	↑				
5. Denial of service	↑	↑		→	→		↑	↑
6. Spam	↓	↑						
7. Phishing	↑		↑		↑	↑	↑	↑
8. Exploit kits	↓		↑		↑		↑	
9. Data breaches	↑			↑		↑		↑
10. Physical damage/theft /loss	↑	↑	↑		↑	↑	↑	↑
11. Insider threat	→	↑		↑		↑	↑	↑
12. Information leakage	↑	↑	↑	↑	↑	↑	↑	↑
13. Identity theft/fraud	↑	↑	↑	↑	↑	↑	↑	↑
14. Cyber espionage	↑	↑		↑	↑	↑		↑
15. Ransomware/ Rogueware/ Scareware	↓		↑					

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing

Table 2: Overview of threats and emerging trends from the ENISA Threat Landscape 2014

Cyber threats are mainly connected to criminal activity to target the ICT networks, where citizens, businesses, or national interest are at stake. In response to the ever emerging cyber threats, adequate digital tools and technologies need to be in place to ensure security and to combat cyber-crime. To achieve

[31] ENISA Threat Report 2014 - https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at_download/fullReport

cyber resilience, incident response capabilities at all levels (private sector, national and EU) must play an essential role in fighting against these threats.[32]

4.2 Early warning intelligence vs. information

Information – in the broad sense – is a key element in the daily operation of a CSIRT to reduce the impact of cyber incidents. Operating early warning systems, using proactive detection methods, and processing and exchanging actionable information are all part of the operational-technical capability of a CSIRT.[33] While open source threat information is valuable to CSIRTs, an emerging service is Cyber Threat Intelligence, which provides added value to the constituents. Cyber Threat Intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets, that can be used to inform decisions regarding the subject's response to that menace or hazard. Based on this, the distinction between information and intelligence can be characterized as follows[34]:

INFORMATION VERSUS INTELLIGENCE	
Raw, unfiltered feed	Processed, sorted information
Unevaluated when delivered	Evaluated and interpreted by trained intelligence analysts
Aggregated from virtually every source	Aggregated from reliable sources and cross-correlated for accuracy
May be true, false, misleading, incomplete, relevant or irrelevant	Accurate, timely, complete (as possible), assessed for relevancy
Not actionable	Actionable

Table 3: Information vs. intelligence

Cyber Threat Intelligence comes as a service from specialized IT security service providers. CSIRTs or network operators should invest in such a service with a clear concept of cost-benefit ratio on IT security[35]. The advantage of this service is to be able to issue probability-based warnings of future cyber-attacks and tailored alerts and warnings to the specific risks and threats of the constituency[36].

[32] Adapted from the Cybersecurity Strategy of the European Union - http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[33] Extensive reading is available on information acquisition and use on ENISA's CERT support section: e.g. proactive incident detection (http://www.enisa.europa.eu/activities/cert/support/proactive-detection), actionable information (http://www.enisa.europa.eu/activities/cert/support/actionable-information), or alerts, warnings and announcements (http://www.enisa.europa.eu/activities/cert/support/awa)

[34] http://www.isightpartners.com/wp-content/uploads/2014/07/iSIGHT_Partners_What_Is_20-20_Clarity_Brief1.pdf

[35] Introduction to Return on Security Investment, ENISA, 2012 - http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment/at_download/fullReport

[36] National/governmental CERTs; ENISA's recommendations on baseline capabilities, ENISA, 2014, p.4 - https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/national-governmental-certs-enisas-recommendations-on-baseline-capabilities/at_download/fullReport

Most national and governmental CSIRTs have established incident detection sensors and properly implemented **Security Information and Event Management** (SIEM) systems[37] to gather early warning intelligence and process threat intelligence. Other detection and early warning arrangements may include monitoring open sources and media coverage, and information exchange between relevant stakeholders. This exchange could take place within a critical infrastructure information exchange forum, which in some cases could include large private companies besides the public stakeholders.[38]

4.3 Information sharing and incident reporting

Information sharing, as an incident coordination tool, is extensively discussed in 'Chapter 3' of WG2 of the NIS Platform (Voluntary information sharing), while mandatory incident notification, as a tool for impact assessment, is dealt with in 'Chapter 5' (Mandatory incident notification) and is briefly listed above in 'Overview and scope of the document'.

[37] Security Information and Event Management (SIEM) technology supports threat detection and security incident response through the real-time collection and historical analysis of security events from a wide variety of event and contextual data sources. It also supports compliance reporting and incident investigation through analysis of historical data from these sources. The core capabilities of SIEM technology are a broad scope of event collection and the ability to correlate and analyze events across disparate sources. http://www.gartner.com/it-glossary/security-information-and-event-management-siem/

[38] Report on Cyber Crisis Cooperation and Management, ENISA, 2014, p.35 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study/at_download/fullReport

5. Incident response in cyber security strategies

The importance of the cyberspace and digital economy has grown over the last 15 years. Citizens, businesses and governments became connected to and dependent on more and more complex ICT systems; the flow of information is borderless and the amount of data and information produced by each interaction in the Internet economy is growing with the speed of light. To safeguard the merits of the Internet, and to ensure the protection of fundamental rights in cyberspace, a new approach to the cyber world was adopted. Cyber security strategies started emerging in recognition of the changing security landscape shifting towards the cyber world. Countries, communities with common interest, and international organisations started publishing their cyber security strategies.

A national cyber security strategy is a strategic framework for a nation's approach to cyber security. It is a tool to improve the security and resilience of national infrastructures and services. It is a high-level, top-down approach to cyber security that establishes a range of national objectives and priorities that should be achieved in a specific timeframe. In general, the key objectives of these security strategies focus on the following aspects[39]:

- to develop cyber defence policies and capabilities;
- to achieve cyber resilience;
- to reduce cyber-crime;
- to support industry on cyber security;
- to secure critical information infrastructures[40].

The EU published its own cyber security strategy in 2013[41], in which the Commission sets out goals to Member States, the private sector and the EU agencies to take steps toward a more resilient European cyberspace. The EU Cyber Security Strategy explicitly makes reference to the existing gaps in terms of capacities, coordination and preparedness, where actions not only at EU level but also at national level are required to follow up the recommendations of the EU Cyber Security Strategy. These proposals focus on the following three areas:

- Member States should meet the baseline requirements in NIS, by which well-functioning CSIRTs shall be set up; competent authorities shall be in place in NIS; critical information infrastructures protection will become a priority; and national NIS strategies and cooperation plans shall be drawn up. The same tasks shall apply to the EU and its institutions to secure the EU IT systems[42].

[39] An Evaluation Framework for National Cyber Security Strategies, ENISA, 2014, p.6 - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies/at_download/fullReport

[40] The example is taken from the Cybersecurity Strategy of the European Union - http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[41] High Representative of the European Union for Foreign Affairs and Security Policy, Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, 07 February 2013 - http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[42] CERT-EU, the Computer Emergency Response Team responsible for the security of the IT systems of the EU institutions, agencies and bodies, was set up in 2012. CERT-EU's mission is to support the European institutions to protect themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and

- Member States should set up coordinated prevention, detection, mitigation and response mechanisms, enabling information sharing and mutual assistance amongst the national NIS competent authorities on the basis of the EU-wide NIS cooperation plan.
- The private sector should also make an effort to develop its own cyber resilience capacities and share best practices across sectors. The tools developed by industry to respond to incidents, identify causes and conduct forensic investigations should also benefit the public sector.

ENISA has carried out extensive work on national cyber security strategies[43] to support Member States in the development, implementation and evaluation of these strategies to overcome the existing gaps in terms of capacities, coordination and preparedness. Since each Member State has its own priorities on cyber security, there is no uniform solution to the content, but as a general guideline, the following components should be addressed when developing a national cyber security strategy[44]:

- setting the vision, scope, objectives and priorities;
- following a national risk assessment approach;
- taking stock of existing policies, regulations and capabilities;
- developing a clear governance structure;
- identifying and engaging stakeholders;
- establishing trusted information-sharing mechanisms;
- developing national cyber contingency plans;
- organising cyber security exercises;
- establishing baseline security requirements;
- establishing incident reporting mechanisms;
- creating user awareness;
- fostering R&D;
- strengthening training and educational programmes;
- establishing an incident response capability;
- addressing cyber-crime;
- engaging in international cooperation;
- establishing a public-private partnership;
- balancing security with privacy.

A national cyber incident contingency plan is designed to respond effectively to a large-scale cyber incident. The focus should be on baseline mechanisms and procedures for communication between national public and private stakeholders in the event of large-scale cyber disruptions, incident response and recovery. The national contingency plans should be based on a national cyber risk assessment of critical information infrastructures and their dependencies.

---

harm the interests of the EU. The scope of CERT-EU's activities covers prevention, detection, response and recovery. (CERT-EU RFC2350 - http://cert.europa.eu/static/RFC2350/RFC2350_CERT-EU_v1_0.pdf)

[43] ENISA's work on cyber security strategies - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss

[44] National Cyber Security Strategies; Practical Guide on Development and Execution, ENISA, 2012, p.35 - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport

Although the national security agency might drive the implementation of a national cyber security strategy, the national and governmental CSIRT usually has an extended role. In the particular case of The Netherlands[45], for instance, GOVCERT.NL, the former Computer Emergency Response Team of the Dutch government, formed the basis of the National Cyber Security Centre (NCSC) tasked with protecting the national (critical) information infrastructures.

The NCSC may have responsibilities that concentrate on developing and offering expertise and advice, supporting and implementing responses to threats or incidents, and strengthening crisis management. The NCSC may also organise and facilitate Information Sharing and Analysis Centres (ISACs), involving intelligence, CSIRT communities and critical infrastructure stakeholders in order to facilitate information-sharing in a trustworthy environment. If ISACs are set up, it also assumes another key element of a national cyber security strategy, which is the establishment of public-private partnerships (PPPs), where an organised relationship is created between the public and private sectors to achieve shared goals.[46] Revision and evaluation of a national cyber security strategy must be undertaken at a higher level. Usually this is done through a National Cyber Security Council, which has members from both the public and private sectors. A council can advise both government and private parties on relevant developments in the area of cyber security, prioritize specific (emerging) IT threats, and ensure that basic values are incorporated in the execution of the strategy.[47]

[45] National Cyber Security Strategy 2 'From awareness' (2013), https://www.ncsc.nl/english/current-topics/news/new-cyber-security-strategy-strengthens-cooperation-between-government-and-businesses.html - The National Cyber Security Strategy (NCSS) 'Strength through cooperation' (2011), https://www.ncsc.nl/english/current-topics/news/national-cyber-security-strategy-launched.html

[46] National Cyber Security Strategies; Practical Guide on Development and Execution, ENISA, 2012, p.35 - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport

[47] National Cyber Security Strategies; Practical Guide on Development and Execution, ENISA, 2012, p.36 - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport

6. Ways of enhancing incident handling cooperation

6.1 Cyber crisis cooperation and management

By definition, a crisis is 'an extraordinary event that differs from the normal and involves serious disturbance or risk for disturbance of vital societal functions'[48]. Depending on the context – EU and national, academia, and best practice – 'cyber crisis' can be defined respectively as:

- "An abnormal and unstable situation that threatens an organisation's strategic objectives, reputation or viability. An event that strikes at the heart of the organization"[49];
- "A serious threat to the basic structures or the fundamental values and norms of a system (in cyber space), which, under time pressure and highly uncertain circumstances, necessitates making vital decisions"[50];
- "Situation where the equilibrium among the basic components of the system on the one hand, and approach of the environment on the other hand, is disrupted in a serious way"[51].

When it comes to defining a cyber crisis, a common approach at national level is to treat it as a general crisis with a cyber element, which implies that managing a crisis is not scenario-driven, but process-oriented[52].

Moreover, most cyber crises will have effects on the physical world, so mostly a combination of cyber- and non-cyber crisis needs to be mitigated.

Cyber crises may also transcend national and geographic boundaries[53]. A proposal for a strong procedural triple-layered framework for cooperation[54] between EU public organisations – supporting the Member

[48] Report on Cyber Crisis Cooperation and Management, ENISA, 2014, p.26 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study/at_download/fullReport

[49] Report on Cyber Crisis Cooperation and Management, ENISA, 2014, p.28 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study/at_download/fullReport. See also in it footnote n. 33 to Snowdon (2014) Managing a Cyber-Crisis. http://www.regesterlarkin.com/news/managing-a-cyber-crisis-what-is-the-most-effective-way-to-prepare-leadership-teams-for-a-high-tech-threat

[50] Report on Cyber Crisis Cooperation and Management, ENISA, 2014, p.28 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study/at_download/fullReport. See also in it footnote n. 34 to Boin,'t Hart, Stern & Sundelius (2005).

[51] Report on Cyber Crisis Cooperation and Management, ENISA, 2014, p.28 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study/at_download/fullReport. See also in it footnote n. 35 to Jirásek, Novák & Požár (2013).

[52] http://isnblog.ethz.ch/intelligence/49634

[53] http://itlaw.wikia.com/wiki/Cyber_crises referring to http://www.dhs.gov/sites/default/files/publications/NSTAC%20Input%20to%20the%20National%20Plan%202001.pdf

[54] Report on the 2nd ENISA International Conference on Cyber-crisis Cooperation and Exercises, ENISA, 2013 - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/report/at_download/fullReport

States' needs – clearly describes a practical approach to the management of large-scale crisis. The elements that are required for the management of a cyber crisis are broken down into three levels:

- The **strategic level** needs to be triggered when the crisis is likely to have a socio-economic impact. The crisis is escalated to this level of decision-making if the daily life of the citizens is at stake, or the situation needs the activation of a national contingency plan. In this case, communication to the public is also the task of the strategic level. In crisis mode, the nature of the crisis is irrelevant to the policy-makers, who make decisions based on the assessment of the operational level, and also on political motivation. Possible actors at this level are the heads of departments, cyber security councils, national defence councils, national crisis management boards, etc. In case several Member States are impacted by a crisis, high-level EU crisis management mechanisms may be triggered, such as the Integrated Political Crisis Response (IPCR)[55].
- The **operational level** focuses on threat analysis, situational assessment and mitigation action measures. Actors at this level are cyber security agencies or authorities, governmental CSIRTs, national communication authorities, and operational crisis management bodies. The recent pan-European exercises showed that the operational EU cyber community is still in the capability-building phase and need to increase their efforts in adopting the EU Standard Operational Procedures (SOPs) in their daily work.
- The **technical level** involves incident handling by monitoring, detecting and handling the incidents, and alerting and informing the operational level with the appropriate raw technical information. Actors at this level include the CSIRTs and abuse teams operating at information systems. CSIRTs have long-standing information exchange channels that work sufficiently on sharing actionable information, especially in the case of large-scale cyber incidents.

The key in effective cyber crisis coordination is the shared responsibility and comprehensive approach among the stakeholders, which involves efficient national information exchange mechanisms and cross-border cooperation between the specific management levels. At the operational level, Standard Operating Procedures (SOPs) need to be in place to ensure the common understanding of actions and measures to be taken in cross-border cyber crisis management. At the technical level, the information exchange mechanisms of the CSIRT networks already have a long history. What is currently lacking at the technical level is the structured manner of incident handling activities in cyber crisis mode. Cyber exercises serve the purpose of addressing this shortcoming.

[55] More information on the EU integrated political crisis response arrangements - http://www.consilium.europa.eu/en/documents-publications/publications/2014/eu-ipcr/

Figure 2: Crisis escalation model based in the EU[56]

6.2 Cyber crisis management steps

According to the literature on crisis management, there are five stages in the resolution of a crisis. The steps described in the figure below should not be regarded as distinct events, but rather as overlapping activities that flow into one another.[57]

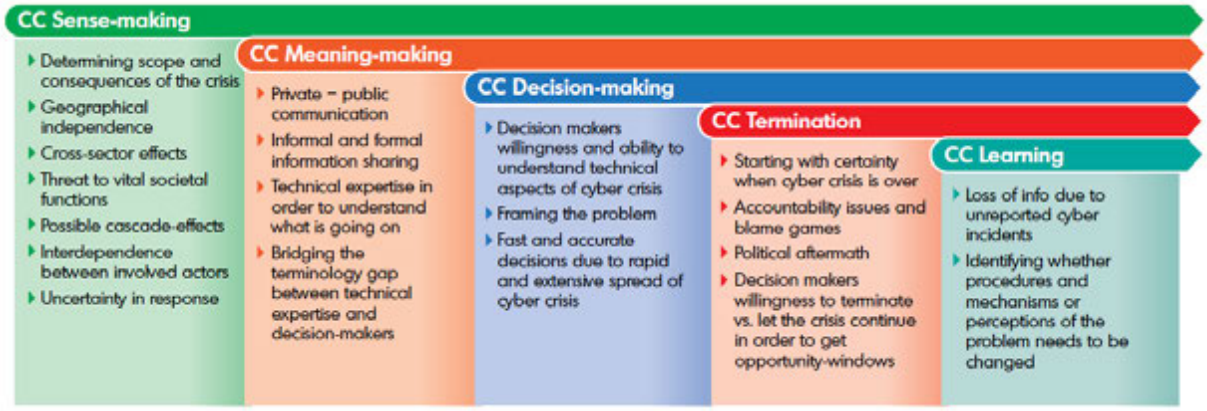

Figure 3: Cyber crisis management steps

[56] Report on Cyber Crisis Cooperation and Management, ENISA, 2014, p.40 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study/at_download/fullReport

[57] Report on Cyber Crisis Cooperation and Management, ENISA, 2014, p.33 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study/at_download/fullReport

6.3 Mutual Aid to boost preparedness

Cyber crisis management is not limited to the mitigation of cyber-attacks only, but also includes the handling of low-probability/high-impact events (Black Swan[58]), which usually occur at the time of natural disasters, cross-border power outages or failures in communication networks (due to technological or human errors). This way, end-users, the ICT traffic capacity, or critical infrastructures may be impacted. Any of these impacts assume a certain level of emergency, where both the physical world and the cyber domain need to be handled with the appropriate level of contingency.

To improve the preparedness level resulting from these Black Swan events, ENISA has carried out a series of studies that deal with the concept of Mutual Aid for Resilient Infrastructures in Europe (MARIE)[59]. The current observations show that Mutual Aid concepts can only be fully exhausted if both the public and private sectors are involved in the mutual aid agreements, and the previously mentioned strategic, operational and technical areas have their role in the crisis management. Mutual Aid assumes an efficiently functioning information exchange mechanism and the cross-border interoperability between ICT systems. Five recommendations have been proposed in the MARIE report[60], as listed below:

- governments should be responsive in creating an environment that supports private sector initiatives that seek to establish Mutual Aid assistance by reducing regulatory obstacles;
- the private sector should develop and maintain a standard Mutual Aid agreement template;
- the private sector entities with critical infrastructure functions should establish formal Mutual Aid assistance with industry peers, cross-sector entities and governments;
- the private sector, in consultation with government, should develop strategies to manage the scarcest resources in order to provide relief for the affected public(s);
- specific plans are needed for the communication of the temporary unavailability of critical infrastructure functions.

[58] http://rationalwiki.org/wiki/Black_swan

[59] Further information on the topic is available at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/mutual-aid-assistance

[60] Mutual Aid for Resilient Infrastructures in Europe (MARIE): Phase II recommendations report, ENISA, 2013, pp.10-20 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/mutual-aid-assistance/m-a-r-i-e-phase-ii-recommendations-report/at_download/fullReport

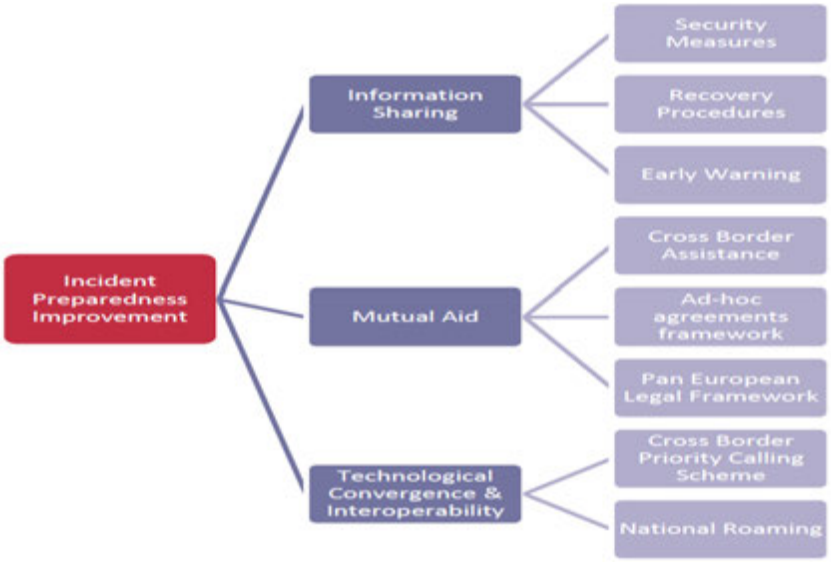

Figure 4: Incident Preparedness Improvement scheme[61]

6.4 European Union Standard Operational Procedures

A tool for cyber crisis cooperation amongst EU and EFTA Member States is the European Union Standard Operational Procedures (EU-SOPs). The objective of the EU-SOPs is to improve information exchange and cooperation between Member States at the time of a cross-border cyber crisis to speed up the common understanding of the effects and causes of the escalated incident and the possible mitigation of their impacts. The community that can use these SOPs consists of all EU as well as EFTA operational bodies from public authorities which can be involved in the management of cross-border cyber crises.[62]

6.5 Exercises to enhance incident handling cooperation

Cyber exercises are an important tool to assess the preparedness of a community against cyber crises, technology failures and critical information infrastructure incidents. According to the EU Cyber Security Strategy, exercises at EU level are essential to simulate cooperation among the Member States and the private sector. The reason for multinational exercises is the fact that the threat of cyber incidents and attacks is borderless, thus the cross-border crisis cooperation mechanisms need to be tested and validated from time to time.

[61] Position Paper of the EP3R Task Forces on Incident Management and Mutual Aid Strategies, ENISA, 2013, p.5 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-masim/at_download/fullReport

[62] Standard Operational Procedures to manage multinational cyber-crises finalised by EU, EFTA Member States and ENISA, ENISA, 2014 - http://www.enisa.europa.eu/media/press-releases/standard-operational-procedures-to-manage-multinational-cyber-crises-finalised-by-eu-efta-member-states-and-enisa

ENISA supports the stakeholders involved in EU cyber exercises[63]. The first exercise involving the Member States was carried out in 2010 ('Cyber Europe 2010[64]'), the second exercise took place in October 2012 ('Cyber Europe 2012[65]'), and the third EU cyber exercise ('Cyber Europe 2014[66]') was carried out in October 2014. The first joint EU-US table-top exercise was carried out in November 2011 ('Cyber Atlantic 2011').[67] Further exercises are planned for the coming years, continuing the Cyber Europe roadmap. Cyber Europe 2012 and 2014 also engaged the private sector, which is a key partner both as the primary target of cyber-attacks as well as in incident handling.

To facilitate the work of Member States, ENISA has produced a document on how to organise cyber exercises[68], with the main focus on the life-cycle of incident response and crisis coordination exercises. In terms of incident response and crisis coordination, a well-planned exercise has multiple benefits. Various elements of the cyber security plans can be tested during an exercise, involving the technical, operational or strategic level, or even all of them, as was the case in Cyber Europe 2014.

When it comes to testing technical capabilities, the most commonly tested aspects are the validity of the incident handling procedures, alerting mechanisms, information sharing mechanisms in the form of scenario-based exercises, or even actual technical capabilities in the form of hands-on exercises, as in the technical phase of Cyber Europe 2014.

Testing operational capabilities could focus on testing general preparedness, reaction times in case of an incident, escalation and alerting mechanisms, as well as drafting of situational awareness reports. Testing cooperation and the associated procedures, dependencies and reporting mechanisms should be the role of the operational level. Both table-top and scenario-based exercises can serve the purpose of testing the operational level.

Testing of the capabilities of the strategic level is difficult to organise, but just as important as the other two levels. For strategic decision-makers, the relevance in the exercise is on the crisis mode, and not the nature of the crisis. The challenge in bringing the decision-makers into the exercise is to be able to invoke their activity by the assessments provided in the course of the exercise by the technical and operational levels. Decision-making processes and public communication are some areas of focus.

---

[63] Executive Summary on National and International Cyber Security Exercises; Survey, Analysis and Recommendations, ENISA, 2012 - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-exercises/exercise-survey2012/at_download/execSummary

[64] Cyber Europe 2012 – Evaluation Report, ENISA, 2012 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2010/ce2010report/at_download/fullReport

[65] Cyber Europe 2012 – Key Findings Report, ENISA, 2012 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report

[66] ENISA CE2014, After Action Report, ENISA, 2015 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/ce2014-after-action-report/at_download/fullReport

[67] High Representative of the European Union for Foreign Affairs and Security Policy, Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, 07 February 2013 - http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

[68] National and International Cyber Security Exercises; Survey, Analysis and Recommendations, ENISA, 2012 - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber_exercises/national-exercise-good-practice-guide/at_download/fullReport

6.6 CSIRT training to enhance capabilities

Last, but not least, training plays an integral part in CSIRT capability enhancement. A number of courses and modules are available to teach and train the staff at CSIRTs. The section above on 'Key challenges in incident response' already touched upon the topic of staff preparedness in tools and techniques.

This section on training is far from being exhaustive, but it lists the main CSIRT training courses that are widely available for the European CSIRT community. There are a number of professional organisations offering training services that focus on incident response in general, or any of its special fields.

The most widely known CSIRT training course is the TRANSITS training, which takes place at least twice a year. ENISA facilitates and supports the TRANSITS courses. The TRANSITS programme consists of basic and advanced (hands-on) courses. The course materials were developed by the former TERENA[69] in collaboration with members of its Task Force of Computer Security Incident Response Teams (TF-CSIRT) and are regularly updated. The TRANSITS-I[70] course is aimed at new or potential CSIRT personnel who wish to gain a good grounding in the main aspects of working in an incident handling and response team. The topics include: 1) organisational, 2) technical, 3) operational, and 4) legal issues. The TRANSITS-II[71] course is aimed at more experienced personnel working for established CSIRTs. It provides an in-depth study of key areas in incident handling and response operations, training in how to improve communications with constituents, along with practical exercises.[72] The advanced topics of the course include: 1) netflow analysis, 2) forensics, 3) communication, and 4) CSIRT exercises.

ENISA also plays an important role in CSIRT training. It has developed a number of training resources that form a module which can be used in organising successful training events or adding a hands-on component to conferences. The ENISA CSIRT training material was introduced in 2008, and was complemented with new exercise scenarios in 2012, 2013 and 2014. The material contains essential components for success in the CSIRT community and in the field of information security. The ENISA website contains the ENISA CSIRT training resources, including a handbook for teachers, a toolset for students and Virtual Image to support hands-on training sessions. Most of the training can therefore be undertaken by using this material. ENISA also offers on-site training. Requests for these training sessions must typically go through the national and governmental CSIRT or another competent authority of an EU Member State. The training resources are structured around: 1) technical, 2) operational, 3) setting up a CSIRT, and 4) legal and cooperational issues. The materials vary from hands-on technical scenarios to handbooks and toolsets. All the resources are built in a way that by going through the module, the CSIRT staff will be able to acquire the basics of the baseline capabilities of incident response.[73]

One of the added values of the CSIRT communities is the continuous training these platforms provide. FIRST, as the largest global CSIRT community, places emphasis on technical CSIRT staff training that focuses on current threats and trends[74]. In the past, FIRST has provided its expertise to the TRANSITS courses and it has also organised hands-on technical courses co-located with the TF-CSIRT TI events. FIRST, as a global organisation, plans to develop an education programme for CSIRTs around the world with the help of the

[69] TERENA and DANTE joined forces in October 2014 to become GÉANT Association. From 1 May 2015, the organisation changed its logo and its name to simply 'GÉANT'. New website: http://www.geant.org/Pages/Home.aspx
[70] https://www.terena.org/activities/transits/transits-i/
[71] https://www.terena.org/activities/transits/transits-ii/
[72] http://www.enisa.europa.eu/activities/cert/events/transits-training
[73] More information on ENISA's training materials - http://www.enisa.europa.eu/activities/cert/training
[74] FIRST Symposia, Technical Colloquia, and Workshops - https://www.first.org/events

global security community. The development of a curriculum based on 'CSIRT Services Framework' will be a collaboration by the community and convened by FIRST.[75]

[75] https://www.first.org/global/education

7. Conclusion

WG2 of the NIS Platform is tasked to address the sharing of cyber threat information and incident coordination in both the public and private segments of the EU. Incident response is among its objectives to identify requirements and issue recommendations on sharing cyber threat information as well as appropriate incident management processes in order to better prevent and best respond to cyber incidents.

There is a wide range of mechanisms that cover the cyber security landscape of a Member State. Incident response is just one of many. CSIRTs, as privileged players in incident response, fulfil their roles as defined by the national plans in cyber security.

The aim of this document is to support and instigate discussion between WG2 members of the NIS Platform on the topic of incident response and cyber crisis coordination and serve as input for the compilation of a related deliverable by the WG.

This document set out to introduce the reader to the basics of incident response on a high level. Besides the main definitions and stakeholders, the separate section was dedicated to the main CSIRT capabilities regarded as 'baseline' which are a desired requirement in the EU Cyber Security Strategy. Some key challenges were raised on the typical issues that slow the incident response mechanisms, and to address these challenges, ways of enhancing incident handling cooperation were given.

Annex A: Some relevant ENISA material

1. A step-by-step approach on how to set up a CSIRT, ENISA, 2006 - https://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide/at_download/fullReport
2. An Evaluation Framework for National Cyber Security Strategies, ENISA, 2014 - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies/at_download/fullReport
3. Baseline capabilities for national/governmental CERTs (Part 2: Policy recommendations), ENISA, 2010 - https://www.enisa.europa.eu/activities/cert/support/files/baseline-capabilities-of-national-governmental-certs-policy-recommendations
4. Baseline capabilities for national/governmental CERTs (Updated recommendations 2012), ENISA, 2012 - https://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012/at_download/fullReport
5. Baseline capabilities for national/governmental CERTs (Part 1: Operational aspects), ENISA, 2009 - https://www.enisa.europa.eu/activities/cert/support/files/baseline-capabilities-for-national-governmental-certs
6. ENISA – CERT Inventory, ENISA, 2015 - https://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe/at_download/fullReport
7. ENISA's Threat Landscape 2014, ENISA, 2014 - https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at_download/fullReport
8. Executive Summary on National and International Cyber Security Exercises; Survey, Analysis and Recommendations, ENISA, 2012 - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-exercises/exercise-survey2012/at_download/execSummary
9. A flair for sharing - encouraging information exchange between CERTs. A study into the legal and regulatory aspects of information sharing and cross-border collaboration of national/governmental CERTs in Europe, ENISA, 2011 - https://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/legal-information-sharing/legal-information-sharing-1
10. Good Practice Guide to National Exercises, ENISA, 2009 - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber_exercises/national-exercise-good-practice-guide/at_download/fullReport
11. Introduction to Return on Security Investment, ENISA, 2012 - http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment
12. Mutual Aid for Resilient Infrastructures in Europe (MARIE): Phase II recommendations report, ENISA, 2013 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/mutual-aid-assistance/m-a-r-i-e-phase-ii-recommendations-report/at_download/fullReport

13. Mutual Aid for Resilient Infrastructures in Europe, ENISA, 2011 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/mutual-aid-assistance
14. National Cyber Security Strategies; Practical Guide on Development and Execution, ENISA, 2012 - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport
15. National/governmental CERTs; ENISA's recommendations on baseline capabilities, ENISA, 2014 - https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/national-governmental-certs-enisas-recommendations-on-baseline-capabilities/at_download/fullReport
16. Position Paper of the EP3R Task Forces on Incident Management and Mutual Aid Strategies, ENISA, 2013 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/tf-masim/at_download/fullReport
17. Report on Cyber Crisis Cooperation and Management, ENISA, 2014 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study/at_download/fullReport
18. Report on Cyber Crisis Cooperation and Management - Common practices of EU-level crisis management and applicability to cyber crises, ENISA 2015 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/eu-level-crisis-man-study
19. Report on the 2nd ENISA Cyber Crisis Cooperation conference, ENISA, 2013 - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference/report/at_download/fullReport
20. Standard Operational Procedures to manage multinational cyber-crises finalised by EU, EFTA Member States and ENISA, ENISA, 2014 - http://www.enisa.europa.eu/media/press-releases/standard-operational-procedures-to-manage-multinational-cyber-crises-finalised-by-eu-efta-member-states-and-enisa
21. Cyber Europe 2012 – Evaluation Report, ENISA, 2012 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2010/ce2010report/at_download/fullReport
22. Cyber Europe 2012 – Key Findings Report, ENISA, 2012 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report
23. ENISA CE2014, After Action Report, ENISA, 2015 - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/ce2014-after-action-report/at_download/fullReport

Annex B: Acronyms

CERT – Computer Emergency Response Team

CIIP – Critical Information Infrastructure Protection

CIRT – Computer Incident Response Team

CNI – Critical National Infrastructure

CSIRT – Computer Security Incident Response Team

DDoS – Distributed Denial of Service

EGC – European Government CERTs group

ENISA – European Network and Information Security Agency

FIRST – Forum of Incident Response and Security Teams

ICT – Information and communications technology

IPCR – Integrated Political Crisis Response

IR – Incident Response

IRT – Incident Response Team

ISAC – Information Sharing and Analysis Centre

MARIE – Mutual Aid for Resilient Infrastructures in Europe

NCSC – National Cyber Security Centre

NIS – Network and Information Security

PGP - Pretty Good Privacy

PPP – public-private partnership

R&D – Research and development

RIPE – Regional Internet Registry

SERT – Security Emergency Response Team

SIEM – Security Information and Event Management

SLA – service level agreement

SOP – Standard Operational Procedure

TERENA – Trans-European Research and Education Networking Association (GÉANT as of 1 May 2015)

TF-CSIRT – Task-Force of Computer Security Incident Response Team

TI – Trusted Introducer Service

WG – Working Group

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

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu