BEST PRACTICES FOR CYBER CRISIS MANAGEMENT

FEBRUARY 2024

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the EU agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the EU's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

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

AUTHORS

ENISA

ACKNOWLEDGEMENTS

LEGAL NOTICE

COPYRIGHT NOTICE

For any use or reproduction of photos or other material that is not under the ENISA copyright, permission must be sought directly from the copyright holders.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This study highlights the **complexities behind the notion of cyber crisis** and the degree of **subjectivity** it involves. **The elevation of a large-scale cyber incident into a cyber crisis relies predominantly on a political decision**, and depends largely on the level of risk that EU Member States (MS) are prepared to tolerate (i.e. 'risk appetite').

Differences in interpretation of what constitutes a cyber crisis between MS pose challenges at the EU level. The definition of cyber crisis is important as it directly influences the way the crisis is managed. In the meantime, identifying the **causes, nature and impact** of a cyber crisis can facilitate the assessment of the crisis and its severity, and influence the selection and adoption of appropriate measures for cyber crisis management.

The management of a cyber crisis involves a variety of actors at the **organisational** or **corporate, sectoral, regional, national** and **EU levels.** A cyber crisis is managed at the **strategic, operational** and **technical levels,** with the operational level playing a key role in bridging the gap between the other two, ensuring that information is shared at all levels and enhancing cooperation and coordination between all relevant stakeholders. In addition, cyber crisis management frameworks are **part and parcel of general crisis management frameworks.** As a result, the **EU has a complex ecosystem of cyber security actors, structures** and **mechanisms,** with a 'highly complex and interwoven system of actors, structures and processes operating in the cyber domain', mainly because cyber crises are often transboundary by nature.

While the EU has developed a **crisis management framework specifically dedicated to the management of cyber crises** – including through the Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises (2017) (Blueprint) ([1]), the Cybersecurity Act (2019) ([2]) or the network and information security (NIS) directive (2016) ([3]) – **the NIS 2 directive (NIS2)** ([4]) **has the strongest impact on cyber crisis management at the strategic, operational and technical levels in the EU.** At the operational level, it will consolidate ENISA's support to MS ([5]) in cyber crisis management, introduce new obligations for MS and assert the EU-Cyber Crises Liaison Organisation Network (EU-CyCLONe) as the key player in cyber crisis management. **NIS2 enables a more coordinated approach through greater cooperation between MS and relevant EU institutions, bodies and agencies (EUIBAs).**

In this study, cyber crisis management at the operational level in the EU is analysed around the four phases of the cyber crisis management cycle, namely **prevention, preparedness,**

([1]) European Commission (2017), Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, pp. 36–58), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017H1584&qid=1702033489333.

([2]) European Parliament and Council of the European Union (2019), Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, pp. 15–69), https://eur-lex.europa.eu/eli/reg/2019/881/oj.

([3]) European Parliament and Council of the European Union (2016), Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, pp.1–30), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148.

([4]) European Parliament and Council of EU, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2020, pp. 80–152), https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

([5]) See Chapter 3.4 'Role and obligations of ENISA in cyber crisis management at the operational level in the EU'.

response and recovery, which should be framed by **an all-hazards approach**, given that threats can have many different origins.

The best practices identified show that MS have already introduced some effective cyber crisis management measures at the operational level. These are likely to continue to grow and evolve, as MS implement NIS2 and develop their own responses to the challenges of cyber crisis management.

The identified best practices are shown below.

The prevention phase aims to better prevent and reduce the risk of cyber crises and to minimise their effects should they arise.

- **BP #1.** Adoption of a national definition of 'cyber crisis', taking into account its transboundary dimension.
- **BP #2.** Development of information security standards specific to the national public sector, to be reviewed and updated regularly.
- **BP #3.** Foster national initiatives which promote the creation of prevention programmes such as centralised distributed denial-of-service attack (DDoS) mitigation programmes.

The preparedness phase aims to develop plans to support response operations.

- **BP #4.** Definition of a governance structure, provision of specific capabilities and appointment of a crisis coordinator, whose nomination is mandatory under NIS2, ensuring their department has the necessary operational and technical cyber skills to directly coordinate stakeholders during a cyber crisis.
- **BP #5.** Mapping and gathering information on critical entities and their most critical assets to enable rapid action.
- **BP #6.** Establishing instantaneous, secured communication channels during a crisis.
- **BP #7.** Formalisation of a clear allocation of roles between the parties involved in responding to a cyber crisis in an overall plan.
- **BP #8.** Development of escalation criteria for activating the cyber crisis plan and deploying the relevant cooperation units/groups, taking into account factors such as time, priority, players involved, severity of the attack, etc.
- **BP #9.** Development of a methodology and risk assessment tools to optimise coordination and interoperability in the event of a crisis.
- **BP #10.** Testing of the overall plan for operations in response to cyber crises through a multiannual programme of cyber crisis management exercises and training sessions.
- **BP #11.** Setting up training sessions for current and future staff responsible for cyber crisis management at the operational level.
- **BP #12.** Development of a communication strategy including a clear format for messaging, stakeholders to involve, priority levels and time factor and communication channels to be used.

The response phase aims to stem the cyber crisis and prevent further damage.

- **BP #13.** Encourage the mobilisation of private-sector certified 'trusted providers' to provide technical assistance to victims.
- **BP #14.** Supporting victims' crisis communication, for instance with a unified and transparent message.

The recovery phase aims to enable quick recovery through tailored measures and return to a level of security that is normal or even higher than before the crisis.

- **BP #15.** Develop and implement business resumption plans (BRP) defined in reference frameworks, with regular reviewing and updates, in consultation with relevant stakeholders.
- **BP #16.** Establishment of a unit tasked with gathering feedback, drawing lessons learnt and producing recommendations for reviewing, updating and modifying procedures and infrastructure, and refining the action plan for cyber crisis management.

Based on the analysis and the way forward of the best practices ([6]), EU-CyCLONe could consider the following recommendations.

Recommendation #1. Coordinate working sessions involving all MS to define a list of EU-wide cyber crisis mechanisms to enable a common assessment of incidents and identify the players to be involved depending on the severity of the incident, leading to a model cyber crisis response plan. These cyber crisis management mechanisms could be regularly updated in line with progress made by the MS, particularly in terms of human and technical resources, situational awareness and impact assessment. They should always be part of overarching national crisis management frameworks, considering the transboundary nature of most crises and the potential for spill-over effects impacting many sectors at the same time.

Recommendation #2. Develop simulation exercises at the EU level which test the operational level players and procedures in particular. These exercises, which should involve all three levels (strategic, operational and technical), aim to practice the allocation of tasks, cooperation and fluidity of action of the MS during a cyber crisis. Actors in charge of cyber crisis management must know each other well to trust one another. To ensure continuity, coherence and overall consistency, each exercise could be organised on the basis of the results of the previous one. The exercises would thus test the operational level's ability to coordinate and exchange information, assess the situation, act as the computer security incident response team's (CSIRTs) interpreter with political decision-makers, and manage crisis communication with stakeholders. EU-CyCLONe can play a key role not only in strengthening capacity-building but also developing long-lasting trust among MS.

Recommendation #3. Support MS in the set-up of secure communication platform(s) to exchange with essential entities, including for informal communication, during a cyber crisis. While the platforms selected by MS should obviously be the result of national choices, EU-CyCLONe could help said choices by publishing guidelines, and even comparative analyses, about the messaging systems best suited to cooperate and exchange information in complete confidentiality.

Recommendation #4. Ensure that MS national cyber crisis management authorities, in coordination with the NIS Cooperation Group ([7]), regularly update critical information system (IS) maps of essential entities in their country. To do so, they could encourage essential entities to send regular updates, in particular during IS change or update of projects. Precise maps are essential for cyber crisis management, enabling more effective operational coordination in the event of an incident. They contribute to a rapid reaction in the event of an incident, to qualify the impact, or to prevent the consequences of the defensive actions carried out.

Recommendation #5. Support the organisation of media training sessions for executives of MS national cyber crisis management authorities, so that they can give coherent and clear updates on the progress of the crisis, in any type of media (press, radio, TV, social networks). As each

---

([6]) See Chapter 4 'Cyber crisis management best practices in the EU'.
([7]) According to NIS2 (Article 14.4), the NIS Cooperation Group is responsible for providing strategic guidance to EU-CyCLONe and for exchanging information relating to the identification of essential and important entities.

MS has its own capacity needs, these communication sessions could be organised at national level, with content adapted to the context of the MS concerned. EU crisis communicators could regularly follow awareness-raising sessions on cyber issues, as well as refresher courses.

1. INTRODUCTION

1.1 EU POLICY CONTEXT

EU policy and legislation framing cyber crisis management have evolved significantly in response to a fast-evolving threat landscape, with the EU actively engaged in shaping a comprehensive cyber crisis management framework. The EU has adopted a proactive stance, acknowledging the potential impact of cyber incidents on the internal market, public security, and society across MS. Strengthening European crisis management governance involves fostering effective cooperation amongst operational actors within the EU, including the creation of synergies between national authorities, MS and EU institutions, bodies, agencies. A key policy measure was enacted in 2016 with the NIS directive. Taking account of the many different crisis response mechanisms across EU institutions, the Blueprint attempted to present, for the first time, a possible EU-wide concept to responding to cybersecurity incidents too large for one or two MS or EU institutions to handle. The EU framework further progressed with key legislative texts including the Cybersecurity Act and the NIS2 directive (2022), which supersedes the Blueprint and underlines the critical need for cybersecurity preparedness and effectiveness in addressing the escalating 'number, magnitude, sophistication, frequency, and impact of incidents'. Most recently, the EU established EU-CyCLONe, tasked with enhancing cooperation and coordination between relevant actors, overcoming the gap between the strategic and technical levels, preparing decision-making at the political level and coordinating cyber crisis management, situational assessment and mitigation action measures in case of massive cyber incidents.

1.2 STUDY CONTEXT

In the wake of the adoption of NIS2 in 2022, this study aims to identify tried and tested practices (best practices) in cybersecurity crisis (cyber crisis) management at the operational level in the EU. It provides an understanding of the specifics of cyber crises, a concept which is understood differently in MS, and of the management thereof at the operational level. It provides insights into key actors, capabilities and procedures to prevent, detect, respond to and recover from this type of event.

The EU is in 'an era of permacrisis and polycrisis' ([8]). It has experienced numerous crises over a short amount of time, including the COVID-19 pandemic, the growing impact of climate change and Russia's war of aggression against Ukraine. The unprecedented scale of these crises threatens the functioning of society and requires a 'rapid response despite the great uncertainty regarding their potential evolution and the effectiveness of available countermeasures' ([9]). The EU's role in crisis management has expanded, from facilitating coordination and solidarity between MS to providing rapid, flexible and cross-sectoral responses ([10]). The EU's added value is 'higher in transboundary crises and incidents that can overwhelm the response capabilities of individual MS' ([11]). As recently mentioned by the

---

([8]) European Commission (2023), Commission communication – 2023 Strategic Foresight Report: Sustainability and people's wellbeing at the heart of Europe's Open Strategic Autonomy, COM(2023) 376, 6 July, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023DC0376.

([9]) European Commission (2022), *Strategic crisis management in the EU*, Independent expert report, Scientific Advice Mechanism, Scientific Opinion No 13, 22 November 2022, p. 6, https://allea.org/wp-content/uploads/2022/11/ec_rtd_sam-crisis-management-opinion.pdf.

([10]) Within the framework of the Union Civil Protection Mechanism, the European Commission is responsible for general preparedness actions and for providing analytical reports for the IPCR arrangements under Implementing Decision (EU) 2018/1993, recital 72 of the NIS2 directive.

([11]) Ibid.

Commission's Scientific Advice Mechanism, European crisis management governance still needs strengthening by fostering synergies between EUIBAs and with MS ([12]).

Cybersecurity has become an integral part of European security ([13]). The increasing dependence on information technology and the societies' growing interconnection has increased vulnerability surfaces, in particular to cyber threats. The World Economic Forum considers cross-border cyberattacks as an area where risk mitigation is still in the early stages of development ([14]). ENISA's *Threat Landscape 2022* report shows that cybersecurity attacks have continued to increase, in terms of vectors, number and impact ([15]). Incidents due to human errors should not be underestimated, as they too can lead to major disruption.

Cyber crises can affect the proper functioning of the internal market and public security in several MS or the EU as a whole ([16]). The EU has worked to develop a dedicated crisis management framework, first with the Blueprint ([17]) and with key texts such as NIS, the Cybersecurity Act and NIS2. The objectives of the latter on cyber crisis management include:

- increasing the capabilities and preparedness of MS to respond to cyber crises;
- improving cooperation, including information sharing and coordination between MS and EUIBAs to deal with cyber crises;
- strengthening the EU's capacity to complement MS action in managing cyber crises.

NIS2 requires MS to develop the structures, entities and procedures needed specifically for cyber crisis management. It formalises EU-CyCLONe, launched informally in 2020, to improve cooperation among MS at the operational level, which is understood as the intermediary between the technical level and the strategic level.

ENISA's strengthened role in cyber crisis management in the EU includes the provision of the secretariat for EU-CyCLONe, and support the secure exchange of information as well as provide necessary tools to support cooperation between MS.

1.3 OBJECTIVES OF THE STUDY

This study aims to:

- update ENISA's cyber crisis management knowledge base ([18]);
- clarify the complexities and nuances of the notion of cyber crisis;
- provide an overview of the framework for cyber crisis management at the operational level in the EU, including the identification of key actors, highlighting their role and obligations;
- identify best practices for cyber crisis management at operational level in the EU.

The study is aimed at all cybersecurity stakeholders keen to improve both their understanding of and capabilities and procedures to manage cyber crises at the operational level.

([12]) Ibid.
([13]) European Commission (2020), Joint communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18, 16 December, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.
([14]) World Economic Forum (2022), *The Global Risks Report 2022 (17th Edition)*, p. 7, https://www.weforum.org/publications/global-risks-report-2022/.
([15]) ENISA (2022), *ENISA Threat Landscape 2022*, October 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport.
([16]) European Parliament and Council of the European Union (2022), Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2020, recital 69), https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
([17]) See footnote (1).
([18]) See 'Annex: ENISA's knowledge base'.

1.4 SCOPE OF THE STUDY

This study covers recent evolutions in cyber crisis management at the operational level in the EU. It focuses on the following elements.

- The transposition of NIS2 into national legislation, especially Article 9, which is dedicated to national cyber crisis management frameworks.
- The operational level, the meaning of which may vary among MS. In this study, the operational level is understood as the cornerstone for facilitating coordination and understanding between the strategic and technical levels.
- Best practices and lessons learned from MS, along with key challenges, to adequately prevent, detect, respond to or recover from cyber crises at the operational level. **'Best practices'** will be defined as 'activities that have been shown through research and evaluation to be effective, efficient, sustainable and/or transferable, and to reliably lead to a desired result' ([19]). These best practices have been proven at the national level or within the national cyber crisis management authority.

1.5 METHODOLOGY

This following methodology was used to identify best practices in cyber crisis management at the operational level in the EU.

Task 1: Data collection

- A research plan was elaborated to identify relevant open sources for data collection.
- Deep-dive desk research was conducted to collect data on cyber crisis management in the EU. Sources are available in Section 7 'Sources'.

Task 2: Expert consultation

- An expert consultation was designed to complement open-source information on best practices in cyber crisis management, to gather feedback from EU-CyCLONe members.
- A workshop, including a presentation and discussion of identified best practices for cyber crisis management, and complementary interviews were conducted to enrich the study's conclusions.
- Individual interviews were conducted with a select number of EU-CyCLONe members.

Task 3: Drafting of deliverables

- Data was analysed, conclusions were drawn and drafts of the study were submitted to and reviewed by ENISA in an iterative fashion.
- The final report was submitted to EU-CyCLONe members for review.

([19]) European Commission (n.d.), "What are 'good practices?'", https://ec.europa.eu/migrant-integration/page/what-are-good-practices_en.

2. DEFINITIONS FOR CYBER CRISIS MANAGEMENT AT THE OPERATIONAL LEVEL IN THE EU

This section sets out to define the term 'cyber crisis'. It provides a brief definition of the notion of crisis in general, and the factors that shape a crisis. It examines the difference between a cybersecurity incident, a large-scale incident and a cyber crisis. It then turns to the management of cyber crises, beginning with a brief definition of crisis management, exploring the different levels at which a cyber crisis can be managed. It describes the capabilities and measures needed to manage cyber crises at the operational level in the EU, looking at the all-hazards approach and the four stages of the cyber crisis management cycle.

2.1 DEFINING A CYBER CRISIS

There are several definitions of a **crisis.** According to ISO 22361, a crisis is an 'abnormal or extraordinary event or situation which threatens an organisation or community and requires a strategic, adaptive and timely response in order to preserve its viability and integrity' ([20]). It can also broadly be defined as 'an extraordinary event that differs from the normal and involves serious disturbance or risk for disturbance of vital societal functions' ([21]). A more granular definition of a crisis is 'a serious threat to the basic structures or the fundamental values and norms of a system, which, under time pressure and highly uncertain circumstances, necessitate making vital decisions' ([22]). Defined more comprehensively, a crisis is 'an event that affects many people and large parts of society and threatens fundamental values and functions. Crisis is a condition that cannot be handled with ordinary resources and organisation. A crisis is unexpected, far removed from the ordinary and mundane. Resolving the crisis requires coordinated action from several players/actors' ([23]). **Factors of uncertainty, risk and potential for severe consequences** are essential in qualifying and measuring the severity of a crisis, in addition to time sensitivity and the transboundary element of crises.

The **time sensitivity factor** is important to understand the nature of a crisis. Three types of crisis can be distinguished:

- a **creeping crisis**, or hidden latent crisis, which simmers under the radar of the authorities, before suddenly and unexpectedly erupting;
- an **acute crisis**, which is sudden, unforeseen and can have a massive impact in a very short amount of time;
- a **recurring crisis**, which occurs on a regular basis as part of a cycle.

([20]) Estall, H. (2023), 'ISO 22361:2022 – Crisis Management Guidelines: a closer look', Continuity Central, https://www.continuitycentral.com/index.php/news/business-continuity-news/8182-iso-22361-2022-crisis-management-guidelines-a-closer-look.
([21]) ENISA (2014), *Report on Cyber Crisis Cooperation and Management*, 6 November, p. 26.
([22]) Ibid.
([23]) Ibid.

The time factor is essential for responding to crises appropriately, effectively and quickly. For example, because a creeping crisis occurs over a longer period of time, there is in theory more room for crisis prevention measures. An acute crisis, on the other hand, occurs over a very short period of time, meaning priority should be given to crisis mitigation measures.

Another factor that helps better define a crisis is its transboundary and cross-sectoral impact. A transboundary crisis can be understood as crossing geographical, organisational and/or political borders. ENISA's work for EU-CyCLONe found that a transboundary crisis could simply be characterised by its tendency to escalate rapidly, transform, proliferate across multiple jurisdictions and (national) borders, affecting various sectors, policy areas and critical infrastructures, straining and even exceeding the capacity of national crisis management systems.

Transborder crises can have different scopes and simultaneously affect several territories, jurisdictions and/or sectors, and pose major challenges for decision-makers, who must cooperate beyond their national structures to respond effectively [24]. Because **factors of scope and time sensitivity are not mutually exclusive,** a crisis can be both transboundary and acute, transboundary and creeping, or transboundary and recurrent.

As such, the **notion of a cyber crisis can be complex to define.** This is largely due to the differences among MS in definitions of the thresholds which make a cybersecurity incident a crisis.

A **cybersecurity incident** refers to 'an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems' [25]. To complement this definition, NIS2 specifies that an incident is considered significant when it has 'caused or is capable of causing severe operational disruption of services or financial loss for the entity concerned' and 'has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage' [26].

A cyber incident becomes a **large-scale cybersecurity incident** when it 'causes a level of disruption that exceeds a MS capacity to respond to it or which has a significant impact on at least two MS' [27]. A cyber incident therefore moves to 'large-scale' status if a MS is unable to take mitigating action on its own, or if more than two MS are affected.

A large-scale cybersecurity incident can further escalate into a **cyber crisis.** As explained, the term is subject to varying definitions in MS, depending largely on the severity of the incident according to the MS and the risk appetite. At the EU level, the notion of cyber crisis has often been defined with direct reference to the notion of (large-scale) cyber incident since such a crisis is directly caused by a cybersecurity incident. The **scope, impact** and **frequency** of the cyber event enables the evaluation of its severity, which is essential to escalate to the level of crisis. Ultimately, the transition to crisis status depends largely on a political decision to treat a large-scale cyber security incident as a crisis or not. This contributes to the complexity of defining a cyber crisis.

---

[24] Ansell, C, Boin, A. and Keller, A. (2010), 'Managing transboundary crises: Identifying the building blocks of an effective response system', *Journal of Contingencies and Crisis Management*, Vol. 18, https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-5973.2010.00620.x.

[25] European Parliament and Council of EU, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2020, Article 6(6)), https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
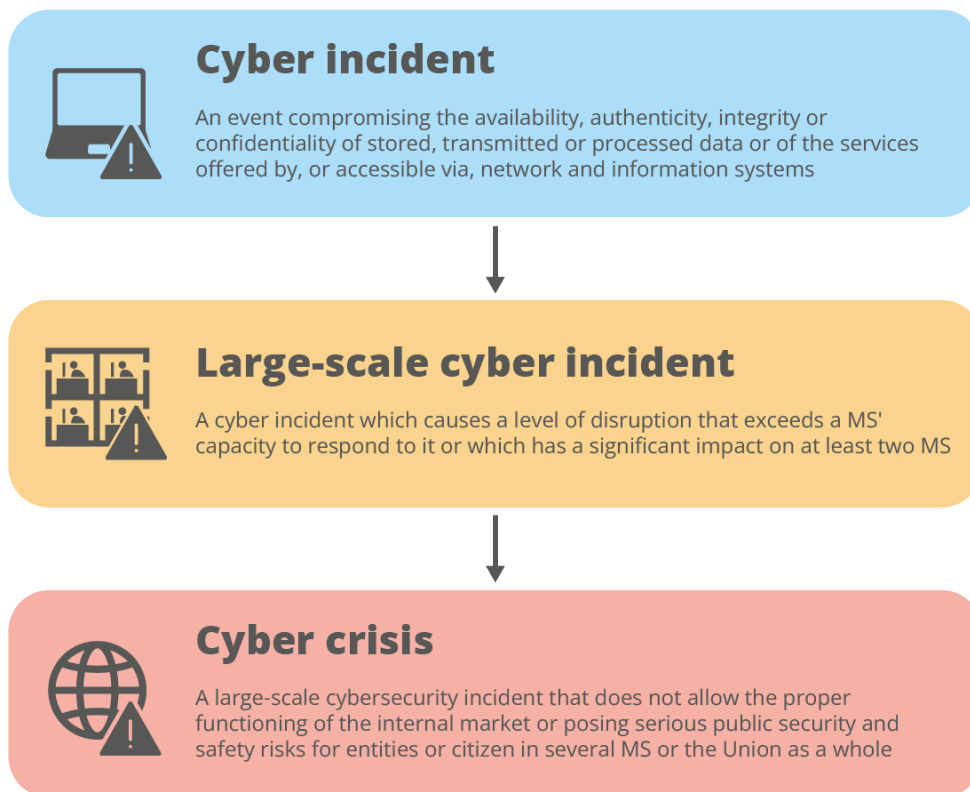
[26] See footnote (25), Article 23.

[27] See footnote (25).

The notion of cyber crisis is based on a number of EU cyber regulations and policies. NIS2 indicates that depending on their cause and impact, a large-scale cybersecurity incident 'may escalate and turn into **fully-fledged crisis** not allowing the proper functioning of the internal market or posing serious public security and safety risks for entities or citizens in several MS or the EU as a whole' ([28]). Previously, the Blueprint (2017) had attempted to give a definition of 'cyber crisis' by differentiating it from a cybersecurity incident, stating that 'a cybersecurity incident [could] be considered a crisis at Union level when the disruption caused by the incident [was] too extensive for a concerned MS to handle on its own or when it [affected] two or more MS with such a wide-ranging impact of technical or political significance that it [required] timely coordination and response at Union political level' ([29]). In addition to this transboundary dimension, a cyber crisis can be characterised by an abnormal and unstable situation that threatens an entity's strategic objectives, its reputation or its viability. The ENISA *Report on Cyber Crisis Cooperation and Management* (2014) further indicates that a cyber crisis is an event that strikes at the heart of an entity and that can have an impact beyond the entity itself ([30]).

Figure 1: Distinguishing between cyber incident, large-scale cyber incident and cyber crisis ([31]) ([32])

Cyber incident

An event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems

Large-scale cyber incident

A cyber incident which causes a level of disruption that exceeds a MS' capacity to respond to it or which has a significant impact on at least two MS

Cyber crisis

A large-scale cybersecurity incident that does not allow the proper functioning of the internal market or posing serious public security and safety risks for entities or citizen in several MS or the Union as a whole

It is thus difficult to find a common definition of the concept of cyber crisis shared by all MS and the EU. Within MS, the escalation from cyber incident to large-scale cyber incident and finally to fully-fledged crisis depends largely on the risk appetite of each MS. Rather than relying on facts alone, declaring a cyber crisis as such at the MS level is above all a political decision linked to

---

([28]) See footnote (13).
([29]) See footnote (14).
([30]) Ibid.
([31]) ENISA (2014), *Report on Cyber Crisis Cooperation and Management*, 6 November, p. 27.
([32]) See footnote (17).

the risk appetite of the MS. The *Report on Cyber Crisis Cooperation and Management* shows that escalation to the status of crisis is largely subjective, with political and organisational perceptions and constraints 'creating' the crisis. Here, crisis exists as an interpretation of the situation rather than as an absolute truth. As a result, what one actor perceives as a crisis may be perceived as daily routine by another, giving a degree of subjectivity to the escalation to crisis status [33]. The escalation to crisis status depends on a MS' risk appetite; beyond a certain threshold of tolerance, the incident can no longer be managed with the usual means: **it is then declared, and thus becomes, a crisis.** Meanwhile, at the EU level, all MS must agree to move to crisis level based on agreed standard operating procedures (SOPs).

A cyber crisis and its severity can be assessed by looking at different factors which include the **causes, nature** and **impact.** Such an assessment is essential, as it should lead to the adoption of appropriate cyber crisis management measures.

The **causes of a cyber crisis** can be multiple and both physical and non-physical. Non-physical causes include targeted action by malicious actors, such as a cyberattack, which may escalate into a crisis. Human errors, malfunctions and malicious actions can also disrupt the functioning of networks and IS and result in a cyber crisis. Causes can also be found in the physical environment [34]. As highlighted by NIS2, theft, fire, flood, telecommunications or power failure, unauthorised physical access or damage can all compromise the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed or services offered by or accessible through networks and IS [35]. Consequently, the **hybrid nature** of the cyber domain poses particular challenges to determining the origins of a cyber crisis, as it combines a 'mixture of conventional and unconventional, military and non-military, overt and covert actions that can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare' [36]. This hybrid nature can act as a brake to the escalation of a cyber incident into a crisis, due to the potentially political connotations of the term and the difficulty of assessing both the physical and non-physical origins of the crisis.

A **cyber crisis can be considered as transborder.** Cyberspace is made up of physical assets scattered across different countries, but which remain (inter)dependent [37]. It knows no geographical boundaries, meaning that a cyber crisis has a serious potential to spread across several entities, jurisdictions or territories. In addition, every sector now has a cyber element, which can lead to a cyber crisis spreading beyond a specific sector. For example, a cyber crisis originating in the energy sector could very well affect the transport sector via its IS. ENISA's work for EU-CyCLONe found that **EU cyber crises could be considered as potentially transborder by definition, as they transcend traditional political, functional and sectoral boundaries within and between MS** [38] [39].

The **impact** of a cyber incident is a determining factor in the escalation to a large-scale cybersecurity incident or a crisis. Impact can be defined by the number of entities affected, whether a number of individuals, companies/organisations, sectors or MS. The type of

---

WannaCry, the first ever case of cyber cooperation at the EU level, a creeping crisis?

In May 2017, the WannaCry ransomware rapidly spread to more than 230 000 computers in 150 countries, encrypting files on the hard drives of Windows systems, preventing users from accessing them and demanding a ransom to decrypt the files. It was a cross-sector propagation that affected several users in several countries, impacting thousands of operating systems [35].

WannaCry was considered a large-scale cyber security incident and was not elevated to the status of a crisis. At the time, only the technical level of cyber crisis management was in place.

WannaCry could be considered a large-scale **creeping cybersecurity incident** because the cyberthreat was hidden in plain sight, evolving gradually over time on computers around the world in a non-linear pattern [39].

---

[33] ENISA(2014), *Report on Cyber Crisis Cooperation and Management*, 6 November.

[34] Physical damage can have repercussions in the virtual world: for example, a flood or fire can disrupt servers, causing a cyber incident that can turn into a crisis. One such example of a cyber incident caused by physical damage occurred in France in March 2021, when a fire broke out in a data centre, causing major disruptions on the servers.

[35] See footnote 13, recital 79.

[36] European Commission (2016), 'FAQ: Joint Framework on countering hybrid threats', April 2016, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_1250.

[37] ENISA (2018), *Good practices on interdependencies between OES and DSPs (November 2018)*, p. 8, https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps.

[38] See footnote (37).

[39] Prevezianou, M.F. (2021), 'WannaCry as a Creeping Crisis', in Boin, A., Ekengren, M. and Rhinard, M. (eds), *Understanding the Creeping Crisis*, Palgrave Macmillan, Cham, pp. 37–50, https://doi.org/10.1007/978-3-030-70692-0_3.

entities affected and whether they operate services considered vital to the functioning of the nation is crucial. Particular attention is therefore paid to services and activities defined by NIS2 as **essential** (energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, ICT service management, public administration and space) and **important** (postal and courier services, waste management, manufacturing, chemicals, production, food, manufacturing, digital suppliers and research) ([40]). If these services are affected, the incident is likely to reach crisis level, given the potential to disrupt vital services.

There are therefore different types of cyber crisis, with different degrees of complexity. This diversity, together with the varying capabilities of each MS to combat cyber crises, influences their classification of a cyber incident as a crisis. The lack of common indicators for defining a 'cyber crisis' at the EU level makes it both complex and sensitive to escalate a large-scale cybersecurity incident into a full-fledged crisis.

2.2 DEFINING CYBER CRISIS MANAGEMENT

This study builds on previous work by ENISA, which defines crisis management as 'an institutional and organisational design process' ([41]), a '[broad] structure [that] encompasses decision-makers [with specific roles and actions]' ([42]). In general terms, crisis management is understood as 'making and effecting difficult decisions under difficult circumstances' ([43]).

The EU's crisis management competences have grown significantly in sectors such as civil protection, terrorism, health, the environment, critical infrastructures and cybercrime ([44]). While **national security remains the prerogative of MS, the EU plays a growing role** in coordinating and improving cooperation between MS in the event of a crisis. The EU has developed the capacity to support MS overwhelmed by a disaster or crisis, to manage transboundary crises and to provide assistance in the event of a crisis outside the EU ([45]). **Crisis management at the EU level involves a highly complex and interwoven system of actors, structures and processes operating at many levels.**

Cyber crisis management is part of a wider crisis management framework. While some consider that every type of existing crisis has a cyber element, others argue that cyber crisis management should be seen as a stand-alone practice. **These approaches are not mutually exclusive and could even be more effective when combined.** Cyber crisis management can be understood as the management of a crisis which has a cyber origin or a significant cyber component.

At the EU level, both approaches exist for cyber crisis management. Cyber crisis management in the EU is handled by different EU institutions and agencies, depending on the type of crisis encountered. The EU's high-level (or generic) crisis management mechanisms can be used and applied in the context of cyber crises specifically, but are not limited to them. This is the case, for example, of the Council's Integrated Policy Response Capability (IPCR) Mechanism, the European Commission's ARGUS system or the European External Action Service's (EEAS) Crisis Response Mechanism (CRM) ([46]) ([47]). **Overall, the cross-sectoral nature of crises means that multiple actors from different sectors must cooperate and**

([40]) See footnote (13), Article 16.
([41]) ENISA (2014), *Report on Cyber Crisis Cooperation and Management*, 6 November.
([42]) Ibid.
([43]) Ibid.
([44]) SAPEA (2022), *Strategic crisis management in the European Union*, Evidence Review Report No11, https://allea.org/wp-content/uploads/2022/11/crisis-management-report.pdf.
([45]) Ibid.
([46]) Ibid.
([47]) See Chapter 3.1 'Overview of the structure of cyber security crisis management at the operational level in the EU'.

share information, and the transboundary nature of cyber crises is a perfect illustration ([48]).

The EU has long been working on a **specific legislative framework for cyber crisis management.** The aim is for MS to comply with minimum requirements for cybersecurity resilience, which includes improving cyber crisis management capabilities. Three major pieces of legislation have structured the development of cybersecurity crisis management, namely NIS, the Cybersecurity Act and, most recently, NIS2 ([49]). In particular, NIS2 introduces new rules to improve the way the EU prevents, manages and responds to large-scale cyber security incidents and crises by establishing clear responsibilities, proper planning and better cooperation within the EU ([50]). **However, even with the development of measures specifically designed for cyber crisis management, the latter remains embedded in the policies and plans of broader crisis management structures, both at the national and EU levels.**

The management of a cyber crisis involves **public and private stakeholders** from the **civilian, law enforcement** and **defence sectors, depending on the nature and impact of the cyber crisis.** These actors operate at different levels.

- **Organisational and corporate level.** Critical entities affected by a cyber crisis are key players in managing cyber crises. Their cooperation and information are essential to ensure that situational awareness is shared in a timely manner and that mitigation measures are properly implemented. They also play a crucial role in crisis prevention, for example by communicating the mapping of their ISs to the national authorities responsible for crisis management, and must be supported to increase their resilience to cyber crises.
- **Sectoral level.** Crisis management can also follow a sectoral approach, incorporating a cyber element for each sector considered critical. This can be envisaged for better coordination and cooperation between actors, providing a cyber crisis management plan tailored to each sector. In this case, NIS2 can serve as a basis since it defines the entities in the sectors considered 'essential' and 'important' ([51]) because they provide vital services to the nation.
- **Regional level.** Within MS, regional authorities can be involved in managing cyber crises, among others, because of their proximity to the entities affected in the event of a crisis.
- **National level.** MS have primary responsibility for cybersecurity, for crisis management, and for the management of cyber crises. Consequently, MS must take the necessary measures to ensure the protection of essential national security interests and to safeguard public order and public security ([52]). While cyber crisis management can be a politically sensitive issue and remains a national competence, MS often choose to work together through coordination mechanisms and networks, with varying degrees of formalisation ([53]). NIS2 now requires MS to draw up a cyber crisis management plan and set up national crisis management authorities.
- **EU level.** NIS2's definition of a cyber crisis implies that the affected MS is either unable to respond to the situation alone, or that the crisis affects at least one other MS. The EU plays an essential role in preventing and mitigating cyber crises, in particular by establishing common benchmarks which contribute to raising the European level of resilience to cyber crises and by strengthening MS crisis management capabilities and improving collective situational awareness ([54]).

([48]) ENISA(2014), _Report on Cyber Crisis Cooperation and Management_, 6 November.
([49]) The Blueprint (2017) was also a key policy initiative that helped refine the definition of a cyber crisis, although it is now outdated.
([50]) European Commission (n.d.), 'Directive on measures for a high common level of cybersecurity across the Union (NIS2 directive) – FAQs', https://digital-strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs.
([51]) Essential entities include the energy, transport, finance, banking, health, drinking water, waste water, digital infrastructure, ICT service management, public administration and space sectors. Important entities include postal and courier services, waste management, manufacturing, chemicals, production, food, manufacturing, digital suppliers and research. (NIS2 directive).
([52]) See footnote (13), recital 9.
([53]) Ibid.
([54]) European Commission, 'FAQ: Joint Framework on countering hybrid threats', April 2016.

- **International level.** Cyber crises can go beyond the borders of MS and involve non-EU countries, requiring international intervention to resolve the situation. Bilateral agreements can be concluded between MS and non-EU countries directly, or between the EU and non-EU countries or other regional organisations worldwide. The cyber diplomacy toolbox, for example, was created to provide 'an appropriate framework for a common EU diplomatic response to malicious cyber activities in order to mitigate and/or deter potential cyber attackers from harming the political, security and economic interests of the European Union' ([55]), beyond the EU's borders.

Different actors from different sectors and levels can be involved in the management of cyber crises. **This study focuses specifically on the EU level.**

In the event of a cyber crisis, MS and the relevant EUIBAs must cooperate 'to properly coordinate the response across the EU' ([56]) at three different levels: the strategic, operational and technical levels ([57]).

- The **strategic level** is responsible for the strategic and political management of both the cyber and non-cyber aspects of a crisis. Actors include MS ministers responsible for cybersecurity, the European Council and its President, the Presidency of the Council of the European Union and the Council of the European Union, the European Commission, including the President or the delegated Vice-President/Commissioner and the EEAS, including the High Representative of the Union for Foreign Affairs and Security Policy ([58]).
- **The operational level focuses on preparing decision-making at the strategic level, coordinating cyber crisis management, and situational awareness, impact assessment and mitigation measures.** It should be noted that the definition of the 'operational' level may vary from one MS to another, in some cases corresponding to the technical level. In this publication, the operational level is defined as the **cornerstone for strengthening cooperation between the various MS and EU institutions,** and for **facilitating coordination between the strategic and technical levels. EU-CyCLONe** was established precisely to fill this gap ([59]).
- The **technical level** involves incident handling during a cyber crisis and incident monitoring and surveillance, including continuous analysis of threats and risks. Actors include the CSIRTs Network, national CSIRTs, the European Commission, EEAS, the Computer Emergency Response Team for the EU institutions, bodies and agencies, ENISA and the European Cybercrime Centre of the European Union Agency for Law Enforcement Cooperation ([60]).

([55]) De Thomas Colatin, S. (2020), 'Si vis cyber pacem, para sanctiones: the EU Cyber Diplomacy Toolbox in action', CCDCOE, https://ccdcoe.org/library/publications/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacy-toolbox-in-action/.
([56]) See footnote (13), recital 69.
([57]) ENISA (2016), *Strategies for incident response and cyber crisis cooperation*, 25 August.
([58]) See footnote (1).
([59]) See footnote 13, Articles 9 and 16.
([60]) Ibid.

Table 1: Strategic, operational and technical levels of cyber crisis management [61] [62]

	Actors	Responsibilities
Strategic level	• MS ministers responsible for cybersecurity • President of the European Council • Presidency of the Council • President or the delegated Vice-President/Commissioner of the European Commission • High Representative of the Union for Foreign Affairs and Security Policy	• Strategic and political management of both the cyber and non-cyber aspects of the crisis
Operational level	• EU-CyCLONe	• Ensure enhanced cooperation and coordination • Bridge the gap between the strategic and technical levels • Prepare decision-making at the political level • Coordinate cyber crisis management, situational assessment and mitigation action measures
Technical level	• CSIRTs Network [63]	• Incident handling during the cyber crisis • Incident monitoring and surveillance, including continuous analysis of threats and risks

Managing a cyber crisis involves a significant number of actors. As ENISA's 2016 *Strategies for incident response and cyber crisis cooperation* report points out, **'the key in effective cyber crisis coordination is the shared responsibility and comprehensive approach among the stakeholders'** [64]. In the EU, the question of who is responsible largely depends on the level(s) at which the cyber crisis occurs. This study however focuses on the **operational level,** as do the best practices identified in the next chapter.

A variety of capabilities and measures can be put in place to manage cyber crises. These **need to be organised in a comprehensive way** to ensure successful cyber crisis management. Indeed, in the cyber domain, crisis management involves 'capabilities to adequately prevent,

---

[61] See footnote (13).
[62] ENISA (2014), *Report on Cyber Crisis Cooperation and Management*, 6 November.
[63] CSIRTs Network (n.d.), official website, https://csirtsnetwork.eu/.
[64] ENISA (2016), *Strategies for incident response and cyber crisis cooperation*, 25 August.

detect, respond to, recover from or mitigate the impact of incidents' ([65]). Since threats can have different origins, management measures should be based on an **all-hazards approach.** This approach aims 'to protect networks, ISs and the physical environment of those systems from events such as theft, fire, flood, telecommunication or power failures, or unauthorised physical access and damage which could compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems' ([66]). The all-hazards approach offers a comprehensive approach to cyber crisis management, taking into account the multiple potential causes of cyber crises, which can originate in both the physical and non-physical worlds.

Taking into account the origins of cyber crises is important to shaping the adequate response, but it is equally important to integrate certain key steps in the development of an effective and coherent cyber crisis management strategy. The ENISA *Report on Cyber Crisis Management and Cooperation* (2014) highlights five key tasks to conduct crisis management in order to resolve any kind of crisis situation. These tasks overlap and flow into each other and include:

- **sense-making,** which involves finding out what is happening and why;
- **meaning-making,** which involves conveying an understanding of the situation to others so that they understand why it is a crisis and why certain actions must be taken;
- **decision-making,** which involves taking action to resolve the situation using available resources, taking into account logistical, time, legal and democratic constraints, ensuring that the objectives of resolving the crisis are achieved at all levels, from strategic to operational and technical;
- **termination,** with decision-makers deciding that the crisis is over and that the crisis management organisation can be dissolved; the situation at this point may not have completely returned to normal, but what remains can be managed using non-crisis measures;
- **learning and reform,** with investigations and potential changes in policies and practices, a crucial step which offers an opportunity to improve and correct the flaws in the system revealed by the crisis.

These **five tasks form the basis for the management of any type of crisis,** as they enable crucial questions to be tackled by authorities responsible for crisis management. Each task brings its own challenges for the organisation of crisis management and can be used to guide the design of crisis management operations ([67]). With regards to cyber crisis management specifically, the ENISA *Report on Cyber Crisis Management and Cooperation* (2014) proposes using the challenges associated with the five tasks as an analytical roadmap to guide the development of cyber crisis management operations ([68]). These challenges are summarised in Figure 2.
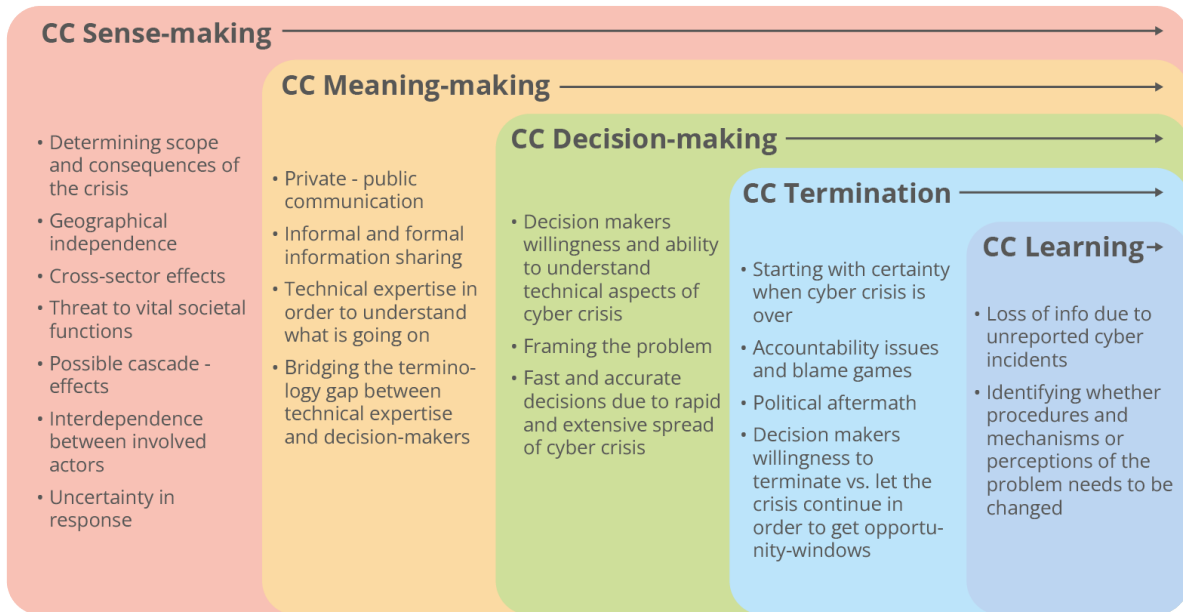

([65]) See footnote (13), recital 120.
([66]) Ibid, recital 79.
([67]) ENISA (2014), *Report on Cyber Crisis Cooperation and Management*, 6 November.
([68]) Ibid.

Figure 2: Cyber crisis management challenges (⁶⁹)

CC Sense-making

- Determining scope and consequences of the crisis
- Geographical independence
- Cross-sector effects
- Threat to vital societal functions
- Possible cascade - effects
- Interdependence between involved actors
- Uncertainty in response

CC Meaning-making

- Private - public communication
- Informal and formal information sharing
- Technical expertise in order to understand what is going on
- Bridging the termino-logy gap between technical expertise and decision-makers

CC Decision-making

- Decision makers willingness and ability to understand technical aspects of cyber crisis
- Framing the problem
- Fast and accurate decisions due to rapid and extensive spread of cyber crisis

CC Termination

- Starting with certainty when cyber crisis is over
- Accountability issues and blame games
- Political aftermath
- Decision makers willingness to terminate vs. let the crisis continue in order to get opportu-nity-windows

CC Learning→

- Loss of info due to unreported cyber incidents
- Identifying whether procedures and mechanisms or perceptions of the problem needs to be changed

These challenges should be taken into consideration when designing comprehensive cyber crisis management measures. The tasks and challenges can then be used to develop and improve best practices at each phase of the cyber crisis management cycle, namely **prevention, preparedness, response and recovery** (⁷⁰). All these phases can include several of the tasks depicted in Figure 2 (sense-making, meaning-making, decision-making, termination, learning).

The four phases are detailed below (⁷¹).

- **Phase 1 – Prevention.** This aims to better prevent and reduce the risk of cyber crises occurring and to anticipate and minimise their potential effects should they arise. Preventive measures are taken before a crisis occurs, but also afterwards as they allow lessons to be learned for the management of future crises.
- **Phase 2 – Preparedness.** This aims to improve the management of crises by developing plans to support response operations. This includes activities such as setting up a resilient crisis organisation, maintaining the confidence of the ecosystem, prioritising the critical activities affected or ensuring that responders know how to act by undergoing training and exercises. Preparedness measures are taken before a crisis occurs.
- **Phase 3 – Response.** This aims to stem the cyber crisis and prevent further damage. At the EU level, response is based on effective technical, operational and strategic cooperation between MS and EUIBAs. An effective and safe response involves activating predetermined measures. These measures are taken during crises.
- **Phase 4 – Recovery.** This aims to enable quick recovery by taking measures when a crisis is over or its end is in sight to return to a level of security and activity that is normal or even higher than before the crisis. This phase covers restoration of affected systems and arrangements or organising lessons learned to better prevent, respond to and mitigate future crises. Such measures are taken after crises occur.

(⁶⁹) ENISA (2014), *Report on Cyber Crisis Cooperation and Management*, 6 November.
(⁷⁰) See Chapter 4 'Cyber crisis management best practices at operational level in the EU' for more information.
(⁷¹) Ibid.

These four phases should always be taken into account for effective management of cyber crises, along with the all-hazard approach, to provide a comprehensive approach to cyber crisis management.

Key takeaways

- The **notion of a cyber crisis is complex**, not least because it leaves room for a degree of subjectivity: a cyber incident may be considered as a crisis in one MS but not necessarily in another. While a given MS may be unable to respond to the situation and therefore require the activation of exceptional measures, another may well have the capacity to manage the incident without having to elevate it to crisis status. Risk assessment is therefore inextricably linked to the notion of cyber crisis and depends largely on the level of risk that each MS is prepared to tolerate.

- At the EU level, this brings about numerous challenges. The **development of clear indicators or decision mechanisms** for escalation to crisis status at the EU level, taking into consideration both national capabilities and priorities, could help alleviate some of those challenges.

- The **causes**, **nature** and **impact** of a cyber crisis can support the assessment of the crisis and its severity and influence the selection and adoption of appropriate measures for cyber crisis management.

- With NIS2, MS have to develop **a specific framework for cyber crisis management.** However, because cyber crises tend to have a transboundary nature, any cyber crisis management framework must remain part of overarching crisis management for overall coherence.

- The management of a cyber crisis involves a variety of actors at the **organisation/company, sectoral, regional, national** and **EU levels.** It is managed at the **strategic, operational** and **technical levels,** with the **operational level playing a key role** in bridging the gap between the other two levels, ensuring information is shared across all levels, greater cooperation and coordination between all relevant stakeholders.

- Cyber crisis management should take into account the **four phases of the cyber crisis management cycle**, i.e. **prevention, preparedness, response and recovery.** These four phases should be framed by an **all-hazard approach,** since threats can have many different origins.

3. STRUCTURE AND ACTORS OF CYBER CRISIS MANAGEMENT AT THE OPERATIONAL LEVEL IN THE EU

This section gives an overview of the EU's complex cybersecurity ecosystem of actors, structures and mechanisms. It first outlines the structure of cyber crisis management at the operational level in the EU, then describes the roles and obligations of the main EU actors in cyber crisis management at the operational level, namely ENISA, MS and EU-CyCLONe.

3.1 OVERVIEW OF THE STRUCTURE OF CYBER CRISIS MANAGEMENT AT THE OPERATIONAL LEVEL IN THE EU

Due to the transboundary nature of cyber crises, a vast network of public actors participates in their management across the EU, leading to a highly complex and overlapping system of actors, structures and processes operating within the cyber domain. In this context, NIS2 aims to bring about a more coordinated approach through greater cooperation between MS and relevant EUIBAs at the technical, operational and strategic levels ([72]).

Several EUIBAs are involved in cyber crisis management at all levels. These include the European Commission and the EEAS, whose work is mainly at the strategic level. The Computer Emergency Response Team for the EU institutions (CERT-EU), bodies and agencies is a CSIRTs Network member and is responsible for EUIBAs. The European Union Agency for Law Enforcement Cooperation is responsible for the fight against cybercrime through its European Cybercrime Centre, through the Law Enforcement Emergency Response Protocol and within the Joint Cyberspace Action Task Force.

EU organisations responsible specifically for cyber crisis management at the strategic, operational, technical levels include, for instance:

- at the strategic level, the Horizontal Working Party on Cyber Issues or the Committee of Permanent Representatives;
- at the operational level, EU-CyCLONe ([73]);
- at the technical level, the CSIRTs Network.

A lot has changed for cyber crisis management in the EU since ENISA's report on EU common crisis management practices and their applicability to cyber crises (2015). At the time, the EU did not yet have its own legislative and operational framework dedicated to cyber crisis management. Instead, it relied on **several crisis management mechanisms,** which follow the guiding principle of complementarity and continue to apply today to cyber crises.

([72]) See footnote (13), recital 69.
([73]) See Chapter 3.4 'Role and obligations of the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) in cyber crisis management at the operational level in the EU'.

- The **Council's IPCR,** to coordinate the policy response to cross-sectoral crises and cyber crises. It can be activated by institutional cybersecurity actors in the event of an EU-wide crisis with a cybersecurity dimension.
- The **European Commission's ARGUS system,** an internal early warning communication system which provides a specific coordination process that can be activated in the event of a multi-sector crisis.
- The **EEAS CRM,** to provide a coordinated and synergistic response to crises and emergencies of an external nature or with an external dimension. It can be activated if a cyber crisis has a Common Foreign and Security Policy or Common Defence Policy dimension, for example impacting EU or MS national security interests.

The EU has since worked to develop an appropriate crisis management framework specifically for cybersecurity. While continuing to build on broader existing crisis management frameworks and integrate new initiatives, the EU now has **specific cybersecurity legislation.** This includes the **Cybersecurity Act** and the **NIS directives,** which shaped European cybersecurity by introducing obligations and relevant sanctions, introducing mechanisms to better manage cyber crises in the EU and strengthening ENISA's role and capabilities in this field.

3.2 ROLE AND OBLIGATIONS OF ENISA IN CYBER CRISIS MANAGEMENT AT THE OPERATIONAL LEVEL IN THE EU

The Cybersecurity Act and NIS2 have significantly strengthened ENISA's mandate. One of the agency's strategic objectives, reaffirmed by the Agency Single Programming Document 2023–2025, is to enable effective cooperation amongst operational actors within the EU in case of large-scale cyber incidents, in particular **by developing tools and methodologies for effective cyber crisis management** [74]. Among other things, ENISA serves as an information hub, enabling all actors involved at the EU level to collaborate and respond to large-scale cyber incidents and crises by [75]:

- enhancing and improving incident response capabilities and readiness across the EU through the CSIRT Network;
- enabling effective European cybersecurity crisis management at the operational level via EU-CyCLONe [76];
- ensuring coordination in cybersecurity crisis management among relevant EUIBAs;
- improving the maturity and capabilities of operational communities (CSIRT Network, EU-CyCLONe and EUIBAs) including cooperation with law enforcement authorities;
- contributing to preparedness, sharing situational awareness, coordinating response and recovery from large-scale cyber incidents and crises in different communities;
- supporting the evolution of an EU joint response by enabling the deployment of EU-level proposals.

NIS2 provides ENISA with new tasks, including [77]:

- developing and maintaining a European vulnerability registry;
- providing the Secretariat of EU-CyCLONE;
- publishing an annual report on the state of cybersecurity in the EU;
- supporting the organisation of peer reviews between MS;

---

[74] ENISA (2023), *ENISA Single Programming Document 2023–2025,* p. 22, https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-report-2023-2025.

[75] ENISA (n.d.), 'Cyber Crisis Management', https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-report-2023-2025.

[76] See Chapter 3.4 'Role and obligations of the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) in cyber crisis management at the operational level in the EU'.

[77] ENISA (2016), 'NIS directive', https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new.

- creating and maintaining a registry for entities providing cross-border services (DNS service providers, TLD name registries, entities providing domain name registration services, cloud computing service providers and data centre providers).

NIS2 makes ENISA responsible for supporting the coordination of cyber crises in the EU by advising and assisting EU-CyCLONe, which supports the coordinated management of large-scale cybersecurity incidents and crises at the operational level [78]. The agency provides EU-CyCLONe with a secretariat, but also with the infrastructure and tools necessary to ensure effective cooperation among MS [79]. ENISA therefore contributes to improved sharing of situational awareness at the operational level across the EU, thereby enhancing the management of large-scale cyber incidents and crises in the EU.

Finally, **ENISA plays a key role in implementing the NIS directives** by providing assistance to the MS on its transposition, for instance with Article 9 of NIS2 on national cyber crisis management frameworks, and by organising exercises.

3.3 ROLE AND OBLIGATIONS OF MS AND COOPERATION MECHANISMS FOR CYBER CRISIS MANAGEMENT AT THE OPERATIONAL LEVEL IN THE EU

MS cyber crisis management procedures are integrated into their own general national crisis management frameworks [80]. **A variety of actors are therefore in charge of cyber crisis management at the operational level within MS.** They are responsible for liaising between the strategic level, often represented by the national crisis management structure, and the technical level, embodied by the appointed CSIRTs Network member [81].

These actors include **'National cybersecurity authorities'** (the exact terminology varies from one MS to another), which tend to be the government agency responsible for cybersecurity, and to be in the lead for national cybersecurity efforts at the technical, operational and sometimes strategic levels. These authorities are represented in EU-CyCLONe in cyber crisis management at the operational level in the EU by **EU-CyCLONe Executives,** i.e. heads of national cybersecurity authorities and **EU-CyCLONe Officers,** i.e. experts in crisis management and/or international relations supporting the decision-makers, prior to and during large-scale incident or crisis situations [82].

The majority of MS rely on a comprehensive national crisis management structure which can be deployed regardless of the origin or nature of the crisis, including cyber. A few MS have developed specific frameworks and structures for cyber crisis management. A high degree of centralisation of cyber crisis management is beneficial in terms of speed and efficiency of decision-making and access to information, but can exclude important stakeholders and overburden certain institutions. Conversely, a decentralised approach is likely to offer flexibility and the ability to adapt to changing needs, but has the disadvantage of hampering government-wide coordination efforts [83].

Much of the current work to improve the management of cyber crises at the EU level has focused on helping MS to **build up their capabilities** in this area, preventing crises and preparing MS to deal with them should they arise. **NIS2 impacts the organisation of cyber**

---

[78] See Chapter 3.4 'Role and obligations of the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) in cyber crisis management at the operational level in the EU'.
[79] See footnote (77).
[80] See footnote (77).
[81] CSIRTs Network (n.d.), official website, https://csirtsnetwork.eu/.
[82] ENISA (2021), 'EU Member States test rapid Cyber Crisis Management', press release, 19 May, https://www.enisa.europa.eu/news/enisa-news/eu-member-states-test-rapid-cyber-crisis-management.
[83] Ibid.

crisis management within MS, as it dictates the development of National cyber crisis management frameworks.

In this respect, **Article 9 of NIS2** extends the obligations of MS in the management of cyber crises. By 2024, MS will have to ([84]):

- designate or establish one or more cyber crisis management authorities competent for the management of large-scale cybersecurity and crises;
- equip such cyber crisis management authorities with the appropriate resources to carry out their mission in line with general national framework for crisis management;
- identify capabilities, assets and procedures to be deployed in case of a crisis;
- adopt a national large-scale cybersecurity incident and crisis response plan highlighting objectives and arrangements for the management of large-scale cybersecurity incidents and crises, including:
    - objectives of national preparedness measures and activities,
    - tasks and responsibilities of cyber crisis management authorities,
    - cyber crisis management procedures, how they integrate into general national crisis management frameworks and channels for information exchange,
    - national preparedness measures (including exercises and training programmes),
    - national procedures and agreements between the competent national authorities and bodies to ensure the effective participation and support of MS in the coordinated management of large-scale cybersecurity incidents and crises at the EU level.

For cyber crisis management at the operational level, MS have benefited from **EU-CyCLONe** since 2020; this was formalised by NIS2 in January 2023.

3.4 ROLE AND OBLIGATIONS OF THE EUROPEAN CYBER CRISIS LIAISON ORGANISATION NETWORK IN CYBER CRISIS MANAGEMENT AT THE OPERATIONAL LEVEL IN THE EU

EU-CyCLONe acts as the key intermediary between the technical and strategic levels during large-scale cybersecurity incidents and crises. Launched in 2020 and formalised in 2023, it supports decision-making at the strategic level while **improving cooperation** at the operational level through the **regular exchange of information between MS** ([85]).

EU-CyCLONe plays a **central role in the European cyber crisis management landscape,** encompassing **representations from both the MS and EUIBAs.** It is composed of representatives of the cyber crisis management authorities of the MS and the European Commission, and its secretariat is provided by ENISA ([86]). It is chaired by the MS holding the Presidency of the European Union ([87]).

Article 16 of NIS2 defines the tasks of EU-CyCLONE:

- to increase the level of preparedness of the management of large-scale cybersecurity incidents and crises;
- to develop a shared situational awareness for large-scale cybersecurity incidents and crises;
- to assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures;

([84]) See footnote (13).
([85]) ENISA (n.d.), 'EU-CyCLONe', https://www.enisa.europa.eu/topics/incident-response/cyclone.
([86]) Ibid.
([87]) Ibid.

- to coordinate the management of large-scale cybersecurity incidents and crises and support decision-making at political level in relation to such incidents and crises;
- to discuss, upon the request of a MS, national large-scale cybersecurity incident and crisis response plans referred to in Article 9(4) of NIS2.

In short, EU-CyCLONe enables rapid cyber crisis management coordination in case of a large-scale cross-border cybersecurity incidents or crises in the EU by providing timely information sharing and situational awareness among competent authorities. The group supports the cooperation among MS, in particular through the regular exchange of information between and among MS and EUIBAs ([88]).

Key takeaways

- At the EU level, **several EU institutions and EUIBAs** are involved in crisis management **at the strategic, operational and technical levels,** and various **crisis management mechanisms** are available (IPCR, ARGUS, CRM). These actors and mechanisms can be used for the management of cyber crises.

- The EU has a **complex cybersecurity ecosystem of actors, structures and mechanisms.** The transboundary nature of cyber crises means a vast network of public actors participate in crisis management across the EU, leading to a 'highly complex and overlapping system of actors, structures and processes operating within the cyber domain'.

- The EU has developed a **crisis management framework specifically dedicated to the management of cyber crises,** including through the Cybersecurity Act, NIS and particularly NIS2. This framework is part of broader existing crisis management frameworks, which include high-level mechanisms such as IPCR, ARGUS or CRM.

- **NIS2 (2022) aims to bring about a more coordinated approach through greater cooperation** between MS and relevant EU institutions and EUIBAs at all levels.

- With regard to the operational level of cyber crisis management in the EU, NIS2 will have the following impacts:

  - an enhanced role for ENISA in cyber crisis management;
  - new obligations for MS, among which the development of specific cyber crisis management plans and the identification of a cyber crisis management national authority;
  - positioning EU-CyCLONe as a key player for cyber crisis management at the operational level in the EU, supporting cooperation and coordination between actors and facilitating information exchange.

([88]) Ibid.

4. CYBER CRISIS MANAGEMENT BEST PRACTICES AT THE OPERATIONAL LEVEL IN THE EU

This section presents 15 best practices in cyber crisis management at the operational level in the EU. Each of these best practices is in line with the provisions of NIS2, particularly Article 9 'National cyber crisis management frameworks' and Article 16 'European cyber crisis liaison organisation network (EU-CyCLONe)'. These best practices are all established, tested and approved in at least one MS or at the EU level, and have been the subject of public communication. Each best practice contains a concrete example of application by a MS, an analysis of its contribution to cyber crisis management at the operational level in the EU and of the way forward, and is linked to NIS2 objectives. This structure provides food for thought to entities seeking to improve their cyber crisis management practices, including in the framework of the implementation of NIS2.

The management of cyber crises can be broken down into different phases. The Blueprint (2017) breaks down the crisis management lifecycle into four phases: prevention, preparedness, response and recovery ([89]).

Figure 3: Cyber crisis management lifecycle

([89]) See footnote (1).

The operational level of cyber crisis management is central to the first two phases of the cycle, i.e. prevention and preparedness, as it is particularly concerned with threat analysis, situation assessment and mitigation measures. It is directly relevant for the other two phases as the crucial interface between the strategic and technical levels.

For the purposes of this study, **'best practices'** are understood as 'activities that have been shown through research and evaluation to be effective, efficient, sustainable and/or transferable, and to reliably lead to a desired result' ([90]).

4.1 PHASE 1 – PREVENTION

The prevention phase aims to support the EU and its MS to improve the prevention and reduce the risk of cyber crises occurring and anticipate ways to minimise their effects. Preventive measures include reinforcing protection and erecting barriers to prevent malicious actors from attacking an IT system, thereby avoiding a crisis. Preventive measures are taken before a crisis occurs, but also afterwards as a result of lessons learned from past crises.

Table 2: Summary of best practices for Phase 1 – Prevention

Phase 1 – Prevention
BP #1. Adoption of a national definition of 'cyber crisis', taking into account its transboundary dimension
BP #2. Development of information security standards specific to the national public sector, to be reviewed and updated regularly
BP #3. Foster national initiatives which promote the creation of prevention programmes such as centralised DDoS mitigation programmes

Best practice #1: Adoption of a national definition of 'cyber crisis', taking into account its transboundary dimension.

- **Example.** Several MS define a 'cyber crisis' by the major impact on the operations of the organisations affected, the need for prompt decision-making and the ineffectiveness of usual incident handling procedures. The Dutch definition focuses more closely on the geographical dimension. The Netherlands identifies eight basic elements which characterise a cyber crisis in its National Crisis Plan Digital (2022) ([91]). Most of these criteria refer to the transboundary nature of such a crisis: a 'technical failure inside or outside the Netherlands', an 'involvement of a statewide or other actor', 'cross-regional effects' (including physical ones), and 'effect of the crisis abroad'. All these elements suggest an international coordination effort to respond to the cyber crisis.
- **Analysis and way forward.** The definition of 'cyber crisis' varies among MS. Most only consider the consequences on their territory, to the detriment of the cross-border effects. A joint understanding of the transboundary nature of this type of event could contribute to a clearer perception of the issues at stake and the resources to be put in place for more efficient management at the EU level. On the basis of NIS2, which points out that a cyber crisis could pose 'serious public security and safety risks for entities or citizens in several MS', the homogenisation of national definitions highlighting the potentially foreign origin and/or consequences would facilitate better European coordination and cooperation. Such

([90]) European Commission (n.d.), 'What are good practices?', https://ec.europa.eu/migrant-integration/page/what-are-good-practices_en.

([91]) National Coordinator for Counterterrorism and Security (2022), *Landelijk Crisisplan Digitaal* (National Crisis Plan Digital), Ministry of Justice and Security, 23 December, pp. 10–11, https://www.nctv.nl/documenten/publicaties/2022/12/23/landelijk-crisisplan-digitaal.

a definition could also include a list of detailed indicators or decision-making mechanisms that would serve as a roadmap on how to operate in a state of crisis. In this respect, EU-CyCLONe could be used to gather input from MS to formulate such a list. However, such a definition should avoid imposing a one-size-fits-all solution and instead take into account the varying capabilities and priorities of MS. EU-CyCLONe could work on developing a sort of 'cybersecurity dictionary', gathering MS' definitions and their equivalents in each jurisdiction, to facilitate mutual understanding ([92]).

- **Matching NIS2 objective**
  - **Article 9.1.** Each Member State shall designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities). Member States shall ensure that those authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them. Member States shall ensure coherence with the existing frameworks for general national crisis management.

Best practice #2: Development of information security standards specific to the national public sector, to be reviewed and updated regularly.

- **Examples**
  - Since 2004, Estonia has required its public administrations to adopt and comply with the ISKE (IT Baseline Security System) standard ([93]). ISKE is an information security standard developed specifically for the Estonian public sector, guaranteeing a sufficient level of security for data processed in IT systems. It is regularly updated and, from 31 December 2023, will be replaced by a new standard, the Estonian Information Security Standard (E-ITS). E-ITS will improve the information security of Estonian public authorities and private companies, and will be updated every autumn ([94]).
  - France's National Agency for the Security of Information Systems (ANSSI) developed a self-assessment tool for cyber crisis preparedness which enables entities to assess their level of preparedness for cyber crises ([95]). The tool allows users to share their anonymised data with ANSSI, enabling the agency to consolidate its understanding of the maturity levels of each sector in France, highlighting those which may require closer attention. Such a tool could be used to support national cyber crisis management authorities in the development of advanced mappings.

- **Analysis and way forward.** The national cyber crisis authority is responsible for developing and implementing information security standards specifically designed for the national public sector. Organisations must comply with these standards, thus increasing their ability to prevent crises, improving their resilience. This facilitates cyber crisis management by lowering the risk of crises. They should be regularly reviewed and updated to account for evolving cyber threats and opportunities to strengthen national IS. This update could include, for instance, risk and compliance assessments to ensure that the standards remain relevant. The standards should guarantee a minimum level of cybersecurity and standardised system protection for public administrations, strengthening the barriers against malicious actors. This practice could be generalised at the EU level for all MS, to guarantee a common level of cybersecurity throughout the EU and better protect European public administrations through increased resilience. Regular updating of these standards would make it possible to assess the effectiveness of the measures and ensure that they take account of the changing nature of cyber threats.

([92]) Interview with a member of EU-CyCLONe.
([93]) Information System Authority (n.d.), 'IT baseline security system ISKE', ISA official website, https://www.ria.ee/en/cyber-security/management-state-information-security-measures/it-baseline-security-system-iske.
([94]) Information System Authority (n.d.), 'Estonian information security standard (E-ITS)', ISA official website, https://www.ria.ee/en/cyber-security/management-state-information-security-measures/information-security-standard-e-its.
([95]) National Agency for the Security of Information Systems (2023), *Publication of a cyber crisis management self-assessment tool*, https://www.ssi.gouv.fr/en/actualite/publication-of-a-cyber-crisis-management-self-assessment-tool/.

- **Matching NIS2 objectives**
    - **Article 9.4.b.** Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan shall lay down, in particular: the tasks and responsibilities of the cyber crisis management authorities.
    - **Recital 57.** As part of their national cybersecurity strategies, MS should adopt policies on the promotion of active cyber protection as part of a wider defensive strategy. Rather than responding reactively, active cyber protection is the prevention […] of network security breaches in an active manner, combined with the use of capabilities deployed within and outside the victim network.

Best practice #3: **Foster national initiatives which promote the creation of prevention programmes, such as centralised DDoS mitigation programmes.**

- **Example.** In several MS, national actors have come together to launch nationwide threat and incident mitigation programmes. For example, the Artemis ([96]) (Poland) and DNS Belgium ([97]) (Belgium) initiatives were respectively designed to research the vulnerability of websites and domain names, alert others to these vulnerabilities and warn of potential consequences. For more large-scale incidents, such as DDoS attacks, the Netherlands has promoted the creation of the Dutch Anti-DDoS Coalition (ADC), of which the National Cyber Security Centre is a member ([98]). The 16 members of this national consortium are Dutch organisations from different sectors, including essential and important ones (government agencies, law enforcement, ISPs, banks, etc.). They work together to improve the resilience of Dutch critical service providers by fighting against DDoS attacks ([99]). This joint initiative aims to share expertise and experience between its members, organise drills, communicate information to the public and promote security standards to help protect against DDoS attacks. As part of the Horizon 2020 project CONCORDIA, ADC is developing the 'DDoS Clearing House', a technical system allowing the continuous and automatic sharing of the metadata of DDoS attacks that have been processed by its members (duration of the attack, addresses, source IP, etc.). This tool consists of an extra layer of security in addition to DDoS mitigation facilities that users must have in place. It aims to broaden users' view of the DDoS attack landscape, while enabling them to proactively prepare their networks for an ongoing DDoS attack, thereby reducing the likelihood of disruption to critical IS and associated consequences ([100]).
- **Analysis and way forward.** ADC's collective management and mitigation model could inspire other types of coalitions. The principle could be the same, i.e. bringing together cooperating organisations to improve the resilience of their digital services by fighting against a type of large-scale attack which has the potential to lead to a cyber crisis, such as supply chain attack and ransomware attack. These new coalitions would conduct three types of activities similar to ADC's, i.e. sharing metadata about attacks through a 'clearing house' (cf. *supra*), organising exercises to test the resilience of participants and sharing information. Its members can be public and/or private actors (government agencies, ISPs, banks, etc.). While the composition of a coalition can be cross-sectoral, it could also focus on a single specific essential or important sector (energy, health, financial market infrastructures, etc.), at the national or EU levels ([101]).

([96]) CERT.PL (2023), 'Artemis – CERT Polska verifies the cybersecurity of Polish organizations', 25 January, https://cert.pl/en/posts/2023/01/artemis-scanning/.

([97]) DNS Belgium (n.d.), 'Partners for a safe Belgian internet', https://www.dnsbelgium.be/en/smart-online/partners.

([98]) Anti-DDoS-Coalitie (n.d.), 'About the coalition', https://www.nomoreddos.org/en/about-the-coalition/.

([99]) According to *ENISA Threat Landscape 2022*, DDoS attacks are significantly on the rise, and are larger and more complex.

([100]) Anti-DDoS-Coalitie (2020), 'Increasing the Netherlands' DDoS resilience together', https://www.nomoreddos.org/en/increasing-the-netherlands-ddos-resilience-together/.

([101]) Cyber Security Competence for Research and Innovation (CONCORDIA) (2022), *DDoS Clearing House Cookbook*, Horizon 2020 Programme (2014–2020), Deliverable D3.6: DDoS Clearing House Platform, https://www.concordia-h2020.eu/wp-content/uploads/2023/03/PREPRINT-D3-6_DDoS_Clearing_House_Cookbook.pdf.

- **Matching NIS2 objective**
  - **Article 16.3.c.** EU-CyCLONe shall […] assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measure.

4.2 PHASE 2 – PREPAREDNESS

The preparedness phase aims to prepare MS and the EU to manage crises by developing plans to support response operations. This includes activities such as setting up a resilient crisis organisation, maintaining confidence within the ecosystem, prioritising the critical activities affected or ensuring that responders will know how to act by organising training sessions and exercises. Preparedness measures are taken before crises occur.

Table 3: Summary of best practices for Phase 2 – Preparedness

Phase 2 – Preparedness
BP #4. Definition of a governance structure, provision of specific capabilities and appointment of a crisis coordinator, whose nomination is mandatory under NIS2, and ensuring their department has the necessary operational and technical cyber skills to directly coordinate stakeholders during a cyber crisis
BP #5. Mapping and gathering information on critical entities and their most critical assets to enable rapid action
BP #6. Establishing instantaneous, secured communication channels during a crisis
BP #7. Formalisation of a clear allocation of roles between the stakeholders involved in responding to a cyber crisis in an overall plan
BP #8. Development of escalation criteria for activating the cyber crisis plan and deploying the relevant cooperation units/groups, taking into account factors such as time, priority, players involved, severity of the attack, etc.
BP #9. Development of a methodology and risk assessment tools to optimise coordination and interoperability in the event of a crisis
BP #10. Test the overall plan for operations in response to cyber crises through a multiannual programme of cyber crisis management exercises and training sessions
BP #11. Setting up training sessions for current and future staff responsible for cyber crisis management at the operational level
BP #12. Development of a communication strategy including a clear format for messaging, stakeholders to involve, priority levels and time factor and communication channels to be used

Best practice #4: Definition of a governance structure, provision of specific capabilities and appointment of a crisis coordinator, whose nomination is mandatory under NIS2, and ensuring their department has the necessary operational and technical cyber skills to directly coordinate stakeholders during a cyber crisis.

- **Example.** In Italy, the Director General of the National Cybersecurity Agency (ACN) was appointed as the national cyber crisis coordinator. While ACN covers the technical and operational levels in cybersecurity, integrating the national CSIRT, the NIS point of contact and the Cybersecurity Team, it is also a member of the CSIRTs Network and EU-CyCLONe at the EU level, enabling it to benefit from shared situational awareness and information from other MS. As a result, its director general has direct access to all the relevant information needed to efficiently support and advise the strategic level in the event of a

cyber crisis ([102]). With its central position, the ACN bridges the gap between the strategic and technical levels and enables better coordination, fulfilling its mission as a key operational player.

- **Analysis and way forward**
  - Designating an authority with operational and technical skills as cyber crisis coordinator speeds up decision-making, which is decisive for any crisis management. In the majority of MS, the national cybersecurity authority has the necessary resources to ensure the national response to cyber incidents ([103]). It often encompasses all the entities at the technical and operational levels, which greatly facilitates their mutual coordination and cooperation. As a member of the CSIRTs Network and EU-CyCLONe, it also has experience of cooperating with other MS, which is crucial when managing a cyber crisis at the EU level. This synergetic architecture is ideal for rapidly consolidating and correlating all the information, alerts and notifications of interest, from the detection of a cyber event to its potential escalation to the state of a cyber crisis, while ensuring that they are shared with other relevant government authorities. This type of entity therefore appears as the ideal player to act as a link between the different levels and ensure an intelligent distribution of tasks, in order to prioritise and facilitate the work of all actors involved. It is also in a privileged position to gather feedback and lessons learnt to improve processes after the crisis has ended, contributing to improved prevention and mitigation of future crises. The entity would play a key role in managing the cyber crisis management plan and should be at the forefront of continuous process improvement ([104]).
  - For effective management and a 360° view of the crisis, the entity should comprise staff from diverse backgrounds and mindsets, ranging from political scientists to engineers. The entity could also include experts in several key areas (judicial, sectoral issues, international relations, etc.) whose specific expertise could be leveraged depending on the type of crisis, allowing to better understand and interact with all affected stakeholders in times of crisis ([105]).
- **Matching NIS2 objective**
  - **Article 9.1.** Each Member State shall designate or establish one or more competent authorities responsible for the management of large-scale cybersecurity incidents and crises (cyber crisis management authorities). Member States shall ensure that those authorities have adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them. Member States shall ensure coherence with the existing frameworks for general national crisis management.

Best practice #5: Mapping and gathering information on critical entities and their most critical assets to enable rapid action.

- **Example.** In France, 'operators of vital importance' who have activities considered essential to the survival of the country must communicate a mapping of their IS to ANSSI ([106]). For example, a French maritime transport company regularly updates the mapping of its IS. It allows this company to have an 'up-to-date view of digital assets, including those linked to critical activities or hosting sensitive or regulated data', but also to prioritise actions 'when not everything can be saved or isolated' ([107]). The shipowner also considers that it is 'important to know which employees manage which systems, because they are often the only ones who can take the precise actions required'. In addition, the mapping of the IS

([102])National Cybersecurity Agency (2022), *National Cybersecurity Strategy 2022–2026*, p. 20, https://www.acn.gov.it/ACN_EN_Strategia.pdf.
([103])Ibid.
([104])Interview with a member of EU-CyCLONe.
([105])Interview with a member of EU-CyCLONe.
([106])National Agency for the Security of Information Systems (2018), *Mapping the information system*, https://www.ssi.gouv.fr/guide/mapping-the-information-system/.
([107])National Agency for the Security of Information Systems (2021), *Crisis of cyber origin: the keys to operational and strategic management*, p. 15, https://www.ssi.gouv.fr/uploads/2022/05/20220516_np_anssi_guide_gestion_crise_cyber_en.pdf.

makes it possible to better understand the connections with customers and partners, and therefore to better communicate in the event of a crisis ([108]). In this regard, as not all actors use the same security standards, ENISA has developed the 'Interdependencies' web tool ([109]), which can be used to find the corresponding information security standards and frameworks of one standard to another.

- **Analysis and way forward.** The precise mapping of IS of essential entities enables more effective operational coordination in the event of an incident. NIS2 deems that these systems are the most critical for MS, and also the most vulnerable given their exposure. The mapping of IS is essential for cyber crisis management. It relates directly to the defence of the IS by allowing for a rapid reaction in the event of an incident, to qualify the impact thereof, or to prevent the consequences of the defensive actions carried out. Mapping also contributes to the resilience of the IS, since it is used to define, for example, the business continuity plan. These mappings, with regard to the critical nature of the activities of an essential entity, could be affixed with a mention of protection or even classification, according to the relevant rules of the MS. The competent authority could ensure that the mappings communicated by the essential entities have been developed, in addition to an approach focused on cybersecurity, to the highest level of granularity, by offering a complete view of the IS and all of its 'visions' (i.e. business, application, infrastructure) and its connections with the outside. The competent authority could encourage essential entities to send regular updates, in particular during IS change or update of projects ([110]). MS could also consider retaining a degree of flexibility when drawing up these mappings, with the possibility of including entities of interest, even if not in the scope of NIS2, in their early warning systems, in order to improve responsiveness and cooperation with all parties concerned in the event of a crisis ([111]).

- **Matching NIS2 objective**
    - **Article 3.3.** By 17 April 2025, Member States shall establish a list of essential and important entities as well as entities providing domain name registration services. Member States shall review and, where appropriate, update that list on a regular basis and at least every 2 years thereafter.

Best practice #6: Establishing instantaneous, secured communication channels during a crisis.

- **Example.** In Germany, the Federal Office for Information Security (BSI) is evaluating the 'Wire' instant messaging system for the exchange of 'restricted' classified information. Its use is currently limited to the authorities connected to the federal government network. More than 30 ministries and authorities use it to exchange information at the restricted level ([112]). However, an extension to users of the 'open network' is planned for a later phase of the project. This would give BSI a secure communication channel for collecting and exchanging sensitive information with private-sector stakeholders, which could be useful in responding to a cyber crisis, particularly when pooling information with affected critical infrastructures operators, or external security service providers ([113]). In terms of performance, Wire messaging enables end-to-end encrypted messages, including attachments, to be sent between two users and in secure group discussions. It is

---

([108]) Ibid.
([109]) ENISA (n.d.), 'Interdependencies', https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/Interdependencies_OES_and_DSPs.
([110]) National Agency for the Security of Information Systems (2018), *Mapping the information system*, https://www.ssi.gouv.fr/guide/mapping-the-information-system/.
([111]) Interview with a member of EU-CyCLONe.
([112]) Federal Office for Information Security (BSI) (2023a), *Sichere, zeitgemäße Kommunikation innerhalb der Netze des Bundes mit Wire* (Secure, up-to-date communication within the federal networks with Wire), pp. 10–12, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2020_02.pdf?__blob=publicationFile&v=4.
([113]) See BP #12: Encourage the mobilisation of qualified security service providers to provide technical assistance to victims.

compatible with the main operating systems, and can be used on smartphones, tablets and computers (114).

- **Analysis and way forward.** In July 2019, an ENISA report highlighted that stakeholders engaged in incident response need secure and reliable communication channels to cooperate and share information (115). Insofar as the essential entities of a cyber crisis are involved in its management, it is important that knowledge be shared with the MS national cyber crisis management authorities, within the framework of a secure communications group. While several types of solutions can be used to create a group discussion, central messaging systems, such as Slack and Mattermost, stand out because they are easy to use, either as software as a service or via a website. Given the sensitivity of the information exchanged, the MS national cyber crisis management authority could ensure that the choice of messaging system takes into account as many requirements as possible. While end-to-end encryption of discussions is the basic criterion, ENISA defines the following seven other features (116):

  - authentication of members using identity-based cryptography,
  - archiving so that all members – even new ones – can access and learn from past discussions,
  - exchange of attachments in all formats,
  - an open specification to enable security audits,
  - a source code under an open source license,
  - availability on all major desktop and mobile operating systems,
  - a 'future-proof' maturity through the development of a stable business model.

Once the messaging system has been selected, the MS national cyber crisis management authority could define it as the default communication platform, even for the most informal exchanges, to make it easier for stakeholders to adapt to its use. The national cyber crisis management authority could, for instance, open channels including representatives from all relevant entities, to ensure smooth cooperation and rapid exchange of information, which would promote rapid action and greater flexibility. Such channels could be opened to critical operators, allowing information on vulnerabilities to be gathered and shared faster and in a more targeted manner, encouraging a faster reaction. Participants could exchange information on a more regular and informal basis, which would foster trust, a key factor in cyber crisis management. In the event of a crisis, more formal rules could be established on the platform, such as the use of specific templates to promote clear messaging, as well as specific channels for questions. Finally, any mapping of participants to be included in such channels ahead of the crisis should be regularly updated (117).

- **Matching NIS2 objectives**

  - **Article 21.1.** Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and IS which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and IS appropriate to the risks posed …

  - **Article 21.2.a and Article 21.2.f.** The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least …: policies on risk analysis and information system security; the use

---

(114) Ibid.
(115) ENISA (2019), *Secure Group Communications for incident response and operational communities*, pp. 6–7, https://www.enisa.europa.eu/publications/secure-group-communications.
(116) See footnote (115).
(117) Interview with a member of EU-CyCLONe.

of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

Best practice #7: **Formalisation of a clear allocation of roles among the stakeholders involved in responding to a cyber crisis in an overall plan.**

- **Example.** In 2017, Belgium adopted a National Cyber Emergency Plan which is subject to annual evaluation and, if necessary, development ([118]). The Centre for Cybersecurity Belgium (CCB) and the National Crisis Centre are responsible for implementing this confidential document, which was designed as a basis for the operational aspects of cyber crisis management at national level. Depending on the intensity of the incident, the plan describes the procedures and security measures to be followed. It formalises the framework for collaboration between the various competent services, and their tasks within the limits of their legal and regulatory powers, to regain control of the situation as quickly as possible (CCB and its CERT.be service, the National Crisis Centre, the Public Prosecutor, Police services, etc.). The plan also promotes the rapid and correct exchange of information between services ([119]).
- **Analysis and way forward.** The key to an effective coordinated response to a cyber crisis is a strict division of roles between the relevant authorities. Drawing up an overall plan detailing the framework for action by the players to be involved, as well as their missions and obligations, helps to prevent overlap throughout the crisis. This document could take into account the nuances and complexities of the cyber crisis and propose, according to several scenarios, the operations and successive measures to be put in place at the national level, but also in cooperation with EU partners. It should be regularly updated, based on experience, feedback and technical progress, in order to develop a MS national cyber crisis management framework. While the overall plan for operations must be confidential for security reasons, the development of a common base for all the MS could encourage and promote a common culture of response to cyber crises across the EU. EU-CyCLONe could be tasked with contributing to this coordination between MS.
- **Matching NIS2 objectives**
    - **Article 9.3.** Each Member State shall identify capabilities, assets and procedures that can be deployed in the case of a crisis …
    - **Article 9.4.c and Article 9.4.f.** Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. This plan shall lay down, in particular:
        - the cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels,
        - national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at the EU level.

Best practice #8: **Development of escalation criteria for activating the cyber crisis plan and deploying the relevant cooperation units/groups, taking into account factors such as time, priority, actors involved, severity of the attack, etc.**

([118]) Centre for Cyber Security Belgium (2021), *Stratégie Cybersécurité Belgique 2.0 (2021–2025)* (Cybersecurity Strategy Belgium 2.0 (2021–2025)), p. 2, https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_FR_DP2.pdf.
([119]) Centre for Cyber Security Belgium (2015), *Annual Report 2015*, pp. 18–19, https://ccb.belgium.be/sites/default/files/documents/FODB13_6002_RA15_Chancelerie_Brochure_Cyber_Security_PP_NL1.pdf.

- **Example.** In 2018, the members of the NIS Cooperation Group published a cybersecurity incident taxonomy ([120]). This taxonomy provides a common, simple and high-level classification for cybersecurity incidents at the strategic and policy levels, and was designed to facilitate the exchange of information across borders and international collaboration. The taxonomy assesses the cyber incident according to its nature (the underlying cause that triggered the incident) and its impact on services and specific sectors of the economy/society, as follows:
  - **nature,**
  - **root cause category:** system failures, natural phenomena, human error, malicious actions, third-party failures,
  - **severity of the threat:** high, medium, low,
  - **impact,**
  - **sectors impacted:** energy, transport, banking, finance, health, drinking water, digital infrastructure, communications, trust and identification services, digital services, government services,
  - **scale of the national impact for the economy and society:** red – very large impact, yellow – marginal impact, green – minor impact, white – no impact,
  - **outlook, i.e. the prognosis for the impact for the economy and society:** improving, stable, worsening.

This taxonomy is only for 'naming' cyber incidents and does not include processes to, for example, notify or escalate incidents.

- **Analysis and way forward.** While the above was developed for the strategic level, it could serve as a basis for operational players to assess and qualify a cyber incident as a crisis using clear escalation criteria. These could lead to the activation of the cyber crisis plan required by NIS2, in order to deploy appropriate measures proportionate to the scale of the crisis. In the future, such a measure could build on the work of the NIS Cooperation Group, bringing an operational perspective that not only qualifies cybersecurity incidents, but also addresses processes to be implemented depending on the level of the crisis. The establishment of escalation criteria would provide a coherent mechanism for objectively assessing cyber incidents, determining the actors to be involved according to the seriousness of the incident and informing decision-makers at all levels of the nature and speed of the response and the procedures to be adopted. These escalation criteria could be developed at the national or the EU level, for instance through a working group coordinated by EU-CyCLONe and involving actors from both the strategic and technical levels, and could be integrated in national crisis plans. While common criteria may be difficult to agree upon, MS should endeavour to reach a mutual understanding, either by adopting a common approach or by developing a tool for rapid understanding, using EU-CyCLONe. Rather than proposing common definitions, this tool would provide an equivalence scale matching varying concepts in the different MS.
- **Matching NIS2 objectives**
  - **Article 9.4.b.** Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan shall lay down, in particular: the tasks and responsibilities of the cyber crisis management authorities.
  - **Article 16.3.c.** EU-CyCLONe shall assess the consequences and impact of relevant large-scale cybersecurity incidents and crises and propose possible mitigation measures.

([120])NIS Cooperation Group (2018), *Cybersecurity Incident Taxonomy (04/2018)*, https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf.

Best practice #9: Development of a methodology and risk assessment tools to optimise coordination and interoperability in the event of a crisis.

- **Example.** The Polish Cybersecurity Strategy (2018) for 2019–2024 sets as an objective the development and implementation of a risk-assessment approach, a Polish government priority for the establishment of a national cybersecurity system. The strategy proposes a 'joint static and dynamic risk-assessment methodology which takes into account the specificity of individual sectors, critical-infrastructure operators, operators of essential services, and digital service providers, shall be introduced for the purpose of cybersecurity management at the national level' [121]. In this way, the government intends to facilitate the comparison of assessments and risk levels, particularly for reporting on national security risks, in line with crisis management regulations [122]. As a result, risk assessment becomes a continuous process which allows the level of risk to be identified in near real time [123]. The Polish government developed a risk assessment method and tools through the National Cybersecurity Platform, a project aimed at creating a prototype for 'a comprehensive, integrated system for monitoring, imaging and warning of threats [to the state's cyberspace]'. This platform is intended to help prevent, detect and minimise the effects of cyber incidents on the information and communication systems that are important to the functioning of the state, while also promoting information sharing on cyber threats [124].

- ENISA has published several reports on risk assessment and interoperability, including *Interoperable EU Risk Assessment Toolbox* (2023) [125] and *Interoperable EU Risk Assessment Framework* (2023) [126]. The former [127] aims to address interoperability issues related to the use of IS risk management methods to facilitate the seamless integration of risk management methods within and between organisations, bridging gaps between different approaches. It thus promotes a common understanding of the risks of interoperable risk assessment results. The latter [128] proposes a methodology to evaluate the potential interoperability of risk management frameworks and methods, proposing, for example, a four-level scale to assess the degree of interoperability of each method and set of characteristics combined.

- **Analysis and way forward.** The development of a risk assessment methodology and tools is essential to enable a progressive approach to the management of large-scale cyber incidents and crises. It not only improves coordination and cooperation between the various levels – strategic, operational and technical – through improved mutual understanding, but also between MS. It is a key measure for promoting information sharing, while at the same time proposing ways of interconnecting and harmonising national approaches. In particular, the operational level would play a key role in bridging the gaps between all the stakeholders involved. This approach could also solve some of the problems associated with the difficulty of defining the notion of a cybersecurity crisis and the subjectivity of what is considered a cyber crisis across MS. It could also easily be integrated into national and European general crisis management frameworks. EU-CyCLONe could elaborate such a methodology, bringing together the perspectives of the MS.

- **Matching NIS2 objectives**

---

[121] Ministry of Digital Affairs (2019), *Cybersecurity Strategy of the Republic of Poland for 2019–2024*, https://www.gov.pl/attachment/6a4aafc6-e339-4cd5-a8e6-cd47257f02d8.

[122] Ibid.

[123] Ibid.

[124] NASK (n.d.), 'National Cybersecurity Platform', https://en.nask.pl/eng/activities/science-and-business/research-projects/2088,National-Cybersecurity-Platform.html.

[125] ENISA (2023), *Interoperable EU Risk Management Toolbox*, https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox.

[126] ENISA (2023), *Interoperable EU Risk Management Framework*, https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework.

[127] ENISA (2023), *Interoperable EU Risk Management Toolbox*, https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox.

[128] ENISA (2023), *Interoperable EU Risk Management Framework*, https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework.

- **Article 9.3.** Each Member State shall identify capabilities, assets and procedures that can be deployed in the case of a crisis …
- **Article 9.4.c and Article 9.4.f.** Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan shall lay down, in particular:
  - the cyber crisis management procedures, including their integration into the general national crisis management framework and information exchange channels,
  - national procedures and arrangements between relevant national authorities and bodies to ensure the Member State's effective participation in and support of the coordinated management of large-scale cybersecurity incidents and crises at the EU level.

Best practice #10: Test the overall plan for operations in response to cyber crises through a multi-annual programme of cyber crisis management exercises and trainings.

- **Examples**
  - Finland has been organising major joint cybersecurity exercises for several years. For the Finnish Transport and Communication Agency's National Cyber Security Centre, these exercises aim to create common situational awareness and coordinating activities between participants and their partners, rather than improving its own internal processes ([129]).
  - At the EU level, ENISA has been organising local, international and EU-wide exercises for the past 15 years, developing cyber exercise platforms available to stakeholders so they may host their own exercises. The agency organises the following specific exercises to test cyber crisis management:
    - **Cyber Europe,** the biannual exercise simulating large-scale cybersecurity incidents which escalate into cyber crises, for both the public and private sectors from the EU and European Free Trade Association MS ([130]),
    - **CyberSOPex,** the biannual exercise to test the CSIRTs Network SOPs,
    - **CySOPex,** the biannual exercise to test the Eu-CyCLONe Officers' SOPs for rapid EU cyber crisis management when faced with large-scale cross-border cyber incidents and crises ([131]),
    - **BlueOLEx,** the annual exercise to test the Eu-CyCLONe Executives' SOPs for rapid EU cyber crisis management when faced with large-scale cross-border cyber incidents and crises.
- **Analysis and way forward.** The programming of cyber exercises over several years could help to develop and strengthen MS' national cyber crisis management frameworks. These exercises should not be considered as isolated events, but rather as a series forming a coherent whole enabling the continuous improvement of all stakeholders, as well as the evolution of capabilities requirements ([132]). They could involve all three levels (strategic, operational, technical), around operational level actors as the federating level, to bridge the gap between the strategic and technical levels. In order to identify training needs, a survey could be conducted at the EU level. Then, in order to match the needs identified, the following phases should be followed: selecting the type of exercise, setting up a planning team, preparing the exercise, supporting observers, carrying out the exercise, providing feedback and drawing lessons learned. Rather than repeating similar exercises every few

---

([129]) National Cyber Security Centre (2020), *Instructions for organising cyber exercises: A manual for cyber exercise organisers*, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Instructions for organising cyber exercises.pdf.

([130]) ENISA (2022), *Cyber Europe 2022: After action report*, https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report.

([131]) ENISA (n.d.), 'Cyber Crisis Management', https://www.enisa.europa.eu/topics/cyber-crisis-management.

([132]) National Cyber Security Centre (2020), *Instructions for organising cyber exercises: A manual for cyber exercise organisers*, p. 29, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Instructions for organising cyber exercises.pdf.

months, different types of exercises could be programmed (tabletop exercise, functional exercise, major joint exercise), just as scenarios could be expanded to involve a growing number of players and critical sectors. Examples of programmes could include, but are not limited to:

- a series of smaller exercises, workshops, and training session, which could be organised more frequently throughout the year, and on specific topics: this would allow participants to benefit from regular reminders about new things they have learned, promote a common vocabulary and knowledge base and build trust between participants ([133]),
- exercises taking into account a sectoral approach, mobilising representatives from critical sectors (banking, energy, transport, etc.) to facilitate discussions between the sector and regulators, promote mutual understanding and improve trust and information sharing ([134]),
- exercises including anticipation scenarios, to prepare and improve response in the event that stakeholders are faced with new situations for which there are not yet clear operational procedures ([135]).

By practising the management of a series of large-scale incidents under realistic conditions, the MS cyber crisis management authorities, the operators of critical and important entities and partners develop methods and reflexes for dealing with real crises ([136]). These exercises could also be used to test internal procedures (such as business continuity plans) and external procedures (such as the quality of information sharing) ([137]). The transposition of NIS2 into national legislation will require MS to adopt response plans for large-scale cyber security incidents and crises, making the organisation of exercises to test national cyber crisis plans particularly relevant.

- **Matching NIS2 objective**

  - Article 9.4.d. Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan shall lay down, in particular: national preparedness measures, including exercises and training activities.

Best practice #11: Setting up training sessions for current and future staff responsible for cyber crisis management at the operational level.

- **Example.** In Portugal, the National Defence Institute has set up a short-term programme called 'Cyber Security and Crisis Management in Cyberspace Course'. The course, which is open by selection, is aimed at senior and middle-level government managers, armed forces and security officers, diplomats, civil society organisations, academics and executives. It prepares them to intervene in the event of a cyber crisis, in particular by promoting the sharing of knowledge, while disseminating a strategic culture of cybersecurity. Among the five teaching modules, which aim to raise awareness and provide training in the various issues at stake in the digital space (security, technology, economy, etc.), the 'Strategic Decision Exercise' module endeavours 'to encourage and raise relevant issues related to crisis management situations in cyberspace' among the attendees, in order 'to improve processes and provide methodologies to be used in decision-making' ([138]).

([133])Interview with a member of EU-CyCLONe.
([134])Interview with a member of EU-CyCLONe.
([135])Interview with a member of EU-CyCLONe.
([136])National Agency for the Security of Information Systems (2021), *Crisis of cyber origin: the keys to operational and strategic management*, https://www.ssi.gouv.fr/uploads/2022/05/20220516_np_anssi_guide_gestion_crise_cyber_en.pdf.
([137])ENISA (2022), *Cyber Europe 2022: After Action Report*, https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report
([138])Instituto da Defesa Nacional (Portugal) (2023), 'Cyber Security and Crisis Management in Cyberspace Course'.

- **Analysis and way forward.** Regular training cycles help to train and improve the skills of personnel responsible for managing cyber crises. In particular, modules specifically dedicated to the operational level could help to bring together the public and private managers (representatives of the national cyber crisis management authority of the MS, key and important entities, etc.) who will be required to work together during a cyber crisis, in order to clearly determine the division of tasks and individual roles. As well as exchanging best practice in cyber crisis management, such training would enable the operational level to be better integrated at the technical and strategic levels. For example, participants could develop and test their knowledge of threat analysis, situation assessment and mitigation measures through feedback, lessons learned and cyber crisis exercises. This type of training could be delivered via an e-learning platform to allow regular updating of knowledge. The educational content of this platform could be populated by the MS' national cyber crisis management authority, in coordination with EU-CyCLONe.
- **Matching NIS2 objective**
  - **Article 9.4.d.** Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan shall lay down, in particular: national preparedness measures, including exercises and training activities.

Best practice #12: Development of a communication strategy, including a clear format for messaging, stakeholders to involve, priority levels and time factor and communication channels to be used.

- **Example.** The Netherlands has developed its communication strategy around the ad hoc establishment of a National Central Crisis Communication Team. This is made up of communication professionals from the National Crisis Centre and relevant ministries. The team coordinates the central government's communication with Dutch society and the press, as well as with the other MS, on the crisis and its visible consequences. As part of a unified approach, it coordinates the timetable and content of messages from all the public and private actors involved, who must express themselves on their own responsibility on their own subjects. For example, local authorities only comment on the implementation of security measures at their level, private companies on the consequences of the crisis on their employees, customers and suppliers, and ministries on the prospects for action at the national level in their areas. In the run-up to a crisis, the centre's Communications Department coordinates communications between central government and public and private partners, providing them with advice, resources and a network of crisis communication experts as required [139].
- **Analysis and way forward.** A crisis communication strategy defines the rules for delivering a clear message at the right time. In the cyber domain, the challenge is to communicate proactively to prevent doubt in public opinion, even though identifying the causes and consequences of an incident is always uncertain. Whatever the organisation of crisis management, a competent unit or department should be designated to coordinate the timing and content of messages, in the interest of a unified and coherent discourse. These communications experts should be included in all meetings, at all stages and at all levels, to contribute to managing the crisis. It is therefore crucial that roles are allocated upstream to clarify the communication tasks of each government actor. Given the complexity of cyber issues, it seems important that the designated communicators master the technical vocabulary, the challenge being to make the general public understand the complexities of a cyber crisis. They must be able to respond effectively to requests for information, both internal (government departments, public partners, etc.) and external (press, citizens, foreign partners, etc.). In terms of deadlines and content, the aim is to inform the public as

---

[139] National Coordinator for Counterterrorism and Security (2022), Landelijk Crisisplan Digitaal, (National crisis plan digital), Ministry of Justice and Security, 23 December, pp. 31–33, https://www.nctv.nl/documenten/publicaties/2022/12/23/landelijk-crisisplan-digitaal.

quickly as possible about what is known, what is not yet known and what measures have been taken. Until it is certain that a cyber crisis is the result of deliberate action, reference to possible causes, duration and scale should be avoided as far as possible.

- **Matching NIS2 objective**
    - **Article 9.3.** Each Member State shall identify capabilities, assets and procedures that can be deployed in the case of a crisis …

4.3 PHASE 3 – RESPONSE

The response phase aims to stem the cyber crisis and prevent further damage. At the EU level, response is based on effective technical, operational and strategic cooperation between MS. An effective and safe response involves activating predetermined measures. These measures are taken during crises.

Table 4: Summary of best practices for Phase 3 – Response

Phase 3 – Response
BP #13. Encourage the mobilisation of private-sector certified 'trusted providers' to provide technical assistance to victims
BP #14. Supporting victims' crisis communication, for instance with a unified and transparent message

Best practice #13: Encourage the mobilisation of private-sector certified 'trusted providers' to provide technical assistance to victims.

- **Examples**
    - In May 2023, BSI published its list of qualified service providers for responding to advanced persistent threat (APT) attacks ([140]). Following a particularly powerful and sophisticated attack (but also beforehand as a preventive measure), German essential entities can consult this list to quickly request assistance from one of these approved actors. Qualified service providers are private companies selected in two stages: applicants must first provide BSI with full documentation for assessment (description of products and services, compliance with defined criteria, existing certifications, etc.), then conduct a technical interview at BSI, during which they must prove their ability to manage an incident in a professional manner, in the framework of a fictitious scenario. Qualified security service providers are presented on the BSI's list according to a number of performance characteristics, including 24x7 availability, ISO 27001 certification, head office location, internal resources for APT incident response, ability to provide other services (legal, crisis communication, etc.), and technical equipment.
    - ANSSI has drawn up a set of requirements for security incident response providers, a set of rules for providers to obtain qualification for their services in this area. It covers requirements relating to the incident response provider, its staff and the way in which incident response services are provided. The following activities are eligible for qualification: system, network and malicious code analysis, and technical monitoring.

([140]) Federal Office for Information Security (BSI) (2023), *Qualifizierte APT-Response Dienstleister* (Qualified APT response service providers), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf?__blob=publicationFile&v=17.

This standard was drawn up in consultation with market players and is regularly updated (^{141}).

- **Analysis and way forward.** The certification of trusted private-sector security service providers could be encouraged to assist targeted critical infrastructure operators. Given the potentially large number of organisations affected during a cyber crisis, the mobilisation of these partners would relieve national cyber crisis management authorities which, if they lack the resources to act on all fronts, could concentrate on other tasks with higher added value. Certified trusted security incident response service providers, approved in advance and compliant with high-level requirements, could be called on directly by an essential entity. To provide an overview of the market for these approved providers, the MS competent authority could publish a directory, enabling the appropriate partner to be found quickly in case of emergency. This list could briefly present certified trusted security service providers, their contact details and their performance characteristics, allowing for a kind of pre-approved, trusted pool of experts. In order to avoid time-consuming research when responding to a cyber crisis, the MS national cyber crisis management authority could ensure that all essential entities have contracted a partnership with a certified trusted security service provider. However, authorities should establish clear procedures for certifying these suppliers, in order to avoid distorting the market and to leave little room for subjectivity and interpretation, in order to maintain a high level of transparency and accountability (^{142}).

- **Matching NIS2 objective**
    - **Article 9.4.e.** Each Member State shall adopt a national large-scale cybersecurity incident and crisis response plan where the objectives of and arrangements for the management of large-scale cybersecurity incidents and crises are set out. That plan shall lay down, in particular: the relevant public and private stakeholders and infrastructure involved.

Best practice #14: Supporting victims' crisis communication, for instance with a unified and transparent message.

- **Example.** In 2017, a car manufacturer was forced to halt production at several of its plants as a result of the WannaCry attack. It was the first company to acknowledge being a victim of this large-scale attack, which disrupted the systems of several organisations across the EU. The company explained it was doing **'everything necessary to counter this attack'**, stating that the first step of the management procedure was to set up measures to stop the spread of the virus (^{143}). Two days later, the Director General of ANSSI spoke to the main French media outlets to say that his teams were working with those of this company, and those of companies that chose to remain anonymous, which he refused to name. He added that ANSSI was 'really trying to restore as quickly as possible in the most problematic cases' (^{144}). His message was quickly picked up by the regional daily press and the specialist press, contributing to the company's transparency and therefore to the protection of its reputation.

- **Analysis and way forward.** The main source of information in managing a cyber crisis should ideally be the organisation that is the victim of the crisis. It is essential for it to be proactive and take the initiative, but not in a hurry. Lies, silence or passivity should be avoided at all costs. To protect the organisation's reputation, the cyber crisis management authority can support the victim organisation's communication to avoid uncertainty. The communications team of the national cyber crisis management authority should be involved at all times, to

---

(^{141}) National Agency for the Security of Information Systems (n.d.), *Référentiels d'exigence: PRIS*, https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/referentiels-exigences/#referentiel-pris.

(^{142}) Interview with a member of EU-CyCLONe.

(^{143}) France24 (2017), "France's Renault hit in worldwide 'ransomware' cyber attack", 14 May, https://www.france24.com/en/20170512-cyberattack-ransomware-renault-worldwide-british-hospitals.

(^{144}) RFI (2017), 'Renault not only ransomware victim in France', 15 May, https://www.rfi.fr/en/economy/20170515-renault-not-only-ransomware-victim-france.

help in managing the crisis (¹⁴⁵). This approach does not mean that everything should be said. As a general rule, it is important to gain time until the extent of the situation is better understood. As the Spanish National Cryptologic Centre states in its report dedicated to good practices in the management of cyber crisis, 'any communication shall avoid mentioning the causes of the incident, the person responsible for it, information that the investigation may reveal or the possible consequences for the organisation or another stakeholder' (¹⁴⁶).

- **Matching NIS2 objective**
    - **Article 9.3.** Each Member State shall identify capabilities, assets and procedures that can be deployed in the case of a crisis …

4.4 PHASE 4 – RECOVERY

The recovery phase aims to enable the MS and the EU to recover quickly by taking measures, as soon as the crisis is over, to return to a level of security that is normal or even higher than before the crisis. Activities include restoring and reintegrating affected systems and arrangements or organising lessons learned to better prevent, respond to and mitigate future crises. Such measures are taken after crises occur.

Table 5: Summary of best practices for Phase 4 – Recovery

Phase 4 – Recovery
BP #15. Develop and implement BRP defined in reference frameworks, with regular reviewing and updates, in consultation with relevant stakeholders
BP #16. Establish a unit tasked with gathering feedback, drawing lessons learnt and producing recommendations for reviewing, updating and modifying procedures and refining the action plan for cyber crisis management

Best practice #15: Develop and implement BRP defined in reference frameworks, with regular reviewing and updates, in consultation with relevant stakeholders.

- **Example.** Predefined frameworks such as NIST 800-34, BS 25999-1, APS 232, NFPA 1600, COBIT, HB 292-2006 or PAS 77 can be used as part of a BRP (¹⁴⁷). National cybersecurity agencies provide guides to help impacted entities recover from a cyber crisis, which could be used to develop robust BRP at a national level. For example, France's ANSSI has developed a guide proposing a gradual approach, describing the different phases that impacted entities should follow to recover their assets and gradually resume their activities (¹⁴⁸).
- **Analysis and way forward.** National cyber crisis management authorities must support the victims of a cyber crisis until its end, i.e. when the essential activities concerned can resume as usual. The measures to be taken in this respect must be formulated in advance to enable smooth activation at the end of a crisis, as part of a BRP and should be regularly updated with lessons learned. The BRP is the final component of a business continuity plan that groups together all the measures that an organisation (public institution, private company, etc.) must take as soon as a crisis occurs in order to continue operating. It also

---

(¹⁴⁵) Interview with a member of EU-CyCLONe.

(¹⁴⁶) National Intelligence Centre (2020), *Gestión de Cibercrisis. Buenas prácticas en la gestión de crisis de ciberseguridad* (Cyber crisis management. Best practices in cybersecurity crisis management), CCN-CERT, p. 23, https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/5425-ccn-cert-bp-20-buenas-pra-cticas-en-la-gestio-n-de-cibercrisis/file.html.

(¹⁴⁷) ENISA (n.d.), 'Business Resumption Plan', https://www.enisa.europa.eu/topics/risk-management/current-risk/bcm-resilience/bc-plan/business-resumption-plan.

(¹⁴⁸) National Agency for the Security of Information Systems (2021), *Crisis of cyber origin: the keys to operational and strategic management*, https://www.ssi.gouv.fr/uploads/2022/05/20220516_np_anssi_guide_gestion_crise_cyber_en.pdf.

includes a business recovery plan, which precedes the BRP and is used to re-establish the processes of the ICT or IS teams following an incident. Indeed, the notions of 'recovery' and 'resumption' should be distinguished: recovery refers to the return of operations back to normal, while resumption refers to the return to business with less capacity and in a different environment ([149]), gradually bringing back into service the digital tools and infrastructure affected. These plans should be developed in consultation with the different stakeholders involved in cyber crisis management, in order to promote a holistic approach. National cyber crisis authorities could also develop guides for different kinds of stakeholders such as essential and important entities, but also smaller structures which may not have the internal resources to develop such plans.

- **Matching NIS2 objective**
  - **Article 21.1.** Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to minimise the impact of incidents on recipients of their services and on other services.

Best practice #16: Establishment of a unit tasked with gathering feedback, drawing lessons learnt and producing recommendations for reviewing, updating and modifying procedures and infrastructure, and refining the action plan for cyber crisis management.

- **Example.** In February 2021, a hospital in France was the target of a ransomware attack, forcing it to reschedule surgical operations. ANSSI was called in to conduct technical investigations. After the crisis, all the teams involved were mobilised in two stages, firstly in a 'hotwash' session and then at a later date. The aim of these feedback sessions was to 'question and improve the practices and procedures of [the] business lines', with a view to being even 'more resilient in the event of a long-lasting crisis' ([150]).

- **Analysis and way forward**
  - In order to develop the cyber crisis management framework, both for the MS and for the organisation affected, each crisis could be immediately followed by the organisation of a feedback session, which would later be evaluated within 30 days ([151]).
  - As soon as the crisis is over, a team could be identified to interview the relevant actors, according to a defined timetable and interview methods. Several themes could be addressed, including governance and the crisis management process, crisis communication, the decision-making and action-monitoring process, technical and operational capabilities and interactions with external stakeholders. The interviews could lead to the drafting of a summary document, which could be supplemented by a digital investigation commissioned from service providers.
  - Based on the data collected, the team would then draft an action plan aimed at improving the national crisis management framework. Feedback could be organised at the level of the MS cyber crisis management authority, which would receive a summary report for its management, along with a more comprehensive document for the technical teams.

- **Matching NIS2 objective**
  - **Article 9.3.** Each Member State shall identify capabilities, assets and procedures that can be deployed in the case of a crisis …

([149])Leal, R. (2021), 'Explanation of the most common business continuity terms', Advisera, https://advisera.com/27001academy/blog/2021/01/18/explanation-of-most-common-business-continuity-terms/.
([150])National Agency for the Security of Information Systems (2021), *Crisis of cyber origin: the keys to operational and strategic management*, p. 65, https://www.ssi.gouv.fr/uploads/2022/05/20220516_np_anssi_guide_gestion_crise_cyber_en.pdf.
([151])Ibid.

5. RECOMMENDATIONS

This final chapter provides a list of recommendations for future development of cyber crisis management at the operational level in the EU.

The best practices identified in this study highlight a number of gaps in cyber crisis management at the operational level in the EU. The imminent transposition of NIS2 into national legislation will formalise the creation of national cyber crisis management authorities. The latter will have to collaborate with – at the MS level – all competent actors in cyber crisis management, including essential entities, and – at the EU level – their EU counterparts through EU-CyCLONe. A number of initiatives could be taken to maximise these efforts.

Based on the analysis and the way forward of the best practices ([152]), EU-CyCLONe could consider the following recommendations.

Recommendation #1. Coordinate working sessions involving all MS to define a list of EU-wide cyber crisis mechanisms to enable a common assessment of incidents and identify the players to be involved depending on the severity of the incident, leading to a model cyber crisis response plan. These cyber crisis management mechanisms could be regularly updated in line with progress made by the MS, particularly in terms of human and technical resources, situational awareness and impact assessment. They should always be part of overarching national crisis management frameworks, considering the transboundary nature of most crises and the potential for spill-over effect impacting many sectors at the same time.

Recommendation #2. Develop simulation exercises at the EU level which test the operational level players and procedures in particular. These exercises, which should involve all three levels (strategic, operational and technical), aim to practice the allocation of tasks, cooperation and fluidity of action of the MS during a cyber crisis. Actors in charge of cyber crisis management must know each other well to trust one another. To ensure continuity, coherence and overall consistency, each exercise could be organised on the basis of the results of the previous one. The exercises would thus test the operational level's ability to coordinate and exchange information, assess the situation, act as the CSIRTs' interpreter with political decision-makers and manage crisis communication with stakeholders. EU-CyCLONe can play a key role not only in strengthening capacity-building but also developing long-lasting trust among MS.

Recommendation #3. Support MS in the set-up of secure communication platform(s) to exchange information with essential entities, including for informal communication, during a cyber crisis. While the platforms selected by MS should obviously be the result of national choices, EU-CyCLONe could help the choices by publishing guidelines, and even comparative analyses, about the messaging systems best suited to cooperate and exchange information in complete confidentiality.

Recommendation #4. Ensure that MS national cyber crisis management authorities, in coordination with the NIS Cooperation Group ([153]), regularly update critical IS maps of essential entities in their country. To do so, they could encourage essential entities to send regular updates, in particular during IS change or project updates. Precise maps are essential for cyber crisis management, enabling more effective operational coordination in the event of an incident.

([152]) See Chapter 4 'Cyber crisis management best practices in the EU'.
([153]) According to Article 14.4 of NIS2, the NIS Cooperation Group is responsible for providing strategic guidance to EU-CyCLONe and for exchanging information relating to the identification of essential and important entities.

They contribute to a rapid reaction in the event of an incident, to qualify the impact or to prevent the consequences of the defensive actions carried out.

Recommendation #5. Support the organisation of media training sessions for executives of MS national cyber crisis management authorities, so that they can give coherent and clear updates on the progress of the crisis, in any type of media (press, radio, TV, social networks). As each MS has its own capacity needs, these communication sessions could be organised at the national level, with content adapted to the context of the MS. EU crisis communicators could regularly follow awareness-raising sessions on cyber issues, as well as refresher courses.

National and EU cyber crisis management procedures will doubtless continue to evolve. Based on the experience of MS (and beyond), ENISA should continue to identify best practices on a regular basis, beginning once NIS2 has been implemented in all MS.

6. BIBLIOGRAPHY

LEGAL DOCUMENTS

European Commission (2017), Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, pp. 36–58), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017H1584&qid=1702033489333.

European Commission (2021), Commission Recommendation (EU) 2021/1086 of 23 June 2021 on building a Joint Cyber Unit, COM(2021) 4520 (OJ L 237, 5.7.2021, pp. 1–15), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021H1086.

European Commission (2023a), Proposal for a Regulation of the European Parliament and of the Council, laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, COM(2023) 209, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0209.

European Parliament and Council of the European Union (2016), Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, pp.1–30), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148.

European Parliament and Council of the European Union (2019), Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, pp. 15–69), https://eur-lex.europa.eu/eli/reg/2019/881/oj.

European Parliament and Council of the European Union (2022), Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, pp. 80–152), https://eur-lex.europa.eu/eli/dir/2022/2555/oj.

OFFICIAL EUIBA DOCUMENTS, STATEMENTS AND WEBSITES

Council of the European Union (2021a), Council conclusions on enhancing preparedness, response capability and resilience to future crises, 14276/21, 23 November 2021, https://data.consilium.europa.eu/doc/document/ST-14276-2021-INIT/en/pdf.

Council of the European Union (2021b), 'Declaration by the High Representative on behalf of the European Union expressing solidarity with the United States on the impact of the SolarWinds cyber operation', press release, 15 April 2021, https://www.consilium.europa.eu/en/press/press-releases/2021/04/15/declaration-by-the-high-

representative-on-behalf-of-the-european-union-expressing-solidarity-with-the-united-states-on-the-impact-of-the-solarwinds-cyber-operation/.

Council of the European Union (2022), Council conclusions on the development of the European Union's cyber posture, 9364/22, 23 May 2022, https://www.consilium.europa.eu/media/56358/st09364-en22.pdf.

CSIRTs Network (n.d.), official website, https://csirtsnetwork.eu/.

ENISA (2013a), *Report on Second International Conference on Cyber-crisis Cooperation and Exercises (24 October 2013)*, https://www.enisa.europa.eu/publications/report/@@download/fullReport.

ENISA (2013b), *National-level Risk Assessments: An Analysis Report (19 November 2013)*, https://www.enisa.europa.eu/publications/nlra-analysis-report/@@download/fullReport.

ENISA (2014), *Report on Cyber Crisis Cooperation and Management*, 6 November, https://www.enisa.europa.eu/publications/ccc-study/@@download/fullReport.

ENISA (2016a), *Common practices of EU-level crisis management and applicability to the cyber crisis (4 April 2016)*, https://www.enisa.europa.eu/publications/eu-level-crisis-man/@@download/fullReport.

ENISA (2016b), *Strategies for incident response and cyber crisis cooperation (25 August 2016)*, https://www.enisa.europa.eu/publications/strategies-for-incident-response-and-cyber-crisis-cooperation/@@download/fullReport.

ENISA (2016c), *NIS Directive*, https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new.

ENISA (2018), *Good practices on interdependencies between OES and DSPs (November 2018)*, https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps/@@download/fullReport.

ENISA (2019a), *EU Member States incident response development status report (27 November 2019)*, https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report/@@download/fullReport.

ENISA (2019b), *Secure Group Communications for incident response and operational communities*, https://www.enisa.europa.eu/publications/secure-group-communications.

ENISA (2021), *EU Member States test rapid Cyber Crisis Management*, https://www.enisa.europa.eu/news/enisa-news/eu-member-states-test-rapid-cyber-crisis-management.

ENISA (2022a), *Cyber Europe 2022: After Action Report*, https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report/@@download/fullReport.

ENISA (2022b), *ENISA Threat Landscape 2022 (October 2022)*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport.

ENISA (2023a), *Cybersecurity Support Action*, https://www.enisa.europa.eu/publications/cybersecurity-support-action.

ENISA (2023b), *Interoperable EU Risk Management Framework*,
https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework.

ENISA (2023c), *Interoperable EU Risk Management Toolbox*,
https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox.

ENISA (2023d), *ENISA Single Programming Document 2023–2025,*
https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-
report-2023-2025.

ENISA (n.d.), 'Cyber Europe', https://www.enisa.europa.eu/topics/training-and-exercises/cyber-
exercises/cyber-europe-programme.

ENISA (n.d.); 'Business Resumption Plan', https://www.enisa.europa.eu/topics/risk-
management/current-risk/bcm-resilience/bc-plan/business-resumption-plan.

ENISA (n.d.), 'Cyber Crisis Management', https://www.enisa.europa.eu/topics/cyber-crisis-
management.

ENISA (n.d.), 'EU-CyCLONe', https://www.enisa.europa.eu/topics/incident-response/cyclone.

ENISA (n.d.), 'Interdependencies', https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-
directive-new/Interdependencies_OES_and_DSPs.

European Commission (2016), 'FAQ: Joint Framework on countering hybrid threats', 6 April
2016, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_16_1250.

European Commission (2020), Joint communication to the European Parliament and the
Council – The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18,
16 December, https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-
decade-0.

European Commission (2022), *Strategic crisis management in the EU*. Independent expert
report, Scientific Advice Mechanism, Scientific Opinion No 13 (22 November 2022),
https://allea.org/wp-content/uploads/2022/11/ec_rtd_sam-crisis-management-opinion.pdf.

European Commission (2023b), 'Joint Statement by United States Secretary of Homeland
Security Mayorkas and European Union Commissioner for Internal Market Breton', 26 January
2023, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_23_394.

European Commission (2023c), Commission communication – 2023 Strategic Foresight Report:
Sustainability and people's wellbeing at the heart of Europe's Open Strategic Autonomy,
COM(2023) 376, 6 July, https://eur-lex.europa.eu/legal-
content/EN/TXT/PDF/?uri=CELEX:52023DC0376.

European Commission (n.d.), 'Directive on measures for a high common level of cybersecurity
across the Union (NIS2 Directive) – FAQs', https://digital-
strategy.ec.europa.eu/en/faqs/directive-measures-high-common-level-cybersecurity-across-
union-nis2-directive-faqs.

European Commission (n.d.), 'What are good practices?', https://ec.europa.eu/migrant-
integration/page/what-are-good-practices_en.

European Economic and Social Committee (2020), EESC opinion: Cybersecurity and Resilience of Critical Entities, TEN/730-EESC-2020, 1.12.2020, https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/cybersecurity-and-resilience-critical-entities.

NIS Cooperation Group (2018a), *Reference document on security measures for Operators of Essential Services*, CG Publication 01/2018, February 2018, https://ec.europa.eu/information_society/newsroom/image/document/2018-30/reference_document_security_measures_0040C183-FF20-ECC4-A3D11FA2A80DAAC6_53643.pdf.

NIS Cooperation Group (2018b), Cybersecurity Incident Taxonomy, CG Publication 04/2018, July 2018, https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf.

OFFICIAL MEMBER STATE DOCUMENTS AND WEBSITES
Belgium

Centre for Cyber Security Belgium (2015), *Annual Report 2015*, https://ccb.belgium.be/sites/default/files/documents/FODB13_6002_RA15_Chancelerie_Brochure_Cyber_Security_PP_NL1.pdf.

Centre for Cyber Security Belgium (2021), *Stratégie Cybersécurité Belgique 2.0 (2021–2025)* (Cybersecurity Strategy Belgium 2.0 (2021–2025)), https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_FR_DP2.pdf.

DNS Belgium (n.d.), 'Partners for a safe Belgian internet', https://www.dnsbelgium.be/en/smart-online/partners.

Germany

Federal Office for Information Security (BSI) (2023a), *Sichere, zeitgemäße Kommunikation innerhalb der Netze des Bundes mit Wire* (Secure, up-to-date communication within the federal networks with Wire), pp. 1–64, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2020_02.pdf?__blob=publicationFile&v=4.

Federal Office for Information Security (BSI) (2023b), *Qualifizierte APT-Response Dienstleister* (Qualified APT response service providers), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf?__blob=publicationFile&v=17.

Estonia

Information System Authority (n.d.), *Kriisivalmisolek ja õppused* (Preparedness for crises and cyber exercises), ISA official website, https://www.ria.ee/kuberturvalisus/kriitilise-infrastruktuuri-kuberkaitse/kriisivalmisolek-ja-oppused.

Information System Authority (n.d.), *IT baseline security system ISKE*, ISA official website, https://www.ria.ee/en/cyber-security/management-state-information-security-measures/it-baseline-security-system-iske.

Information System Authority (n.d.), *Estonian information security standard (E-ITS)*, ISA official website, https://www.ria.ee/en/cyber-security/management-state-information-security-measures/information-security-standard-e-its.

Spain

Asociación Española para el Fomento de la Seguridad de la Información (2020), *Guía para la Gestión de Crisis por Ciberincidente en la cadena de suministro* (Guidance for cyber incident crisis management in the supply chain), ISMS Forum, May 2020, https://www.ismsforum.es/ficheros/descargas/guia-para-la-gestion-de-crisis-por-ciberincidente.pdf.

National Intelligence Centre (2020), *Gestión de Cibercrisis. Buenas prácticas en la gestión de crisis de ciberseguridad* (Cyber crisis management. Best practices in cybersecurity crisis management), CCN-CERT, https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/5425-ccn-cert-bp-20-buenas-pra-cticas-en-la-gestio-n-de-cibercrisis/file.html.

France

National Agency for the Security of Information Systems (2018), *Mapping the information system*, https://www.ssi.gouv.fr/guide/mapping-the-information-system/.

National Agency for the Security of Information Systems (2020), *Référentiels d'exigence: PRIS*, https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/referentiels-exigences/#referentiel-pris.

National Agency for the Security of Information Systems (2021a), *Crisis of cyber origin: the keys to operational and strategic management*, https://www.ssi.gouv.fr/uploads/2022/05/20220516_np_anssi_guide_gestion_crise_cyber_en.pdf.

National Agency for the Security of Information Systems (2021b), *Organising a cyber crisis management exercise*, https://www.ssi.gouv.fr/uploads/2021/09/anssi-guide-organising_a_cyber_crisis_management_exercise-v1.0.pdf.

National Agency for the Security of Information Systems (2022), *Anticipating and managing your cyber crisis communication*, https://www.ssi.gouv.fr/uploads/2022/05/20220516_np_anssi_guide_com_crise_cyber_en1.pdf.

National Agency for the Security of Information Systems (2023), *Publication of a cyber crisis management self-assessment tool*, https://www.ssi.gouv.fr/en/actualite/publication-of-a-cyber-crisis-management-self-assessment-tool/.

Italy

National Cybersecurity Agency (2022), *National Cybersecurity Strategy 2022–2026*, https://www.acn.gov.it/ACN_EN_Strategia.pdf.

Lithuania

Government of the Republic of Lithuania (2016), *Resolution on the approval of the National Cyber Incident Management Plan (29 January 2016)*, https://www.e-tar.lt/portal/en/legalAct/2a916390c5b211e583a295d9366c7ab3.

Netherlands

Anti-DDoS-Coalitie (2020), 'Increasing the Netherlands' DDoS resilience together', https://www.nomoreddos.org/en/increasing-the-netherlands-ddos-resilience-together/.

Anti-DDoS-Coalitie (n.d.), 'About the coalition', https://www.nomoreddos.org/en/about-the-coalition/.

National Coordinator for Counterterrorism and Security (2022), *Landelijk Crisisplan Digitaal* (National Crisis Plan Digital), Ministry of Justice and Security, 23 December, https://www.nctv.nl/documenten/publicaties/2022/12/23/landelijk-crisisplan-digitaal.

National Cyber Security Centre (2022), *Crisismanagement en crisiscommunicatie bij digitale incidenten (Crisis management and crisis)*, Ministry of Justice and Security (March 2022).

Poland

CERT.PL (2023), 'Artemis – CERT Polska verifies the cybersecurity of Polish organizations', 25 January, https://cert.pl/en/posts/2023/01/artemis-scanning/.

Ministry of Digital Affairs (2019), *Cybersecurity Strategy of the Republic of Poland for 2019–2024*, https://www.gov.pl/attachment/6a4aafc6-e339-4cd5-a8e6-cd47257f02d8.

NASK (n.d.), 'National Cybersecurity Platform', https://en.nask.pl/eng/activities/science-and-business/research-projects/2088,National-Cybersecurity-Platform.html.

Portugal

Instituto da Defesa Nacional (n.d.), *Cyber Security and Crisis Management in Cyberspace Course*, https://www.idn.gov.pt/en/education/coursescatalogue/stp/cyber.

Finland

National Cyber Security Centre (2020), *Instructions for organising cyber exercises: A manual for cyber exercise organisers*, https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Instructions for organising cyber exercises.pdf.

RESEARCH

Ansell, C, Boin, A. and Keller, A. (2010), 'Managing transboundary crises: Identifying the building blocks of an effective response system', *Journal of Contingencies and Crisis Management*, Vol. 18, pp. 195–207, https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-5973.2010.00620.x.

Backman, S. (2021), 'Conceptualizing cyber crises', *Journal of Contingencies and Crisis Management,* Vol. 29, No 4, pp. 429–438, https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-5973.12347.

Backman, S. (2023), 'Making sense of large-scale cyber incidents', *Stockholm Studies in International Relations 2023(1)*, pp. 1–45, https://www.diva-portal.org/smash/get/diva2:1745765/FULLTEXT01.pdf.

Backman, S. and Rhinard, M. (2018), 'The European Union's capacities for managing crises', *Journal of Contingencies and Crisis Management*, Vol. 26, No 2, pp. 261–271, https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-5973.12190.

Boecke, S. (2017), 'National cyber crisis management: Different European approaches', *Governance*, Vol. 31, No 2, pp. 1–16, https://www.researchgate.net/profile/Sergei-Boeke/publication/319483832_National_cyber_crisis_management_Different_European_appro

aches/links/5bf3cb30299bf1124fdfa37f/National-cyber-crisis-management-Different-European-approaches.pdf.

Boin, A. (2019), 'The transboundary crisis: Why we are unprepared and the road ahead', *Journal of Contingencies and Crisis Management*, Vol. 27, No 1, pp. 95–99, https://onlinelibrary.wiley.com/doi/epdf/10.1111/1468-5973.12241.

Boin, A., Ekengren, M. and Rhinard, M. (2020), 'Hiding in plain sight: Conceptualizing the creeping crisis', *Risk, Hazards & Crisis in Public Policy*, Vol. 11, No 2, pp. 116–138, https://onlinelibrary.wiley.com/doi/epdf/10.1002/rhc3.12193.

Boin, A. and Rhinard, M. (2022), 'Crisis management performance and the European Union: the case of COVID-19', *Journal of European Public Policy,* Vol. 30, No 4, pp. 655–675, DOI:10.1080/13501763.2022.2141304, https://www.tandfonline.com/doi/full/10.1080/13501763.2022.2141304.

Collier, J. (2017), 'Strategies of cyber crisis management: Lessons from the approaches of Estonia and the United Kingdom', in Taddeo, M. and Glorioso, L. (eds) (2017), *Ethics and Policies for Cyber Operations*, Springer, Cham, pp. 187–212, https://ora.ox.ac.uk/objects/uuid:58dedb26-9851-463d-88a6-c8ad80769485/download_file?file_format=application/pdf&safe_filename=strategies-of-cyber-crisis-management+(published).pdf&type_of_work=Working+paper.

Cyber Security Competence for Research and Innovation (CONCORDIA) (2022), *DDoS Clearing House Cookbook*, Horizon 2020 Programme (2014–2020), Deliverable D3.6: DDoS Clearing House Platform, https://www.concordia-h2020.eu/wp-content/uploads/2023/03/PREPRINT-D3-6_DDoS_Clearing_House_Cookbook.pdf.

De Thomas Colatin, S. (2020), 'Si vis cyber pacem, para sanctiones: the EU Cyber Diplomacy Toolbox in action', CCDCOE, https://ccdcoe.org/library/publications/si-vis-cyber-pacem-para-sanctiones-the-eu-cyber-diplomacy-toolbox-in-action/.

Estall, H. (2023), 'ISO 22361:2022 – Crisis Management Guidelines: a closer look', Continuity Central, https://www.continuitycentral.com/index.php/news/business-continuity-news/8182-iso-22361-2022-crisis-management-guidelines-a-closer-look.

EU Cyber Direct (2018), 'EU Coordinated Response to Large-Scale Cybersecurity Incidents and Crises', https://eucyberdirect.eu/atlas/sources/eu-coordinated-response-to-large-scale-cybersecurity-incidents-and-crises.

Ezioni, L. and Siboni, G. (2021), 'Chapter 1 – Cyber crisis management regulation', in Ezioni, L. and Siboni, G. (eds), *Cybersecurity and Legal-Regulatory Aspects*, World Scientific, 2021, https://www.worldscientific.com/doi/abs/10.1142/9789811219160_0001.

France24 (2017), "France's Renault hit in worldwide 'ransomware' cyber attack", (14 May), https://www.france24.com/en/20170512-cyberattack-ransomware-renault-worldwide-british-hospitals.

Government of South Australia (2020), *Premier and Cabinet Circular: Cyber Security Incident Management (PC042)*, https://www.security.sa.gov.au/documents/documents/Premier-and-Cabinet-Circular-042-Cyber-Security-Incident-Management.pdf.

Le Gédard, M. (2020), 'Gestion de crise et chaînes cyber: organisation européenne et française' (Crisis management and cyber chains: European and French organisation), Institut des hautes

études du ministère de l'Intérieur, https://www.ihemi.fr/articles/organisation-france-europe-cybersecurite-cyberdefense-V2.

Leal, R. (2021), 'Explanation of the most common business continuity terms', Advisera, https://advisera.com/27001academy/blog/2021/01/18/explanation-of-most-common-business-continuity-terms/.

National Cyber Security Centre, 'Incident management', https://www.ncsc.gov.uk/section/about-ncsc/incident-management.

Norwegian Ministries (2019), *National Cyber Security Strategy for Norway*, Norwegian Government Security and Service Organisation, https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf.

Prevezianou, M.F. (2021), 'WannaCry as a Creeping Crisis', in Boin, A., Ekengren, M. and Rhinard, M. (eds), *Understanding the Creeping Crisis*, Palgrave Macmillan, Cham, https://doi.org/10.1007/978-3-030-70692-0_3.

Prime Minister's Office, National Cyber Directorate (Israel) (2018), *National cyber concept for crisis preparedness and management*, Cyber Israel, https://www.gov.il/BlobFolder/news/cybercrisispreparedness/en/Management%20of%20crisis%20situations%20english%20final.pdf.

RFI (2017), 'Renault not only ransomware victim in France', 15 May, https://www.rfi.fr/en/economy/20170515-renault-not-only-ransomware-victim-france.

SAPEA (2022), *Strategic crisis management in the European Union*, Evidence Review Report No. 11, https://allea.org/wp-content/uploads/2022/11/crisis-management-report.pdf.

Schuetze, J. (2021), 'The EU's Response to SolarWinds', Council on Foreign Relations, https://www.cfr.org/blog/eus-response-solarwinds.

Seabrooke, L. (2018), 'Europe's fast- and slow-burning crises', *Journal of European Public Policy*, Vol. 26, No 9, pp. 468–481, https://www.tandfonline.com/doi/epdf/10.1080/13501763.2018.1446456?needAccess=true&role=button.

Segal, E. (2021), '7 Crisis Management Lessons From Colonial Pipeline's Response To Cyber Attack', 8 May, Forbes, https://www.forbes.com/sites/edwardsegal/2021/05/08/colonial-pipeline-cyber-attack-is-providing-crisis-management-lessons-in-real-time/?sh=2671f5d83d82.

World Economic Forum (2022), *The Global Risks Report 2022 (17th Edition)*, https://www.weforum.org/reports/global-risks-report-2022/.

ANNEX: ENISA'S KNOWLEDGE BASE

This table summarises ENISA's knowledge base per phase.

Phase	Source
Phase 1 – Prevention	- ENISA (2018), *Good practices on interdependencies between OES and DSPs (November 2018)*, https://www.enisa.europa.eu/publications/good-practices-on-interdependencies-between-oes-and-dsps. - ENISA (2019), *Secure Group Communications for incident response and operational communities*, https://www.enisa.europa.eu/publications/secure-group-communications. - ENISA, 'Interdependencies', https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/Interdependencies_OES_and_DSPs.
Phase 2 – Preparedness	- ENISA (2013), *National-level Risk Assessments: An Analysis Report (19 November 2013)*. - ENISA (2013), *Report on Second International Conference on Cyber-crisis Cooperation and Exercises (24 October 2013)*. - ENISA (2014), *Report on Cyber Crisis Cooperation and Management*, 6 November. - ENISA (2016), *Common practices of EU-level crisis management and applicability to the cyber crisis (4 April 2016)*. - ENISA (2022), Cyber Europe 2022: After Action Report. - ENISA (2023), *Cybersecurity Support Action*, https://www.enisa.europa.eu/publications/cybersecurity-support-action. - ENISA (2023), *Interoperable EU Risk Management Framework*, https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-framework. - ENISA (2023), *Interoperable EU Risk Management Toolbox*, https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox. - ENISA, 'Cyber Europe', https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme. - ENISA, 'Cyber Crisis Management', https://www.enisa.europa.eu/topics/cyber-crisis-management. - ENISA, 'EU-CyCLONe', https://www.enisa.europa.eu/topics/incident-response/cyclone.
Phase 3 – Response	- ENISA (2016), *Strategies for incident response and cyber crisis cooperation (25 August 2016)*. - ENISA (2019), *EU Member States incident response development status report (27 November 2019)*. - ENISA (2023), *Cybersecurity Support Action*, https://www.enisa.europa.eu/publications/cybersecurity-support-action.
Phase 4 – Recovery	ENISA, 'Business Resumption Plan', https://www.enisa.europa.eu/publications/cybersecurity-support-action.

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the EU agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, ENISA contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the EU's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.