NATIONAL CYBER CRISIS MANAGEMENT PROGRAMME

57th session of the Government of the Republic of Croatia

Zagreb, 9 January 2025

NATIONAL CYBER CRISIS MANAGEMENT PROGRAMME

January 2025

Content:

List of abbreviations:

R.No.	Abbreviation	Full name
1.	CARNET	The Croatian Academic and Research Network
2.	EU	European union
3.	EU-CyCLONe Network	EU *Cyber Crisis Liaison Organisation Network* (European Network of Cyber Crisis Liaison Organisations)
4.	HACZ	Croatian Civil Aviation Agency
5.	HAKOM	Croatian Regulatory Agency for Network Industries
6.	HANFA	Croatian Financial Services Supervisory Agency
7.	HNB	Croatian National Bank
8.	HUP	Croatian Employers' Association
9.	IICB	*Interinstitutional Cybersecurity Board* (Interinstitutional Cybersecurity Committee)
10.	MO	Ministry of Defence
11.	MPUDT	Ministry of Justice, Administration and Digital Transformation
12.	MUP	Ministry of Interior
13.	MZOM	Ministry of Science, Education and Youth
14.	National CERT	CERT and CSIRT body set up within CARNET
15.	NCSC-HR	*National Cyber Security Centre* (National Cyber Security Centre organised within SOA)
16.	CROATIA	Republic of Croatia
17.	SOA	Security Intelligence Agency
18.	SOP	Standard Operating Procedures
19.	TLP protocol	*Traffic Light Protocol* (Traffic protocol for harmonised handling of data sharing and sharing)
20.	UVNS	Office of the National Security Council
21.	CERT MO and OS of the Republic of Croatia	CERT of the Croatian Ministry of Defence and Armed Forces
22.	VSOA	Military Security Intelligence Agency
23.	ZSIS	The Information Systems Security Bureau

Glossary

(1) **CSIRT** is the abbreviation for Computer Security Incident Response Team, which also uses CERT (Computer Emergency Response Team)

(2) **CSIRT Network** (CNW Network) is a network of national CSIRTs established to develop trust and confidence and to promote swift and effective operational cooperation among EU Member States, composed of representatives of the competent authority for the prevention and protection against cyber incidents of the EU (CERT-EU) and the EU Cybersecurity Agency (ENISA) alongside representatives of national CSIRTs.

(3) **Escalation** is a procedure implemented to change the way cyber crisis is managed and to involve all the necessary governance actors;

(4) **EU-CyCLONe Network** the European Cyber Crisis Liaison Organisation Network is established with the aim of acting at an operational level as an intermediary between the authorities responsible for handling cyber incidents (CNW networks) and the political level, with a view to creating an efficient operational assessment and management process during large-scale cybersecurity incidents and cyber crises, as well as supporting decision-making processes on complex cybersecurity issues at strategic and political level;

(5) **ICT** is information-communication technology;

(6) **Cyber incident** means an event that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered or accessible by network and information systems;

(7) **Large-scale cybersecurity incident** an EU-wide incident that causes disruptions that exceed one Member State's incident response capability or that has a significant impact on at least two Member States, as well as an incident at national level that causes disruptions that exceed the capability of the sectoral CSIRT of an incident response authority, or which has a significant impact on at least two sectors, is triggering cyber crisis management procedures, aligned with the existing national general and EU cyber crisis management frameworks;

(8) **Cyber crisis** the situation that may arise in contemporary society is due to a high degree of dependence on network and information systems, and as a result an increasing number of incidents and attacks can cause serious disruptions in social, political and economic terms, affecting human security, the democratic system, political stability, the economy, the environment and other national values, i.e. Croatia's national security in general.

(9) **Competent CSIRT and CERT authority respectively** are NCSC-HR, National CERT, CERT MO and OS RH.

1. Introduction

The adoption of specific implementing acts elaborating on all relevant issues relating to the management of large-scale cybersecurity incidents and cyber crises (hereinafter: cyber crisis management) reflects the need for a systematic EU-wide approach to cyber crisis management.

NIS2 sets the obligation to adopt national cyber crisis response plans[1]. The NIS2 Directive sets out exhaustively the issues that such plans or programmes should regulate in greater detail and introduces an obligation for EU Member States to notify the European Commission and the EU-CyCLONe of their adoption, amendment or adoption of new programmes, as well as the name of the authority designated in the Member State as responsible for cyber crisis management.

NIS2 has been transposed into Croatian legislation by the Cyber Security Act (NN No 14/24).[2]), which is also the national legislative framework for cyber crisis management.

In addition to the Law on Cyber Security, by adopting the National Cyber Crisis Management Programme (hereinafter: National programme) regulates the cyber crisis management system in Croatia in an integrated manner.

Pursuant to Article 56(2) The National Programme shall be adopted by the Government of the Republic of Croatia (hereinafter: Government) on a proposal from SOA, as the authority responsible for cyber crisis management.

As required by Article 9. NIS2 Directives, Article 56(3) The Cyber Security Act establishes that the National Programme describes cyber crisis management capabilities, resources and processes and specifies:

- cyber crisis management objectives, including the development of national preparedness measures, as well as coherence with the EU cyber crisis management framework
- coherence with the national general crisis management framework
- measures and actions to strengthen national preparedness
- a plan for the implementation of national preparedness measures, including a plan of training activities and exercises that shall form an integral part of the cybersecurity exercise plan referred to in Article 58. Of the Cyber Security Act
- tasks and responsibilities of the authorities involved in cyber crisis management
- the role of the public and private sectors and infrastructures relevant to cyber crisis management; and
- the national procedures and coordination at national level necessary to ensure support for the coordinated management of cyber crises carried out at EU level and the effective participation of Croatia in such management.

Cyber crisis management is an important and highly complex segment of national crisis management, for which a separate legislative act focusing exclusively on cyber crises is envisaged, due to their specificities and characteristics that are very different from other types of physical crises.

However, when developing the cyber crisis management framework separately, it should be borne in mind that the management system established by the National Programme is also an integral part of the national crisis management system under the Homeland Security System established by the Homeland Security System Act (NN No 108/17), with the National Security

[1]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 (OJ L 330/80, 27.12.2022).

[2] Entered into force on 15 February 2024.

Council as the central body of the Homeland Security System and the Coordination for the Homeland Security System (hereinafter: KSUDOS) as operational implementation body.

Acknowledging that contemporary crises are often reflected in multiple areas at the same time, the Homeland Security System Act has created the conditions for security risk management activities, including crisis management, to involve all relevant resources of the state and society in a systematic, coordinated, efficient and rational manner and provide the assumptions for guiding and coordinating the actions of the authorities of the Homeland Security System.[3] under all conditions and in all aspects of security risk management, including in crisis management, irrespective of the area in which the crisis is caused.

Therefore, the National Programme needs to ensure the establishment and development of a cyber crisis management system that complies with all relevant national regulations concerning cybersecurity risk management and incident management measures, as well as with the above-mentioned legal framework establishing a Homeland Security System and defining a framework for strategic decision-making and coordinated action by all relevant stakeholders in emergency and crisis situations posing a risk to national security, regardless of the origin of those situations.

The purpose of the adoption of the National Programme is to provide organisational frameworks for the timely and harmonised implementation of the operational procedures applied to prevent and resolve a cyber crisis, by introducing a new, operational level of national coordination in matters of cyber crisis management, bearing in mind that the National Programme does not alter the competences of the authorities involved arising from the law establishing those bodies, nor the competences resulting for those bodies from other laws and bylaws, nor does it affect the conduct of other procedures and mechanisms, which, in accordance with specific regulations, apply in cases where the crisis has an impact on Croatia's foreign, security or defence policy.

The objective of the deployment of an operational level of cyber crisis management is to provide a framework to monitor and coordinate the work of all authorities responsible for responding to incidents at technical level, as well as to link them more effectively to other competent authorities with tasks and responsibilities relevant to the operational handling of a possible evolution of a cyber incident into a large-scale cybersecurity incident or a cyber crisis, and ultimately to a strategic and political level, responsible for taking decisions on security risk management relevant to national security and crisis action, according to the roles and responsibilities established under the Homeland Security System.

Cyber incident response authorities at technical level are those which, within their regular competences and tasks, handle cyber incidents in different sectors, namely NCSC-HR, National CERT, CERT MO and OS RH.

Authorities responsible for the handling of cybersecurity incidents, in the case of large-scale cybersecurity incidents and cyber crises, shall operationally coordinate in close coordination with the competent authorities for the implementation of cybersecurity requirements and the competent authorities for the enforcement of specific laws, according to their respective competences set out in the Cybersecurity Act.

In addition, national authorities also play a very important role in the operational management of cyber crises, given the sectoral competences conferred on them by specific laws.

[3]The Homeland Security system consists of the resources of home affairs, defence, security intelligence, civil protection, firefighting, foreign affairs services and other bodies that perform tasks and tasks to identify, assess, mitigate and/or address security risks of relevance to Croatia's national security in an organised and coordinated manner.

The strategic and political level in terms of the National Programme is the existing general crisis management mechanisms set out in the Homeland Security System Act, which are implemented through the National Security Council and KSUDOS.

The introduction of Cyber Crisis Management Coordination (hereinafter: Coordination), as the new operational levels of cyber crisis management, the National Programme shall establish a national cyber crisis management mechanism based on the need:

- strengthening capacity to detect cyber threats and incidents in a timely manner;
- analyse and understand the full spectrum of different cyber-threats as well as global cybersecurity trends;
- steer and align national processes and activities with international frameworks and strengthen international cooperation on cybersecurity;
- use all existing capabilities of authorities involved in cyber crisis management at operational level;
- the use of strategic and political decision-making mechanisms established through the work of KSUDOS and the National Security Council;
- ensuring information-sharing mechanisms during a cyber crisis and effective coordination mechanisms for the actors involved in addressing a cyber crisis;
- provide all necessary resources and coordination necessary for the recovery of infrastructure of national interest as soon as possible;
- ensuring a high level of awareness of large-scale cybersecurity incidents and crises and a better understanding of the complex technical issue of the cybersecurity domain through the preparation of situation reports and other reporting acts understandable to the strategic and political level responsible for decision-making.

2. General crisis management frameworks

2.1. EU legislation

(1) When major and complex crises occur within or outside the EU and which have a wide impact or political significance, the EU has several response mechanisms at its disposal.

(2) To this end, the Council of the EU adopted in 2006 Emergency and Crisis Coordination Arrangements, which until 2013 served as a platform for information exchange and coordination of action between EU Member States. Based on these Arrangements, the Integrated Political Crisis Response Arrangements (IPCR) were adopted in 2013 (*Integrated Political Crisis Response* — IPCR, 'the IPCR': IPCR).

(3) In the event of a crisis, the IPCR encourages swift and coordinated joint decision-making at political level to ensure the EU's stability as soon as possible. This enhanced crisis response mechanism involves the EU institutions, the affected EU Member States and other actors. Such a mechanism has several advantages over the initial arrangements, such as more flexibility, more upgradability and better use of existing resources.

(4) These arrangements were legally codified in 2018 by an implementing decision of the Council of the EU.[4].

(5) One of the biggest threats to the EU's internal security is certainly the cyber risks that pose a major threat to the emergence of crises at EU level. This is why a new level of cyber crisis management, the EU-CyCLONe network, which was formalised in early 2023, with the entry into force of the NIS2 directive, was launched in 2020.

[4]Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements (OJ L 320/28, 17.12.2018).

(6) The EU-CyCLONe network was established to support coordinated cyber crisis management at operational level and to ensure the regular exchange of relevant information between EU Member States and EU institutions, bodies, offices and agencies.

2.2. National legislation

(7) In order to systematically manage security risks relevant to national security and crisis operations, a homeland security system has been established in Croatia.

(8) Homeland security is composed of resources from home affairs, defence, security intelligence, civil protection, environmental protection, health, finance, judiciary, firefighting, foreign affairs services and other bodies that perform the tasks and tasks of identifying, assessing, mitigating and/or addressing security risks of relevance to national security in an organised and coordinated manner.

(9) The Central Authority of the Homeland Security System is the National Security Council, which examines and assesses security threats and risks and adopts guidelines, decisions and conclusions on how to protect and pursue national security interests. KSUDOS is responsible for aligning and coordinating the work of the Homeland Security System.

(10) An important segment of national crisis management is cyber crisis management processes that will ensure a rapid and effective response to large-scale cybersecurity incidents that, depending on the cause and impact, can spread very quickly and evolve into a large-scale cyber crisis and thus its consequences. Therefore, the National Programme introduces and develops a cyber crisis management model that will include preventive measures, measures to increase national preparedness and clear frameworks for a coordinated and real-time response to a cyber crisis, including not only addressing a cyber crisis, but also ensuring a swift recovery from its consequences.

(11) Raising the level of regulation of cybersecurity, organisational centralisation and encouraging the development of educational programmes in this area started in Croatia with the adoption of the National Cybersecurity Strategy (NN No 108/15) and continued with the adoption of the Act on Cybersecurity of Operators of Essential Services and Digital Service Providers[5] and accompanying Regulations[6] 2018 as NIS1 transposition regulations[7]these have been upgraded by the transposition of the NIS2 Directive into national legislation and the implementation of NIS2 of the transposition law – the Cyber Security Act.

(12) On the basis of the National Cybersecurity Strategy, the National Cyber Security Council was established in 2016 as an interdepartmental body to monitor the implementation of the Strategy, propose amendments to it and, inter alia, address issues relevant to cyber crisis management and propose efficiency measures. At the end of 2019, the National Cybersecurity Council defined the area of 'cyber crisis management' as one of the key areas for which it was concluded that it needed to be developed in a conceptual manner as part of the 2015 review and update of the National Cybersecurity Strategy.

(13) Since 2020, a position has been agreed at the level of the National Cyber Security Council on the need for Croatia's active participation in the work of the EU-CyCLONe network and the SOA has been designated as the representative of the Republic of Croatia to the EU-CyCLONe network.

(14) In recent years, Croatia's approach to cyber crisis management has been aligned with the approach developed into the EU through the establishment and progressive definition of the

[5] (NN No 64/18).
[6] (NN No 68/18).
[7] 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).

EU-CyCLONe framework, and the National Programme continues to align national cyber crisis management frameworks with cyber crisis management frameworks formally established at EU level by NIS2 Directive.

(15) The national programme shall ensure that the cybersecurity activities of all competent authorities are carried out in a harmonised manner and that authorities responsible for handling cybersecurity incidents are more effectively connected to a strategic and political level. Ultimately, it is also the purpose of NIS2 to establish a new, operational level of cyber crisis management through EU-CyCLONe and to define the EU-CyCLONe cooperation mechanisms with other stakeholders involved in cyber crisis management at EU level.

3. Cyber crisis management in Croatia

3.1. Objectives and principles of cyber crisis management

(16) A cyber crisis management system shall be established with the aim of:

- responding effectively to cyber crises and addressing the consequences of cyber crises;
- operational coordination and coordinated work by all authorities responsible for cybersecurity, establishing a national capability to monitor and analyse the full spectrum of cyber threats and allowing for appropriate threat assessment and situational reporting to decision-makers;
- ensuring the efficient and coordinated use of all existing resources, but also further developing the capabilities and capacities of the authorities involved;
- ensuring that a single taxonomy is used to monitor risks that can lead to a cyber crisis;
- define a framework for public and private sector participation and cooperation in strengthening Croatia's cyber resilience.

(17) Cyber crisis management procedures shall ensure that competent authorities act in a coordinated manner in cyber crisis management and shall monitor the principles of:

- proportionality, in terms of aligning the level of resolution of the cyber crisis with the scale of the cyber crisis;
- subsidiarity, in terms of coordinated action by the competent authorities depending on the type and place of occurrence of each individual cyber incident that may or has led to a cyber crisis;
- complementarities, in terms of the use of available and regulatory instruments which complement each other through sectoral, national and international frameworks;
- confidentiality, in terms of mutual information to crisis-handling stakeholders and information to the public, taking into account any requirements to be respected in relation to legally protected categories of data, which include, inter alia, the use of a secure and resilient communication and information infrastructure for the exchange of information, as well as protocols for their further exchange within and outside the authorities involved in addressing the cyber crisis.

3.2. Scope

(18) Cyber crisis management includes monitoring the full spectrum of cyber threats with a view to preventing, handling and recovering from cyber incidents that may lead to significant disruptions in Croatia, but also to trigger a cyber crisis with the risk of cross-border spillovers, as well as to identify and prevent all types of cyber threats, which can be a potential current or future source of cyber crises.

(19) As part of the monitoring of the full spectrum of cyber threats, particular attention shall be paid to state-sponsored cyber-attacks and APT campaigns.[8]they pose a high risk to the emergence of a cyber crisis, particularly in the public sector, as well as in the area of national critical infrastructure and additionally to other sectors of high criticality identified by the Cybersecurity Act. Particular attention shall also be given to any other large-scale cybersecurity incident.

3.3. Authorities involved in cyber crisis management and their tasks and responsibilities

(20) The bodies primarily responsible for implementing the activities referred to in the National Programme are:

- SOA as the central government authority for cybersecurity, authority responsible for cyber crisis management, competent authority for the implementation of cybersecurity requirements for a total of 14 sectors[9] and the competent CSIRT authority for a total of 16 sectors[10]. The performance of these SOA tasks is carried out by the NCSC-HR.
- UVNS as the central government authority for information security and the competent authority for the implementation of cybersecurity requirements for the public sector.
- MZOM as the state administration body responsible for science and education and the competent authority for the implementation of cybersecurity requirements for the research sector, the education system sector and the registry of top-level national internet domain names from the digital infrastructure sector.
- MPUDT as the state administration body responsible for the development of the digital society and the competent authority for the implementation of cybersecurity requirements for trust service providers in the digital infrastructure sector.
- HAKOM as the competent regulatory authority for the electronic communications, postal services and rail passenger rights sector and the competent authority for the implementation of cybersecurity requirements for providers of public electronic communications networks and providers of publicly available electronic communications services from the digital infrastructure sector.
- CARNET as the competent authority for the prevention and protection against cyber-threats of public information systems in Croatia and the competent CSIRT authority for five sectors[11]. The performance of these tasks by CARNET shall be carried out by the National CERT.
- ZSIS as the central government authority to carry out tasks in the technical areas of information security and the authority responsible for cybersecurity certification and the conduct of cybersecurity audits in state administration and other state authorities.
- MUP as the state administration body responsible for combating cybercrime.
- MO OS of the Republic of Croatia and VSOA as authorities responsible for the defence sector, cyberspace as the domain of military cyber operations and for carrying out the tasks of CERT MO and OS of the Republic of Croatia.
- HNB as the competent authority for the enforcement of special laws for the banking sector.

[8] The APT campaign (Advanced Persistent Threat) is a type of cyber attack characterised by a high level of expertise and covertness of the perpetrator of a cyber attack over a long period of time, with the ultimate aim of theft of confidential information, blackmailing or damage.

[9] Energy, transport, health, human water, waste water, digital infrastructure, ICT (B2B) service management, space, postal and courier services, waste management, manufacture, production and distribution of chemicals, food production, processing and distribution, manufacturing, and digital service providers.

[10] Energy, transport, health, human water, waste water, digital infrastructure, ICT (B2B) service management, space, postal and courier services, waste management, production, production and distribution of chemicals, food production, processing and distribution, manufacturing, research, education system, digital service providers.

[11] Banking, financial market infrastructure, research, the education system and partly the digital infrastructure sector.

- HANFA as the competent authority for the enforcement of specific laws for the FMI sector.
- HACZ as the competent authority for the enforcement of specific laws for the air transport subsector (transport sector).

(21) In addition to the primary competent authorities referred to in point 20, coordination activities, irrespective of how it works, for the purposes of coordination, prevention, education, conducting cybersecurity exercises or addressing a cyber crisis, may, as assessed by the authority responsible for cyber crisis management and depending on the needs of Coordination's action, involve other stakeholders:

- State administration bodies, other state bodies and legal persons with public powers and local and regional self-government units
- representatives of the private sector or other professional associations representing the private sector in a broad sense which, through the public-private partnership process, facilitate the involvement of relevant private sector representatives in the national cyber crisis management process;
- academic and research entities to implement educational activities, adapt existing and develop new education programmes, and develop advanced cybersecurity technologies and tools.
- essential entities, important entities and entities that are not categorised as essential or important entities but implement the voluntary cybersecurity protection mechanisms of the Cybersecurity Act.

3.4. Coordination for cyber crisis management and the authority responsible for cyber crisis management

(22) The coordination shall be the interdepartmental authority responsible for the operational level of cyber crisis management and shall be composed of representatives of the authorities referred to in point 20.

(23) Each body referred to in point 20 shall appoint its representatives, a member and an alternate member in Coordination, who shall be authorised to represent the bodies in the activities falling within the scope of the National Programme.

(24) The other stakeholders referred to in point 21 may be involved in the work of Coordination during its regular operation, as appropriate, and in particular in cases of thematically linked discussions or exchanges of information.

(25) Representatives from other public sector bodies or private sector legal persons that are affected by the cyber crisis being addressed or who, due to their capabilities and available capacities, may also be involved in the work of Coordination during the application of the escalation process, taking coordinated actions to address the resulting crisis, public awareness or recovery and mitigation of the consequences of large-scale cyber incidents or cyber crises, as appropriate, in addition to the stakeholders referred to in point 21.

(26) The representative of the NCSC-HR shall chair and organise the work of the Coordination and the NCSC-HR shall provide expert-administrative support.

(27) Coordination shall adopt rules of procedure governing the organisation and the manner in which it operates (hereinafter: Rules of Procedure).

(28) The Rules of Procedure shall, taking into account the need for effective implementation of the requirements of the National Programme, lay down the rules for convening Coordination meetings, the way in which coordination meetings are to be conducted, and the arrangements for implementing escalation and de-escalation procedures. The Rules of Procedure shall also govern matters relevant to Coordination's decision-making, including the way in which decisions are taken, as well as all necessary actions and preconditions to be met in the case of

decision-making and the implementation of Coordination activities handling classified information. Furthermore, the Rules of Procedure will specify the rules of procedure concerning the involvement of the other stakeholders referred to in point 21 in the work of Coordination and the implementation of the activities referred to in points 24 and 25.

(29) Only representatives of the authorities referred to in point 20 for whom the necessary requirements for the use of classified information have been met in terms of the availability of relevant physical premises, classified network and information systems and certificates for access to classified information issued for designated representatives in Coordination may participate in Coordination's Coordination activities.

(30) The Rules of Procedure shall be used only for the official use of the competent authorities referred to in point 20 and the representatives of those bodies in the work of Coordination and shall not be made public, but shall, where appropriate, be made available to the other stakeholders referred to in point 21 for their participation in the Coordination's work.

(31) All authorities participating in Coordination's work shall comply with appropriate procedures for the exchange of information, such as the TLP protocols referred to in the explanatory notes in Annex 7.2, as well as the rules for the handling of classified or other information for which specific rules of procedure have been laid down to protect its confidentiality or confidentiality.

3.5. Cyber crisis management levels

(32) Cyber crisis management levels are operational, strategic and political levels.[12].

(33) For the purpose of systematic cyber crisis management, the National Programme shall establish a level of operational cyber crisis management, in order to ensure a better connection of all authorities with cybersecurity responsibilities and to inform the strategic and political level more effectively of the circumstances relevant for strategic decision-making.

(34) The core objectives of the operational level of cyber crisis management are:

- coordinated cyber crisis resolution;
- mutual exchange of relevant data between stakeholders involved in addressing a cyber crisis;
- appropriate information to the public.

3.5.1. Operational level of cyber crisis management

(35) The operational level of cyber crisis management is the cyber crisis management at coordination level.

(36) The operational level of cyber crisis management shall be involved in the handling of large-scale cybersecurity incidents on the basis of a proposal to escalate the situation from the regular mode of operation Coordination in alert mode or crisis mode of operation in accordance with the procedures described in Chapters 3.7.2 and 3.7.3.

(37) The scope of cyber crisis management at operational level shall include:

- addressing a cyber crisis at national level through coordinated cooperation between all authorities responsible for handling cybersecurity incidents and involving all other stakeholders relevant for the effective handling of the cyber crisis, including internal teams of affected entities responsible for the prevention and protection against cyber incidents;

[12] The strategic and political level within the meaning of this National Programme is made up of the National Security Council, KSUDOS and UVNS.

- contributing to the resolution of cyber crises at international level that may also have an impact on Croatia;
- consideration and activation of available EU and other international assistance mechanisms;
- exchange of data between all stakeholders involved in addressing a cyber crisis at operational level;
- strategic and political outreach;
- the coordination of public information activities or the establishment of an appropriate means of crisis communication with the public.

3.5.2. Strategic and political level of cyber crisis management

(38) The strategic and political level of cyber crisis management is the level of strategic and political decision-making within the broader national crisis management system established by the Homeland Security System Act.

(39) The escalation of cyber crisis management from operational to strategic and political levels shall be carried out primarily with a view to recovering from the cyber crisis and mitigating the consequences of the cyber crisis.

(40) Escalation to a strategic and political level shall also be carried out for the purpose of establishing appropriate crisis communication with the public, in particular for the purpose of mobilising additional resources and mechanisms to recover from a cyber crisis, in part of its consequences in physical and physical resources, while only addressing the cyber crisis in cyberspace is primarily carried out at operational level.

(41) The scope of cyber crisis management at strategic and political level is proposed through the Cyber Crisis Management Plan and includes the following KSUDOS activities:

- strategic communication activities with the public
- strategic decision-making in the recovery phase from the cyber crisis, especially in part of physical space and resources;
- consider and propose to the Government appropriate follow-up actions and ways to respond to the cyber crisis.

3.6. Criteria for confirming the state of a cyber crisis and escalating the resolution of a cyber crisis to a higher level

(42) The cyber crisis validation criteria may be general and specific, with escalation to operational level primarily carried out to address a cyber crisis, according to Chapter 3.5.1, and escalation from operational to strategic and political level primarily with a view to recovering from the cyber crisis and mitigating the consequences of a cyber crisis, according to Chapter 3.5.2.

(43) The general criteria for confirming the cyber crisis situation and escalation to the operational level shall represent the circumstances leading to the inability to handle the cyber incident using the regular activities of the directly competent CSIRT or CERT body referred to in point 20.

(44) The inability to deal with a cyber incident referred to in point 43 may be due to the complexity, sophistication or scale of the cyber incident, which therefore goes beyond the jurisdiction or exceeds the capabilities and capabilities of the individual, directly competent CSIRT or CERT authority in the affected sector or type of entities, and shall be identified following a joint assessment by the competent CSIRT or CERT authority and the body referred to in point 20, or other central sector authority affected by the cyber incident.

(45) The general and specific cybersecurity crisis validation criteria shall be laid down in the SOPs of each of the competent authorities referred to in point 20, according to sector-specific characteristics. The criteria referred to above shall be agreed upon in Coordination.

(46) The SOPs shall develop general cybersecurity crisis validation criteria within the meaning of paragraph 44, as well as specific criteria in terms of the possible setting of thresholds for the qualification and quantification of individual elements of relevance for confirming the situation of a cyber crisis, such as the sector, subsector, types of entities and number of entities, services and sensitive data affected by the cyber incident, namely criteria related to assessing the trend of the evolution of the cyber crisis and assessing the level of impact of the cyber crisis on society as a whole. In doing so, it shall ensure a consensual and harmonised approach to the handling of an incident by the competent CSIRT or CERT body in coordination with the competent sector-specific authority and in accordance with the division of competences as set out in Annex III. The Cybersecurity Act, i.e. under other relevant sectoral regulations.

(47) When elaborating the general and specific cyber crisis validation criteria, the taxonomy set out in Annex 7.1 shall be used.

3.7. Standard Operating Procedures (SOPs) Cyber Crisis Management Coordination and Competent Authorities in Cyber Crisis Management

(48) In order to ensure that all key activities are carried out, this Chapter defines the Standard Operating Procedures of Coordination and introduces three modes of its operation that ensure the continuous conduct of the activities of all competent authorities referred to in point 20 in cyber crisis management.

(49) The three modes of Coordination, illustrated in Tables 1, 2 and 3, are as follows:

- regular operating mode
- warning mode of operation
- crisis mode.

Table 1*: Overview of the main activities and results of Coordination's work for* ***regular operating mode*** *the competent authorities referred to in point 20 in cyber crisis management shall:*

Main activities:	**Preparedness**	**Situational awareness**	**Cooperation on cyber crisis management planning**	**Cyber crisis management and decision-making**
Regular operating mode:	— The development, continuous harmonisation and improvement of the SOPs of the competent authorities referred to in point 20. — Establishing, maintaining and continuously developing cyber capabilities and capabilities	— Quarterly exchange of situation reports from all competent authorities referred to in point 20.	— Regular Coordination meetings	— Regular annual situational awareness of the strategic and political level

	— Security awareness raising and continuous training of operators — Continuous assessment of the state of cybersecurity — Prompt reporting of any significant and media monitored cyber incidents to other coordinating representatives — Continuous monitoring of international trends in cyber crisis management and proposing coordination of national development measures			

***Table 2**: Overview of the main activities and results of Coordination's work for **warning mode of operation** the competent authorities referred to in point 20 in cyber crisis management shall:*

Main activities:	**Preparedness**	**Situational awareness**	**Cooperation on cyber crisis management planning**	**Cyber crisis management and decision-making**
Warning mode of operation:	—	— An explanatory proposal and a warning situational report (initial, intermediate, final) – the competent authority and the competent CSIRT referred to in paragraph 20. (escalation initiativeers) and NCSC-HR delivery — NCSC-HR consultations with escalation initiators — Production of an alert situation report from the other competent authorities referred to in point 20. (initial, transitional, final)	— Extraordinary coordination and coordination of the operational level — Production of an operational level alert situation report (initial, intermediate, final) for the strategic and political level — Escalation and de-escalation at the proposal of the competent authority and the competent CSIRT referred to in point 20. (escalation and de-escalation initiators)	— Remarkable understanding of the strategic and political level

Table 3: *Overview of the main activities and results of Coordination's work for* ***crisis mode*** *the competent authorities referred to in point 20 in cyber crisis management shall:*

Main activities:	**Preparedness**	**Situational awareness**	**Cooperation on cyber crisis management planning**	**Cyber crisis management and decision-making**
Crisis mode:	—	— A proposal for escalation with justification and the production of a crisis situation report (initial, intermediate, final) – the competent authority and the competent CSIRT referred to in point 20. (escalation initiators) and NCSC-HR delivery — NCSC-HR consultations with escalation initiators — Produce a crisis situation report from the other competent authorities referred to in point 20. (initial, transitional, final)	— Crisis-alignment of the operational level — Development of a cyber crisis management plan (Escalation Initiative, NCSC-HR and Cyber Crisis Management Coordination) — Production of an operational level crisis situation report (initial, intermediate, final) (e.g. escalation initiative, NCSC-HR and Cyber crisis management coordination) — Escalation and de-escalation at the proposal of the competent authority and the competent CSIRT referred to in point 20. (escalation and de-escalation initiatives)	— Crisis management at operational level through the implementation of the agreed cyber crisis management plan — Crisis coordination of the operational, strategic and political levels

3.7.1. Regular operating mode

(50) As part of the regular coordination mode, coordination between the stakeholders involved and continuous monitoring of the cybersecurity situation shall be ensured, with the competent authorities referred to in point 20 continuously evaluating and improving SOPs within the segment of their competence. The other stakeholders referred to in point 21 shall, where appropriate, participate in Coordination and continuously evaluate and enhance the cybersecurity risk management measures they take to ensure their business continuity and cyber crisis management, subject to the framework established pursuant to Article 30(1), indent 3. The Cybersecurity Act or similar cybersecurity measures they implement pursuant to other obligations.

(51) The SOP of each competent authority and the measures of other stakeholders must lay down all necessary internal procedures for the implementation of the activities of the authorities and stakeholders in accordance with the rules and procedures set out in the National Programme, taking into account the rules, procedures and obligations arising for those authorities from their role in the implementation of the crisis response procedures of the EU, the North Atlantic Treaty Organisation or other international organisations to which the Republic of Croatia is a member. All SOPs of the competent authorities referred to in point 20 shall be coordinated at operational level within the framework of Coordination and shall be adopted by the heads of the authority.

(52) During Coordination's regular operation, each competent authority referred to in point 20 shall produce periodic situational reports and exchange them at least quarterly with the other competent authorities referred to in point 20. They shall also establish, maintain and continuously develop their own cyber capabilities and capabilities and shall carry out activities aimed at raising security awareness and continuous training of entities within their areas of competence. Furthermore, the authorities referred to in point 20 shall conduct a continuous assessment of the cybersecurity situation in the domain of their competence, report promptly to the other coordinating authorities on all significant and medialy monitored cyber incidents within their jurisdiction, and continuously monitor international trends in cyber crisis management and propose, where appropriate, the coordination of measures for national developments in cyber crisis management. In addition, the authorities referred to in point 20 shall, where appropriate, coordinate national cyber crisis management procedures with the relevant procedures of international organisations of which the Republic of Croatia is a member.

(53) In regular mode, the NCSC-HR shall organise a Coordination meeting at least once a quarter.

(54) In regular mode, the NCSC-HR produces an annual report for the purposes of the strategic and political level, including an overview of all escalations in the Coordination's alert or crisis mode, carried out during the reporting year. The annual report shall be agreed and approved by Coordination before transmission to the strategic and political level.

3.7.2. Warning mode of operation

(55) Escalating the situation from regular operating mode to alert mode, jointly proposed by the competent CSIRT and the sector-specific authority referred to in point 20. (hereinafter: escalation originators), when they estimate, on the basis of the data they hold within their jurisdiction or through information received from other sources:

- the potential occurrence of a cyber crisis; or
- the possible evolution of a cyber incident from its competence into a large-scale cyber incident, i.e. a potential cyber crisis.

(56) A proposal for escalation with the initial situational situational reports of the escalation originator shall be submitted to the NCSC-HR. The NCSC-HR shall consult the escalation initiators on the reasons for the escalation and, if necessary, request amendments to the situation report submitted. Once agreed and completed, the NCSC-HR shall submit a proposal for escalation to all other competent authorities referred to in point 20 together with the agreed initial situational warning report.

(57) Upon receipt of the proposal referred to in point 56, the other competent authorities referred to in point 20 shall review the situation in their area of competence and, without delay, within two days of receipt of the initial escalation warning reports by the originator, draw up their initial situational alert report, informing the other competent authorities referred to in point 20 of the situation in the area within their jurisdiction and giving an opinion on the proposal of the originator of the escalation.

(58) On the basis of the initial situational reports received from all the competent authorities referred to in point 20, the NCSC-HR shall convene an extraordinary Coordination meeting without delay, no later than two days from the receipt of the initial situational alert reports. An extraordinary session shall decide on escalation in the warning mode.

(59) In the event of a decision by Coordination on escalation in the warning mode of operation, the proposal for an initial situational report shall be prepared by the initiating agents of the escalation, with the assistance of the NCSC-HR, and the proposal shall be approved and agreed at the second extraordinary coordination meeting, no later than two days after the decision on escalation has been taken. The accepted proposal for escalation and the initial Coordination Situation Warning Report shall be referred without delay to KSUDOS to inform the strategic and political level of the alert situation.

(60) All activities referred to in points 56 to 59 shall be repeated for the final phase of the warning mode and a transitional reporting phase shall be introduced in case of a duration of more than 30 days, i.e. the collection of new and important information.

(61) The de-escalation proposal shall be submitted by escalation originators, accompanied by the mandatory submission of their final warning situational reports. Upon receipt of a de-escalation proposal, the other competent authorities shall check the situation within their area of competence and draw up their final situational situational report without delay and at the latest within two days of receiving the final situational situational reports of the escalation initiator. On the basis of the proposal received for the de-escalation of the situation from the alert to the regular mode and the final situational situational reports of all the competent authorities referred to in point 20, the NCSC-HR shall convene the third extraordinary meeting of Coordination without delay and at the latest within two days of receipt of the proposals for de-escalation and final situational reports. The Extraordinary Session of Coordination shall decide on de-escalation in the regular or further alert mode of Coordination and on the implementation of activities pursuant to point 60.

(62) In the event of a decision by Coordination on de-escalation in a regular manner, the proposal for a final situational report shall be prepared by the initiators of the escalation, with the assistance of the NCSC-HR, and approved and agreed at the final extraordinary meeting of Coordination, no later than two days after the adoption of the de-escalation decision. The adopted proposal for a final Coordination situational alert report shall be referred without delay to KSUDOS for the purpose of communicating de-escalation to the strategic and political level.

3.7.3. Crisis mode

(63) A proposal to escalate the situation from a regular mode or a warning mode into a Coordination crisis mode, shall be submitted by the escalation initiators referred to in point 55 and shall be based on their joint assessment of the inability to deal with a cyber incident due to:

- the scope of the cyber incident going beyond the competence of the directly competent CSIRT or CERT authority in the affected sector or type of entities;
- the scope of the cyber incident exceeding the capabilities and capabilities of the individual, directly competent CSIRT or CERT authority in the affected sector or type of entities;
- the high complexity and sophistication of a cyber incident that can be a broader national or cross-border threat.

(64) The escalation proposal with the initial crisis situation report shall be submitted to the NCSC-HR. The NCSC-HR shall consult the escalation initiators on the reasons for the escalation and, if necessary, request amendments to the situation report submitted. Once agreed and completed, the NCSC-HR shall submit a proposal for escalation together with the initial crisis situation report to all other competent authorities referred to in point 20.

(65) Upon receipt of the proposal referred to in point 64, the other competent authorities referred to in point 20 shall, without delay and at the latest within 24 hours of receipt of the proposal, draw up their initial situational crisis report, taking into account the state of their competence in relation to the initial escalation report, and communicate their initial crisis situational reports to the other authorities referred to in point 20.

(66) Upon receipt of all crisis situation reports, the NCSC-HR shall, without delay and at the latest within 24 hours of receipt of the report, convene a crisis meeting of Coordination, where the coordination shall be carried out at operational level, and decide to escalate into a crisis mode of operation at operational level. The accepted escalation proposal in crisis mode shall be notified without delay to KSUDOS.

(67) Escalation initiators and NCSC-HR shall draw up an initial crisis situational report by Coordination and a proposal for a cyber crisis management plan, and the draft plan shall be approved and agreed at the second Coordination crisis session, no later than 24 hours after the decision to escalate into a crisis mode. The Cyber Crisis Management Plan and the initial Coordination Crisis Situation Report shall be submitted to KSUDOS to inform the strategic and political level of the situation and to decide on the need to activate additional crisis management mechanisms, such as those used in the context of crisis management in the civil protection system.

(68) All activities referred to in points 64 to 67 shall be repeated for the final phase of the crisis mode and a transitional reporting phase shall be introduced in case of a crisis mode of operation longer than 30 days, i.e. gathering new and important information.

(69) The de-escalation proposal shall be submitted by escalation originators. On the basis of a proposal for de-escalation from the crisis situation in the alert or regular mode and the final situational crisis reports of all the competent authorities referred to in point 20, a third crisis meeting of Coordination shall be convened, at the latest within two days of receipt of the proposal and of the final situational crisis report. An extraordinary session of Coordination shall decide on de-escalation in a warning or regular mode of operation or continuation of the crisis mode of operation of Coordination.

(70) In the event of a decision by Coordination on de-escalation in a warning or regular manner, the proposal for a final situational situation report shall be drawn up by the escalation initiators, with the assistance of the NCSC-HR, and the proposal shall be approved and agreed at the final crisis session of Coordination, no later than two days after the adoption of the de-escalation decision. The adopted proposal for a final situational crisis report shall be sent by Coordination to KSUDOS without delay for the purpose of communicating de-escalation to the strategic and political level.

3.8. Cyber crisis management plan

(71) When drawing up the proposal for a cyber crisis management plan referred to in point 67, escalation initiators and NCSC-HR shall be guided by the principles of proportionality, subsidiarity, complementarity and confidentiality referred to in point 17 and shall elaborate in the draft plan the phases of resolution of the cyber crisis, possible mitigation measures and the cyber crisis recovery phase.

(72) The cyber crisis management plan shall be drawn up using the form forming an integral part of the Rules of Procedure referred to in point 27.

(73) The cyber crisis management plan shall set out:

- the tasks of the competent authorities referred to in point 20 and the role and tasks of other stakeholders in addressing the resulting cyber crisis, with a view to their coordinated action;
- how to inform each other's cyber crisis stakeholders about the situationality;
- a plan of needs for the involvement of the strategic and political level and the actors and means of communicating with the public.

(74) The adoption of the cyber crisis management plan shall aim to define the necessary activities to effectively address and recover from a cyber crisis, including activities related to the exchange of data between all crisis-resolution actors and to inform the public for the purpose of mitigating adverse effects and preventive impact on perpetrators of a cyber-attack.

3.9. Capabilities and infrastructures relevant to the cyber crisis management system and data sharing

(75) For the purposes of cyber crisis management, the authorities referred to in point 20 shall ensure a high level of availability and readiness of all existing capabilities and infrastructure used within their jurisdiction for the handling of cyber incidents.

(76) The exchange of data between the representatives of the authorities referred to in point 20 in Coordination shall be carried out primarily through the national platform for collecting, analysing and sharing data on cyber threats and incidents referred to in Article 43. The Cyber Security Act, and other means of communication as defined in the Rules of Procedure, will be used as appropriate.

(77) The various public service media available shall be used to communicate with the public, in accordance with the means and requirements of crisis communication developed in the cyber crisis management plan referred to in Chapter 3.8.

4. National preparedness measures in the field of cyber crisis management

(78) National preparedness measures in the field of cyber crisis management shall be regulated as a set of related activities consisting of the following elements:

- increase national capabilities to detect and respond to cyber threats and incidents
- continuous analysis of the state of implementation and improvement of cybersecurity measures in the national environment and continuous situational reporting to decision-makers with a view to raising security awareness;
- monitor the effectiveness of the established cyber crisis management processes, taking into account lessons learnt from cyber crisis management exercises, previous cyber crisis resolution situations, analysis of the consequences of cyber crises and the scope and complexity of the activities undertaken to recover from the consequences of cyber crises;

- raising cybersecurity awareness at national level through comprehensive educational and information activities aimed at informing legal and natural persons about threats, risks and practices related to cyber crisis management.

(79) In order to support cyber crisis management activities and to continuously develop and increase Croatia's national cybersecurity capabilities and capacities, as well as to reduce the risk of a cyber crisis, it shall be implemented by:

- continuous cooperation and exchange of data between the competent authorities referred to in point 20 on cyber-threat spectrum in their area of competence;
- cooperation between the competent authorities referred to in point 20, in accordance with their respective competences, with the relevant international bodies;
- analysis of the data collected and preparation of situation reports by the competent authorities referred to in point 20, to support decision-making processes, develop security awareness and propose to improve cyber resilience measures;
- monitoring and assessing security risks in the deployment and use of emerging technologies in a national and global environment.

(80) In order to strengthen national preparedness in the field of cyber crisis management, Coordination shall undertake the following activities:

- during its regular working mode, hold quarterly sessions to exchange information and experience between the authorities and other stakeholders involved in Coordination's work;
- organise thematic lectures at Coordination meetings held by representatives of the bodies involved in Coordination's work or by representatives of other stakeholders;
- organise and conduct periodic preparedness reviews at the level of the institutions involved in Coordination's work and plan the implementation of national cyber crisis management exercises, which shall be duly included in the Cybersecurity Exercise Implementation Plan to be adopted every two years by the Government on a proposal from the Central State Authority for Cybersecurity, pursuant to Article 58. The Cyber Security Act.

(81) The competent authorities involved in the work of Coordination shall, within the scope of their competences, encourage, plan or implement appropriate activities with a view to raising their level of preparedness, by means of preparedness checks, education and awareness-raising in the entities for which they are responsible under the law establishing those bodies or under the competences conferred on them by other legislative and regulatory acts, in particular their competences deriving from the regulations governing cybersecurity.

5. National cyber crisis management exercises

(82) In order to achieve a maximum level of preparedness in the event of cyber crises, cyber crisis management exercises shall be carried out to verify available cybersecurity capacities and capabilities, to test established procedures and communication tools, as well as to share lessons learned, experience and best practices and to strengthen trust.

(83) Cyber crisis management exercises shall be identified, organised and conducted on the basis of the Cybersecurity Exercise Implementation Plan referred to in Article 58. The Cyber Security Act.

(84) Coordination shall address national needs in the field of cyber crisis management and propose that appropriate exercises be carried out in a national and/or international framework, with a view to including them in the Blueprint; conduct the cybersecurity exercises referred to in Article 58. Of the Cyber Security Act.

(85) Within each exercise carried out, Coordination shall analyse the lessons learned from

the participants in the exercise and propose appropriate training plans, the adaptation of organisational and other rules and policies, as well as the need to adapt or improve the technical and other capacities of the competent authorities at national level.

6. Coherence with the general national and cyber crisis management frameworks at EU level

6.1. Consistency with the general national crisis management framework

(86) Homeland security authorities shall provide KSUDOS with information within their scope that is relevant as indicators of the occurrence or rise of a security threat, or the occurrence of a crisis that may pose a risk to national security.

(87) In the event of a gradually emerging or sudden crisis, which poses a risk to national security, KSUDOS shall propose to the Government to declare the crisis, to establish a crisis management headquarters and how to respond to the crisis.

(88) The described general crisis management approach shall also be appropriately applied for cyber crisis management.

(89) Two levels of governance are involved in the response to the cyber crisis: operational, strategic and political levels. The operational level shall ensure that the necessary procedures are in place for the competent expertise and coordination of the work of the competent CSIRTs and CERT bodies, as well as for assessing the impact of cyber incidents and their trend, effectively linking technical information on a cyber incident with the potential to develop a cyber crisis incident and ensuring that it is presented in the form of impact and growth trends, which are required by the strategic and political level of national crisis management for the decision-making process on the activation of additional mechanisms established under the Homeland Security System.

Figure 1 Cyber crisis management levels

<table>
<tr><th colspan="2">Cyber crisis management levels</th></tr>
<tr><td>Strategic and political level</td><td>KSUDOS</td></tr>
<tr><td>National Security Council</td><td rowspan="2">  </td></tr>
<tr><td>Operational level</td></tr>
<tr><td colspan="2">SOA (NCSC-HR)

+ MUP, MORH, MZOM, UVNS, ZSIS, MPUDT, HAKOM, CARNET, HNB, HANFA, HACZ</td></tr>
</table>

6.2. Croatia's compliance with the cyber crisis management framework at EU level

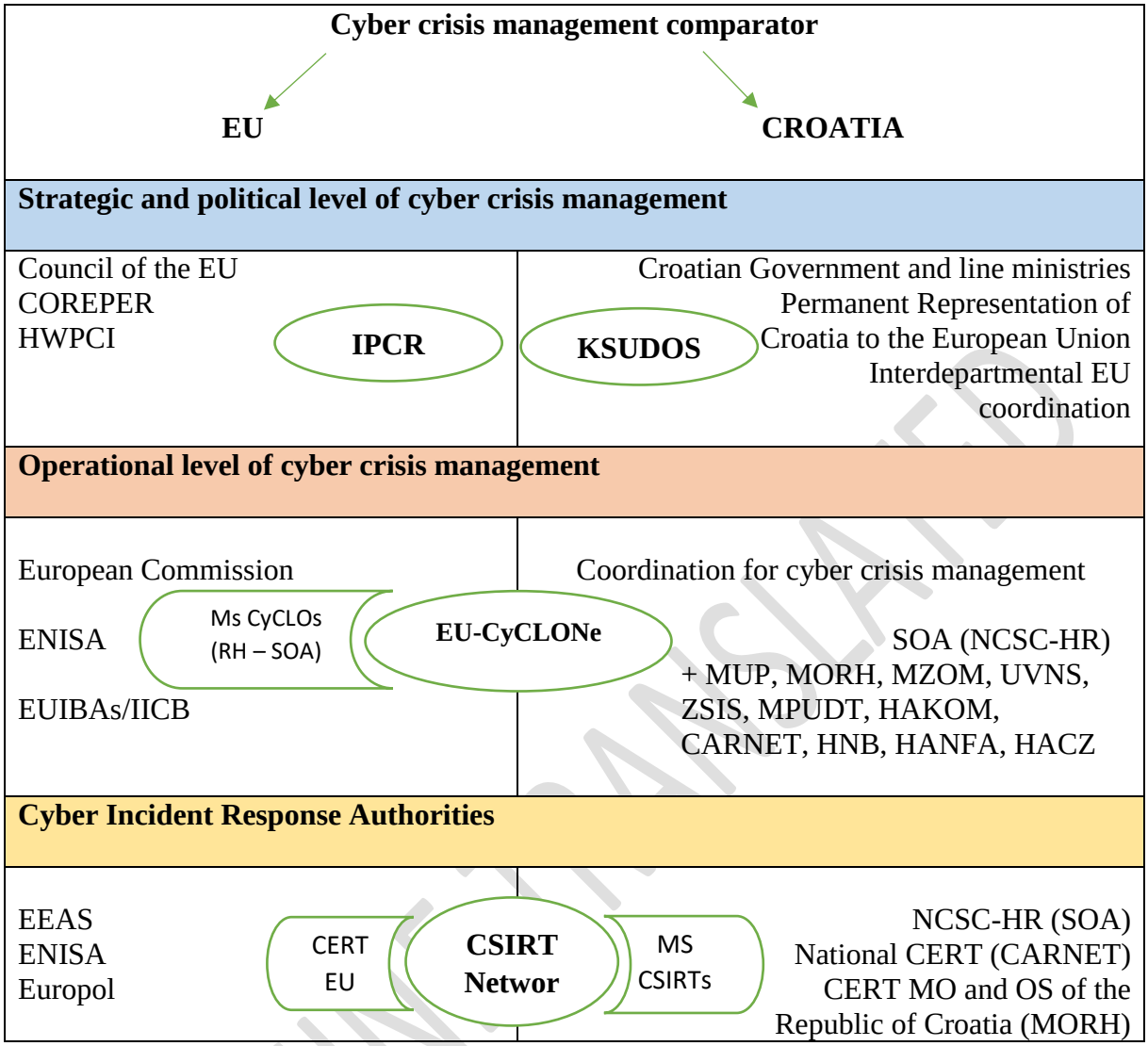
(90) The EU's objective on cyber crisis management is to establish:

- The EU-CyCLONe network as an operational level of governance to provide the necessary procedures for managing cyber crises and improving awareness of large-scale cyber incidents and cyber crises, as well as situational awareness raising;
- more effective coordination between a number of competent CSIRTs authorities, at EU and Member State level, through the use and exchange of globally collected data from relevant authorities of partner countries;
- mediation between the technical complexity of cyber incidents and the information required by the political level (IPCR), focused on the impact and development trends of incidents, ensured through the operational level of management.

(91) Croatia through the National Programme in a similar way:

- establish coordination at national level as an operational level of governance ensuring the necessary procedures for effective cyber crisis management, sharing relevant data and proposing and planning activities aimed at raising situational awareness of the potential scale and severity of cyber incidents;
- closely interlinks the competences set out in the Cybersecurity Act for national authorities in charge of the implementation of cybersecurity requirements, national authorities in charge of implementing specific laws and CSIRTs responsible for responding to cybersecurity incidents, as well as related competences of authorities under other laws, and through the use and sharing of relevant data, including globally collected data from relevant authorities of partner countries;
- it performs mediations between the technical complexity of cyber incidents and the needs of the political level, namely KSUDOS, which focus primarily on the impact and trends of cyber incidents, ensured through a new operational level of governance, namely the National Programme and Coordination.

Figure 2: Comparative overview of cyber crisis management at EU and Croatian level



6.3. Croatia's obligations towards the EU-CyCLONe network

(92) The SOP EU-CyCLONe is in the process of preparation and the EU Member States are expected to implement a cyber crisis management approach at national level that will provide support for coordinated cyber crisis management implemented at EU level, including active participation in the work of the EU-CyCLONe network.

(93) The SOA, as the body responsible for cyber crisis management in Croatia, informs the European Commission and the EU-CyCLONe without delay of the adoption of the National Programme and any amendments thereto, and, where appropriate, directs the work of Coordination and links it to the activities carried out within the EU-CyCLONe network.

7. ATTACHMENT

7.1. Taxonomy

(94) The taxonomy of cyber crisis descriptions shall be governed by a common vocabulary of terms that describe in a structured manner the results of the work of the incident handling authorities, namely the competent CSIRT and CERT bodies and the operational levels of cyber

crisis management. The objective of the taxonomy is to ensure that the results of the work are easier to understand and interpret each other when communicating between different stakeholders of a cyber crisis as well as between the operational level and the strategic and political levels of cyber crisis management.

(95) The taxonomy of cyber crisis descriptions aligns with existing national and EU cyber-incident taxonomies, which further facilitates the mutual exchange of information between actors dealing with cyber crises at national and international level.

(96) A structured description of the cyber crisis using the taxonomy of cyber crisis descriptions must include data on the assessment of the nature of the incident (cause, severity level) and the impact of the crisis stage (sectors affected, assessment of the level of impact and trend of crisis development).

(97) The crisis stage taxonomy shall be used at the operational level of cyber crisis management, for the purpose of mediation between the cyber incident response level and the strategic and political levels.

(98) The cyber crisis stage description taxonomy (Table 4) consists of two groups of descriptive terms covering the nature and impact of the crisis stage. The nature of the crisis stage shall be subdivided into: the root cause of the crisis (5 categories) and the level of severity of the crisis (3 levels). The impact of the crisis stage is divided into affected sectors (2 categories with sub-categories), an assessment of the level of impact on social and economic activities (4 levels) and an assessment of the trend of the evolution of the crisis situation (3 categories).

(99) Clarification of the terms:

1. *Nature of the crisis stage*

   Root cause[13]:

   i. *System cancellation*: denotes an incident that occurred due to a system failure, with no external influence (e.g. failure/switch failure, procedural defect or software error that triggered the incident).

   ii. *Natural disaster*: denotes an incident caused by a natural occurrence (e.g. storms, floods, earthquakes, fires, etc., which initiated the incident)

   iii. *Human error*: indicates an incident due to a human error (e.g. correct system used in wrong way, fault of the operator or negligence that caused the incident)

   iv. *Malicious activities*: indicates an incident caused by malignant activities (e.g. cyber or physical assault, vandalism, sabotage, attack from inside, theft, etc., which initiated the incident)

   v. *Cancellation of third party services*: means an incident resulting from a disruption of third party services (e.g. power supply interruption, internet blackout, etc., which are the cause of the incident).

   The severity level of a crisis state or security risk posed by a cyber-attack and/or an attacker shall be divided into three assessed[14] levels:

   i. *High,*

   ii. Medium,

   iii. *Low*.

[13] The categorisation of the root cause of a cyber crisis may sometimes change between the initial and the final situational report, i.e. during data collection and incident analysis.

[14] The assessment is carried out by the authority/level responsible for cyber crisis management

Level indicates the potential impact of the incident or the risk posed by the threat or attacker (for example, the severity level may be high if a strong storm occurs, a massive DDoS attack or a massive APT campaign of a sophisticated APT group is ongoing, or a widespread vulnerability that can be easily exploited is detected).

The factors to be taken into account when assessing the level of severity are:

- risk to capture new organisational entities, through likelihood of dissemination and potential impact
- additional effort or costs required for mitigation, protection or recovery purposes
- potential damage that could be caused by the threat
- speed of incident/threat spread
- whether the attacks are still ongoing;
- the degree of criticality of potentially exposed systems compromises
- feasibility or availability of solutions for protective measures or mitigation of threats
- the applicability of industry standards and good practices in mitigating threats.

2. *Impact of the crisis stage/sectors affected*

The impact in sectors identified by the Cybersecurity Act as high criticality and other critical sectors is qualified and quantified in the competent legal and regulatory acts and used in the assessments carried out by competent authorities for the purpose of cyber crisis management. The specific criteria necessary for the assessment under this taxonomy shall be developed in SOPs of the entities referred to in paragraph 20, taking into account the number and types of entities affected, the types of services affected, as well as the legally defined levels of significant impacts of incidents.

The sectors are divided into two groups with subsectors and types of entities:

i. *Sectors of high criticality*

ii. *Other critical sectors*

Sectors, subsectors and types of entities are defined in Annex I and Annex II. Of the Cybersecurity Act and listed in Table 4.

3. *The assessment of the level of impact on social and economic activities is divided into four assessed[15] levels:*

i. *Very strong impact;*

ii. *Strong influence;*

iii. *Low impact;*

iv. *None.*

Impact on social and economic activities means any impact on the physical world, society and economy, disruption at the level of the state or a major part of the state, such as raising the level of risk to the health or safety of citizens, the level of physical damage or financial cost, etc.

[15] The assessment shall be carried out by the authority/level responsible for cyber crisis management.

Factors to be taken into account when assessing the level of impact[16] are:

- risk to the health and safety of the population, for example through the impact of the incident on emergency services
- impact on economic activities, such as large financial losses
- damages and costs for citizens and entities affected by the incident
- disruption of daily life
- cascading effects on other critical sectors
- media influence and state coverage of media programmes
- political influence and significance.

4. *The assessment of the evolution of the crisis situation is divided into three estimated levels:*

    i. *Improving,*

    ii. No change,

    iii. *Deterioration*.

    The assessment of the further trend in the development of the incident shall be made in a short timeframe (e.g. next hours or days, depending on the type and characteristics of the cyber incident). The assessment includes the impact on the physical world, as well as the availability of electronic services, seen at the level of economic and societal activities that are adversely affected.

Table 4: *Cyber crisis stage taxonomy:*

1. Nature of the crisis stage
a. Root cause of the crisis stage
i. System failure
ii. Natural disaster
iii. Human error
iv. Malicious activity
v. Failure of a third party
b. Level of severity of the crisis state or security risk posed by the cyber-attack and/or attacker
i. High
ii. Middle
iii. Low
2. Impact of the crisis stage
a. Sectors affected
i. High criticality sectors/subsectors
a) Energy/Electricity, district heating and cooling, oil, gas, hydrogen

[16] In the event of a minor impact incident affecting a large number of organisations, an assessment should be made from the societal angle and an assessment of the severe impact on society as a whole should be considered, although the incident itself is of a lower impact at the individual level of the entities affected.

b) Transport/air, rail, waterborne, road

c) Banking

d) Financial market infrastructures

e) Healthcare

f) Water for human consumption

g) Waste water

h) Digital infrastructure/internet exchange centres, DNS services, register of national top-level online HR domain names, cloud computing, data centres, content delivery networks, trust services, public electronic communications networks, publicly available electronic communications services

i) ICT Service Management (B2B)

j) Public sector

k) Space

ii. Other critical sectors/subsectors

a) Postal and courier services

b) Waste management

c) Manufacture and distribution of chemicals

d) Food production, processing and distribution;

e) Manufacture of medical devices and in vitro diagnostic medical devices, manufacture of computers, electronic and optical devices, manufacture of electrical equipment, manufacture of machinery and apparatus n.e.c., manufacture of motor vehicles, trailers and semi-trailers, manufacture of other means of transport

f) Digital service providers

g) Research

h) Education system

b. Assessment of the level of impact for the economy and society

i. Very strong impact

ii. Strong impact

iii. To a limited extent

iv. No impact

c. Assessment of the evolution of the crisis situation

i. Improving

ii. No change

iii. Deterioration

(100) The Cyber Crisis Modification Taxonomy aims to ensure a better understanding and translation of the complex technical issue of the cyber domain into operational impact and situational state understandable to a wider range of cyber crisis resolution stakeholders, in particular strategic and political decision-making levels.

7.2. Use of TLP protocols for data sharing, confidentiality and data privacy

(101) The TLP Protocol is used for the purposes of data sharing in the implementation of the National Programme, which is widely spread across the global CERT Authority community and is an easy and easy-to-understand approach to limiting the distribution of individual operational data to end-users (further distribution of recipients).

(102) The base four levels of the TLP Protocol shall be used (https://www.first.org/tlp/), in addition to the possibility of using the additional parameter 'strict' for the level 'Amber', it has the following meaning for the purposes of the National Programme:

- **TLP:RED** TLP:RED **not for further exchange; limited to participants only** a specific meeting or meeting, members of Coordination or stakeholder representatives involved in addressing a specific cyber crisis. The code is used when additional recipients are unable to make effective use of the data, or when an extended list of recipients in case of abuse could affect privacy, reputation or some operational activities being carried out.
- **TLP:AMBER+STRICT** (TLP:AMBER+STRICT) — **onward sharing limited to employees of the stakeholders involved** cyber crisis management. The code shall be used when information requests support, such as one of the authorities referred to in point 20, or support to their representatives in Coordination. In so doing, sharing this information outside the organisations involved in cyber crisis management could carry privacy, reputational risks or risks to the implementation of some operational activities.
- **TLP:AMBER** TLP:AMBER **onward sharing restricted exclusively to the employees of the organisations involved and the clients of that organisation;**. The label shall be used when the information is to be provided to the authorities referred to in point 20, as well as to clients in the area of their responsibility, such as for the potential development of a cyber crisis, for the purpose of preventive activities or verifications. At the same time, sharing more broadly could carry a risk of privacy, reputation, or a risk to the implementation of some operational activities.
- **TLP:GREEN** TLP:GREEN **onward sharing limited to the community of organisations** which stakeholders are involved in addressing the cyber crisis in the plan, i.e. that have been assessed as organisations that may be directly affected by the incident. **Recipientsmay carry out further exchanges** TLP:GREEN data within their sector or community that may be affected by the incident but cannot publicly disclose the data.
- **TLP:CLEAR** (TLP:CLEAR) — **No further exchange is restricted**it is used for data with minimal or no risk of misuse, and data is subject to the usual rules and procedures for use by recipients and for public disclosure.

The use of additional parameters under the TLP Protocol, depending on the needs of Coordination, will be defined in the Rules of Procedure.

(103) Where classified information is generated or used in the implementation of cyber crisis management or where personal data are processed, specific regulations on their protection or labelling shall apply to such information.

(104) The authorities referred to in point 20 shall be responsible, in accordance with their respective competences, for assessing the classification level of classified information exchanged with other competent authorities referred to in point 20 or provided to other stakeholders in addressing a cyber crisis. The exchange of classified information may take place only between receiving authorities which are eligible for handling classified information at a given security classification level.

7.3. Requirements for forms

(105) The forms used under the National Programme are: cyber crisis management plan template situation report forms and an escalation proposal form.

(106) The template for the cyber crisis management plan shall contain, in essence: a description of the cyber crisis management plan, a description of the cyber crisis state and affected entities, the cyber crisis resolution stakeholders and their tasks, the cyber crisis resolution plan, possible mitigation measures, the measures to recover from the cyber crisis and the need for and plan to inform the public.

(107) The Situation Report forms are broken down into: periodic situational report (regular operation), warning situational report (warning mode), and crisis situation report (crisis mode). Depending on the intended purpose, these forms contain summaries, observations, justifications of escalation procedures, taxonomy of status descriptions and detailed descriptions of the situation.

(108) The model proposal for escalation essentially contains: the name of the authorities proposing an escalation, a description of the situation giving rise to the request for escalation, an indicative statistical overview of the entities affected by the cyber incidents, the measures taken prior to the escalation proposal to respond to the cybersecurity incident, the statement of agreement of the head of the competent authority and the competent CSIRT of the proposed escalation authority.

(109) The model of the cyber crisis management plan, the layout reports forms and the escalation proposal form shall be laid down in the Rules of Procedure referred to in point 27.