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

Contents:

List of acronyms:

No.	Acronym	Full title
1.	CARNET	Croatian Academic and Research Network
2.	EU	European Union
3.	EU-CyCLONe	EU Cyber Crisis Liaison Organisation Network
4.	CCAA	Croatian Civil Aviation Agency
5.	HAKOM	Croatian Regulatory Authority 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
10.	MO	Ministry of Defence
11.	MJPADT	Ministry of Justice, Public Administration and Digital Transformation
12.	MI	Ministry of the Interior
13.	MSEY	Ministry of Science, Education and Youth
14.	National CERT	CERT/CSIRT body established within CARNET
15.	NCSC-HR	National Cyber Security Centre (established within the framework of SOA Security and Intelligence Agency)
16.	RH	The Republic of Croatia
17.	SOA	Security and Intelligence Agency
18.	SOP	Standard operative procedures
19.	TLP	Traffic Light Protocol
20.	UVNS	Office of the National Security Council
21.	CERT MO and OS RH	CERT of the Ministry of Defence and the Armed Forces of the Republic of Croatia
22.	VSOA	Military Security and Intelligence Agency
23.	ZSIS	Information System Security Bureau

Glossary

(1) **CSIRT** is the acronym for the Computer Security Incident Response Team, the competemnt authority for the prevention and protection from cybernetic incidents, also known under the abbreviation CERT (Computer Emergency Response Team)

(2) **CSIRT network** (CNW network) is a network of national CSIRTs established for the purpose of developing trust and confidence as well as promoting swift and efficient operational cooperation among EU Member States, composed of, apart from representatives of national CSIRTs, representatives of the competent authority of the European Union for the prevention and protection against cybersecurity incidents (CERT-EU), and the European Union Agency for Cybersecurity (ENISA)

(3) **Escalation** is a procedure carried out with the aim of changing the method of managing a cyber crisis and involving all necessary crisis management stakeholders

(4) **EU-CyCLONe network** is the European Cyber Crisis Liaison Organisation Network, established with the aim of operating at the operational level as an intermediary between the authorities responsible for handling cyber incidents (the CNW network) and the political level, in order to create an effective process for operational assessment and management during large-scale cybersecurity incidents and cyber crises, as well as to support decision-making processes on complex cybersecurity issues at the strategic and political levels.

(5) **ICT** is information and communication technology

(6) **A cyber incident** is an event that compromises the availability, authenticity, integrity, or confidentiality of data that is stored, transmitted, or processed, or of services provided by or accessible through network and information systems

(7) **A large-scale cybersecurity incident** is an incident at the level of the European Union which causes disruptions that exceed a Member State's capacity to respond to it or which has a significant impact on at least two Member States, as well as an incident at the national level which causes disruptions that exceed the capacity of a sector CSIRT body to respond to it or which has a significant impact on at least two sectors, and in those cases cyber crisis management procedures are started in accordance with the existing national general crisis management framework and the European Union cyber crisis management framework

(8) **A cyber crisis** is a situation that may arise in modern society due to a high level of dependence on network and information systems, whereby an increasing number of incidents and attacks can cause serious disruptions in social, political, and economic terms, thereby affecting the safety of individuals, the democratic system, political stability, the economy, the environment, and other national values – in other words, the overall national security of the Republic of Croatia

(9) **Competent CSIRT or CERT authories** are NCSC-HR, the National CERT, and the CERT of the Ministry of Defence and the Armed Forces of the Republic of Croatia.

1. Introduction

The adoption of specific implementing acts that elaborate all key issues related to the management of large-scale cybersecurity incidents and cyber crises (hereinafter: cyber crisis management) reflects the need for a systematic approach to the area of cyber crisis management, which has been recognised at the level of European Union.

The obligation to adopt national plans or programmes for responding to cyber crises is established by the NIS2 Directive [1]. The NIS2 Directive explicitly sets out the issues that such plans or programmes should regulate in more detail and imposes an obligation on EU Member States to notify the European Commission and the EU-CyCLONe network of their adoption, as well as of any amendments or the adoption of new programmes, including the name of the authority designated in the Member State as the authority competent for cyber crisis management.

The NIS2 Directive has been transposed into Croatian legislation by the Cybersecurity Act (Official Gazette14/24[2]), which also serves as the national legislative framework for cyber crisis management.

Alongside the Cybersecurity Act, the adoption of the National Cyber Crisis Management Programme (hereinafter: The National Programme) provides a comprehensive framework for the cyber crisis management system in the Republic of Croatia.

Pursuant to Article 56, paragraph 2 of the Cybersecurity Act, the National Programme is adopted by the Government of the Republic of Croatia (hereinafter: The Government) upon the proposal of the Security and Intelligence Agency (SOA), as the authority responsible for cyber crisis management.

In accordance with the requirements of Article 9 of the NIS2 Directive, Article 56, paragraph 3 of the Cybersecurity Act stipulates that the National Programme shall describe the capacities, resources, and procedures for cyber crisis management and shall further define the following:

- the objectives of cyber crisis management, including the objectives for the development of national preparedness measures, as well as alignment with the EU cyber crisis management framework
- coherency with the national general framework for crisis management
- measures and activities for strengthening national preparedness
- a plan for the implementation of national preparedness measures, including a training activity plan and the conduct of exercises, which are an integral part of the cybersecurity exercise plan referred to in Article 58 of the Cybersecurity Act
- the tasks and responsibilities of the bodies involved in cyber crisis management
- the role of the public and private sectors and the infrastructures critical for management during cyber crises, as well as
- national procedures and coordination at the national level necessary to ensure support for coordinated cyber crisis management carried out at the EU level and the effective participation of the Republic of Croatia in such management.

Managing cybercrises is a very importand and complex segment of national crisis management for which the adoption of a separate legislative act focused exclusively on cyber crises is envisaged, due to their unique nature and characteristics that differ significantly from other types of crises in the physical realm.

However, when developing a separate framework for cyber crisis management, it is necessary to take into account that the management system established by the National Programme is also an integral part of the national crisis management system within the homeland security system, established by the Homeland Security System Act (Official Gazette 108/17), with the National

[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] Entred into force on 15 February 2024.

Security Council as the central authority of the homeland security system and the Coordination for the Homeland Security System (hereinafter: CHSS) as the operational implementing authority.

Recognising that contemporary crises often impact multiple areas simultaneously, the Homeland Security System Act has created conditions for the systematic, coordinated, effective, and rational inclusion of all relevant state and societal resources in security risk management activities, including crisis management. It thereby ensures the prerequisites for guiding and coordinating the actions of the authorities within the homeland security system[3] in all conditions and from every aspect of security risk management, including crisis management, regardless of the area in which the crisis originates.

Therefore, the National Programme must ensure the establishment and development of a cyber crisis management system that complies with all relevant national regulations related to the cybersecurity risk management measures and the handling of cyber incidents, as well as with the aforementioned legal framework establishing the homeland security system and defining the framework for making strategic decisions and coordinating the actions of all relevant stakeholders in emergency and crisis situations that pose a risk to national security, regardless of their cause.

The purpose of adopting the National Programme is to provide organisational frameworks for a timely and coordinated implementation of operational procedures applied to prevent and resolve cyber crises, by introducing a new operational level of national coordination in cyber crisis management issues. This should be done while ensuring that the National Programme does not alter the competences of the involved authorities as established by the laws under which they were founded, nor the competences arising for these authorities from other laws and secondary legislation, and does not affect the implementation of other procedures and mechanisms that, according to special regulations, apply in cases where a crisis impacts the foreign, security, or defence policy of the Republic of Croatia.

The objective of introducing an operational level of cyber crisis management is to provide a framework for monitoring and coordinating the work of all authorities competent for responding to cyber incidents at the technical level, as well as to enable their more effective connection with other competent authorities that have tasks and responsibilities crucial for operational action in the event that a cyber incident escalates into a large-scale cyber incident or cyber crisis and, ultimately, with the strategic and political levels responsible for making decisions on managing security risks important to national security and crisis response, in accordance with the roles and responsibilities established within the homeland security system.

Authorities responsible for responding to cyber incidents at the technical level are those that, within their regular competences and duties, handle cyber incidents across various sectors, namely NCSC-HR, the National CERT, and the CERT of the Ministry of Defence and the Armed Forces of the Republic of Croatia.

In cases of large-scale cybersecurity incidents and cyber crises, authorties responsible for dealing with cyber incidents must operate in close coordination with the authorities responsible for enforcing cybersecurity requirements and the authorities responsible for implementing special acts, according to their competences established by the Cybersecurity Act.

Additionally, state administration authorities play a very important role in the operational management of cyber crises, given the sectoral competences assigned to them by special acts.

[3] The homeland security system comprises the resources of internal affairs, defence, the security and intelligence system, civil protection, firefighting, foreign affairs services, as well as other authorities that systematically and coordinately perform duties and tasks related to the identification, assessment, reduction, and/or elimination of security risks important to the national security of the Republic of Croatia.

The strategic and political level, in terms of the National Programme, consists of the existing general crisis management mechanisms established by the Homeland Security System Act, which are implemented through the National Security Council and the Coordination for the Homeland Security System (CHSS).

With the introduction of the Coordination for Cyber Crisis Management (hereinafter: The Coordination) as a new operational level of cyber crisis management, the National Programme establishes a national mechanism for cyber crisis management, based on the need to:

- strengthen capacities for timely detection of cyber threars and inicidents
- analyse and understand the full spectrum of various cyber threaths as well as global cybersecurity trends
- direct and align national processes and activities with international frameworks, and strengthen international cooperation in the field of cybersecurity
- use all existing capacities of the authorities involved in the management of cyber crises at the operational level
- use mechanisms established through the work of the Coordination for the Homeland Security System (CHSS) and the National Security Council for making strategic and political decisions
- ensure mechanisms for information sharing during a cyber crisis and mechanisms for effective coordination of the stakeholders involved in resolving the cyber crisis
- ensure all necessary resources and coordination required for the fastest possible recovery of infrastructure of national interest
- ensure a high level of awareness of large-scale cybersecurity incidents and cyber crises, and improve the understanding of the complex technical issues in the field of cybersecurity through the preparation of situational reports and other reporting documents comprehensible to the strategic and political levels responsible for decision-making.

2. General cisis management frameworks

2.1. EU legislation

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

(2) For this purpose, in 2006 the Council of the European Union adopted the Arrangements for Coordinating Responses to Emergency and Crisis Situations, which served until 2013 as a platform for information exchange and coordination of action among EU Member States. Pursuant to these Arrangements, the Integrated Political Crisis Response (IPCR) arrangements were adopted in 2013 (hereinafter: IPCR).

(3) In the event of a crisis, the IPCR encourages the swift and coordinated adoption of joint decisions at the political level in order to restore stability within the EU as quickly as possible. This enhanced crisis response mechanism involves EU institutions, affected EU Member States, and other stakeholders. The mechanism offers several advantages over the initial arrangements, such as greater flexibility, enhanced scalability, and improved utilisation of existing resources.

(4) The aforementioned arrangements were legally codified in 2018 by a Council Implementing Decision (EU)[4].

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

(5) One of the greatest threats to the internal security of the EU are undoubtedly cyber risks, which pose a significant danger of triggering crises at the EU level. For this reason, in 2020, the establishment of a new level of cyber crisis management began — the EU-CyCLONe network — which was formally established in early 2023 with the entry into force of the NIS2 Directive.

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

2.2. National legislation

(7) For the purpose of systematically managing security risks relevant to national security and responding to crises, the Homeland Security System has been established in the Republic of Croatia.

(8) The Homeland Security System consists of the resources of internal affairs, defence, the security and intelligence system, civil protection, environmental protection, health, finance, judiciary, fire services, the foreign service, and other bodies that perform tasks and duties in an organised and coordinated manner aimed at identifying, assessing, reducing and/or eliminating security risks relevant to national security.

(9) The central body of the Homeland Security System is the National Security Council, which considers and assesses security threats and risks, and adopts guidelines, decisions, and conclusions on how to protect and realise national security interests. The Coordination for the Homeland Security System (CHSS) is responsible for aligning and coordinating the work of the Homeland Security System.

(10) An important segment of national crisis management are the procedures for managing cyber crises, which will ensure a rapid and effective response to large-scale cybersecurity incidents that, depending on their cause and impact, can quickly spread and escalate into a large-scale cyber crisis and its consequences. Therefore, the National Programme introduces and elaborates a cyber crisis management model that will include preventive measures, measures to raise national preparedness, and clear frameworks for coordinated action in real time in the event of a cyber crisis, encompassing not only the resolution of the cyber crisis but also ensuring a rapid recovery from its consequences.

(11) Raising awareness of the the regulatory framework in the field of cybersecurity, organisational centralisation, and the promotion of educational programmes development in this area began in Croatia with the adoption of the National Cybersecurity Strategy (Official Gazette 108/15) and continued with the adoption of the Act on Cybersecurity of Operators of Essential Services and Digital Service Providers[5], and the accompanying regulation[6] in 2018, as transposition legislation for the NIS1 Directive[7], and were were further developed through the transposition of the NIS2 Directive into national legislation and the implementation of the NIS2 transposition law – the Cybersecurity Act.

(12) Pursuant to the National Cybersecurity Strategy, the National Cybersecurity Council was established in 2016 as an interdepartmental body to monitor the implementation of the Strategy, propose its amendments, and, among other tasks, consider issues crucial for managing cyber crises and propose measures to enhance effectiveness. In late 2019, the National Cybersecurity Council defined the area of "Cyber Crisis Management" as one of the key areas

[5] Official Gazette 64/18.
[6] Official Gazette 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).

that needed to be conceptually developed within the revision and update of the 2015 National Cybersecurity Strategy.

(13) Since 2020, the National Cybersecurity Council has reached a consensus on the need for Croatia's active participation in the work of the EU-CyCLONe network, and SOA has been designated as Croatia's representative in the EU-CyCLONe network.

(14) Croatia's approach to managing cyber crises has been aligned over the past years with the approach developed within the EU through the establishment and gradual definition of the operational framework of the EU-CyCLONe network. The National Programme continues to align national cyber crisis management frameworks with the cyber crisis management frameworks formally established at the EU level by the NIS2 Directive.

(15) The National Programme ensures the coordinated implementation of activities by all competent authorities in the area of cybersecurity and more effective linking of the authorities responsible for responding to cyber incidents with the strategic and political level. This is ultimately the purpose of the new operational level of cyber crisis management established by the NIS2 Directive through the functioning of the EU-CyCLONe network, as well as the definition of cooperation mechanisms between the EU-CyCLONe network and other stakeholders involved in cyber crisis management at the EU level.

3. Managing cybersecurity crises in the Republic of Croatia

3.1. Objectives and principles in management of cybersecurity crises

(16) The cyber crisis management system is established with the aim of:

- effective response to cyber crises and resolution of the consequences of cyber crises
- operational coordination and harmonised work of all authorities competent for cybersecurity, thereby establishing a national capability to monitor and analyse the full spectrum of cyber threats and enabling appropriate threat assessment and situational reporting to decision-makers
- ensuring the effective and coordinated use of all existing resources, as well as the further development of the capabilities and capacities of the involved authorities
- ensuring the use of a unified taxonomy in monitoring risks that may lead to a cyber crisis
- defining the framework for participation and cooperation between the public and private sectors in strengthening Croatia's cyber resilience.

(17) Cyber crisis management procedures ensure the coordinated actions of the competent authorities in managing cyber crises and adhere to the principles of:

- proportionality, in terms of aligning the level of response to 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 location of occurrence of each individual cyber incident that may lead to or has led to a cyber crisis
- complementarity, in terms of the use of available and legally prescribed instruments that mutually complement each other through sectoral, national, and international frameworks
- confidentiality, in terms of mutual informing of stakeholders involved in crisis resolution and informing the public, considering all requirements that must be

respected regarding legally protected categories of data, which, among other things, include the use of secure and resilient communication and information infrastructure for information exchange, as well as protocols for their further exchange within and outside the authorities involved in managing the cyber crisis.

3.2. Scope of application

(18) Cyber crisis management encompasses the monitoring of the full spectrum of cyber threats with the aim of preventing, resolving, and recovering from cyber incidents that may cause significant disruptions in the Republic of Croatia, as well as trigger a cyber crisis with potential cross-border spillover effects. It also aims to identify and prevent all types of cyber threats that could be a potential current or future source of cyber crises.

(19) Within the scope of monitoring the full spectrum of cyber threats, special attention is given to state-sponsored cyberattacks and APT (Advanced Persistent Threat) campaigns[8], which pose a high risk of triggering a cyber crisis, particularly in the public sector and in the area of national critical infrastructure, as well as in other high-criticality sectors defined by the Cybersecurity Act. Special attention is also directed towards all other large-scale cybersecurity incidents.

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

(20) The authorities primarily competent for the implementation of the National Programme are:

- The Security and Intelligence Agency (SOA), as the central state authority for cybersecurity, the body responsible for cyber crisis management, the competent authority for implementing cybersecurity requirements across a total of 14 sectors[9], and the designated CSIRT authority for 16 sectors[10]. These tasks are carried out by SOA through the NCSC-HR (National Cyber Security Centre – Croatia).
- The National Security Council (UVNS), as the central state authority for information security and the competent authority responsible for implementing cybersecurity requirements for the public sector.
- The Ministry of Science, Education, and Youth (MSEY), as a state administration body responsible for science and education, and the competent authority for implementing cybersecurity requirements for the research sector, the education system sector, and the registry of top-level national internet domain names within the digital infrastructure sector.
- The Ministry of Physical Planning, Construction and State Assets (MPPCSA), as a state administration body responsible for the development of the digital society, and the

[8] An APT (Advanced Persistent Threat) campaign is a type of cyberattack characterised by a high level of expertise and stealth on the part of the attacker over an extended period, with the ultimate goal of stealing confidential information, extortion, or causing damage.

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

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

competent authority for implementing cybersecurity requirements for trust service providers within the digital infrastructure sector.

- HAKOM, as the competent regulatory authority for the electronic communications sector, postal services, as well as railway services and passenger rights in railway transport, and the competent authority for implementing cybersecurity requirements for providers of public electronic communications networks and providers of publicly available electronic communications services within the digital infrastructure sector.
- CARNET, as the competent authority for the prevention of and protection against cyber threats to public information systems in the Republic of Croatia, also serves as the designated CSIRT authority for five sectors[11]. These tasks of CARNET are carried out by the National CERT.
- The State Centre for Information Security (ZSIS), as the central state authority responsible for performing tasks in the technical areas of information security, and the authority competent for cybersecurity certification and for conducting cybersecurity audits in state administration bodies and other state institutions.
- The Ministry of the Interior (MI), as a state administrative body responsible for combating cybercrime.
- The Ministry of Defence (MOD), the Croatian Armed Forces (OS RH), and the Military Security and Intelligence Agency (VSOA) as the auhorities responsible for the defence sector, the cyberspace domain of military cyber operations, and for performing the tasks of the Ministry of Defence and Armed Forces CERT.
- The Croatian National Bank (CNB) as the competent authority for the enforcement of special laws in the banking sector.
- The Croatian Financial Services Supervisory Agency (HANFA) as the competent authority for the enforcement of special acts in the financial market infrastructure sector.
- The Croatian Civil Aviation Agency (CCAA) as the competent authority for the enforcement of special acts in the air traffic subsector (transport sector).

(21) In addition to the primary competent authorities referred to in item 20, in the activities of the Coordination, regardless of its mode of operation, other stakeholders may be involved for the purpose of coordination, prevention, education, conducting cybersecurity exercises, or resolving a cyber crisis, based on the assessment of the body responsible for cyber crisis management and depending on the operational needs of the Coordination:

- state administrative bodies, other state authorities and legal entities with public powers, as well as local and regional self-government units
- representatives of the private sector or other professional associations representing the private sector in a broader sense, which, through the public-private partnership process, enable the inclusion of relevant private sector representatives in the national cyber crisis management process
- entities from the academic and research sector for the purpose of conducting educational activities, adapting existing and developing new educational programmes, as well as developing advanced technologies and tools in the field of cybersecurity
- key entities, important entities, and entities that are not categorised as key or important but implement voluntary cybersecurity protection mechanisms under the Cybersecurity Act.

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

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

(22) The Coordination is an interdepartmental authority responsible for the operational level of cyber crisis management, composed of representatives of the authorities listed in item 20.

(23) Each authority referred to in item 20 shall appoint its representatives – a member and a deputy member – to the Coordination, who are authorised to represent their respective bodies in activities falling within the scope of the National Programme.

(24) Other stakeholders referred to in item 21 may, as necessary and particularly in the case of thematically related discussions or information exchange, be included in the work of the Coordination during its regular mode of operation.

(25) During the application of the escalation procedure, the implementation of coordinated activities to resolve an ongoing crisis situation, public communication, or the recovery and mitigation of the consequences of large-scale cyber incidents or cyber crises, in addition to the stakeholders from item 21, representatives of other public sector bodies or private sector legal entities affected by the cyber crisis in question, or those who, due to their capabilities and available resources, can support the Coordination's activities, may be involved as needed in the work of the Coordination.

(26) A representative of NCSC-HR chairs and organises the work of the Coordination, and NCSC-HR provides expert and administrative support.

(27) The Coordination shall adopt the Rules of Procedure governing in more detail its organisation and manner of operation (hereinafter: The Rules).

(28) The Rules shall, considering the need for effective implementation of the requirements of the National Programme, prescribe the rules for convening meetings of the Coordination, the working methods during its meetings, and the procedures for escalation and de-escalation. The Rules shall also regulate matters essential for decision-making within the Coordination, including the decision-making process itself, as well as all necessary procedures and preconditions that must be met when decisions are made and Coordination's activities are implemented that involve handling classified information. Furthermore, the Rules shall define in more detail the rules of procedure concerning the inclusion of other stakeholders from item 21 in the work of the Coordination and the implementation of activities under items 24 and 25.

(29) Only representatives of the authorities referred to in item 20 who meet the necessary requirements for the use of classified data, specifically with regard to the availability of appropriate physical premises, classified network and information systems, and access certificates for classified data issued to the appointed representatives, may participate in the activities of the Coordination involving such data.

(30) The Rules shall be used solely for the official use of the competent authorities listed in item 20 and their representatives involved in the work of the Coordination. They will not be published but may, if necessary, be made available for inspection by other stakeholders referred to in item 21 for the purpose of their participation in the work of the Coordination.

(31) All the authorities participating in the work of the Coordination are obliged to adhere to appropriate procedures for data exchange, such as the TLP protocol as explained in Annex 7.2, as well as rules on the handling of classified or other types of data that are subject to specific regulations for the protection of their secrecy or confidentiality.

3.5. Levels of cyber crisis management

(32) The levels of cyber crisis management are the operational level and the strategic and political level[12].

(33) For the purpose of systematic cyber crisis management, the National Programme establishes the operational level of cyber crisis management to ensure better coordination among all authorities with competences in the field of cybersecurity and to enable more effective communication of circumstances relevant to strategic decision-making to the strategic and political level.

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

- coordinated resolution of cyber crises,
- mutual exchange of relevant data between stakeholders involved in resolving cyber crises,
- appropriate public communication.

3.5.1. Operational level of cyber crisis management

(35) The operational level of cyber crisis management refers to the management of cyber crises at the level of the Coordination.

(36) The operational level of cyber crisis management is engaged in the resolution of large-scale cyber incidents based on a proposal to escalate the status from the regular mode of operation of the Coordination to the warning mode or crisis mode, in accordance with the procedures described in sections 3.7.2 and 3.7.3.

(37) The scope of cyber crisis management at the operational level includes:

- resolving the cyber crisis at the national level through coordinated cooperation of all bodies responsible for handling cyber incidents and involving all other stakeholders relevant for effective crisis resolution, including internal teams of affected entities responsible for prevention and protection against cyber incidents,
- participation in resolving cyber crises at the international level that may affect or are affecting the Republic of Croatia,
- considering and activating available EU and other international assistance mechanisms,
- mutual exchange of data between all stakeholders involved in resolving the cyber crisis at the operational level,
- informing the strategic and political level,
- coordination of activities related to public communication, i.e., establishing an appropriate method 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 the operational to the strategic and political level is primarily carried out with the aim of recovery from the cyber crisis and mitigation of its consequences.

(40) Escalation to the strategic and political level is also carried out for the purpose of establishing appropriate crisis communication with the public, particularly to activate additional

[12] The strategic and political level, within the meaning of this National Programme, consists of the National Security Council, KSUDOS, and the Office of the National Security Council (UVNS).

resources and mechanisms for recovery from the cyber crisis, especially regarding its consequences in physical space and physical resources, while the actual resolution of the cyber crisis in the cyber domain is primarily conducted at the operational level.

(41) The scope of cyber crisis management at the strategic and political level is proposed through the cyber crisis management plan and includes the following activities of the Coordination for the Homeland Security System:

- strategic communication activities with the public,
- making strategic decisions during the recovery phase from the cyber crisis, especially regarding physical space and resources,
- considering and proposing to the Government appropriate additional measures and methods of response to the cyber crisis.

3.6. Criteria for confirming a cyber crisis situation and escalating crisis management to a higher level

(42) Criteria for confirming a cyber crisis situation may be general or specific, whereby escalation to the operational level is primarily carried out for the purpose of resolving the cyber crisis, in accordance with part 3.5.1, and escalation from the operational to the strategic and political level is primarily for the purpose of recovery from the cyber crisis and mitigation of its consequences, in accordance with part 3.5.2.

(43) General criteria for confirming a cyber crisis situation and escalating to the operational level represent circumstances that cause the inability to resolve a cyber incident by applying regular activities of the directly competent CSIRT or CERT authority referred to in item 20.

(44) The inability to resolve the cyber incident from item 43 may result from the complexity, sophistication, or scope of the cyber incident, which therefore exceeds the competence or surpasses the capacities and capabilities of a single directly competent CSIRT or CERT authority in the affected sector or type of entity. This is determined based on a joint assessment of the competent CSIRT or CERT authority and the authorities listed in item 20, or another central authority competent for the sector affected by the cyber incident.

(45) General and specific criteria for confirming a cyber crisis situation are established by the SOPs of each competent authority from item 20, according to the specificities of the individual sectors. These criteria are preliminarily harmonised within the Coordination.

(46) The SOPs elaborate the general criteria for confirming a cyber crisis situation in the sense of item 44, as well as specific criteria regarding possible threshold determinations for qualification and quantification of individual elements relevant for confirming the cyber crisis situation, such as sector, subsector, types of entities, and number of affected entities, services, and sensitive data impacted by the cyber incident, as well as criteria related to the assessment of the development trend of the cyber crisis and the assessment of the level of impact of the cyber crisis on society as a whole. In doing so, a harmonised and coordinated approach is ensured in incident handling, to be carried out by the competent CSIRT or CERT authority in coordination with the competent sectoral authority and in accordance with the distribution of competences under Annex III of the Cybersecurity Act or other relevant sectoral regulations.

(47) When elaborating general and specific criteria for confirming a cyber crisis situation, the taxonomy referred to in Annex 7.1 shall be used.

3.7. Standard operating procedures (SOPs) of the Coordination for cyber crisis management and competent authorities in cyber crisis management

(48) To ensure the implementation of all key activities, this chapter defines the standard operating procedures of the Coordination and introduces three modes of its operation that guarantee the continuous execution of activities by all competent authorities referred to in item 20 in managing cyber crises.

(49) The three modes of operation of the Coordination, clearly presented in Tables 1, 2, and 3, are:

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

Table 1*: Overview of the main activities and outcomes of the Coordination's work in the* ***regular mode of operation*** *of the competent authorities from item 20 in cyber crisis management:*

Main activities:	**Preparedness**	**Situational awareness**	**Cooperation in cyber crisis management planning**	**Cyber crisis management and decision-making**
Regular mode of operation:	- development, permanent alignment, and improvement of SOPs of the competent authorities referred to in item 20 - establishment, maintenance, and continuous development of cyber capabilities and capacities - raising security awareness and continuous education of entities - continuous assessment of the cybersecurity status - prompt reporting to other representatives in the Coordination of all significant and media-covered cyber incidents - continuous monitoring of international trends in cyber crisis management and proposing national	- quarterly exchange of situational reports from all competent authorities referred to in item 20	- regular meetings of the Coordination	- regular annual situational briefing for the strategic and political level

	development measures to the Coordination			

***Table 2**: Overview of the main activities and outcomes of the Coordination's work in the **warning mode of operation** of the competent authorities from item 20 in cyber crisis management:*

Main activities:	**Preparedness**	**Situational awareness**	**Cooperation in cyber crisis management planning**	**Cyber crisis management and decision-making**
Warning mode of operation:	-	- proposal for escalation with justification and preparation of a warning situational report (initial, transitional, final) – by the competent authority and the competent CSIRT referred to in item 20 (escalation initiators) and submission to NCSC-HR - NCSC-HR consultations with the escalation initiators - preparation of a warning situational report by other competent authorities referred to in item 20 (initial, transitional, final)	- extraordinary coordination and alignment at the operational level - preparation of a warning situational report at the operational level (initial, transitional, final) for the strategic and political level - escalation and de-escalation upon the proposal of the competent authority and the competent CSIRT referred to in item 20 (initiators of escalation or de-escalation)	- extraordinary briefing for the strategic and political level

Table 3: *Overview of the main activities and outcomes of the Coordination's work in the* ***crisis mode of operation*** *of the competent authorities from item 20 in cyber crisis management:*

Main activities:	**Preparedness**	**Situational awareness**	**Cooperation in cyber crisis management planning**	**Cyber crisis management and decision-making**
Crisis mode of operation:	-	- proposal for escalation with justification and preparation of a crisis situational report (initial, transitional, final) – by the competent authority and the competent CSIRT referred to in item 20 (escalation initiators) and submission to NCSC-HR - NCSC-HR consultations with the escalation initiators - preparation of a crisis situational report by other competent authorities referred to in item 20 (initial, transitional, final)	- crisis coordination at the operational level - preparation of a cyber crisis management plan (escalation initiator, NCSC-HR, and Coordination for Cyber Crisis Management) - preparation of a crisis situational report at the operational level (initial, transitional, final) (escalation initiator, NCSC-HR, and Coordination for Cyber Crisis Management) - escalation and de-escalation upon the proposal of the competent authority and the competent CSIRT referred to in item 20 (initiators of escalation or de-escalation)	- crisis management at the operational level through the implementation of an agreed cyber crisis management plan - crisis coordination at the operational level as well as the strategic and political level

3.7.1. Regular mode of operation

(50) Within the framework of the regular mode of operation of the Coordination, mutual coordination of the stakeholders concerned and the continuous monitoring of the state of cybersecurity shall be ensured, whereby the competent authorities referred to in item 20, within the scope of their competences, shall, on an ongoing basis, evaluate and enhance the SOPs. The other stakeholders referred to in item 21 shall, where necessary, participate in the work of the Coordination and shall continuously evaluate and enhance the measures for the management of cybersecurity risks which they implement with a view to ensuring the continuity of their operations and the management of cybersecurity crises, in compliance with the framework established pursuant to Article 30, paragraph 1, indent 3 of the Cybersecurity Act or with similar cybersecurity measures implemented pursuant to other obligations.

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

(52) During the regular mode of operation of the Coordination, each competent authority referred to in item 20 shall draw up periodic situational reports and shall exchange them with the other competent authorities referred to in item 20 at least on a quarterly basis. The authorities shall also establish, maintain and on an ongoing basis develop their own cyber capabilities and capacities and shall carry out activities aimed at raising security awareness and providing ongoing training for entities within their respective competences. Furthermore, the authorities referred to in item 20 shall conduct ongoing assessments of the state of cybersecurity within their respective domains of competence, shall promptly inform the other authorities within the Coordination of any significant and publicly reported cybersecurity incidents within their competences, and shall on an ongoing basis monitor international trends in the field of cybersecurity crisis management and, where necessary, propose to the Coordination measures for the national development of the field of cybersecurity crisis management. In addition to the above, the authorities referred to in item 20 shall, where necessary, align the national procedures for cybersecurity crisis management with the corresponding procedures of international organisations of which the Republic of Croatia is a member.

(53) In the regular mode of operation, the NCSC-HR shall organise a meeting of the Coordination at least once on a quarterly basis.

(54) In the regular mode of operation, the NCSC-HR shall draw up an annual report for the purposes of the strategic and political level, which shall also include an overview of all escalations into the warning or crisis mode of operation of the Coordination carried out during the reporting year. The annual report shall, prior to being submitted to the strategic and political level, be coordinated and approved by the Coordination.

3.7.2. Warning mode of operation

(55) The escalation of the situation from the regular mode of operation to the warning mode of operation shall be jointly proposed by the competent CSIRT and the authority responsible for the relevant sector referred to in item 20 (hereinafter: the initiators of the escalation), when, on the basis of the data they possess within the scope of their competences or through information received from other sources, they assess:

- the potential for the occurrence of a cybersecurity crisis or,
- the possible development of a cybersecurity incident within their competence into a broader-scale cybersecurity incident, or into a potential cybersecurity crisis.

(56) The proposal for escalation, together with the initial warning situational reports of the initiators of the escalation, shall be submitted to the NCSC-HR. The NCSC-HR shall conduct consultations with the initiators of the escalation regarding the grounds for escalation and, where necessary, shall request amendments to the submitted situational report. Upon coordination and completion, the NCSC-HR shall submit the proposal for escalation, together with the coordinated initial warning situational report, to all other competent authorities referred to in item 20.

(57) Upon receipt of the proposal referred to in item 56, the other competent authorities referred to in item 20 shall verify the state of affairs within their respective areas of competence and, without delay, and in any event no later than two days from the receipt of the initial warning reports of the initiators of the escalation, shall draw up their own initial warning situational report, by which they shall inform the other competent authorities referred to in item 20 of the state of affairs within their respective areas of competence and shall provide an opinion regarding the proposal of the initiators of the escalation.

(58) Pursuant to the initial situational reports received from all competent authorities referred to in item 20, the NCSC-HR shall convene an extraordinary session of the Coordination without delay, and in any event no later than two days from the receipt of the initial warning situational reports. At the extraordinary session, a decision shall be made regarding the escalation to the warning mode of operation.

(59) In the event that the Coordination decides to escalate to the warning mode of operation, the draft initial warning situational report of the Coordination shall be prepared by the initiators of the escalation, with the assistance of the NCSC-HR, and the draft shall be approved and coordinated at a second extraordinary session of the Coordination, no later than two days following the adoption of the decision on escalation. The approved draft of the escalation and the initial warning situational report of the Coordination shall be submitted without delay to the Coordination for the Homeland Security System for the purpose of informing the strategic and political level of the warning situation.

(60) All activities referred to in items 56 to 59 shall be repeated for the final phase of the warning mode of operation, and in the event that the warning mode of operation lasts longer than 30 days, or in the event of the collection of new and significant information, a transitional reporting phase shall be introduced.

(61) A proposal for the de-escalation of the situation shall be submitted by the initiators of the escalation, accompanied by their final warning situational reports. Upon receipt of the proposal for de-escalation, the other competent authorities shall verify the state of affairs within their respective areas of competence and, without delay, and in any event no later than two days from the receipt of the final warning situational reports of the initiators of the escalation, shall draw up their own final warning situational report. On the basis of the received proposal for de-escalation from the warning mode to the regular mode of operation and the final warning situational reports of all competent authorities referred to in item 20, the NCSC-HR shall convene a third extraordinary session of the Coordination without delay, and in any event no later than two days from the receipt of the proposal for de-escalation and the final warning situational reports. At the extraordinary session of the Coordination, a decision shall be made regarding the de-escalation to the regular mode of operation or the continuation of the warning mode of operation of the Coordination and the implementation of activities in accordance with item 60.

(62) In the event that the Coordination decides on the de-escalation to the regular mode of operation, the draft final warning situational report of the Coordination shall be prepared by the initiators of the escalation, with the assistance of the NCSC-HR, and the draft shall be approved and coordinated at the final extraordinary session of the Coordination, no later than two days following the adoption of the decision on de-escalation. The approved draft final warning situational report of the Coordination shall be submitted without delay to the Coordination for the Homeland Security System for the purpose of informing the strategic and political level of the de-escalation.

3.7.3. Crisis mode of operation

(63) A proposal to escalate the situation from the regular mode of operation or the warning mode of operation to the crisis mode of operation of the Coordination shall be submitted by the initiators of the escalation referred to in item 55, and shall be based on their joint assessment of the inability to resolve the cybersecurity incident due to:

- the scope of the cybersecurity incident exceeding the competences of the directly competent CSIRT or CERT authority in the affected sector or type of entity;
- the scope of the cybersecurity incident exceeding the capacities and capabilities of the individual directly competent CSIRT or CERT authority in the affected sector or type of entity;
- the high complexity and sophistication of the cybersecurity incident, which may constitute a broader national or cross-border threat.

(64) The proposal for escalation, together with the initial crisis situational report, shall be submitted to the NCSC-HR. The NCSC-HR shall conduct consultations with the initiators of the escalation regarding the grounds for escalation and, where necessary, shall request amendments to the submitted situational report. Upon coordination and completion, the NCSC-HR shall submit the proposal for escalation, together with the initial crisis situational report, to all other competent authorities referred to in item 20.

(65) Upon receipt of the proposal referred to in item 64, the other competent authorities referred to in item 20 shall, without delay, and in any event no later than 24 hours from the receipt of the proposal, draw up their own initial crisis situational report, reflecting on the state of affairs within their respective areas of competence in relation to the initial report of the initiators of the escalation, and shall submit their initial crisis situational reports to the other authorities referred to in item 20.

(66) Upon receipt of all crisis situational reports, the NCSC-HR shall, without delay, and in any event no later than 24 hours from the receipt of the reports, convene a crisis session of the Coordination, at which operational-level coordination shall be conducted and a decision on the escalation to the crisis mode of operation at the operational level shall be adopted. The approved proposal for escalation to the crisis mode of operation shall be communicated without delay to the Coordination for the Homeland Security System.

(67) The initiators of the escalation and the NCSC-HR shall prepare the initial crisis situational report of the Coordination and a draft cyber crisis management plan, and the draft plan shall be approved and coordinated at a second crisis session of the Coordination, no later than 24 hours following the adoption of the decision on escalation to the crisis mode of operation. The cyber crisis management plan and the initial crisis situational report of the Coordination shall be submitted to the Coordination for the Homeland Security System for the purpose of informing the strategic and political level of the situation and for the adoption of decisions regarding the need to activate additional crisis management mechanisms, such as mechanisms used in the framework of crisis management within the civil protection system.

(68) All activities referred to in items 64 to 67 shall be repeated for the final phase of the crisis mode of operation, and in the event that the crisis mode of operation lasts longer than 30 days, or in the event of the collection of new and significant information, a transitional reporting phase shall be introduced.

(69) A proposal for the de-escalation of the situation shall be submitted by the initiators of the escalation. On the basis of the received proposal for de-escalation from the crisis mode to the warning or regular mode of operation and the final crisis situational reports of all competent authorities referred to in item 20, a third crisis session of the Coordination shall be convened, no later than two days from the receipt of the proposal and the final crisis situational report. At the extraordinary session of the Coordination, a decision shall be made regarding the de-escalation to the warning or regular mode of operation or the continuation of the crisis mode of operation of the Coordination.

(70) In the event that the Coordination decides on the de-escalation to the warning or regular mode of operation, the draft final crisis situational report of the Coordination shall be prepared by the initiators of the escalation, with the assistance of the NCSC-HR, and the draft shall be approved and coordinated at the final crisis session of the Coordination, no later than two days following the adoption of the decision on de-escalation. The approved draft final crisis situational report of the Coordination shall be submitted without delay to the Coordination for the Homeland Security System for the purpose of informing the strategic and political level of the de-escalation.

3.8. Cyber crisis management plan

(71) In the preparation of the draft cyber crisis management plan referred to in item 67, the initiators of the escalation and the NCSC-HR shall be obliged to act in accordance with the principles of proportionality, subsidiarity, complementarity, and confidentiality referred to in item 17, and shall, in the draft plan, elaborate the phases of managing the cyber crisis, possible measures to mitigate the consequences of the cyber crisis, and the phases of recovery from the cyber crisis.

(72) The cyber crisis management plan shall be prepared using the form that forms an integral part of the Rules of Procedure referred to in item 27.

(73) The cyber crisis management plan shall establish:

- the tasks of the competent authorities referred to in item 20, as well as the roles and tasks of other stakeholders in managing the resulting cyber crisis, with a view to ensuring their coordinated action
- the manner of mutual information-sharing among the stakeholders involved in managing the cyber crisis regarding the state of the situation
- the plan for the involvement of the strategic and political level, as well as the responsible entities and the manner of communication with the public.

(74) The purpose of adopting the cyber crisis management plan shall be to define the necessary activities for the effective management of the cyber crisis and recovery from the crisis, including activities related to the exchange of data among all stakeholders involved in managing the crisis and the informing of the public, with a view to mitigating negative effects and exerting a preventive influence on perpetrators of the cyber attack.

3.9. Capacities and infrastructure relevant to the cyber crisis management system and data exchange

(75) For the purposes of managing cyber crises, the authorities referred to in item 20 shall ensure a high level of availability and readiness of all existing capacities and infrastructure which they utilise within the scope of their competences for responding to cybersecurity incidents.

(76) The exchange of data among representatives of the authorities referred to in item 20 within the Coordination shall be conducted primarily through the national platform for the collection, analysis, and exchange of data on cyber threats and incidents referred to in Article 43 of the Cybersecurity Act, and, where necessary, other means of communication defined in the Rules of Procedure shall also be used.

(77) For communication with the public, various available public media shall be used, in accordance with the method and requirements of crisis communication elaborated 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 interconnected activities, consisting of the following elements:

- increasing national capacities for detecting and responding to cyber threats and incidents,
- continuous analysis of the implementation and improvement of cybersecurity measures in the national environment, as well as continuous situational reporting to decision-makers to raise security awareness,
- monitoring the effectiveness of established cyber crisis management procedures, considering lessons learned from cyber crisis management exercises, previous cyber crisis response situations, analysis of the consequences of cyber crises, and the scope and complexity of activities undertaken for recovery from the effects of cyber crises,
- raising cybersecurity awareness at the national level through comprehensive educational and informational 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 the continuous development and enhancement of the national capabilities and capacities of the Republic of Croatia in the field of cybersecurity, as well as to reduce the risk of a cyber crisis, the following is carried out:

- continuous cooperation and data exchange between the competent authorities referred to in item 20 on the spectrum of cyber threats within their area of competence,
- cooperation of the competent authorities referred to in item 20, in accordance with their responsibilities, with relevant international authorities,
- analysis of collected data and preparation of situational reports within the competent authorities referred to in item 20, to support decision-making processes, development of security awareness, and proposals for improving cyber resilience measures,
- monitoring and assessing security risks associated with the introduction and use of emerging technologies in the national and global environment.

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

- during regular operations, it holds quarterly meetings for mutual exchange of information and experiences among the authorities and other stakeholders involved in the work of the Coordination,

- organises thematic presentations at Coordination meetings delivered by representatives of the authorities involved in the work of the Coordination or by representatives of other stakeholders,
- organises and conducts periodic readiness checks at the level of institutions involved in the work of the Coordination and plans the implementation of national cyber crisis management exercises, which are appropriately incorporated into the Cybersecurity Exercise Implementation Plan, adopted by the Government every two years at the proposal of the central state authority for cybersecurity, pursuant to Article 58 of the Cybersecurity Act.

(81) The competent authorities involved in the work of the Coordination shall, within the scope of their competences, promote, plan, or carry out appropriate activities aimed at raising their level of preparedness, through readiness checks, training, and awareness-raising within the entities for which they are responsible pursuant to the act establishing such authorities or pursuant to the competences conferred on them by other statutory and subordinate legislation, in particular those competences arising from regulations governing the field of cybersecurity.

5. National cyber crisis management exercises

(82) In order to achieve the highest level of preparedness for cyber crises, to verify the availability of capacities and capabilities in the field of cybersecurity, to test established procedures and communication tools, as well as to exchange acquired knowledge, experience, and best practices and to strengthen trust, cyber crisis management exercises shall be conducted.

(83) Cyber crisis management exercises shall be established, organised, and conducted pursuant to the Cybersecurity Exercise Implementation Plan referred to in Article 58 of the Cybersecurity Act.

(84) The Coordination shall assess national requirements in the field of cyber crisis management and shall propose the implementation of appropriate exercises within the national and/or international framework, for their inclusion in the Cybersecurity Exercise Implementation Plan referred to in Article 58 of the Cybersecurity Act.

(85) Within the framework of each conducted exercise, the Coordination shall analyse the lessons learned by the participants in the exercise and shall propose appropriate training plans, the adjustment of organisational and other rules and policies, as well as the need to adapt or enhance the technical and other capacities of the competent authorities at the national level.

6. Alignment with the general national crisis management framework and the EU level cyber crisis management framework

6.1. Alignment with the general national crisis management framework

(86) The authorities within the homeland security system shall provide the Coordination for the Homeland Security System with information within their remit that is relevant as indicators of the emergence or escalation of a security threat, or of the occurrence of a crisis that may constitute a risk to national security.

(87) In the event of a gradually emerging or sudden crisis that constitutes a risk to national security, the Coordination for the Homeland Security System shall propose to the Government the declaration of a crisis, the formation of a crisis management headquarters, and the manner of responding to the crisis.

(88) The described approach to general crisis management shall be applied appropirately to the management of cyber crises.

(89) The response to a cyber crisis involves two levels of management: the operational level and the strategic and political level. The operational level shall ensure the implementation of the necessary procedures for competent technical handling and the coordination of the work of the competent CSIRT and CERT authorities, as well as for assessing the impact of cyber incidents and their development trends, thereby effectively linking technical information regarding a cyber incident with the potential evolution of the incident into a cyber crisis, and ensuring its presentation in the form of impact and growth trends, which are required by the strategic and political level of national crisis management for decision-making regarding the activation of additional mechanisms established within the homeland security system..

Diagram 1: Levels of cyber crisis management

<table>
<tr><th colspan="2">Levels of cyber crisis management</th></tr>
<tr><td>Strategic and political level</td><td>The Coordination for the Homeland Security System</td></tr>
<tr><td>National Security Council</td><td>  </td></tr>
<tr><td>Operative level</td><td>Cyber Crisis Management Authority (SOA) and the Coordination for Cyber Crisis Management</td></tr>
<tr><td>SOA (NCSC-HR)

+ MI, MOD, MSEY, UVNS, ZSIS, MJPADT, HAKOM, CARNET, CNB, HANFA, CCAA</td><td>  </td></tr>
</table>

6.2. Alignment of the Republic of Croatia with the EU-level cyber crisis management framework

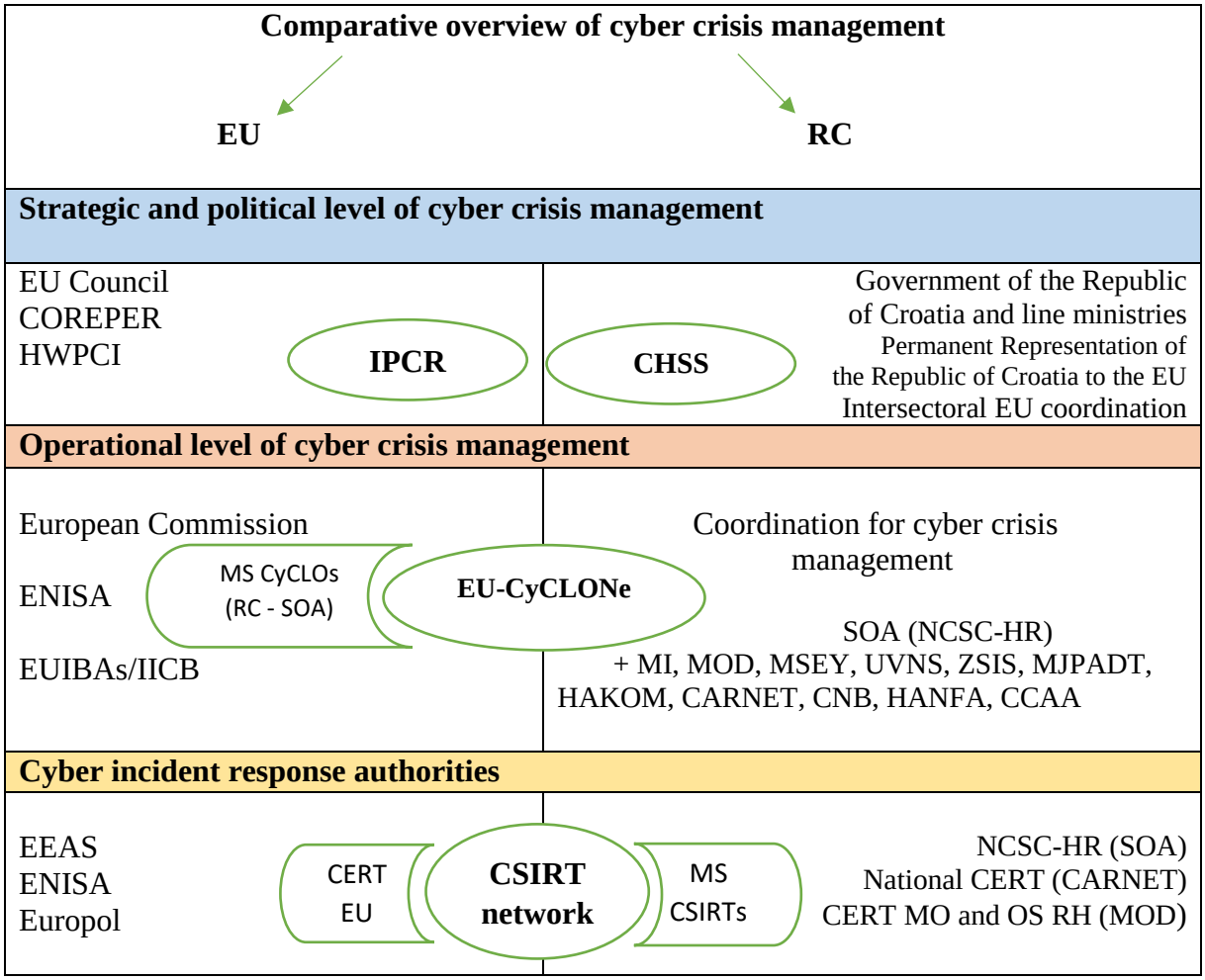
(90) The EU's objective regarding cyber crisis management is to establish:

- the EU-CyCLONe network as the operational level of management, which would ensure the necessary procedures for managing cyber crises and improve awareness of large-scale cyber incidents and cyber crises, as well as enhance situational awareness,
- more effective coordination among a number of competent CSIRT authorities, at both EU and Member State levels, through the use and mutual exchange of globally collected data from the relevant authorities of partner countries,
- mediation between the technical complexity of cyber incidents and the information required at the political level (IPCR), focusing on the impact and trends in the development of incidents, which is ensured through the operational level of management.

(91) The Republic of Croatia, through the National Programme, in a similar manner:

- at the national level, establishes the Coordination as the operational management level, which ensures the necessary procedures for effective cyber crisis management, the exchange of relevant data, and the proposal and planning of activities aimed at enhancing situational awareness of the potential scale and severity of cyber incidents,
- closely links the competences under the Cybersecurity Act assigned to national authorities responsible for implementing cybersecurity requirements, national authorities responsible for implementing specific laws, and CSIRT authorities competent for responding to cyber incidents, as well as the related competences of authorities under other laws, and through the use and mutual exchange of relevant data, including globally collected data from the competent authorities of partner countries,
- carries out mediation between the technical complexity of cyber incidents and the needs of the political level, i.e. the Coordination for the Homeland Security System, which are primarily focused on the impact and trends of cyber incidents, which is ensured through the new operational management level, namely the National Programme and the Coordination.

Diagram 2: Comparative overview of cyber crisis management at the EU and Croatian levels



6.3. Obligations of the Republic of Croatia towards the EU-CyCLONe network

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

(93) The SOA, as the authority responsible for cyber crisis management in the Republic of Croatia, shall promptly notify the European Commission and the EU-CyCLONe network of the adoption of the National Programme and any of its amendments, and, as necessary, shall guide the work of the Coordination and align it with activities carried out within the framework of the EU-CyCLONe network.

7. ANNEX

7.1. Taxonomy

(94) The taxonomy for describing cyber crises establishes a common vocabulary of terms used to describe, in a structured manner, the outputs of authorities responsible for incident response, i.e. the competent CSIRT and CERT bodies, and the operational level of cyber crisis management. The purpose of the taxonomy is to ensure easier understanding and mutual interpretation of work outputs in communication between different stakeholders of a cyber

crisis, as well as between the operational level and the strategic and political level of cyber crisis management.

(95) The taxonomy for describing cyber crises is aligned with existing national and EU cyber incident taxonomies, thereby further simplifying the mutual exchange of information between stakeholders involved in cyber crisis management at the national and international level.

(96) The structured description of a cyber crisis, which uses the taxonomy for describing cyber crises, must include information on the assessment of the nature of the incident (cause, severity level) and the impact of the crisis situation (affected sectors, assessment of the level of impact, and trend in the development of the crisis).

(97) The taxonomy for describing a crisis situation is used at the operational level of cyber crisis management, for the purpose of mediation between the incident response level and the strategic and political level.

(98) The taxonomy for describing a cyber crisis situation (Table 4) consists of two groups of descriptive terms covering the nature and impact of the crisis situation. The nature of the crisis situation is further divided into: the root cause of the crisis (five categories) and the severity level of the crisis (three levels). The impact of the crisis situation is divided into affected sectors (two categories with subcategories), assessment of the level of impact on social and economic activities (four levels), and assessment of the trend in the development of the crisis situation (three categories).

(99) Explanation of terms:

1. *Nature of the crisis situation*

   Root cause[13]:

   i. *System failure:* refers to an incident that occurred due to a system failure, without external influence (for example, hardware failure/malfunction, procedural deficiency, or software error that triggered the incident).

   ii. *Natural disaster:* refers to an incident caused by a natural event (for example, storm, flood, earthquake, fire, etc., that triggered the incident)

   iii. *Human error:* refers to an incident caused by human error (for example, a correctly functioning system used incorrectly, operator mistake, or negligence that caused the incident)

   iv. *Malicious activities:* refers to an incident caused by malicious actions (for example, a cyberattack or physical attack, vandalism, sabotage, insider attack, theft, etc., that triggered the incident)

   v. *Third-party service failure:* refers to an incident caused by the disruption of third-party services (for example, power outage, Internet outage, etc., that caused the incident).

   The severity level of the crisis situation or security risk posed by a cyberattack and/or attacker is 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 final situational report, i.e., during data collection and incident analysis.

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

The 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 in the event of a severe storm approaching, during a massive DDoS attack or a large-scale APT campaign by a sophisticated APT group, or if a widely spread vulnerability that can be easily exploited is discovered).

The factors considered when assessing the severity level are:

- the risk of affecting new organisational entities, considering the likelihood of propagation, and potential impact
- additional effort or costs required for mitigation, protection, or recovery
- potential damage that could result from the threat
- speed of incident/threat propagation
- whether attacks are still ongoing
- criticality level of systems potentially exposed to the threat
- feasibility or availability of solutions for protective measures or threat mitigation
- applicability of industry standards and best practices in mitigating the threat.

2. *Impact of the crisis situation / Affected sectors*

The impact on sectors identified by the Cybersecurity Act as high-criticality sectors and other critical sectors is qualified and quantified in the relevant legal acts and subordinate legislation, and is used in assessments conducted by competent authorities for the purpose of managing cyber crises. Specific criteria needed for assessment within this taxonomy are elaborated in the SOPs of the authorities referred to in item 20, taking into account the number and types of affected entities, the types of impacted services, as well as the legally defined levels of significant incident effects.

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

i. *High-criticality sectors*

ii. *Other critical sectors*

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

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

i. *Very strong impact,*

ii. *Strong impact,*

iii. *Weak impact,*

iv. *No impact.*

Impact on social and economic activities refers to any effect on the physical world, society, and the economy, disruption at the national level or across a large part of the country, for example, an increased risk to citizens' health or safety, levels of physical damage, financial costs, etc.

[15] The assessment is carried out by the authority/level responsible for managing the cyber crisis.

The factors considered when assessing the level of impact[16] are:

- the risk to public health and safety, for example through the impact of the incident on emergency services
- the impact on economic activities, for example major financial losses
- the damage and costs for citizens and entities affected by the incident
- the disruption of daily life
- cascading effects on other critical sectors
- the impact on the media and the coverage of the country by media programmes
- political impact and significance.

4. *Assessment of the trend in the development of the crisis situation is divided into three assessed levels:*
    i. *Improving,*
    ii. *No change,*
    iii. *Deteriorating*

    The assessment of the further trend in the development of the incident is carried out in the short term (e.g., the 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, observed at the level of economic and social activities negatively affected.

Table 4: *Taxonomy for describing a cyber crisis situation:*

1. Nature of the crisis situation
a. Root cause of the crisis situation
i. System failure
ii. Natural disaster
iii. Human error
iv. Malicious activity
v. Third-party failure
b. Severity level of the crisis situation or security risk posed by a cyberattack and/or attacker
i. High
ii. Medium
iii. Low
2. Impact of the crisis situation
a. Affected sectors
i. High-criticality sectors/subsectors
a) Energy / electricity, district heating and cooling, oil, gas, hydrogen

[16] In the case of an incident of minor impact that affects a large number of organisations, the assessment should be carried out from the perspective of society and consideration should be given to assessing a strong impact on society as a whole, even though the incident itself has only a minor impact at the individual level of the affected entities.

b) Transport/air transport, rail transport, maritime transport, road transport

c) The banking sector

d) Financial market infrastructure

e) Healthcare

f) Drinking water

g) Wastewater

h) Digital infrastructure/Internet exchange centres, DNS services, registry of the national top-level .HR domain, cloud computing, data centres, content delivery networks, trust services, public electronic communications networks, publicly available electronic communications services

i) ICT services management (B2B)

j) Public sector

k) Space

ii. Other critical sectors/subsectors

a) Postal and courier services

b) Waste management

c) Manufacturing, production, and distribution of chemicals

d) Production, processing, and distribution of food,

e) Manufacturing/production of medical devices and in vitro diagnostic medical devices, production of computers and electronic and optical products, production of electrical equipment, production of machinery and equipment, motor vehicle, trailer and semi-trailer manufacturing, production of other transport equipment

f) Digital service providers

g) Research

h) Education system

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

i. Very strong impact

ii. Strong impact

iii. Weak impact

iv. No impact

c. Assessment of the trend in the development of the crisis situation

i. Improving

ii. No change

iii. Deteriorating

(100) The taxonomy for describing a cyber crisis situation aims to ensure better understanding and translation of complex technical issues in the cyber domain into operational impact and situational status that is understandable to a wider range of stakeholders involved in cyber crisis management, particularly at the strategic and political decision-making level.

7.2. Use of the TLP protocol for data exchange, data confidentiality, and privacy

(101) For the purposes of data exchange within the implementation of the National Programme, the TLP protocol shall be used. This protocol is widely adopted within the global CERT community and represents a simple and easily understood approach to restricting the distribution of specific operational data to end users (further recipient distribution).

(102) The four basic levels of the TLP protocol (https://www.first.org/tlp/) shall be used, with the possibility of applying the additional "Strict" parameter to the "Amber" level. For the purposes of the National Programme, these levels shall have the following meanings:

- **TLP:RED** (TLP:RED) – **not intended for further distribution and is restricted solely to the participants** of a specific meeting or session, members of the Coordination, or representatives of stakeholders involved in managing a particular cyber crisis. This designation is used when additional recipients would not be able to use the information effectively, or when an expanded list of recipients, in the event of misuse, could affect privacy, reputation, or certain operational activities being conducted.
- **TLP:AMBER+STRICT** (TLP:AMBER+STRICT) - **further distribution is restricted exclusively to the employees of the stakeholders** involved in cyber crisis management. This designation is used when the information requires support, for example, from one of the authorities referred to in item 20, or support from their representatives within the Coordination. In this context, the exchange of such information outside the organisations involved in cyber crisis management could pose a risk to privacy, reputation, or the execution of certain operational activities.
- **TLP:AMBER** (TLP:AMBER) – **further distribution is restricted exclusively to the employees of the involved organisations and their clients**. This designation is used when the information needs to be provided to the authorities referred to in item 20, as well as to clients within their area of responsibility, for preventive activities or assessments, for example, regarding the potential development of a cyber crisis. In this context, distribution beyond the aforementioned parties could pose a risk to privacy, reputation, or the execution of certain operational activities.
- **TLP:GREEN** (TLP:GREEN) – **further distribution is restricted to the community of organisations** that are stakeholders included by the plan in managing the cyber crisis, or that are assessed as organisations potentially directly affected by the incident. **Recipients may further distribute** TLP:GREEN information within their sector or the community that could be impacted by the incident, but they may not publish the information.
- **TLP:CLEAR** (TLP:CLEAR) – **further distribution is not restricted** and applies to information that carries minimal or no risk of misuse. Such information shall be subject to the usual rules and procedures for use by recipients and for public disclosure.

The use of additional parameters within the TLP protocol, depending on the needs of the Coordination, shall be defined in the Rules of Procedure.

(103) In the event that classified data is generated or used in the implementation of cyber crisis management, or if personal data is processed, such data shall be subject to the special regulations governing their protection and, where applicable, their classification.

(104) The authorities referred to in item 20 shall be responsible, within the scope of their competences, for assessing the level of classification of classified data exchanged with other competent authorities referred to in item 20 or provided to other stakeholders involved in managing a cyber crisis. The exchange of classified data may occur only between recipient authorities that meet the requirements for handling classified data of the relevant classification level.

7.3. Form requirements

(105) The forms used pursuant to the National Programme are: the cyber crisis management plan form, situational report forms, and the escalation proposal form.

(106) The cyber crisis management plan form shall, in substance, include: a description of the procedures for managing a cyber crisis; a description of the cyber crisis situation and the affected entities; the stakeholders involved in managing the cyber crisis and their respective tasks; the plan for addressing the cyber crisis; possible measures to mitigate its consequences; measures for recovery from the cyber crisis; and the need for, and plan of, public communication.

(107) Situational report forms are classified as: periodic situational reports (regular mode of operation), warning situational reports (warning mode of operation), and crisis situational reports (crisis mode of operation). Depending on their purpose, these forms contain summaries, observations, explanations of escalation procedures, taxonomies for describing the situation, and detailed descriptions of the situation.

(108) The escalation proposal form shall include: the name of the authorities proposing the escalation; a description of the state of the situation prompting the request for escalation; an indicative statistical overview of the entities affected by the cyber incidents; measures taken in response to cyber incidents prior to the escalation proposal; and a statement of consent by the heads of the competent authority and the competent CSIRT authority regarding the proposed escalation.

(109) The cyber crisis management plan form, situational report forms, and the escalation proposal form shall be established by the Rules of Procedure referred to in item 27.