D E C I S I O N

No. 814 , dated 30.12.2025

ON

ADOPTION OF PROCEDURES FOR THE IDENTIFICATION, CLASSIFICATION, ESCALATION AND MANAGEMENT OF CYBER CRISES

Pursuant to article 100 of the Constitution and article 28, paragraph 9, of law no. 25/2024, "On cybersecurity", and upon the proposal of the Prime Minister, the Council of Ministers,

HEREBY D E C I D E D:

1. To adopt the procedures for the identification, classification, escalation, and management of cyber crises, pursuant to the text attached to this decision, which forms an integral part thereof.
2. The National Cybersecurity Authority, the sectoral CSIRTs, the CSIRTs of information infrastructure operators, as well as all responsible structures and institutions assigned specific roles and responsibilities under the procedure for the identification, classification, escalation, and management of cyber crises, are empowered to implement this decision.

This decision shall enter into force upon its publication in the "Official Journal".

PRIME MINISTER

EDI RAMA

PROCEDURES FOR THE IDENTIFICATION, CLASSIFICATION, ESCALATION, AND MANAGEMENT OF THE CYBER CRISIS

1. **INTRODUCTION**

The increasing reliance on digital information and communication technologies, as well as digital services, has led to cybersecurity threats becoming increasingly prevalent and sophisticated. This now global phenomenon knows no borders, making the management of cyber incidents and cyber crises a significant challenge for all states. Cybersecurity incidents may range from low-impact attacks to highly sophisticated attacks, resulting in the disruption of critical services, the theft of sensitive information, or the destruction of critical and important information infrastructures.

Following a significant increase in cyberattacks, the legal framework for the management of and response to large-scale cyber incidents with escalation into a cybersecurity crisis is an instrument to ensure that Albania is prepared to address any potential cybersecurity incident or crisis, by protecting critical and important information infrastructures and ensuring the continuity of key services. In order to ensure coordinated and efficient management of large-scale incidents and cybersecurity crises, it is substantial to involve all relevant actors, including the government, independent institutions, the private sector, and civil society. Through cooperation, coordination, and continuous training in the field of cybersecurity, Albania will be better positioned to face cybersecurity challenges and to respond in a rapid and efficient manner with the aim of minimizing consequences. The drafting of this procedure aims to establish a comprehensive and structured framework for the identification, classification, and management of cybersecurity crises that may threaten the normal functioning of Albanian society and the national economy.

The effective capacity for managing cybersecurity crises depends on effective capacities at the strategic political, operational, and technical levels, as well as on close cooperation between these levels, as emphasized in European Commission Recommendation (EU) 2017/1584 of 13 September 2017 on the coordinated response to large-scale incidents and cybersecurity crises.

The management of a national cybersecurity crisis involves many stakeholders, such as ministries, regulatory authorities, independent institutions, law enforcement institutions, etc., as they lead the State's defensive efforts to address attacks and their consequences. Cyber resilience is the ability to maintain the continuity of critical and important services for the country, regardless of the severity of cyber impacts directed at their information infrastructures.

In this context, this document aims to:

- to define the procedures for the identification, classification, escalation, and management of a cybersecurity crisis;
- to ensure coordination and cooperation between state institutions, the private sector, and international organizations in order to establish a secure and reliable network for the response to and management of cybersecurity crises, to assist minimize consequences, as

well as to ensure the rapid and efficient exchange of information and protective measures among actors involved in the field of cybersecurity, institutions, and states;
- to prepare institutions and critical and important information infrastructures to respond to cybersecurity crises, including measures to prevent the escalation of large-scale cyber incidents and lessons learned from previous situations;
- to increase response and intervention capacities to successfully manage cybersecurity crisis situations and to ensure the continuity of critical and important functions and services of information infrastructures.

2. PROCEDURES FOR THE IDENTIFICATION, CLASSIFICATION, ESCALATION, AND EFFECTIVE MANAGEMENT OF THE CYBERSECURITY CRISIS

2.1 Cyber Crisis

A cyber crisis is a situation during which the security of information in information systems or the security of electronic communications networks is seriously compromised, thereby posing a threat to the public interest of the Republic of Albania.

The identification, escalation, and management of a cyber crisis are based on the ENISA document "On Cooperation and Cyber Crisis Management". According to ENISA, a cybers crisis begins when an ordinary cyber incident turns into an extraordinary event, meaning that it deviates from normal conditions and involves serious concern or a risk of disruption of vital functions of society.

A cyber crisis is addressed on the basis of the following two fundamental elements, assessed in interaction with the circumstances in both the cyber and physical domains:

1. The potential of a cyber incident to cause real damage, to disrupt or compromise the functional continuity of critical and important information infrastructure services, as well as its potential to escalate into a national state of emergency.
2. In cases of emergency situations caused by non-cyber physical factors, such as armed conflicts, terrorist acts, or natural disasters, consideration is given to the increased level of risk for the outbreak of a cyber crisis and the intensification of malicious cyber activity.

2.2 Cyber crisis phases

A cyber crisis goes through several phases:

- The alert phase;
- The phase of situational evaluation and identification of the cyber crisis;
- The phase of response to and management of the cyber crisis;
- The post-cyber crisis recovery phase.

2.2.1 The alert phase in a cyber crisis

The alert phase in a cyber crisis is the moment when an identified cyber incident is assessed as a serious threat that may affect the normal functioning of the system or information infrastructure,

requiring the immediate activation of response structures. At this phase, the critical nature of the event is confirmed, the alert level is determined according to internal protocols, and key operational and decision-making stakeholders are notified, including technical teams, senior management, and the competent national authorities, with the aim of ensuring rapid and structured coordination to prevent the spread of damage and to initiate active real-time management of the situation.

Cyber alert levels are defined and used as a formal mechanism for assessing the level of vigilance and institutional readiness to address risks in the cyber and physical domains. The Authority, in coordination with the affected information infrastructure, determines the cyber alert level based on the situational evaluation, which relies on verified information, facts, and joint technical and operational analyses. In accordance with the level of the identified cyber incident, the Authority determines the corresponding cyber alert level and activates the relevant response procedures, ensuring the functioning of coordination and intervention mechanisms. Upon the declaration of a cyber alert level, the responsible entities immediately implement the measures and actions specified for the corresponding alert level, with the aim of limiting the impact of the incident and reducing the risk of damage to the information infrastructure.

Timely annoucement of the cyber alert level is mandatory and is intented to prevent the escalation of cyber incidents into a cyber crisis, as well as to limit damage when a cyber crisis is identified.

Failure to declare, or delay in declaring, the cyber alert level increases the risk of large-scale damage to information infrastructures and the continuity of critical services.

2.2.1.1 Escalation scheme of the cyber alert level

The escalation scheme of the cyber alert level is determined according to Table 1 of this procedure and is implemented by the Authority and the entities in charge, in accordance with the level of risk and impact of the cyber incident.

Routine protection situation – In the absence of a declared cyber alert state, the critical information infrastructure is considered to be in a routine protection situation and is required to implement standard cybersecurity measures, conduct routine operations, and update cyber protection plans, without any interruption to the normal functioning of the information infrastructure.

Initial level escalation situation – Activated when a significant threat to a critical service or a risk of disruption to the normal functioning of the information infrastructure is identified, even if the cyber origin of the threat has not yet been confirmed.

Medium level escalation situation – Activated when damage to critical information infrastructures is detected that significantly affects the continuity of core processes.

High level escalation situation – Activated when prolonged and widespread damage occurs to critical information infrastructures, causing major harm to core processes and the continuity of the affected information infrastructure services.

Phase	Description
Routine Protection	Routine protection level: there are no indicators of disruption to the functional continuity of critical information infrastructure services
Escalation	Initial level: a substantive threat to a critical information infrastructure service. The functional continuity of a critical information infrastructure service may be at risk.
	Medium level: damage to critical information infrastructure services may cause significant malfunction in the continuity of core processes
	High level: prolonged and large-scale damage to critical information infrastructure services causes significant damage to critical processes and to the continuity of service operation

Table 1. Cyber Alert Escalation Scheme

2.2.1.2 Indicators for determining the cyber alert level in the cyber and physical domains

The cyber alert level shall be determined by assessing risk through indicators of the severity of the threat and the likelihood of their materialization, by analyzing the actions that need to be undertaken, as well as the resources and means that need to be used. Since emergencies caused by a non-cyber factor (such as war, natural phenomena, terrorist activities, malfunction, etc.) frequently serve as opportunities for cyber attackers to increase their efforts, precisely when the normal functioning of critical information infrastructure services becomes even more essential, the cyber alert level shall be determined not only by circumstances in the cyber domain, but also by circumstances in the physical domain. Two significant aspects in the context of the correlation between indicators and alert levels are as follows:

1. Use of indicators: A specific indicator does not necessarily determine a specific level of cyber alert. Indicators are tools used in a situational evaluation to determine the level of cyber alert.
2. Pre-incident alert declaration: A cyber alert can be activated even without the detection of actual damage to critical services. Activation may be based on intelligence service reports regarding potential threats or on circumstances that increase the importance of the normal functioning of the information infrastructure. In this way, an alert level (e.g., A or B) may be set as a result of an incident with low or considerable impact, particularly during emergencies caused by non-cyber factors, while simultaneously maintaining routine protection measures.

2.2.1.3 Cyber alert levels and indicators for determining each level

Routine protection: Represents the predefined situation when circumstances in the cyber domain and in the physical domain do not show indicators of a disruption to the normal functioning of the information infrastructure, or any need to increase the level of protection. Under these circumstances, there are no indicators of high alert levels.

Cyber domain indicators determine whether visible cyber incidents have occurred without disrupting the functioning of the information infrastructure, or whether no visible cyber incidents have occurred.

Physical domain indicators determine general alerts regarding the possibility of the occurrence of cyber incidents.

Cyber alert level A: Cyber Alert Level A (low-level incident) shall be determined following a situational evaluation, when at least one of the following indicators is met:

Cyber domain indicators:

- *Warning of a cyber incident:* An isolated cyber incident has occurred, indicating possible disruption to the normal functioning of a non-critical service at an information infrastructure operator, but there are no indicators affecting the entire sector or a branch of the information infrastructure operator.

- *Receipt of an informational alert:* Information related to a threat or vulnerability in information systems that may affect one or more non-critical services of the information infrastructure operator.

- *Global events affecting directly or indirectly the Republic of Albania:* Cyberattacks occurring outside the territory of the Republic of Albania but directly or indirectly affecting our country, e.g. cyberattacks against companies that have branches in our country, or attacks against allied countries.

Physical domain indicators:

- *Operational or technical problem:* An operational or technical malfunction in a non-critical service and/or at the location where the relevant information infrastructure is located;

- *Global events indirectly affecting Albania:* A warning of an abnormal security event (such as, for example, an escalation of missile launches toward allied countries).

Cyber alert - level B: Cyber Alert Level B is determined following a situational evaluation, when at least one of the following indicators is met:

Cyber domain indicators:

- *Warning of a cyberattack:*The national CSIRT is informed by intelligence services, CSIRTs of allied states, or international organizations of possible cyberattacks targeting a service of a critical sector

- *Damage to critical services as a result of a cyberattack*: The result consists of a possible disruption to the continuity of a critical information infrastructure service, but there is no evidence of spread across the entire sector.

Physical domain indicators:

- *Physical damage:* Physical damage to services that are critical (such as power outages, disruption of healthcare services) but which are localized only within a single information infrastructure operator.

- *Global events directly affecting Albania:* An attack occurring somewhere in another country, but attributed to Albania.

Cyber Alert - Level C: Cyber Alert Level C comprises the high level, where the circumstances that triggered the declaration of this state may escalate into a national emergency state. Cyber Alert Level C shall be determined following a situational evaluation, when at least one of the following indicators is met:

Cyber domain indicators:

- *Damage to several critical services as a result of cyberattacks* : Damage to several critical services of the information infrastructure operator, which leads to the disruption of several core processes and the functional continuity of the economy (such as intersectoral impact).

Physical domain indicators:

- *Ongoing physical damage:* Physical damage to several infrastructures and services that are important for the country's economy.

- *Preparation for the outbreak of a war:*Serious preparations for war or a large-scale military operation.

Cyber Alert - Level D: Level D is the state of national emergency, which is the highest level of cyber alert. Cyber Alert Level D shall be determined following a situational evaluation, when at least one of the following indicators is met:

Cyber domain indicators :

- *Large-scale damage to critical services as a result of cyberattacks*: Major and/or continuous damage to the critical services of critical and important information infrastructure operators, leading to the disruption of many vital basic services as well as the economy (such as intersectoral impact)

Physical domain indicators :

- *Ongoing physical damage:* Multiple and/or continuous physical damage to information infrastructures that enable the provision of services that are important for the country's economy.

War situation: War or a large-scale military operation.
State of emergency: Declaration of a state of emergency conditioned by stay-at-home measures or a "civil emergency event".

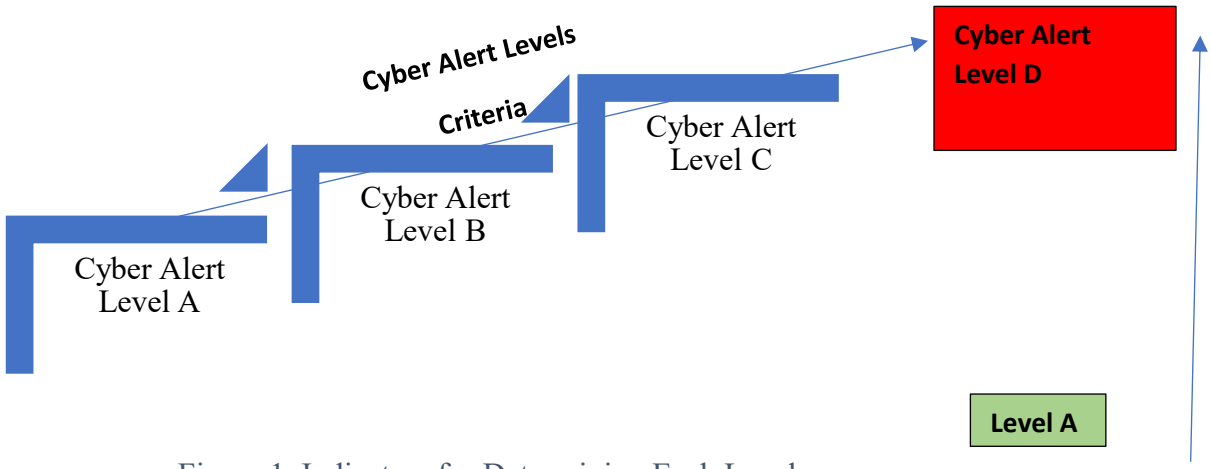

Figure 1. Indicators for Determining Each Level

2.2.1.4 The determination of the cyber alert level is made by NCSA after coordination with the affected infrastructure, based on a situational evaluation report.

2.2.1.5 Principles for changing the cyber alert state

During each alert state, each information infrastructure carries out a situational evaluation, reviews the Cyber domain indicators and in the physical domain, and then determines whether there is a need to change the alert state.

Increase of the cyber alert level:

The increase of the cyber alert level is impacted by the escalation of the situation under certain circumstances and requires the undertaking of further actions or the intensification of measures already in place. The purpose of these actions is to prevent the situation from worsening or to minimize potential damage.

- Gradual alert increase: The alert level should be determined and raised gradually based on situational indicators, analyzing any change in the risk or potential impact on critical services.
- Exceptions: In extreme situations, the cyber emergency level may be declared immediately skipping the other alert levels, in order to ensure prompt intervention and continuous protection of critical infrastructure.

Decrease of the cyber alert level:

The cyber alert level is decreased if the relevant indicators that led to the determination of the alert level are no longer present. The alert level is reduced gradually, by one category at a time, until routine cyber protection is restored.

1.2.1 Phase of situational assessment and identification of the cyber crisis

The situation assessment and cyber crisis identification phase is carried out as follows:

Start of assessment: The situation assessment commences as soon as the cyber alert level reaches level C. This includes analyzing the causes, scope, and potential impact of cyber incidents on a large scale for information infrastructure operators.

Alert escalation: If the analysis indicates that the alert state has escalated from level C to level D (cyber emergency), and at the same time the operator's critical services are disrupted, severely compromising information security and cannot be restored within a defined timeframe, the situation is considered for cyber crisis identification.

Cyber crisis identification: A cyber crisis is determined on a case-by-case basis, taking into account:
a) The scale of impact on critical services;
b) The duration of the disruption to normal operations;
c) The inability to quickly restore the security and functionality of the infrastructure.

A cyber crisis may be identified on a case-by-case basis.

At the national level – A cyber crisis is identified following a threat or circumstances that may escalate into a national emergency state/cyber crisis, where several critical sectors or all critical sectors of the economy are involved, with nationwide scope.

At the sectoral level – A cyber crisis is identified following a threat or circumstances that may escalate into a national emergency state/cyber crisis, even for one of the vital sectors with nationwide scope and impact (e.g. when the energy sector is affected, paralysing all other sectors). The declaration of a cybersecurity crisis at the sectoral level makes it mandatory for all structures that are part of that sector to move into an alert state. The declaration of a cyber alert level in a specific sector may not be mandatory for other sectors, but it shall indicate that certain circumstances exist in the cyber domain that must also be addressed by other sectors.

2.2.2.1 Steps for the declaration of a cybersecurity crisis

1. When the Authority receives a notification of a serious cybersecurity incident that has significant impact and wide scope on critical information infrastructure operators, the

Authority shall initiate a preliminary assessment of the incident in order to determine its political, economic, and security impact.

2. Following the situation assessment, the Authority shall prepare a preliminary report.
3. When the preliminary report concludes that the situation constitutes a potential cyber crisis, the Authority shall immediately notify the other responsible security and defence entities in accordance with point (a) of article 11 of Law no. 25/2024 "On Cybersecurity", initiating a coordination and consultation process for the assessment of the situation at the national level.
4. Following a coordinated assessment with the other security and defence entities in charge, a decision must be taken on whether or not to propose the declaration of the cyber crisis.
5. In the event that it is decided to propose the declaration of the cyber crisis, the Authority shall submit to the Prime Minister the proposal for the declaration of the cyber crisis and the measures for addressing the situation.
6. Upon receiving the proposal from NCSA, the Prime Minister proposes to the Council of Ministers the declaration of the cyber crisis state.
7. The declaration of the cyber crisis shall be effected by means of a Decision of the Council of Ministers.
8. The Council of Ministers may decide to extend the period of the cyber crisis state, provided that such extension does not exceed a period of 30 days.

3. RESPONSE AND MANAGEMENT PHASE OF THE CYBERSECURITY CRISIS

The response and management phase of the cyber crisis includes coordinated steps and the implementation of countermeasures and playbooks to minimize impact, to recover affected systems, and to ensure the continuity of critical operations of the information infrastructure. The objective at this phase is to enable the control, containment, neutralization, as well as the recovery from the consequences of a cyberattack escalated into a cyber crisis, while ensuring institutional coordination and clear communication. This phase is activated following the official declaration of the cyber crisis state by a Decision of the Council of Ministers.

3.1 Steps for response to and management of the cyber crisis

The steps followed for the response to and management of the cyber crisis are as follows:

3.1.1 Activation of structures

3.1.1.1 The National Cybersecurity Authority shall request the immediate transition to a high readiness level of the Cyber Incident Response Team at the operator of the sector/sectors affected by the cyber incident escalated into a cyber crisis (CSIRT at the operator), as well as their transition to a state of cyber emergency.

3.1.1.2 The National Cybersecurity Authority immediately places the National Cyber Incident Response Team (National CSIRT) at a high readiness level and transitions to a state of cyber emergency, and initiates response and coordination procedures.

3.1.1.3 The Cybersecurity Emergency and Crisis Response Team (CERT) shall be established, with the number of experts and their profiles determined based on the complexity of the situation, the nature of the attack, and the number of affected information infrastructures, in accordance with the provisions of the Decision of the Council of Ministers on the establishment, organization, and functioning of the cybersecurity emergency and crisis response team.
3.1.1.4 In all cases, communication between structures shall be conducted through secure communication channels, for the purpose of exchanging technical information, notifying responsible stakeholders, and coordinating urgent measures.

3.1.2 Updating information and immediate situation assessment

Authority, in cooperation with CERT, shall collect and manage real-time data from CSIRTs at operators as well as from sectoral CSIRTs, regarding the affected systems and networks, through which technical and operational analysis is carried out on the scope of the attack, the impact on critical services, the identification of potential actors, and the determination of intervention priorities. The Authority shall update the situation report every 24 (twenty four) hours or as deemed necessary.

3.1.3 Interinstitutional and Operational Coordination – Updating Information and Immediate Situation Assessment

Authority shall coordinate the response at the national and international level. Daily meetings shall be organized with:

a) CSIRTs at operators and sectoral CSIRTs (e.g. finance, energy, telecommunications, transport).
b) CERT;
c) Security agencies (Albanian State Police, State Intelligence Service (SIS));
ç) International partner agencies (e.g. ENISA, Europol EC3, NATO CCDCOE).

3.1.4. Determination, implementation, and updating of protective measures and cyber countermeasures

The Authority shall determine and implement general protective measures and cyber countermeasures for the management of the cyber crisis and update them in accordance with the evolution of the situation.

3.1.5. Management of public communication and transparency

The Authority, in coordination with the structure responsible for media and information under the authority of the Prime Minister shall prepare public statements to inform citizens while avoiding panic or disinformation. The information must be accurate and based on the current situation, and must not contain sensitive technical information. Media management in the event of a cybersecurity crisis shall be carried out in accordance with Annex I of this procedure.

3.2 Information collection and data management

The Authority, in cooperation with CERT shall collect, analyze, and store data and information that may assist in the identification, mitigation, and recovery from the consequences of large-scale incidents. The key elements for information collection and data management are as follows:

3.2.1 Real-time data collection

- Security monitoring systems shall be employed to collect information in real time. These systems may identify suspicious network activities and record data related to potential incidents, such as suspicious IP addresses, abnormal requests, and unauthorized data movements.
- Activities on systems and servers shall be logged in order to create a complete trace of what has occurred. This may include system logs, network logs, and security event records.

3.2.2. Data classification and filtering

- Information shall be classified in order to distinguish important information from information that may not be necessary. This classification includes separating data into categories such as sensitive data, threat information, suspicious activities, etc.
- Data shall be filtered, as not all data are necessary for analysis. Data filtering to identify the most relevant information supports the investigation of the cyber incident and may assist in identifying the source of the attack.

3.2.3. Data storage and security

- The collected data shall be stored securely so that they can be analyzed in the future and used as evidence if necessary. Storage may include the use of dedicated secure servers, employing encryption and access controls to keep the data protected.
- Data shall be stored with full integrity. Data must not be manipulated or modified by unauthorized third parties. The use of encryption methods and integrity controls may help ensure the security of these data.

3.2.4. Data analysis and threat identification

- The collected and stored data shall be analyzed in order to understand the nature and scale of the cyber incident and to identify suspicious characteristics, with the objective of understanding the manner in which information systems and networks have been compromised.
- *Threat intelligence shall be employed*, a process that includes the collection of external information on current threats and its use to improve the response to the cyber incident.

3.3 National resources and capacities for response to and management of the cybersecurity crisis in Albania

Addressing cybersecurity crises requires effective coordination and the utilization of national resources and capacities across all sectors. Ministries, state institutions, operational structures, and non-governmental actors possess specific capacities, which must be integrated into a comprehensive approach in order to ensure an effective response to cybersecurity crises.

3.3.1 Entities in charge:

1. Council of Ministers;
2. Prime Minister;
3. National Cybersecurity Authority / National CSIRT;
4. CERT / Cybersecurity Emergency and Cyber Security Crisis Response Team;
5. Sectoral CSIRT;
6. CSIRT at the operator;
7. Commissioner for the Right to Information and the Protection of Personal Data;
8. Albanian State Police.

3.3.2 Roles and responsibilities of the entities responsible for cybersecurity in the response phase

3.3.2.1. The Council of Ministers, in its capacity as a collegial body, upon the proposal of the Prime Minister, shall adopt decisions on:

a) The declaration of the cyber crisis for a period of 7 days.
b) The extension of the period of the cyber crisis, provided that such extension does not exceed a period of 30 days.

3.3.2.2 The Prime Minister **shall** submit to the Council of Ministers the proposal for declaring a cyber crisis state for a period of 7 days, as well as the extension of the cyber crisis state period, provided that such extension does not exceed 30 days, following the receipt of the proposal for declaring the cyber crisis state from the Authority.

3.3.2.3 The National Cybersecurity Authority / National CSIRT is an authority vested with with regulatory and coordinating competences, cyber incident and cybersecurity crisis response team, and exercises the following roles and responsibilities:

a) Proposes to the Prime Minister, in coordination with security and defence institutions as provided for in, point (a) of article 11, of Law no. 25/2024 "On Cybersecurity", the declaration of a cyber crisis state and emergency measures to address the situation;
b) Convene the *ad hoc* CERT structure;
c) Coordinate the management of the cybersecurity crisis;
ç) Issue decisions of a general nature or adopt protective measures of a general nature.

3.3.2.4. CERT, the Cybersecurity Emergency and Security Crisis Response Team

It is an ad hoc structure that serves as the first line of protection for the handling of cybersecurity emergencies and crises.

Main tasks shall include the following:

a) Coordination and rapid intervention for the handling of large-scale cyber incidents and cybersecurity crises;
b) Drafting the emergency measures plan;
c) Management and resolution of the cybersecurity emergency and crisis;

ç) Supports the drafting of recommendations to restore information systems and networks to normal operation within information infrastructures after a large-scale incident and a state of cybersecurity emergency and crisis.

3.3.2.5. Sectoral CSIRT, in its capacity as the cyber incident response team of the respective sector shall:

a) Report to the National CSIRT the cyber incident that has occurred in the information infrastructures of the respective sector;
b) Coordinate with CSIRTs at operators to respond to the situation.

3.3.2.6. CSIRT at the operator, in its capacity as the cyber incident response team of the respective operator shall:

a) Report the incident that has occurred in the information infrastructures at the operator at the National CSIRT and the Sectoral CSIRT;
b) Coordinate with the national CSIRT and the sectoral CSIRT to respond to the situation

3.3.2.7. Commissioner for the Right to Information and the Protection of Personal Data inits capacity as the institution in charge for drafting policies for the protection of individuals' personal data, shall monitor the implementation of the relevant legislation in cases of large-scale incidents and cybersecurity crises:

a) Manage, oversee, and monitor the implementation of the legislation in force on the protection of personal data.

3.3.2.8 Albanian State Police, in its capacity as the institution responsible for the investigation of cybercrime, in implementation of the legislation in the criminal field, shall carriy out the following actions:

a) Carry out the necessary operational/ procedural actions within the framework of the implementation of criminal legislation.
b) Cooperate with the National CSIRT and the CSIRT at the operator for the analysis and investigation of the cyber incident
c) Carry out procedural actions within the framework of the implementation of penal legislation.

4. RECOVERY PHASE

4.1 Recovery of services after the cybersecurity crisis

Post-cyber crisis recovery constitutes a coordinated process aimed at restoring the critical services and functions of the information infrastructure to a stable state. This process shall ensure the continuity of operations and the restoration of security, minimizing the long-term impacts of the crisis and improving preparedness for future incidents. Actions shall include assessing damages, gradually restoring systems and services, continuous monitoring for stability and security during the recovery process, as well as documenting lessons learned to improve procedures and playbooks for managing future incidents.

4.2 Post-crisis assessment and resilience improvement

4.1.1 After the stabilization of the situation, NCSA shall proceed to the retrospective analysis phase (*post-incident review*), which includes the following actions:

a) Document all events, responses, and lessons learned;
b) Analyze whether the security protocols were sufficient;
c) Prepare the Final Cybersecurity Crisis Report, which includes:
    i. the technical description of the event;
    ii. the assessment of damage and costs;
    iii. the measures taken;
    iv. recommendations for improvement.

4.1.2.This report shall be submitted to the Prime Minister and, as applicable, to the Parliamentary Committee on National Security.

4.1.3. Based on the Final Cybersecurity Crisis Report, NCSA shall draft or update:

a) Procedures for responding to cyber incidents;
b) National digital security policies;
c) Training and awareness plans for public personnel and critical infrastructure operators.

ANNEX I

MEDIA MANAGEMENT IN A CYBER CRISIS SITUATION

1. The importance of media management in the event of a cyber incident

The National CSIRT, in coordination with law enforcement institutions, relevant regulators, line ministries, and the media, play a decisive role in managing media channels in the event of a cyber crisis. Citizens must receive reliable, up-to-date, and verified information.

These institutions must provide effective information that can save lives, reduce the scope of damage, and encourage the population to take the necessary protective measures. In such cases, **communication that is proactively initiated** has proven to be more effective in defining the boundaries of an incident when shared with the public, in order to prevent panic and ensure credibility to the population

2. During coordination with the media, the following elements shall be taken into consideration

a) **Public criticism**- Cyber incidents that receive media attention sometimes lead to criticism that may come from cybersecurity professionals who may not be directly involved in the operational details, as well as from stakeholders who routinely work with the affected entity.
b) **Attacker identity**–The attacker, particularly a state or activist, seeks media attention and visibility regarding the attack and its impact on the public. Often, one of the objectives of an attack is to generate a media "buzz". Sometimes, the attacker will attempt to impersonate

another entity in order to confuse or hinder attribution. The attacker's identity is the most interesting topic for the media, but it is important to note that the attacker's identity is usually uncertain and requires time during a cyber investigation to link it to a specific actor.

c) **Differences between infrastructures**–The public will not always be able to distinguish between critical infrastructure and private responsibility as opposed to national responsibility

ç) **Cybersecurity is a complex technological language** that is largely difficult for the public to understand, and there are knowledge gaps among different population groups.

d) **Cyber incidents have political implications** – Certain statements may affect relations with other countries and influence subsequent actions.

dh) **The type and nature of the attack** usually do not generate media interest; rather, it is the consequences that attract attention, although there are cases that generate interest when the incident is particularly sophisticated.

e) **Everything shall be interconnected** – Cybersecurity affects all aspects of life.

ë) **The cyber attacker may cause damage to physical assets** (infrastructure, services, operational continuity, transport disruptions, etc.) and damage to situational awareness (undermining national resilience, creating uncertainty, , impairing preventive capabilities, and causing systemic failures).

Target Audience	Objectives and goals of the information
Population directly affected by the incident – clients, entities, residents of a specific area, etc.	▪ The incident and the situation shall be described in a credible manner ▪ Guidance shall be provided ▪ Trust shall be ensured in the various entities and in their ability to manage the incident ▪ Disinformation shall be avoided ▪ Unified messages shall be conveyed by all involved parties ▪ Messages shall be adapted to the different populations affected by the incident- level of awareness, technological literacy, languages, cultural differences, different communication channels, and influencers.
General public	▪ Public trust shall be strengthened ▪ Transparency shall be ensured ▪ Disinformation shall be avoided ▪ Unified messages shall be conveyed by all involved parties
Communications from different service providers	▪ Unified messages shall be conveyed ▪ Transparency shall be ensured

	▪ Disinformation shall be avoided ▪ Trust shall be strengthened in the service provider entity and in its capacity to manage the incident
Government bodies	▪ Unified messages shall be conveyed ▪ Transparency shall be ensured ▪ Disinformation shall be avoided ▪ Trust shall be strengthen in the capacity to manage the incident
Regional arena (adversaries and opponents)	▪ Prevent / hinder the adversaries' achievements
International arena	▪ Consolidation of partnerships/coalitions against the attacker ▪ Delegitimization of the attacker and the attack

Table 2. Summary of the Target Audience

3. Challenges in Crisis Communication

a) **Maintaining a balance between speed and caution in the provision of information** – while rapid reporting, even if partial, helps guide communication, it is necessary to pay attention to statements that make strong claims, as they may not be fully verified and could subsequently prove inaccurate.
b) **Avoiding disclosure when there is no information available** – in situations of risk and crisis, **the absence of information** can be a major factor in generating public panic;
c) **Maintaining public trust in state authorities and in the digital space** – it is important to provide comprehensive and reliable information, to demonstrate commitment and strength in the actions undertaken to manage the incident, and to show that the crisis can be handled. Furthermore, responsibility must be assumed where necessary, demonstrating leadership and improvements or lessons learned.

4.Cases in which issuing a notification should be considered favorably

a) Damage to or attempts to damage information infrastructures that lead to the disruption of critical services for the public, such as transport, supply of goods, healthcare services, water, electricity, etc.
b) Damage to a service that is of public interest or to a specific group of individuals.
c) Damage to an information infrastructure that is interconnected with other infrastructures and poses a risk to them; in such cases, it is necessary to warn stakeholders associated with the affected information infrastructure.

ç) Attempts with broad economic impact that do not result in damage to physical assets and have been successfully stopped.

d) Disclosure of information that is of public interest or importance to the general public or to a large group of people.

dh) Disruption of important databases.

e) An activity that "creates noise" or has wide-ranging consequences for the public.

ë) Damage to a service, a government symbol, or a symbolic entity.

f) Financial impact– a targeted or widespread incident that causes significant damage to a financial institution and may undermine public confidence in the Albanian financial system.

g) Causing significant damage to information infrastructures that results in a significant negative impact on the functioning of a large number of information infrastructures, affecting the continuity of their services or essential processes.

gj) An incident that affects people's mindset and/or disinformation that affects public trust as a result of the cyber event. This includes the damage (defacement) of a major central website or an information bulletin board containing vital information.

h) Attempts aimed at damaging public safety and societal security, or an incident that, directly or indirectly, results in personal harm to an individual.

5. Addressing disinformation and fake news

Fake news and disinformation constitute a global problem. During an incident, it is recommended to address the phenomenon quickly and effectively by using the following tools:

a) Monitor false information through online discussion monitoring systems and/or by assigning a person within the infrastructure to actively search social media channels. It is possible to establish a command center to monitor and respond, or to use existing operations rooms.

b) Decision-making on the type of content to be addressed– identifying which disinformation is relevant according to certain criteria, which undermines public trust, and what is misleading and may cause harm.

c) Disseminate reliable information continuously and promptlyin order to prevent the creation of a vacuum that will be filled with theories and falsehoods.

ç) Establish authority and trust in the institution's information and channels by using domestic or external experts, videos, images, and texts.

d) Provide examples by using the disinformation itself – demonstrate what is false and why in order to refute the claim. The public is encouraged to share accurate information. For example, take a screenshot of fake news and add a label stating "Fraud / Warning! Fake news!". An article may be published explaining the issue alongside the false information.

dh) When the media disseminate fake news or disinformation, it is important to clearly indicate their error.

e) Use external individuals who will act and respond to false information.

ë) Highlight specific cases in the media to raise public awareness of the phenomenon, explain the phenomenon, define what constitutes false information, and how it can be debunked. Encourage critical thinking.