REPUBLIKA E SHQIPËRISË
AUTORITETI KOMBËTAR PËR SIGURINË KIBERNETIKE

Nr.1128 prot. Tiranë, më 27.12.2024

U R DH Ë R

Nr.534 datë 27/12 / 2024

"PËR
MIRATIMIN E PLANIT KOMBËTAR PËR REAGIMIN NDAJ INCIDENTEVE TË SIGURISË KIBERNETIKE NË SHKALLË TË GJERË DHE NDAJ KRIZËS KIBERNETIKE"

Në zbatim të nenit 28, pika 8 të ligjit nr. 25/2024 "Për sigurinë kibernetike",

U R DH Ë R O J:

1. Miratimin e Planit Kombëtar për Reagimin ndaj Incidenteve të Sigurisë Kibernetike në Shkallë të Gjerë dhe ndaj Krizës Kibernetike, sipas tekstit që i bashkëlidhet këtij urdhri dhe është pjesë përbërëse e tij.

2. Ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike dhe të gjitha institucionet përgjegjëse, të cilat kanë role dhe përgjegjësi specifike të përcaktuara në Planit Kombëtar për Reagimin ndaj Incidenteve të Sigurisë Kibernetike në Shkallë të Gjerë dhe Ndaj Krizës Kibernetike, për zbatimin e këtij urdhri.

3. Ky urdhër hyn në fuqi menjëherë

DREJTOR I PËRGJITHSHËM

Igli TAFA

Adresa: Rruga "Papa Gjon Pali II" nr.3Tiranë;
Faqe web: www.aksk.gov.al E-mail: info@aksk.gov.al
Tel./Fax : 04 2221 039

REPUBLIC OF ALBANIA
NATIONAL CYBER SECURITY AUTHORITY

No. 1128 Prot Tirana, on 27.12.2024

ORDER

No. 534 date. 27/12/2024

ON
"APPROVAL OF THE NATIONAL PLAN FOR RESPONSE TO LARGE-SCALE CYBERSECURITY INCIDENTS AND CYBER CRISIS"

Pursuant to article 28, paragraph 8, of law no. 25/2024, "On Cyber Security",

I HERBY ORDER:

1. Approval of the National Plan for response to large-scale cybersecurity incidents and cyber crisis, according to the text attached to this order, which constitutes an integral part thereof.

2. The National Cyber Security Authority and all responsible institutions, which have specific roles and responsibilities defined in the National Plan for response to large-scale cybersecurity incidents and cyber crisis, are charged with the implementation of this order.

3. This order enters into force immediately.

GENERAL DIRECTOR
IGLI TAFA

Signature

NATIONAL PLAN FOR RESPONSE TO LARGE-SCALE INCIDENTS AND CYBER CRISIS

Table of Contents

Section 1. Basic information

Section 1A: The cybersecurity situation in Albania

Cybersecurity in Albania has received special attention in recent years, especially due to the serious attacks that have occurred on the country's digital infrastructure. Albania, like many other countries, faces considerable challenges in this field due to increasing digitalization, the lack of robust protective infrastructure, and limited awareness of cyber threats.

Current state of cybersecurity in Albania

1. Cyber-attacks experienced
   - In 2022, Albania faced several significant cyber-attacks that were attributed to a foreign state. The attacks targeted government services and electronic communications infrastructure.
   - Platforms such as *e-Albania* and other digital systems suffered disruptions, affecting the delivery of public services.
   - This incident revealed vulnerabilities in the protection of critical systems and prompted swift interventions to strengthen security.
2. Cybersecurity infrastructure and policies
   - Since 2017, Albania has established the responsible authority for cybersecurity. The National Cybersecurity Authority, based on the provisions of law no. 25/2024 "For cyber security", is the institution responsible for monitoring and protecting networks and information systems from cyberattacks.
   - The National Cybersecurity Strategy, adopted by Decision of the Council no.1084, dated 24.12.2020 "On the Approval of the National Cybersecurity Strategy and Action Plan 2020–2025," aims to strengthen capacities and increase awareness.
   - Cooperation with international partners such as NATO, the European Union, and other agencies is key to enhance cybersecurity standards.
3. Major challenges
   - Lack of cybersecurity experts: The country faces a shortage of specialists in the field of cybersecurity.
   - Lack of awareness: Individuals and businesses often do not recognize the threats and best practices for data protection.
   - Outdated technology: Many systems and information networks rely on outdated infrastructure and are vulnerable to cyber threats.
4. Measures undertaken
   - Increased investments in cyber defence and new technologies.
   - Modernization of the legal framework.
   - 24/7 real-time monitoring of information infrastructures.
   - Organization of trainings for institutions, businesses, and individuals.
   - Legal provision for the establishment of a CERT, an ad hoc structure for managing and coordinating large-scale incidents and cyber crises.
   - Implementation of cybersecurity measures for critical sectors such as energy, finance, telecommunications, and others.

The role of international partners

Due to NATO membership and the EU integration processes, Albania has received technical and financial assistance to improve cybersecurity. International partners provide:

- Training and expertise to strengthen capacities in the field of cybersecurity.
- Technology and financial support to modernize the systems and information infrastructures networks.

In summary, cybersecurity in Albania is in a development phase, but significant challenges remain due to low awareness and outdated technology. Nevertheless, with international support and the commitment of local institutions, the country is on the right track to improving protection against cyber threats.

Introduction and background

In recent years, with the increased use of information and communication technologies, as well as the advancement of digital services and infrastructures, cybersecurity threats have become increasingly prevalent and sophisticated. This phenomenon is global and knows no borders, making the management of cyber incidents and crises a significant challenge for all states. Cybersecurity incidents can range from simple attacks to more sophisticated ones, such as disruption of critical services, theft of sensitive information, or the destruction of critical and important information infrastructures.

Albania, as a NATO member state aspiring to join the European Union, has taken significant steps to establish a strong cybersecurity framework, considering it a high-level priority. In March 2024, Albania adopted the cybersecurity law, partially aligned with Directive NIS 2, No. 2022/2555**,** of the European Parliament and Council, dated 14 December 2022, "On measures for a high common level of cybersecurity across the European Union," which amended Regulation (EU) No. 910/2014 and Directive (EU) No. 2018/1972**,** and repealed Directive (EU) No. 2016/1148"**,** which marked a significant step in modernizing the legal framework with the aim of achieving a high level of cybersecurity for networks and information systems in the Republic of Albania. The law has been followed by numerous activities aimed at building national capacities and improving cooperation among various institutions.

Following a significant increase in cyberattacks, the Albanian government began strengthening structures for managing and responding to cyber incidents by establishing and operationalizing the National Cybersecurity Operations Centre under the National Authority for Cybersecurity, while intensifying cooperation with NATO, the European Union, and partner countries.

This national plan is an instrument to ensure that Albania is prepared to face any potential cybersecurity incident or crisis, protecting information infrastructures and ensuring the continuity of key services. To achieve coordinated and effective management of cyber incidents and crises, it is essential to involve all relevant actors, including the government, the private sector, and civil society. Through collaboration, coordination, and continuous cybersecurity training, Albania will be able to confront cybersecurity challenges and respond swiftly and efficiently to minimize potential impacts. The development of this plan for responding to large-scale cybersecurity incidents and crises aims to establish a comprehensive and structured framework for identifying, managing, and responding to cybersecurity incidents and crises that could threaten the normal functioning of Albanian society and economy.

Within this context, the plan aims to:

1. Coordinate and cooperate among state institutions, the private sector, and international organizations to create a secure and reliable network for managing cyber incidents, assisting in minimizing the impact of cyber crises, and ensuring the rapid and efficient exchange of information and protective measures among states, agencies, and other actors involved in cybersecurity.
2. Prepare institutions and infrastructures to respond to cybersecurity threats, including measures for incident prevention and lessons learned from previous situations.
3. Enhance response and intervention capacities to successfully manage significant cybersecurity incidents and ensure the continuity of public and private services and functions.

Importance, aims, and objectives of the National Plan for responding to large-scale incidents and cyber crisis

- The importance of a National Plan for responding to large-scale incidents and cyber crisis

Albania's approach to digitalizing services and interconnected technologies has significantly increased its vulnerability to cyber threats, which range from attacks *ransomware* on critical information infrastructures, destruction and exfiltration of data, and even disinformation campaigns. These threats can disrupt public services, harm the economy, and erode public trust. A national plan offers a coordinated and systematic approach to address these challenges, ensuring that Albania is prepared to manage large-scale incidents and complex cyber crises. A National Plan for responding to large-scale incidents and cyber crises is a critical instrument for any state aiming to protect its key infrastructures, guarantee national security, and ensure the continuity of essential services during cyber crises. Such a plan provides a framework for identifying, analysing, and managing potential risks before, during, and after incidents. The plan enables a coordinated and effective response by defining the roles and responsibilities of all actors involved, including state institutions, the private sector, and other parties involved in cyber defence, thereby avoiding confusion and optimizing the response in emergency situations. Furthermore, the plan establishes mechanisms to ensure continuity of operations and rapid recovery of systems after an attack. This is essential to prevent long-term disruptions that could have significant economic and social impacts. By drafting and adopting this plan, Albania demonstrates its commitment to enhancing the level of national cyber security and aligning with the international standards and best practices. The plan serves a strategic guide aimed at providing a clear framework to ensure preparedness for responding to large-scale incidents and cyber crises.

- Objectives of the National Plan for responding to large-scale incidents and cyber crisis

The Plan is based on three main aims:

1. Prevention of incidents and risk reduction: Proactively identifying vulnerabilities, improving protective measures, and minimizing the likelihood of cyber crises.
2. Effective incident response: Establishing robust mechanisms for detecting and mitigating cyber incidents to reduce their impact on national security, the country's economy, and its citizens.

3. Recovery and continuity: Ensuring the rapid recovery of critical and essential systems and services, maintaining their continuity without interruption.

- Objectives of the National Plan for responding to large-scale incidents and cyber crises

The Plan is structured around three main objectives, each essential for increasing the level of cyber security, protecting Albania's national security, and ensuring economic stability and social well-being, as follows:

1. Providing an effective proactive and reactive framework for large-scale incidents and cyber crisis

A well-defined, effective proactive and reactive framework for incidents is the foundation of the National Plan for responding to large-scale incidents and cyber crisis. It establishes clear protocols for preparedness, detection, analysis, and resolution of cyber incidents in a rapid and efficient manner. This framework ensures that all actors, state institutions, private organizations, and critical information infrastructure operators are equipped with the necessary tools, knowledge, and communication channels to mitigate threats. By standardizing effective proactive and reactive actions, the plan minimizes confusion during crises and facilitates a rapid return to normal operations.

2. Minimizing the impact of large-scale incidents and cyber crisis

The plan aims to reduce the potential damages caused by cyber incidents to Albanian's national security, the economy, and society. Cyber-attacks may disrupt essential services, compromise sensitive data, and erode public trust. By implementing proactive measures such as risk assessment, continuous monitoring, and rapid recovery strategies, the plan ensures that critical infrastructure and services remain operational even in the face of major disruptions. This approach not only protects Albania's digital assets but also strengthens public confidence in the country's ability to confront with cyber threats.

3. Coordination among key actors

Effective coordination between state institutions, the private sector, and international partners is essential for a comprehensive response to cyber crises. The National Plan for responding to large-scale incidents and cyber crises fosters cooperation by defining roles and responsibilities, encouraging information sharing, and leveraging the expertise of all actors. Cooperation with international organizations, such as NATO and the European Union, ensures that Albania benefits from global best practices and contributes to collective efforts for cyber security.

Summary

1. Country context and risk profile

With the increasing use of the internet and the digitalization of services, Albania is becoming increasingly exposed to cyber threats. These threats may originate from individuals, criminal groups, states, or other actors with varying objectives, including espionage, sabotage, and theft of sensitive information. In this context, Albania faces an urgent need to ensure a rapid and coordinated response to large-scale incidents and cyber crises, with the aim of safeguarding services continuity and protecting information infrastructures and national security.

Cyber attacks against Albania peaked in 2022, several weeks after the expansion of online services. During this period, Albania faced a distinct cyber risk profile, where despite the shutdown of some key services, the country managed to withstand these unprecedented cyber attacks, especially those from the state of Iran, ensuring that information on its networks and systems remained secure.

Cyber threats occur due to several factors such as:

- Albania's geostrategic position, NATO membership, and international cooperation make it a potential target for cyber attacks from other states seeking to create instability or steal sensitive information. This risk is also possible due to Albania's various interactions in international affairs.
- Unlimited access by employees to the networks and information infrastructure systems. Cyber threats and incidents may also originate from insider actors, such as employees who have access to information systems and infrastructures.
- The lack of investment in information infrastructures, exposure to natural hazards and technological disasters. These are factors that may cause significant damages, such as data loss, service disruptions, and difficulties in managing cyber crises.

In this context, the National Plan for responding to large-scale cyber security incidents and cyber crises should be an instrument that addresses a wide range of threats and risks present in Albania, with a primary focus on close cooperation and coordination between state institutions, the private sector, and international partners, with the aim of minimizing possible impacts and providing rapid assistance for the restoration and normalization of the situation in the event of large-scale incidents or cyber crises.

1.1 Guiding principles for responding to large-scale incidents and cyber crises

1.1.1. Proactivity

The principle of proactivity in responding to large-scale incidents and cyber crises is an essential approach to facing and mitigating the impact of cyber threats. This principle involves preventive actions and preparation for rapid response before incidents occur, based on continuous monitoring, risk analysis, and possible cyber crisis scenarios.

When a large-scale cyber crisis occurs, proactivity ensures a rapid, coordinated, and effective response, including:

1. Identification and isolation of the threat in real time.
2. Coordination of all stakeholders to manage the crisis (technical teams, leadership, law enforcement institutions).
3. Assessment of the impact to understand the consequences of the cyber security crisis and to prioritize actions.
4. Rapid recovery of compromised information systems and data.
5. Clear public communication to ensure transparency and minimize panic.

1.1.2. Clear communication

The principle of clear communication during the response to large-scale incidents and cyber crises is essential to ensure effective coordination, rapid problem resolution, and minimization of the impacts of the cyber crisis. This principle focuses on the dissemination of accurate, structured, and timely information to all involved parties.

Steps for effective communication during a cyber crisis are as follows:

1. Identification of the communication team: Defining the persons responsible for official communication.
2. Preparation of pre-drafted messages for different cyber crisis scenarios to reduce response time.
3. Coordination of internal and external communication to ensure a consistent message.
4. Clear and transparent statements that describe the situation without creating panic.
5. Monitoring of public perception to address misunderstandings or misinformation.

1.1.3. Responsibility and role

The principle of responsibility and role in responding to large-scale incidents and cyber crisis is essential to ensure that every person, team, or entity involved has clear duties and responsibilities. This principle ensures that the response to large-scale incidents is organized, efficient, and avoids delays or miscoordination in critical situations. This principle includes:

1. Clear definition of roles and responsibilities for individuals and teams involved in the response process.
2. Establishment of a hierarchy and organized structure to enable rapid response.
3. Ensuring that every involved party knows exactly what is expected of them to fulfill their duties during a large-scale incident and cyber crisis.

1.1.4 Continuous risk assessment

The principle of continuous risk assessment in response to large-scale incidents and cyber crisis is essential to ensure that the information infrastructure has a clear framework of existing, new, and emerging risks throughout the entire cyber incident management cycle. This principle focuses on the ongoing analysis of risks in order to make informed decisions and proactively and effectively minimize the impact of the cyber crisis.

Continuous risk assessment is a dynamic process that aims to:

a. Identify new and existing risks throughout the entire cyber crisis situation.
b. Analyse and assess the impact of these risks.
c. Continuously monitor to detect changes in the level of cyber threats.
ç. Taking preventive and corrective measures to reduce the effects of cyber incidents.

1.2 Legal and regulatory framework

The legal and regulatory framework forms the foundation of Albania's National Plan responding to large-scale incidents and cyber crises, providing clear guidance for the prevention, management, and response to cyber incidents/threats. This framework integrates national legislation, international instruments, and best practices to ensure a safe and resilient digital environment.

By harmonising national legislation with *acquis* of the EU and international best practices, Albania demonstrates its commitment to maintaining a secure and resilient digital ecosystem. This framework not only addresses current challenges but also positions Albania to adapt to the dynamic nature of future cyber threats.

The National Plan for responding to cyber incidents and crises of Albania derives from the obligations set forth in law no. 25/2024 "On Cybersecurity" and its implementing secondary legislation. This plan provides a strategic reference framework for responding to large-scale

cyber incidents and crises, aiming to ensure effective management of cyber crisis situations and the protection of information infrastructures and national security.

Summary of legislation on cyber security in Albania

Albania has implemented a series of legal measures to address the evolving challenges of cyber security:

Law No. 25/2024 "On Cyber Security"

- Establishes the legal framework for the protection of information infrastructures.
- Defines the obligations of the subjects of the law (operators of information infrastructures) regarding the adoption of security measures to enhance the level of cybersecurity in networks and information systems.
- Sets clear obligations for information infrastructures operators regarding the mandatory reporting of cyber incidents to the National Cyber Security Authority to ensure timely handling of incidents and minimize their consequences.
- Defines clear structures for incident handling and cyber crisis management, including the Cybersecurity Incident Response Team (CSIRT) at the national, sectoral and operator levels, the Cybersecurity Emergency and Crisis Response Team (CERT), and the National Cybersecurity Operations Centre (SOC).
- Identifies other entities responsible for the security of networks and information systems in the Republic of Albania.
- Strengthens the concept of cooperation between the National Cyber Security Authority and national and international institutions, as well as other bodies in the field of cyber security.

Law on the Protection of Personal Data

- Regulates the collection, processing, storage, and destruction of personal data.
- Establishes strict measures to protect sensitive information from unauthorized access and breaches.

Law on Electronic Communications

- Ensures the integrity and security of electronic communications networks and services.
- Introduces measures for incident response and disaster recovery in the telecommunications sector.

National Cybersecurity Strategy

- Provides a strategic vision for improving Albania's cyber security resilience.
- Emphasizes capacity building, intelligence sharing on cyber threats, and cooperation with international partners.
- Sets concrete objectives regarding the enhancement of the level of cyber security in networks and information systems in the Republic of Albania, as well as the roles and responsibilities of the institutions responsible for cyber security in the country.

Compliance with *acquis* of the EU and international best practices

The legal framework in the field of cyber security of Albania is aligned with *acquis* of the European Union and international standards to ensure consistency and interoperability.

NIS 2 Directive, No. 2022/2555, of the Parliament and the Council, dated 14 December 2022, "On measures for a high common level of cyber security throughout the European Union, which has amended Regulation (EU) No. 910/2014 and Directive (EU) No. 2018/1972, as well as repealed Directive (EU) No. 2016/1148.

- Strengthens cyber security measures in essential services and critical information infrastructure sectors.

- Sets standards for risk management and the reporting of cyber incidents, which Albania has integrated into its national legislation.

General Data Protection Regulation (GDPR), No. 679/2016, of the European Parliament and of the Council, dated 27 April 2016, on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

- National legislation for the protection of personal data complies with the requirements of the GDPR, ensuring the secure processing of personal data and compliance with EU standards.

Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime, adopted by the Council of Europe in 2001, is the main international agreement aimed at addressing cybercrime and improving international cooperation in this field. Albania has ratified this Convention, incorporating it into the national legal framework for combating cybercrime. The main points of the Convention and its significance for Albania include:

1. The criminalization of cyber activities

The Convention defines actions that should be considered as criminal offences, including:

- Unauthorized access to computer systems (hacking).
- Disruption of data or services (DDoS attacks).
- Interference with data (manipulation or deletion).
- Production and distribution of malware.
- Piracy and infringement of intellectual property rights.
- Computer fraud and online identity theft.

2. Electronic evidence

- The Convention lays down rules for the collection, preservation, and use of electronic evidence in investigative and judicial proceedings.
- It defines methods for temporary data preservation (*protection of data*), which is particularly important for prosecuting crimes committed online.

3. International cooperation

- Establishes a framework for rapid and effective cooperation between member countries to investigate and prosecute cybercrimes.
- Includes the exchange of information, mutual legal assistance, and the execution of requests for evidence or extradition.

4. Albania's role in the region

- As a Western Balkan country, Albania plays an important role in regional cooperation on cybercrime, benefiting from the mechanisms of the Convention for the exchange information and joint investigations.

5. Awareness-raising and capacity building

- Through the Convention, Albania has access to international programs for capacity building in the fight against cybercrime.
- Trainings and technical assistance from international partners help Albanian authorities address technological challenges.

6. Enhancing security and public trust

- Implementing the Convention's standards helps increase the security of computer systems and protect citizens from cybercrime.
- Promotes public and investor confidence in Albania's digital infrastructure.

The ratification of the Budapest Convention and its effective implementation are important steps for Albania in protecting cybersecurity and prosecuting cybercrime in an increasingly digitalized environment.

1.3 Sustainable Development Goals

The Sustainable Development Goals (SDGs) are highly relevant in the field of large-scale incident and cyber crisis management, as they link social, economic, and technological aspects to build a safer and digitally sustainable cyberspace. Managing large-scale incidents and cyber crises is particularly connected to several of these goals to ensure resilience, security, and overall societal development.

1**. Digital infrastructure security is key to industrial development and innovation**

- Purpose: Develop secure and resilient information infrastructures capable of withstanding cyberattacks.
- Strategies:
  - Strengthening cybersecurity in critical information networks and systems such as energy, finance, water, health, telecommunications, etc.
  - Invest in new technologies to prevent and detect cyberattacks and risks.
  - Promote scientific research for digital security.

2. Cybersecurity is a key part of the digitalisation process of services and sustainable communities.

- Purpose: Ensuring intelligent systems and the protection of citizens' data in digital spaces.
- Strategies:
  - Establish protective systems for information infrastructures for digital services.
  - Strengthening policies for data privacy.
  - Preparing society to cope with cyber crises through response plans.

3. Education with the aim of increasing awareness and skills to cope with cyber threats

- Purpose: Education on cybersecurity from the early stages of schooling.
- Strategies:
  - Development of training programs for digital skills and cyber crisis management.
  - Public awareness of security practices and the importance of information protection.
  - Creating a culture of cybersecurity at all levels of society.

4. Encouraging businesses to invest in secure networks and systems

The modern economy depends on digital ecosystems that must be protected to ensure sustainable growth.

- Purpose: Protection of businesses and the labor market from cyber-attacks.
- Strategies:
  - Increasing investments in cybersecurity for the protection of businesses.
  - Creation of new jobs for cybersecurity experts.
  - Support for MSMEs (Micro, Small and Medium Enterprises) to implement security standards.

5. Creation of sustainable policies with the aim of increasing the level of cybersecurity in networks and information systems

- Purpose: Development of sustainable policies for protection against cyber-attacks and promotion of a secure digital environment.

- Strategies:
  - Establishment of a sustainable legal framework for cybersecurity and the fight against cybercrime.
  - Strengthening the capacities of responsible institutions to manage cyber crises.
  - International cooperation for the exchange of information on global threats.

6. **International cooperation in the fight against cyber crises.**
   - Purpose: Establishment of international partnerships to address cyber threats.
   - Strategies:
     - Cooperation with international organizations for the exchange of knowledge and best practices.
     - Establishment of joint response mechanisms to cyber crises.

1.4 The role of AI in responding to large-scale incidents and cyber crises

Artificial Intelligence (AI) plays an increasingly important role in addressing the complex challenges of cybersecurity, especially in cases of large-scale incidents and cyber crises. Below are some of the main ways in which AI contributes to this field:

1. Real-time threat detection
   - Behaviour analysis: AI uses advanced analytics to identify abnormal behaviours in networks and information systems. This includes monitoring network traffic and user behaviour to detect potential cyber-attacks.
   - Pattern identification: AI algorithms can detect patterns and anomalies that are too complex to be captured by traditional monitoring systems.
2. Automation of response to cyber threats
   - Rapid response: AI can make automated decisions to isolate a compromised system, preventing the spread of the cyber-attack.
   - Orchestration of responses: In the event of a cyber crisis, AI can coordinate the response between different teams and involved systems.
3. Forecasting and prevention
   - Risk modeling: AI uses historical data and predictive analytics to assess vulnerabilities and suggest preventive measures.
   - Continuous learning: With each new cyber incident, AI algorithms learn and improve to address similar threats in the future.
4. Cyber crisis management
   - Processing of massive data: AI can analyse a large volume of data from multiple sources, including system logs, communications, and IoT sensors, to provide a complete overview of the situation.
   - Real-time decision making: AI can assist in determining the exact response measures by suggesting optimal solutions based on its analyses.
5. Strengthening Security Operations Centres (SOC)
   - Reduction of false alarms: AI can filter and prioritize cyber events to reduce the overload of false alarms.
   - Support for analysts: Provides recommendations and detailed analyses for security teams, improving their efficiency.
6. Improvement of communication during cyber crises

- Natural language analysis: AI can analyse reports, emails, and other communications to extract important information during a cyber incident.
- Global coordination: Enables the rapid exchange of information between geographically distributed teams.

7. Dealing with advanced and repeated attacks
   - Analysis of attacker patterns: AI can assist in identifying the methods used by threat actors by creating detailed profiles for advanced and recurring threats.

1.5 Risk assessment and the cyber threat landscape

Albania's digital landscape is increasingly vulnerable to a wide range of cyber threats due to the rapid adoption of technology in both the public and private sectors. Cyber-attacks targeting critical information infrastructure, data systems, and public services have increased in sophistication and frequency. Common cyber threats include:

- **Cyber Attacks**: Persistent cyber threats, such as attacks with *Distributed Denial of Service* (DDoS) and phishing campaigns, which disrupt operations and compromise sensitive information.
- **Disinformation**: Coordinated campaigns aim to destabilize public trust by spreading false information, often targeting political and social processes.
- **Ransomware:** Malware attacks that encrypt critical information systems and demand ransom for decryption have become a major concern, especially for the healthcare, finance, and government sectors.
- **Insider threats**: Vulnerabilities arising from human errors or malicious intent within the information infrastructure increase the risk of breaches and data loss.

These continuously evolving threats underscore the need for a robust cybersecurity strategy, tailored to the geopolitical and technological environment of the Republic of Albania.

Possible impacts on critical information infrastructure and public services

The potential consequences of cyber threats to Albania's critical information infrastructure and public services can result in serious and wide-ranging impacts, such as:

- Disruption of essential services: Cyberattacks can disrupt power networks, water systems, communication networks, and others, causing major social and economic consequences.
- Economic damage: Breaches in financial institutions can result in significant financial losses, decreased public and investor confidence, and hindered economic growth.
- Data compromise: Unauthorized access to sensitive information can jeopardize national security, undermine public trust, and expose individuals to identity theft and fraud.
- Operational disruption: Prolonged service interruptions in critical sectors, such as healthcare, transport, and others, can have life-threatening consequences.

The interconnected nature of these information infrastructures amplifies the chain effects of a single attack, highlighting the critical need for comprehensive cyber risk management.

Categories of cyber risks

➢ Threats to national security
- Cyberattacks against defence systems, intelligence databases, or border control mechanisms can weaken Albania's security posture.

- State-sponsored cyber operations and espionage activities pose significant risks to the sovereignty and diplomatic relations of Albania.

➢ Economic risks
- Ransomware attacks and financial fraud disrupt business operations, leading to revenue loss and damage to reputation.
- Cyberattacks targeting e-commerce platforms and financial institutions significantly reduce consumer trust in digital services.

➢ Social destabilization
- Disinformation campaigns manipulate public opinion, exacerbating social divisions and undermining democratic processes.
- Cyberattacks against public services can create panic and reduce society's trust in governance.

1.6 Organization of the response system to large-scale incidents and cyber crisis

1.6.1 Introduction

The organization of the response system to large-scale incidents and cyber crisis in Albania is a structured process aimed at enhancing the resilience and response of institutions and critical sectors in the face of cyber threats. This system relies on coordination among state, private, and international actors to minimize impacts and ensure the continuous functioning of society and the economy.

The structure of the response system to large-scale cyber incidents and cyber crises in Albania

1. Legal and strategic framework

The response system is based on national cybersecurity legislation and strategy, which include:

- The National Cybersecurity Strategy, which sets the priorities for the protection of information infrastructures and the development of capacities.
- Law no. 25/2024 "On Cyber Security", which sets out:
  - ➢ The identification of critical and important information infrastructures operators and the services provided by them.
  - ➢ The obligation of information infrastructure operators to implement cybersecurity measures for risk management.
  - ➢ Obligations for reporting cybersecurity incidents and the implementation of general protective measures.
  - ➢ The responsibilities of other entities responsible for cybersecurity.
- Bylaws pursuant to Law no. 25/2024 "On Cyber Security" which regulate:
  - ➢ The management of cybersecurity incidents.
  - ➢ The categorization of cybersecurity incidents.
  - ➢ The identification of information infrastructures.
  - ➢ The assessment and analysis of the level of cybersecurity.
  - ➢ The identification, classification, escalation, and management of cybersecurity crises.

The legal framework for the protection of personal data, which addresses the security and privacy of personal data.

1.6.2 The framework for the management of large-scale incidents and cybersecurity crisis

The framework for the management of large-scale incidents and cybersecurity crises provides Albania with a strategic and operational roadmap for addressing the complexity of cybersecurity incidents and crises. This framework covers the response to large-scale incidents and cybersecurity crises, adhering to the principles of coordination, transparency, and accountability, with the aim of strengthening the ability to protect information infrastructures, maintaining public trust, and enhancing national security in the face of evolving cyber threats. This framework not only addresses current challenges but also positions Albania to adapt to the dynamic nature of cybersecurity risks in the future.

The National Cyber Security Authority (AKSK) is the responsible institution in Albania for the managing cybersecurity incidents and coordinates actions with the relevant structures in the event of a cybersecurity crisis. The Authority, in its capacity as the National CSIRT, provides support and coordination to all institutions and operators of information infrastructures in the event of large-scale incidents and cybersecurity crises.

1.6.3 Institutions and structures responsible for responding to large-scale incidents and cybersecurity crises in Albania

1. Structure and main functions of AKSK
   - Monitoring and analysis: AKSK monitors networks and information systems to identify and analyse potential cyber threats and incidents.
   - Coordination of response: In the event of cybersecurity incidents/crisis, AKSK coordinates the response between various institutions and provides guidance for managing the situation.
   - Training and education: AKSK provides training and awareness-raising activities to enhance the capacities of institutions and individuals in the field of cybersecurity.
   - National and international cooperation: AKSK cooperates with national and international authorities, as well as international organizations, to improve cybersecurity at the national and international level.
2. Information infrastructure operators have the following responsibilities:
   - Risk management: Implementation of cybersecurity measures to protect information systems and networks.
   - Reporting of cyber incidents: Immediate reporting of any cyber incident to AKSK and sectoral CSIRTs to enable a coordinated response regarding the management of cyber incidents.
   - Cooperation: Cooperation between AKSK and sectoral CSIRTs for the purpose of information sharing during a large-scale incident and cyber crisis.
   - Continuity plan: Drafting and activation of business continuity plans to ensure the uninterrupted provision of services during a cyber incident.
3. Law enforcement agencies have the following responsibilities:
   - Investigation of cybercrimes: Identification and apprehension of individuals or groups responsible for cyberattacks.

- Digital analysis: Conducting digital analyses to determine the scope and nature of cyber incidents.
- Public security: Coordination with other agencies to maintain public safety and order during a cyber crisis.

4. International Partners

Albania's engagement with international partners is essential for addressing cross-border cyber threats. Their role includes:

- Intelligence sharing: Sharing intelligence on threats and best practices with Albanian cybersecurity actors.
- Technical support: Provision of expertise, tools, and resources to assist in the management of complex cyber incidents.
- Capacity building: Supporting Albania in strengthening its cybersecurity capacities through training and resource allocation.
- Coordination of crisis response: Cooperation for joint responses to cyber crises that have regional or global implications.

1.6.4 Responsible entities in cyber crisis management

To manage the cyber crisis at the national level, the roles and responsibilities of each actor must be defined, starting from the highest executive levels, including:

1. Council of Ministers;
2. Prime Minister;
3. Interministerial Committee on Cybersecurity;
4. Ministers;
5. National Cybersecurity Authority/ National CSIRT;
6. CERT/ Cyber Emergency and Crisis Response Team;
7. The Head of the Institution;
8. Sectoral CSIRT;
9. CSIRT at the operator level;
10. Commissioner for the Right to Information and Protection of Personal Data;
11. State Police.

1.6.5 Identification, classification and investigation of the incident

Identification of the cybersecurity incident includes confirming that a suspicious activity constitutes a cyber incident. The identification of a cyber incident is carried out by analysing alarms and suspicious activities to determine if they are real and consistent.

The identification of a cybersecurity incident may be carried out by the National CSIRT, the Sectoral CSIRT, the infrastructure itself/CSIRT at the operator, or by automated systems managed by the relevant structure at the National Cybersecurity Authority and at the infrastructure operators.

In the case of identification of the incident by the National CSIRT or by the infrastructure operator itself, the relevant structure at the National Cybersecurity Authority (SOC T1) and the CSIRT at the operator, according to the categorization of the incident, in order to address the incident, execute the specific Playbook, in accordance with the provisions of the Regulation "On procedures for the management of cybersecurity incidents, countermeasures and playbooks" approved by order of the Director General of the Authority.

Classification of the cybersecurity incident includes the categorization of the incident based on its type and importance, with the purpose of planning actions for handling and resolving the cybersecurity incident pursuant to the Regulation approved by order of the Director General of the Authority "On the categorization of cybersecurity incidents".

Cybersecurity incident analysis includes a detailed investigation of the incident to understand the cause, profile, behaviour, and damage caused. This phase helps in developing strategies to prevent similar incidents in the future.

1.6.6 Phases of response to cybersecurity incidents

The phases of response to incidents defined in the National Plan for large-scale incidents and cybersecurity crisis in Albania provide a structured and effective approach to managing cyber threats. By emphasizing preparedness, efficient detection, rapid response, and continuous improvement, Albania strengthens its resilience against incidents and cybersecurity crises. This proactive and comprehensive framework ensures the protection of information infrastructure, public services, and national security in an increasingly digital age.

Response to cybersecurity incidents involves several phases, among which the most important are: **Preparation** which includes the creation of security policies, the formation of response teams to cybersecurity incidents (CSIRT), the development of response strategies, the determination of communication flows, the establishment of documentation systems, the provision of necessary tools, and the training of the team to ensure preparedness in cases of large-scale incidents.

The preparation phase focuses on building the foundations for an effective response to cybersecurity incidents by equipping actors with the necessary tools, capacities, and knowledge. The main activities include:

- Capacity building: Establishment of teams capable of responding to cybersecurity incidents within the National Cyber Security Authority and the operators of information infrastructures.
- Implementation of advanced technologies: Deployment of advanced technologies for monitoring, detection, and response to cyber threats, such as systems *Security Information and Event Management* (SIEM) and endpoint detection tools.
- Policy development: Drafting and regularly updating policies, protocols, and procedures for the management of incidents and cyber crisis.
- Awareness and training: Organizing regular training sessions, simulations, and awareness campaigns to ensure preparedness in the public and private sectors.
- Information sharing networks: Establishing robust communication channels among stakeholders, including international partners, for sharing intelligence and best practices regarding cyber threats.

Detection of the cyber incident which includes the processes and technologies for monitoring networks and information systems to identify suspicious activities, using monitoring systems, traffic analysis, and cyber threat intelligence, with the aim of detecting potential security breaches.

The detection phase involves identifying and understanding the nature of the cyber incident to determine its scope and potential impact. The main steps include:

- Monitoring of cyber threats: Using real-time monitoring tools to detect anomalies and suspicious activities within the digital ecosystem.
- Identification of cyber incidents: Classification of cyber incidents based on their significance, type, and potential impact, ensuring the prioritization of cyber threats.

Identification of the cyber incident which includes confirming that a suspicious activity constitutes a cyber incident. The identification of the incident is carried out through the analysis of alerts and suspicious activities to determine if they are real and consistent.

Communication and coordination with infrastructures, international Partners, and others, which includes a series of critical activities aimed at ensuring a synchronized and coordinated response to the incident. This phase is important to guarantee that all stakeholders, including critical and important information infrastructures, international partners, etc., are informed and effectively engaged.

Registration of the cyber incident, which includes documenting all important information about the incident, including the time of occurrence, the nature of the incident, the affected systems, and the actions taken up to that point.

Categorization of the incident, which includes the categorization of the incident based on its type and importance, with the aim of planning actions for the handling and resolution of the cyber security incident based on the Regulation approved by order of the General Director of the Authority "On the categorization of cyber security incidents".

Prioritization of the cyber incident, which involves assessing the significance and impact of the incident by taking into account factors such as impact on infrastructure, scale of spread, and potential risk, on the basis of which a task force is designated, which will undertake measures to respond to the incident as well as to analyse the incident based on the Regulation approved by order of the General Director of the Authority " On the categorization of cyber security incidents".

Analysis of the cyber incident, which includes a detailed investigation of the incident to understand the cause, profile, behaviour, and damage caused. This phase helps in developing strategies to prevent similar incidents in the future. The analysis phase includes:

- Collection and analysis of data: Gathering relevant data from affected systems and networks to analyse the root cause, attack vectors, and targeted objectives.
- Impact assessment: Assessment of the potential consequences of the incident on national security, critical infrastructure, and public services to guide the response strategy.

Isolation, deletion, and restoration of the service/data which include actions to stop the spread of the incident, to clean the affected systems, and to restore services and data to their normal state. This includes the use of tools and techniques to exclude threats and to repair the damage caused.

This phase focuses on minimizing the impact of the cyber incident, neutralizing the threat, and restoring affected systems and services. The main actions include:

- Isolation: Implementation of measures to limit the spread of the attack, such as isolating affected systems or temporarily shutting down compromised services.

- Elimination: Removal of malicious elements from affected systems, such as malware or unauthorized access points, ensuring that the threat is fully neutralized.
- Restoration of services: Rebuilding or restoring compromised systems using secure backups, ensuring their integrity and functionality.
- Service Continuity: Activation of business continuity plans to maintain essential services during recovery efforts.
- Communication with Stakeholders: Providing regular updates to all relevant actors, including the public, to maintain transparency and trust.

Support for the isolation, deletion, and restoration of the Service/Data, which includes the assistance provided by the National CSIRT to infrastructure operators with the purpose of stopping the spread of the incident, cleaning the affected systems, and restoring services and data to their normal state.

Post-incident activity which includes reviewing the incident response to identify possible improvements in security processes and policies through lessons learned, updating documentation, and developing strategies to prevent similar incidents in the future, as well as updating the training program. This phase focuses on post-incident review with the aim of learning lessons and implementing measures to prevent its recurrence in the future. The main activities include:

- Incident report: Documenting the details of the incident, including its nature, impact, and the measures taken in response.
- Incident analysis: Conducting thorough investigations to identify underlying vulnerabilities or systemic issues.
- Updating policies and procedures: Reviewing existing protocols and policies based on lessons learned to improve future preparedness.
- Information sharing with stakeholders: Engaging all actors to share findings and recommendations for improvement.
- Training and simulations: Integrating lessons learned into training programs and future simulations to test and improve updated response strategies.

1.6.7 Strategies for communication of large scale cyber incident and crisis

Effective communication is a cornerstone of the National Plan for large-scale cyber incidents and crises in Albania, ensuring that all actors are informed and involved during a cyber incident/crisis. Clear communication helps manage public expectations, facilitates efficient coordination, and prevents the spread of misinformation. This document outlines strategies for achieving seamless communication, both domestically and internationally.

Effective communication strategies for cyber incidents and crises are essential to minimize impact and protect the reputation of the infrastructure. They help ensure transparency, safeguard the interests of stakeholders, and coordinate the response. Some of the key aspects of communication strategies should include:

1. **Preparation**

- Development of a specific communication plan for cyber incidents.
- Designation of the crisis communication team, including managers, technical experts, and media spokespersons.

- Drafting preliminary messages for common scenarios, such as ransomware attacks, data breaches, or service disruptions.
- Continuous training of staff to understand how to respond effectively to the media and the public.

2. **Communication**
   - Early notification of incidents to internal and external stakeholders.
   - Ensuring that the initial information is factual and verified to avoid confusion.
   - Maintaining a transparent stance, without concealing potential impacts.
   - Avoiding speculation or providing inaccurate information.
3. **Notification of parties in the event of cyber incidents and crises:**
   - Notification of personnel: Use of internal communication to keep staff informed.
   - Notification of clients and partners: Use of communication and provision of information regarding the impact on them and the steps taken to protect them.
   - Informing the public and the media: Communication and informing the public and the media regarding the situation caused by the incident and the cyber crisis, as well as the steps undertaken to respond with the aim of protecting the reputation of the infrastructure.
4. **Communication channels should include:**
   - Internal channels: Email, work management platforms, virtual meetings.
   - Public channels: Official websites of the infrastructures, social networks, press conferences.
   - Dedicated channels for clients: Helpdesk and customer service for questions and concerns.
5. **Media relationship management**
   - Preparation of spokespersons to deliver consistent and professional messages.
   - Ensuring that all statements are synchronized with the technical and legal teams.
   - Use of the media to calm the situation and to communicate progress in resolving the incident and the state of the cyber crisis.
6. **Monitoring and responding to public reactions**
   - Monitoring social networks and media to understand public perception.
   - The use of feedback to tailor messages and address concerns.
   - Rapid response to speculations or misinformation that may be circulating.
7. **Post-incident/cyber crisis communication**.
   - Informing stakeholders of the preventive actions taken after the incident and the state of the cyber crisis.
   - Reporting the results of the analyses and corrective measures.
   - Improvement of communication and training plans based on lessons learned.

1.7 Response modes/states of large-scale incidents and cyber crises

The activities described in this Plan are supported through three modes of cooperation:

1. Permanent mode/state
2. Warning mode/state
3. Full activation mode/state

Below are presented the Modes/states as follows:

1.7.1 Permanent mode

The permanent mode refers to the normal operation of information infrastructure, during which situational awareness is maintained and preparedness activities for cybersecurity incidents are carried out. Communications are maintained through regular reporting of cybersecurity incidents in accordance with the formats defined by the applicable legal framework for cybersecurity.
The identification of large-scale incidents that lead to a cyber crisis situation is carried out by the national CSIRTs, information infrastructure operators, as well as other entities that identify such incidents.

1.7.2 Warning mode

The Warning mode is activated upon receipt of evidence and/or information from information infrastructures or other affected entities indicating an increased risk of a large-scale incident in a specific sector or across various sectors. This mode involves communication with the parties involved in the public and private sectors, as appropriate, to strengthen information exchange and cooperation to prevent the possible spread of the incident.
Furthermore, this mode serves as a filter to determine whether escalation/transition to *the Full Activation Mode.*

- **Activation of the Warning Mode**

Activation may be carried out by the National CSIRT, which activates the warning following receipt of a report on the identification of a cyber incident that is unavoidable to prevent. Activation may also be initiated upon the request of other actors (other institutions, information infrastructures, entities that are not information infrastructure), who may likewise initiate this process when there is specific information that an entity or an entire sector is at risk from a particular incident.
During the period in which the Warning Mode/State is in force, where two or more information infrastructures are affected, the structures responsible for cyber security, as defined in this plan, are engaged for the purpose of incident response and sharing information regarding its progress. The necessary information will be distributed through secure communication channels, including the exchange of information, analysis, results regarding affected equipment or networks, possible risks to the infrastructure and the affected services.

- **Exit from the Warning Mode**

During the Warning Mode/State, meetings or information sessions are organized to discuss the ongoing incident response process, necessary for:
- Preventing the spread of the incident and exiting the Warning Mode or
- Escalation to Full Activation mode.

There are two possible outcomes:
1. Elimination or control of the risk. If the risk to the critical sector is considered to have been successfully eliminated, mitigated, or brought under control, then the Warning mode is closed. Remaining follow-up actions may be carried out by the infrastructure itself or by the National CSIRT when support is required.

2. Escalation to full activation mode. If risks continue to increase and there is no foreseeable solution in the short term, or if the incident is causing or is likely to cause significant operational disruption to a critical sector, then a decision is made to move to the full activation phase of the crisis state and the activation of the Emergency and Cyber Crisis Response Team (CERT).

1.7.3 Full Activation Mode/State

This state is activated in the event of a large-scale incident that meets the threshold of a national cyber emergency/crisis, which requires the activation of the CSIRT+CERT at the Authority to ensure an effective, coordinated structure for intergovernmental response aimed at containment, mitigation, and/or recovery.

The AKSK, in coordination with other responsible security and defence structures, presents to the Prime Minister the state of emergency in which the country finds itself for the purpose of proposing the declaration of a cyber crisis situation.

The decision to move to Full Activation Mode and declare a cyber crisis is made by the Council of Ministers upon the proposal of the Prime Minister. This decision may follow a period in which the Warning Mode was active. However, it is also possible to decide to move directly to Full Activation if an incident appears serious enough in the initial reporting.

- Exit from Full Activation Mode

Exiting a cyber crisis requires meeting a set of conditions to ensure that the situation is under control and services have been restored to acceptable levels. The main criteria for exiting a cyber crisis include:

- Restoration of the critical systems functionality;
- All information systems that support critical services must be fully functional and operational.
- Priority reconnection of network communications;
- Affected communication networks and systems must be reconnected and ready for normal operation, giving priority to critical services;
- Reinforcement devices and systems in working condition;
- All technological reinforcements and additional resources engaged must be active and effective in managing the situation;
- Identification of the root cause and initiation of corrective measures;
- The root cause of the cyber crisis must be fully identified and be in the process of resolution to prevent recurrence;
- Consensus of the responsible structures on the achievement of objectives;
- The members of the responsible structures related to the response to the cyber emergency situation must agree that the objectives for ending the crisis have been achieved and that acceptable levels of services have been restored.

1.8 Post-incident activity after a large scale incident

After the end of a cyber emergency, it is essential to analyse and document the experience to promote continuous improvement. The main post-incident activities include:

1. Preparation of the post-cyber emergency/crisis report

The experience and lessons learned from incident management will be included in a post-cyber emergency/crisis report.
This report will contain a detailed analysis of the incident response and will identify possible improvements in:

- Processes;
- Policies;
- The technological infrastructure.

2. Updating of plans and guidelines

- The post-cyber emergency/crisis report, and other findings will be used to update the National response plan for large-scale incidents and cyber crisis and the incident response manuals.
- These updates ensure the continuous improvement of the response process and preparedness for the future.

3. Periodic testing exercises

These exercises aim to:

- Testing the National plan for responding to large-scale incidents and cyber crisis as well as the sectoral response plans.
- Simulation of different situations to identify shortcomings and to improve existing measures.

4. Improvement of response at all levels

- The findings from the exercises and post-incident analyses will be used to strengthen:
  - Response to incidents at the unit and sector level.
  - Coordination at the national and international level.
- The involvement of all stakeholders ensures continuous improvement in the management of cyber incidents.

1.9 Financing of the cybersecurity system

The cybersecurity protection budget of institutions according to the sectors defined in the annexes of Law no. 25/2024 "On Cyber Security" is composed of:

I. The state budget, in which Annex III of Law no. 25/2024 "On Cyber Security" details the financial effects for a 5-year period for central institutions, regional institutions, independent institutions, and law enforcement institutions. This budget consists of three main pillars where investments are required with the aim of increasing the level of cybersecurity in the country, and specifically:

- Cost for infrastructure for cybersecurity (all technology, hardware equipment, software, licenses, systems, etc.).
- Cost for the establishment and implementation of standards.
- Costs for capacity building (trainings).

II. The sources of funding for the National Cyber Security Authority consist of:

- The state budget.
- Other lawful sources.

More specifically, in Annex III of the law "On Cyber Security", it is foreseen that the National Cyber Security Authority must allocate in the budget for the next 5 (five) years from the moment of the law's approval, 40% of its annual budget for investments in the above-mentioned 3 (three) pillars for cybersecurity. Meanwhile, NAIS must allocate in its budget for

the next 5 (five) years from the moment of the law's approval, 30% of its annual budget for investments in the above-mentioned 3 (three) pillars for cybersecurity. Regional institutions, independent institutions, and law enforcement institutions must allocate in their budgets for the next 5 (five) years from the moment of the law's approval, 30% of their annual budgets for investments in the above-mentioned three pillars for cybersecurity.

1.10 Cooperation

1.10.1 Introduction

The National Plan for responding to large-scale incidents and cybersecurity crises of Albania emphasizes the importance of cooperation at all levels to address the complexity of modern cyber threats. Through partnerships with NATO, the EU, regional initiatives, and the private sector, Albania builds a resilient and secure digital ecosystem. These cooperative efforts ensure that resources, expertise, and information are effectively mobilized to protect national security, critical infrastructure, and public trust.

Cooperation with national and international partners is a critical component of the National Plan for responding to large-scale incidents and cybersecurity crises in Albania. In an interconnected and globalized digital landscape, cyber threats transcend borders, requiring coordinated efforts among governments, organizations, and sectors. This document outlines the mechanisms and strategies to foster effective cooperation to strengthen Albania's cyber resilience.

1.10.2 National cooperation

National cooperation in cases of response to large-scale incidents and cyber crises is a key factor in managing situations of large-scale incident response and cyber crisis. This cooperation includes state institutions, the private sector, educational institutions, and civil society, ensuring a coordinated and effective response to incidents that may threaten national security, the economy, and social life.

1.10.3 International cooperation

International cooperation in the management of large-scale incidents and cyber crises is essential for addressing threats that often have a global reach and affect more than one country. Cyber threats are transnational, and effective confrontation with them requires a coordinated global approach through cooperation mechanisms, information exchange, and joint responses. The AKSK cooperates with international bodies in the field of cybersecurity and the authorities national authorities of other countries through joint agreements in accordance with the applicable legislation on international agreements.

Coordination mechanisms with NATO, the EU, and regional initiatives for cybersecurity

Albania leverages its memberships and partnerships with international organizations to improve its cyber resilience:

1. NATO

- Cooperation in Cyber Defence: Participation in the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) programs to strengthen Albania's defensive capabilities.
- Intelligence sharing on threats: Engagement in NATO platforms for sharing cyber intelligence to gain access to real-time threat insights and improve situational awareness.

- Joint Exercises: Participation in NATO-led cyber exercises to test and improve response protocols.

2. European Union (EU)

- Financing and technical support: Utilization of EU funding sources and mechanisms, such as the Digital Europe Programme, for capacity building and infrastructure development.
- Participation in ENISA initiatives: Cooperation with the European Union Agency for Cybersecurity (ENISA) to strengthen detection and response capabilities against threats.
- Participation in Hybrid CoE to strengthen detection and response capabilities against hybrid threats.

3. OSCE

Albania's cooperation with the OSCE in the field of cybersecurity consists of providing technical assistance, training, and promoting international dialogue, supporting Albania in building a sustainable and secure system for managing cyber incidents and crises.

4. Participation in international forums for Cybersecurity

- Albania's membership in FIRST (Forum of Incident Response and Security Teams) with the purpose of information exchange in cases of cyber crises.
- Engagement in regional platforms: Participation in forums such as the Western Balkans Cybersecurity Forum to share best practices and resources with neighboring countries.
- Development of joint crisis response plans: Drafting coordinated plans with regional partners to address cross-border cyber threats.

1.10.4 Cooperation with the private sector

The private sector plays an essential role in Albania's cybersecurity ecosystem, as it owns and operates a substantial part of the country's critical infrastructure. Close and effective cooperation with the private sector ensures a unified approach to the management of cyber incidents/crises. This cooperation consists of:

1. Intelligence sharing

- Creation of secure platforms for intelligence sharing on threats between state institutions and private entities to detect and mitigate risks at early stages.

2. Resource allocation

- Facilitating cooperation in the deployment of advanced cybersecurity tools, such as artificial intelligence-based threat detection systems, to protect both public and private infrastructure.

3. Cooperation in capacity building

- Partnership with private sector leaders to provide training programs, simulations, and knowledge-sharing sessions for cybersecurity teams.

4. Cooperation for incident response

- Development of joint protocols for incident response to ensure rapid and coordinated actions during cyber incidents affecting both the public and private sectors.

Section 2 Prevention/Mitigation

Phase of prevention/ mitigation consists of structured measures and processes aimed at reducing the likelihood of cyber incidents occurring and mitigating their consequences if they do occur. It includes two main components, prevention and mitigation which constitute an essential component of a comprehensive strategy for the protection and resilience of critical infrastructures and society against cyber threats.

2. Prevention

Prevention aims to reduce the chances of incidents by preparing organizations and improving security. The main goal of the prevention phase is to lower the risk of incidents occurring through proactive and planned measures. This includes:

1. **Cyber security policies and strategies**
   - Drafting detailed policies: institutions and infrastructures must have well-defined policies for security management.
   - Establishing international standards: Such as ISO 27001 for information security management.

2. Risk assessment

- Identification of vulnerabilities: Assessment of critical systems to identify possible technical or organizational vulnerabilities.
- Continuous monitoring: Implementation of systems for real-time threat detection.

3. Cooperation and information exchange

- Interaction between institutions: Cooperation between the private and public sectors for the sharing of information on threats and incidents.
- Building national and international networks: Promoting partnerships for cyber protection.

4. Education and awareness

- Training of staff and users: Preparing personnel and users to recognize and manage cyber threats.
- Public awareness campaigns: Educating the public on safe online practices.

2. 1 Mitigation

Mitigation ensures a rapid and effective response to minimize the impact of large-scale incidents and cyber crises. This phase focuses on reducing the impact of incidents and includes coordinated response and effective crisis management. This phase includes the following elements:

1. Response planning

- Drafting emergency plans: Preparing detailed scenarios for managing different crisis situations.
- Decision-making hierarchy: Identifying the roles and responsibilities for the teams that will respond.

2. Deployment of specialized teams

- Incident response teams (CSIRT): Establishment of specialized units to address cyber incidents.
- Technical solution experts: Engaging experts to restore systems to operation as quickly as possible.

3. Coordination structures

- The national structure for cyber crisis management aimed at coordinating responses in the event of a cyber crisis.
- Real-time information exchange: Systems for sharing and analysing information among various actors.

4. Simulations and exercises

- Testing of response plans: Organizing simulations to test the readiness of teams and systems.
- Regular drills: Periodic exercises to prepare for unforeseen situations.

2.2 Roles and responsibilities of entities responsible for cybersecurity in the prevention phase

To manage cyber incidents at the national level, the roles and responsibilities of each actor must be defined in the incident prevention phase, starting from the highest leadership levels including:

1. National Cybersecurity Authority / National CSIRT;
2. Head of the Institution;
3. Sectoral CSIRT;
4. CSIRT at the operator level;
5. The Commissioner for the Right to Information and Protection of Personal Data.

1. **National Cyber Security Authority**/ National CSIRT, the Emergency Response Team, is an Authority with regulatory and coordinating competencies, and exercises the following roles and responsibilities:

a. Drafts cybersecurity policies based on internationally recognized security standards as well as by-laws implementing Law no. 25/2024 "On Cyber Security";
b. Establishes the incident response team/National CSIRT and instructs the creation of the operator's incident response team/CSIRT at the operator;
c. Develops national level trainings and regular simulation exercises to ensure a trained and prepared national cyber incident response team to respond to incidents, and reviews the preparation phase and documents new threats as they are discovered;
ç. Develops response strategies that prioritize risks based on the significance of their impact;
d. Develops a detailed communication plan to inform infrastructures, stakeholders, and law enforcement agencies about cyber incidents. Contact points are designated for all members of the response team and an encrypted communication flow is ensured;
dh. Ensures, as the national CSIRT, the availability of the necessary tools and solutions for incident response;
e. Ensures and guides access control through the implementation of security measures and protocols to guarantee that only authorized persons have access to sensitive resources. sensitive.

2. The head of the institution in the capacity of the head of the institution:

a. They lead their institution in coordinating the necessary processes during the prevention phase;
b. They formally inform the National CSIRT about the cyber status of services in their institution.

3. **Sectoral CSIRT**, in the capacity of the incident response team for cyber security incidents of the relevant sector:

a. Ensures the increase of staff capacities through periodic trainings and certifications according to the sectors they cover.

4. **CSIRT at the operator level** in the capacity of the team of incident response team for cyber security incidents of the relevant operator:

a. Implements cyber security policies based on internationally recognized security standards and bylaws pursuant to law no. 25/2024 "On Cyber Security";

b. Ensures training and participation in regular simulation exercises to provide a cyber incident response team that is trained and ready to respond to incidents, as well as reviews the preparation phases and documents new threats as they are discovered;

c. Develops response strategies that prioritize risks based on the significance of their impact;

ç. Develops a detailed communication plan to inform stakeholders and law enforcement authorities about cyber incidents. Contact points are defined for all members of the response team and ensures an encrypted communication flow;

d. Ensures the availability of the necessary tools and solutions for response to incidents;

dh. Ensures access control through the implementation of security measures and protocols to ensure that only authorized persons have access to sensitive resources.

5. **The Commissioner for the Right to Information and Protection of Personal Data** in its capacity as the authority responsible for drafting policies on the protection of individuals' personal data, monitors the implementation of the relevant legislation in the event of incidents and the cyber crisis:

a. Handles, oversees, and monitors the implementation of the applicable legislation on the protection of personal data.

Section 3: Preparedness

3. Preparedness

All actors, both individuals and organizations who can contribute to cyber defence efforts must be properly prepared. To achieve this, it is essential that they have a clear understanding of the National Plan for response to large-scale incidents and cyber crises, including their specific roles and responsibilities, as well as how they integrate into the inter-institutional framework.

The main objective of the preparedness phase in the protection of cybersecurity and the management of large-scale incidents and cyber crises is to minimize the negative impacts on critical systems, data, health, property, and digital operations as a result of cyber incidents or large-scale threats. The key elements of preparedness include the establishment and strengthening of capacities for the protection of critical infrastructure and the training of institutions and organizations to anticipate, cope with, and recover from the consequences of cyberattacks or crises with chain effects. This phase includes the following components:

3.1. Information and education

1. Public awareness:
   - Conducting periodic informational campaigns to raise awareness of basic threats and methods of protection.
   - Educating individuals on good internet usage practices, such as using strong passwords and identifying suspicious emails.

2. Training for professionals:
   - Specific courses on cyber incident management and threat analysis.
   - Exercises and simulations to prepare professionals for real-life situations.
3. Policies and Protocols:
   - Drafting and implementation of response plans for cyber incidents and crises.
   - Coordination between the public and private sectors for an integrated response to cyber incidents.
4. Cooperation networks:
   - The creation of cyber incident response teams (CSIRT) to share information and to act quickly.
   - Participation in international initiatives to share experiences and best practices.

3.1.1. Preparedness campaign activities

Preparedness campaigns aim to raise awareness, educate, and prepare individuals, organizations, and institutions to respond effectively to cyber incidents and major crises. Campaigns can be conducted across all sectors, ranging from children in schools, public institutions, to the private sector industry. The campaign or activity may be modified to suit the audience, but many of the principles remain the same. Below are some of the main activities that can be carried out:

1. Education and public awareness
   - Webinars and seminars: Organizing online and in-person sessions on cyber threats and best practices for security.
   - Informative campaign: Distribution of educational materials (brochures, posters, videos) through social media, television, and other media platforms.
   - National Cybersecurity Day: Establishing a dedicated day for cybersecurity awareness, with public activities such as demonstrations and open lectures.
2. Training and simulations
   - Training for technical staff and management: Courses are offered for staff of public and private organizations on incident management and the use of advanced tools for threat identification.
   - Incident simulations: Conducting drills to test teams' responses to simulated attacks, such as DDoS attacks, ransomware, or system intrusions.
   - National and regional exercises: Organizing coordinated inter-institutional exercises to improve cooperation in case of a crisis.
3. Establishment of information and support infrastructure
   - Awareness platform: Development of websites or applications that provide clear guidance for the reporting and management of cyber incidents.
   - Help centres: Establishment of helplines and support centres to assist citizens and businesses during incidents.
   - Early warning systems: Implementation of mechanisms for early warning of new cyber threats.
4. Information sharing and inter-institutional cooperation
   - Cooperation networks: Establishment of computer security incident response teams (CSIRT) to share information and resources.

- Public private partnerships: Promoting cooperation between the public and private sectors to increase the collective response capability.
- International workshops: Organizing meetings with international organizations for the exchange of best practices and standards.

5. Support and promotion of security technologies
   - Testing and improvement of systems: Encouraging organizations to test vulnerabilities in their infrastructures and to implement new protective measures.
   - Adoption of new technologies: Promoting the use of technologies such as artificial intelligence and blockchain to enhance security and protection.
   - Cybersecurity grants: Provision of funding for businesses and institutions that invest in cybersecurity.
6. Spreading the culture of cybersecurity
   - Internal campaigns: Organizing activities to raise staff awareness about attacks such as phishing and social engineering.
   - Engagement of the IT community: Involving developer and expert communities to help identify and prevent threats.
   - Educational programs for children and students: Educating the new generation on cybersecurity through courses and school activities.
7. Assessment and improvement of readiness plans
   - Security audits: Conducting regular audits to identify vulnerabilities in existing systems and procedures.
   - Improvement based on experience: Analysis of data and results from simulations and incidents to adjust and enhance response plans.
   - Impact reports: Publication of periodic reports to raise awareness and transparency regarding risks and measures taken.

3.2 Early Warning

Early warning is an essential component in the management of cyber incidents and crises, aiming to identify and communicate potential risks in a timely manner to minimize negative impacts on critical systems and society in general. The purpose of early warning is:

1. Forecasting cyber threats: Identifying early signs of potential attacks, such as unusual activities on networks or the release of new malware.
2. Preparation of relevant actors: Informing infrastructures and individuals to take preventive measures and prepare for an effective response.
3. Damage reduction: Preventing the spread of the impact of attacks by responding in a timely manner and improving protection before a major incident occurs.

The main components of the early warning process are:

1. Threat detection: Identification of suspicious activities or early signs of a possible cyber attack.
2. Impact assessment: Analysis of risk potential and evaluation of the possible impact on critical systems and organizations.
3. Warning communication: Sending information to relevant actors through secure and structured channels.
4. Activation of preventive measures: Implementation of technical and organizational measures, such as security updates and activation of emergency plans.

3.2.1. Surveillance, monitoring, and prediction systems

Systematic monitoring of risks arising as a result of cyber threats requires the precise determination of the roles and responsibilities of monitoring and information/notification institutions and structures, as well as those of protection. Furthermore, the establishment of clear lines of communication, information, and reporting between monitoring and information/notification structures and the protection structures is necessary.
Surveillance, monitoring, and prediction systems play an essential role in addressing large-scale incidents and cyber crises. These systems are designed to identify, analyse, and respond to cyber threats, helping infrastructures to minimize the impact and recover quickly. These systems and strategies are necessary for a proactive and sustainable approach to cybersecurity, minimizing risks and increasing resilience to crises.

The monitoring procedure is carried out by the relevant structures within the National CSIRT as well as by those within the operator for the purpose of detecting and responding to possible cyber-attacks or incidents on information networks and systems.
The National CSIRT, in the framework of its monitoring activity, in cases of identification of cyber threats, warns, notifies, and disseminates information to critical and important information infrastructures, as well as to responsible entities regarding possible risks, vulnerabilities, and cyber incidents.

3.3 Training and Capacity Building

3.3.1 Training and Capacity Building

The success of the National Plan for response to cyber security incidents and crises depends on the availability of skilled professionals and a well-informed public and private sector. Effective training and capacity-building initiatives are essential in developing the expertise necessary to address cyber threats and to foster a culture of cyber security awareness at all levels of society.

Training and development are extremely broad concepts and one of the most important aspects to be taken into consideration are their specifics. Training can be conducted at a personal, professional, and academic level, as well as in teams, at the sector level, institutional or organizational level. Training and development in partnership are strongly encouraged and are usually efficient from the perspective of cost. When considering a multi-year plan for training and exercises, a clear responsible institution must be identified, which for Albania will be the AKSK.

The multi-year plan for training and exercises is a strategic and guiding document implemented by the National Cybersecurity Authority (AKSK). As a dynamic document, it is subject to regular annual updates and improvements to reflect new developments in the field of cybersecurity.

This plan provides a detailed roadmap for the AKSK, information infrastructures, and public and private institutions, defining the key skills that need to be developed. It is closely linked with national priorities and includes the necessary trainings and exercises to acquire or validate these skills.

The plan also includes a detailed model of the training and exercise calendar, which outlines the proposed activities for the planned period. This model aims to provide an organized and coordinated approach for capacity building in response to cyber incidents and crises.

3.3.2 Skills Development for Cybersecurity Professionals

Building a strong group of professionals in cybersecurity is vital for Albania's resilience to cyber threats. Key initiatives include:

1. Specialized Training Programs
   - Creation and expansion of training programs for cybersecurity professionals, focusing on the detection of cyber threats, response to cyber incidents, and management of cybersecurity risks.
   - Collaboration with academic institutions to offer specialized courses and certifications in cybersecurity.
2. Capacity Building for Incident Response Teams
   - Equipping national cyber incident response teams with the latest tools and techniques to manage complex cybersecurity crises.
   - Organization of regular exercises and simulations to test and improve the technical skills of cyber incident response teams.
3. International Cooperation
   - Partnership with NATO, the EU, and other international organizations to facilitate knowledge exchange and provide training opportunities in the field of cybersecurity.
   - Encouraging participation in international forums on cybersecurity issues.
4. Development of Professional Continuity
   - Implementation of initiatives to promote continuous learning to keep professionals updated on emerging threats and technologies.
   - Ensuring access to online resources, training platforms, and expert networks in order to keep cybersecurity experts updated.
5. Increasing Awareness in the Public and Private Sectors
   Cybersecurity is a shared responsibility that requires active participation from public institutions and private entities.

3.3.3 The main strategies within the framework of training and capacity building include:

1. Public awareness campaigns
   - Launching national campaigns to educate citizens on basic cybersecurity practices, such as recognizing phishing attempts and securing personal devices.
   - Development of materials such as brochures, videos, and websites to distribute advice and guidance on cybersecurity.
2. Tailored training for the sector
   - The ongoing organization of tailored training sessions for key sectors, including energy, finance, healthcare, and telecommunications, to address cybersecurity risks, and the management of cybersecurity incidents and crises.
   - Providing executive-level training for leaders in government and private organizations to emphasize the strategic importance of cybersecurity.
3. Public private cooperation
   - Encouraging partnerships between government agencies and private companies to share knowledge, tools, and best practices in the field of cybersecurity.

- Encouraging private organizations to adopt and promote robust cybersecurity measures among employees and other stakeholders.

4. Integration into education
   - The introduction of cybersecurity topics into the school curriculum to cultivate early awareness among students.
   - Supporting extracurricular programs such as coding clubs and cybersecurity competitions to inspire future professionals.

3.3.3 Coordination

The AKSK, in accordance with the provisions of law No. 25/2024 "On Cyber Security", by order of the Director General and in cooperation with the operators of critical and important information infrastructures, develops and promotes, whenever deemed necessary, training for the personnel of these operators, within the framework of effectively fulfilling their duties.

Also, based on the National Cybersecurity Strategy 2020-2025[1] one of the main objectives foreseen is the increase of awareness and professional skills of public and private institutions regarding cybersecurity, which includes:

- Periodic training to deepen knowledge in cybersecurity, according to the dynamics of the field, for administrative staff at both central and local levels.
- Increase and support of research capacities and business innovation through the promotion of the establishment of scientific research centres in the field of cybersecurity.
- Increasing the capacities of national-level CSIRTs and the executive level of public administration through trainings and cyber exercises.
- Raising society's awareness about cybersecurity and cyber threats.

3.3.4 Development cycle

The development cycle, based on the current status of AKSK and its strategic partners, the Multi-Year Training and Exercise Plan must be developed functionally and be based on specific, measurable, achievable, realistic, and time-based objectives or according to their type.

3.3.5 Testing and simulation exercises

Testing and simulation exercises are essential components of the National Plan for large-scale incidents and cybersecurity crises. These activities ensure that the country's cybersecurity measures are effective, appropriate, and well-coordinated. By replicating real cyber threats, actors can identify vulnerabilities, improve cooperation, and increase overall preparedness in defending against them. Testing and simulation exercises are vital to ensuring the effectiveness of the National Plan for large-scale Incidents and cybersecurity crises. By regularly assessing response protocols, strengthening coordination, and adapting to evolving threats, these exercises increase Albania’s preparedness and resilience in facing large-scale cyber incidents and cyber crises. The commitment to continuous improvement through testing underscores the country’s proactive approach to protecting its digital ecosystem.

The importance of regular drills and simulations consists of:

1. **Response Protocols**
   - Drills help in the practical testing of response protocols, ensuring that they are effective and adapted to real scenarios.

[1]Adopted by Decision of the Council of Ministers No. 1084, dated 24.12.2020, “On the approval of the National Cyber Security Strategy and its action plan 2020-2025”.

- Simulations reveal gaps in preparedness, providing opportunities for improvement.

2. **Improving Coordination of Stakeholders**
   - Regular drills promote cooperation between government agencies, private sector entities, and international partners.
   - Ensure that all stakeholders understand their roles and responsibilities in a cybersecurity crisis situation.
3. **Building trust**
   - Training in simulated conditions builds trust between cybersecurity teams and decision-making structures.
   - Strengthens the confidence of the public and private sectors in Albania's ability to manage complex cyber incidents and cope with cyber crisis situations.
4. **Adaptability to cyber threats**
   - Cyber threats are constantly evolving, simulations help test new tactics and technologies to address new risks.

3.3.5.1 Tabletop exercises (*Table Top Exercise* - TTX)

Simulated exercises in cybersecurity include senior staff members, elected or appointed public officials, and personnel from various sectors. These exercises aim to discuss simulated scenarios of cyber threats and incidents, or to assess the types of systems needed to direct prevention, response, and recovery from a cyber emergency.

This type of exercise aims to:

- Promotes strategic and operational discussions on various issues related to a hypothetical cyber situation, such as DDoS attacks, ransomware, or compromises of critical infrastructure.
- Assess the cybersecurity plans, policies, and procedures to identify strengths and weaknesses.
- Test the decision-making and coordination systems, preparing participants for the prevention, response, and recovery from cyberattacks.

Objectives of simulated exercises for cybersecurity

- Facilitating the understanding of concepts: Through in-depth discussions, participants gain a better understanding of cyber threats and protective measures.
- Development of decision-making skills: In a controlled and calm-paced environment, participants practice solving complex cyber problems without the pressure of a real emergency.
- Improvement of policies and procedures: Recommendations from the discussions help in reviewing and updating existing strategies.

The benefits and cost-effectiveness of simulated exercises

Unlike operation-based exercises and complex games, tabletop simulated exercises (TTX) are cost-effective tools and can be used alongside more complex exercises. Their use in the context of cybersecurity includes:

- **In-depth discussions**: Participants are encouraged to analyse cyber scenarios in detail and provide solutions.
- **Gradual implementation of improvements**: TTXs allow for the modification and adaptation of policies and procedures in a calm and structured environment.

- **Building a security culture**: Participants acquire new concepts and approaches that help improve readiness against cyber incidents.

3.3.5.2 Practical Simulations (Live-Action Simulations)

Practical simulations, also known as *Live-Action Simulations,* are realistic exercises that test the technical, operational, and strategic capabilities of an organization to prevent, detect, respond to, and recover from cyber incidents. In these simulations, conditions are created as close as possible to real situations to comprehensively assess capacities and weaknesses in a controlled environment.

Practical simulations are one of the most effective tools for testing and strengthening the cyber defence of an infrastructure. They help assess the technical and organizational readiness against complex incidents, providing a clear overview of necessary improvements. Although they require considerable resources, the long-term benefits outweigh the costs, helping infrastructures to better protect themselves against challenges in an increasingly complex cyber environment.

3.3.5.3 Sector-specific tailored exercises

Sector-specific tailored exercises are a focused method for testing and improving cybersecurity capabilities, considering the specific requirements, threats, and regulations related to different sectors. These exercises are designed to address the unique challenges of each sector, ensuring that infrastructures are prepared to manage cyber risks in their specific environment.

- **Description:** Simulations tailored for critical sectors, including energy, finance, healthcare, and telecommunications.
- **Frequency:** They are conducted twice a year, focusing on the specific vulnerabilities of the sectors and response mechanisms.
- **Objectives:** Strengthening the resilience of the sectors and integrating sector-specific plans with the national framework.

3.3.5.4 Cybersecurity exercise training (Drills)

Specialty drills in cybersecurity are structured and supervised activities aimed at testing and improving a specific function or a particular operation within an organization. They are designed to provide focused training and to thoroughly test technical and operational capabilities, helping organizations improve their response and abilities in managing cyber incidents.

The use and purpose of cyber exercise drills

1. Training on new technologies:
   - The implementation of new equipment or software to ensure that personnel can use them.
2. Testing of new procedures:
   - Verification of new cybersecurity protocols to ensure that they function as intended.
3. Maintaining and improving capabilities:
   - Ensuring that existing staff skills are fresh and up to date with best practices.
4. Identification of vulnerabilities:
   - Exploration of technical and operational vulnerabilities through focused simulations.

3.3.5.5 Joint international drills

Joint international drills are a strategic initiative to enhance cooperation between countries and organizations in addressing global cyber threats. By bringing together experts from the public and private sectors, these drills aim to improve coordination, information sharing, and capabilities to respond to complex incidents that cross national borders.

International drills are an essential element for strengthening cybersecurity. They help build a stronger cooperation infrastructure, increase interaction between countries, and ensure that global threats are addressed effectively and in a coordinated manner. With the increasing complexity of cyber threats, these drills are becoming ever more indispensable.

- **Description:** Cooperative exercises with NATO, the EU, and regional partners to address cross-border cyber threats.
- **Frequency:** They are planned every year to strengthen Albania's role in regional and global efforts for cybersecurity.
- **Objectives:** Improvement of coordination, sharing of intelligence on threats, and joint response capabilities.

3.4 Maintenance of the plan

The National Plan for responding to large-scale incidents and cyber crises is a document that must be kept up to date and suitable for the evolving challenges and threats of cybersecurity. It must be reviewed and updated regularly to reflect existing and new legislation and policies, the experiences gained from incidents and exercises, as well as to adapt to conditions and technologies that are continuously evolving.
The National Plan for responding to large-scale incidents and cyber crises will be reviewed every 2 years to:

- identify new vulnerabilities and risks;
- adapt to new technologies;
- have an improved international approach, striving for harmonization with international protocols and strengthening cross-border cooperation in the fight against cyber threats;
- improve response and capabilities after cyber incidents or simulations, following in-depth analyses and lessons learned;
- reflect the National Cybersecurity Risk Assessment;
- reflect changes in the early warning system;
- adapt to legal and policy changes in the field of cybersecurity

During the review of the implementation of the National Plan for responding to large-scale incidents and cyber crises, AKSK will take into consideration the most effective practices and lessons learned from previous exercises, drills, and cyber incidents, as well as assess new processes and technologies. Effective practices include planning for the continuity of cyber operations, which ensures the maintenance of security measures regardless of threats and attacks. New processes and technologies should enable Albania to efficiently adapt to evolving risks, use data to better understand the location, context, and interdependencies within its cyber infrastructures, and enable rapid and effective coordination at all levels of response to cyber incidents.

3.5 Resources and infrastructures

The effective implementation of the National Plan for responding to large-scale incidents and cyber security crises relies on strong resources and infrastructures. Sufficient technical and financial resources are essential for building and maintaining a secure and resilient digital ecosystem, while the improvement of cyber security infrastructure ensures Albania's preparedness to address and confront evolving cyber threats.

Required technical and financial resources

1. Technical resources
   - Threat detection systems: Deployment of advanced monitoring tools such as *Security Information and Event Management* (SIEM) systems, intrusion detection systems (IDS), and automated threat intelligence platforms.
   - Incident response tools: Provision of tools for malware analysis, digital forensics, and data recovery to enable quick and efficient responses to cyber incidents.
   - Secure communication channels: Establishment of encrypted networks and platforms for secure communication between stakeholders during cyber incidents and crises.
   - Backup and recovery systems: Implementation of robust data backup solutions to ensure integrity and rapid recovery in the event of attacks.
2. Financial resources
   - Budget allocation: Dedicated financing from the national budget to support cybersecurity initiatives, infrastructure improvements, and the development of cybersecurity experts.
   - Public-private investments: Encouraging financial contributions from the private sector to improve the overall cybersecurity ecosystem.
   - International financing: Utilizing grants and support from international organizations as well as strategic partners, including the EU and NATO, for capacity building and technology acquisition.

3.6 Risk identification, exposure vulnerability analysis, and risk assessment

In the framework of responding to cyber incidents and potential crises, risk identification, vulnerability analysis, exposure assessment, and risk evaluation are essential elements that ensure an effective and rapid response. This process involves several important steps, which allow infrastructures and authorities to be prepared to face various threats in the field of cybersecurity.

1. Risk identification

Risk identification is a process that involves assessing the likelihood of cyberattacks that may affect critical infrastructures and services. This process includes:

- Determining potential threats: This includes attacks from external actors (hackers, criminal groups) or from within (abuse by authorized users).
- Identification of vulnerabilities: Every system has weaknesses that can be exploited for intrusion. This includes outdated software, lack of staff training, and deficiencies in security configurations.
- Assessment of potential cyber threats: Identification of possible types of attacks such as malware, ransomware, DDoS, phishing attacks, etc.

- Description of the possibilities of attacks and suspicious activity: Analysis of the possibilities for attacks on critical infrastructures and the consequences they may cause.

2. Vulnerability analysis

Vulnerability analysis focuses on identifying the weaknesses of information systems and infrastructures that may affect the protection and preservation of data integrity. This process includes:

- Definition of critical resources: Identification of systems and data that are essential to the functioning of an infrastructure and that may become the target of attacks.
- Description of internal vulnerabilities: For example, the use of weak passwords, unauthorized access to critical systems, or non-compliance with security rules.
- Testing and auditing of systems: Security testing of systems to detect vulnerabilities that may be exploited by attackers.

3. Exposure assessment

Exposure assessment focuses on measuring the level of sensitivity that an infrastructure has to potential threats and attacks. This process includes:

- Analysis of the sensitivity of information and systems: The more information is accessible or sensitive, the greater the likelihood of exposure to cyber-attacks.
- Description of possible external access opportunities: This includes potential external connections, such as internet networks and systems that are connected to other international or institutional systems.
- Assessment of the risk of data breach: How exposed the information is in situations where this information may be manipulated or stolen.

4. Risk assessment

Risk assessment is the process of gathering and analysing data to determine the impact and likelihood of a cyber incident occurring, focusing on the potential consequences for the security and stability of critical infrastructure and services. This process includes:

- Assessment of likelihood and impact: By evaluating the likelihood that a particular attack may occur and the impact it may have on critical systems and services.
- Selection of risk management measures: Identification of measures that can be taken to reduce the likelihood of attacks occurring and to minimize their impact.
- Risk prioritization: Assessment of various security aspects and classification of threats according to likelihood and importance, to determine which should be addressed immediately and which can be delayed.

3.7 Measures in the preparedness phase

Thanks to information, specialized knowledge, tailored training, early warning, and risk assessment, preparedness to face cyber emergencies should ensure functional and responsive systems. These systems must be equipped with sufficient resources to guarantee an appropriate response to cyber risks and incidents.

A comprehensive and coordinated approach, involving inter-institutional cooperation and the participation of civil society, is essential to ensure a high level of preparedness for cyber emergencies. In this way, Albania and its infrastructures can respond effectively to threats and ensure resilience in the face of cyber risks.

3.8 Continuity of business and services

Continuity of business and services is an essential element for the protection of critical infrastructure, management of cyber incidents, and ensuring the uninterrupted operation of infrastructures. This concept includes a set of measures and procedures aimed at protecting systems, preserving data integrity, and securing services even in the event of cyberattacks or incidents. Part of this process also involves preparing for the continuation of operations under emergency conditions and recovery after a possible crisis.

1. Business continuity planning

Business continuity planning is a process aimed at ensuring that infrastructures can continue to provide critical services even in times of crisis. This plan should include:

- Identification of critical services: These are services that cannot be interrupted due to their importance for the functioning of the infrastructure or for services to citizens and users.
- Preparation of recovery plans: The cyber emergency recovery plan includes procedures and techniques for restoring systems, services, and data after a cyber incident.
- Securing alternative resources and infrastructures: This includes the use of alternative resources and support systems to ensure the uninterrupted operation of services during and after crises.

2. Risk management and services continuity

An essential part of services continuity is risk management, which includes:

- Identification and assessment of cyber risks: Infrastructures must understand the threats that may affect service continuity and prevent them before they occur.
- Protection from cyber-attacks: The use of security measures such as firewalls, antivirus, intrusion detection systems, and encryption to prevent intrusions into systems and services.
- Control of the consequences of attacks: If an incident occurs, measures must be taken to limit the consequences and to ensure operational continuity through recovery plans.

3. Training and testing of business continuity

Preparing staff and structures to respond to cyber crises is important to ensure a successful continuity process. This process includes:

- Staff training: Staff must be trained to respond quickly and effectively to cyber incidents and to know how to manage emergency situations.
- Exercises and simulations: Exercises and tests are essential for assessing the readiness of the infrastructure to maintain service continuity and to test recovery plans and procedures in conditions like real ones.

4. Monitoring and updating the continuity plan

To ensure that a continuity plan is always appropriate and effective, it is necessary for it to be continuously monitored and updated, including:

- Monitoring of systems and services: This ensures that any potential vulnerability or risk is identified and that measures are taken to minimize the impact on business continuity.
- Updating security and recovery plans: The plan must be updated regularly to include new technologies and threats that may arise, by ensuring that it remains effective and suitable for any situation.

5. International cooperation and coordination

The continuity of cyber services and operations is not just an internal matter but also requires broad coordination with international partners and other agencies. This coordination includes:

- International assistance and shared resources: In the event of major cyber incidents, international cooperation is required to manage and recover quickly.
- Common standards and legal frameworks: Adoption of common standards for cybersecurity and harmonized policies to ensure service continuity even beyond borders.

3.9 Roles and responsibilities of entities responsible for cybersecurity in the preparedness phase

To manage cyber incidents at the national level, the roles and responsibilities of each actor must be defined in the preparedness phase, starting from the highest management levels, including:

1. National Cyber Security Authority / National CSIRT;
2. Head of the Institution;
3. Sectoral CSIRT;
4. CSIRT at the operator level;
5. The Commissioner for the Right to Information and Protection of Personal Data.

1. National Cyber Security Authority/ National CSIRT, the Emergency Response Team, is an Authority with regulatory and coordinating competences, and exercises the following roles and responsibilities:

a. Ensures the implementation of cybersecurity policies based on internationally recognized security standards as well as Law no. 25/2024 "On Cyber Security" and its implementing bylaws;

b. Keeps the national incident response team/National CSIRT on standby and instructs the creation of the operator's incident response team/CSIRT at the operator level;

c. Develops national-level trainings and regular simulation exercises to ensure a nationally trained and ready incident response team to respond to incidents, and reviews the preparedness phase and documents new threats as they are discovered;

ç. Ensures the implementation of response strategies that prioritize risks based on the significance of their impact;

d. Updates the detailed communication plan to inform infrastructures, stakeholders, and law enforcement agencies regarding cyber incidents. Points of contact for all incident response team members are designated, and an encrypted communication flow is ensured;

dh. As the national CSIRT, ensures the availability of the necessary tools and solutions for incident response;

e. Ensures and instructs access control through the implementation of security measures and protocols to guarantee that only authorized persons have access to sensitive resources.

2. The head of the institution in the capacity of the head of the institution:

a. They lead their institution for the coordination of the necessary processes in the preparedness phase;

b. Officially inform the National CSIRT about the communication plan, availability of tools, implementation of cyber measures, and security protocols to ensure that only authorized persons have access to the sensitive resources of services in their institution;

3. **Sectoral CSIRT**, in the capacity of the incident response team for cybersecurity of the relevant sector:

a. Ensures the enhancement of staff capacities through periodic trainings and certifications according to the sectors they cover.

4. **CSIRT at the operator** level in the capacity of the incident response team for cybersecurity of the relevant operator:

a. Implements cybersecurity policies based on internationally recognized security standards and bylaws pursuant to Law no.25/2024 "On Cyber Security";
b. Keeps the incident response team/CSIRT at the operator on standby;
c. Ensures training and participation in regular simulation exercises to guarantee an incident response team that is trained and ready to respond to incidents, as well as also reviews the preparation phases and documents new threats as they are discovered;
ç. Ensures the implementation of response strategies that prioritize risks based on the significance of their impact;
d. Updates the communication plan to inform stakeholders and law enforcement agencies about cybersecurity incidents. Contact points are designated for all members of the response team and an encrypted communication channel is ensured;
dh. Ensures the availability of the necessary tools and solutions for incident response;
e. Ensures access control through the implementation of security measures and protocols in order to guarantee that only authorized persons have access to sensitive resources.

5. Commissioner for the Right to Information and Protection of Personal Data in its capacity as the institution responsible for drafting policies for the protection of individuals' personal data, monitors the implementation of the relevant legislation in the case of cyber incidents and crises:

a. Handles, controls, and monitors the implementation of the applicable legislation on the protection of personal data.

Section 4: Response

The response phase to large-scale cybersecurity incidents and crises involves coordinated measures to minimize the impact, recover affected systems, and ensure the continuity of critical operations. This process requires preparation, planned execution, and continuous monitoring.

The main objectives of the response phase

- Minimizing damages: Reducing the impact of the incident on systems, data, and operations.
- Ensuring transparency: Providing clear and reliable information to stakeholders.
- Preparation for the recovery phase: Establishing the foundations for restoring resilience and improving systems to prevent future incidents.

This phase is essential for ensuring a swift and effective response to crises, minimizing disruptions, and protecting national and international interests.

4.1 Gathering information and data management

The collection of information and data management in cases of large-scale cybersecurity incidents is an important process to ensure a rapid, coordinated, and efficient response. This process includes the collection, analysis, and retention of data and information that may assist in identifying, mitigating, and recovering from the consequences of incidents. Information gathering and data management are the main pillars of an effective response to cyber crises. With the integration of AI and other advanced technologies, infrastructures can improve their

speed, accuracy, and efficiency to address complex and ongoing threats. The key elements for information gathering and data management are as follows:

1. Real time data collection

- The use of security monitoring systems helps to collect information in real time. These systems can identify suspicious activities on the network and can record data related to potential incidents, such as suspicious IP addresses, abnormal requests, and unauthorized movements of data.
- Activities on systems and servers must be recorded to create a complete audit trail of what has occurred. This may include system logs, network logs, and security event records.

2. Classification and filtering of data

- Once the information has been collected, it is important to classify it to distinguish the important information from that which is not necessary. This classification may include dividing the data into categories such as sensitive data, threat information, suspicious activities, etc.
- The data must be filtered, as not all data is necessary for analysis. Filtering the data to identify the most important information helps in the investigation of the incident and may assist in finding the source of the attack.

3. Storage and security of data

- The data collected from cyber incidents must be stored securely, so that they can be analysed in the future and used as evidence if necessary. Storage may include the use of dedicated secure servers, using encryption and access controls to keep the data impervious.
- It is important that the data is preserved with full integrity. This means they must not be capable of being manipulated or modified by unauthorized third parties. The use of methods such as *hashes* and integrity checks can help to secure this data.

4. Data analysis and threat identification

- Once the data has been collected and stored, it must be analysed to understand the nature and scale of the incident. The use of analysis tools to identify suspicious characteristics, as well as to understand how information systems and networks have been compromised.
- The use of *threat intelligence* is a process that involves gathering external information about current threats and using it to improve incident response.

5. Coordination with third parties and partners

- In cases of large-scale incidents, such as state-sponsored or state-supported cyberattacks, it may be necessary to coordinate with cybersecurity structures, partners, and international institutions. These can assist in gathering information and coordinating the response.
- Many cybersecurity incidents involve partners, and the collection of information and data management must also include these parties to identify the source of the attack and prevent its spread.

4.1.1 Information and awareness on risks

In a cyber crisis, informing and raising awareness among the parties involved is an important component to ensure a rapid, coordinated, and effective response. This phase requires strategic communication, preparation to educate users, and prevention of further spread of damage. Information and awareness are critical to minimizing the impact of large-scale cyber incidents

and cyber crises. Through good communication strategies and the use of advanced technologies, infrastructures can respond better and protect their interests during a crisis.

The role of information and awareness

Information and awareness help to:

- Minimizing panic: Clearly explaining the situation to prevent misunderstandings and the spread of fear.
- Improving decision-making: Providing accurate and detailed information to help leaders and teams take appropriate measures.
- Preventing the spread of threats: Educating users not to take actions that could worsen the situation (such as opening suspicious emails).

4.1.2 Situational awareness

Situational awareness is essential for managing and responding to large-scale cyber incidents and cyber crises, which include the ability to:

- **Identifying** the current status of the network, systems, and resources.
- **Understanding** the impact of an incident on the organization and its interests.
- **Envisaged** the possible escalation of threats and the effects of response measures.

Situational awareness is the foundation of a successful response to large-scale cyber incidents and cyber crises. Infrastructures that invest in modern technology, training, and reinforce cooperation can build a better capacity to understand, manage, and prevent cyber threats.

Importance of situational awareness for the management and response to large-scale cyber incidents and cyber crisis:

- Provides information to improve decision-making.
- Enables a rapid and coordinated response to incidents.
- Helps in setting priorities and allocating resources.

Phases the importance of situational awareness for the management and response to large-scale cyber incidents and cyber crisis is as follows:

1. Collection of information
   - The collection of information from multiple sources, including system logs, network traffic analysis, and reports from stakeholders.
   - The use of threat intelligence platforms to obtain information on global attack trends.
2. Understanding of information
   - Analysis of the collected data to build a clear understanding of the risk and impact of the incident.
   - Classification of information to determine priorities and optimize resources.
3. Prediction
   - Prediction of the possible evolution of the situation using historical analysis and machine learning models.
   - Planning measures to prevent the escalation of the crisis and to restore operations to normal.

4.2 Activation of the response in Albania

With the increase in cyber-attacks and their impact on critical infrastructures, Albania has adopted a structured approach to address cybersecurity incidents and crises in this field. This

process includes legal, technological, and organizational mechanisms aimed at ensuring a rapid and effective response to cyber threats.

The activation of the response in Albania in cases of large-scale cyber incidents involves a series of coordinated steps and immediate measures, which are necessary to manage and reduce the potential impact of these incidents.
This process requires the commitment of state institutions, the sectors involved, as well as cooperation among various cybersecurity actors. Some of the key elements included in the activation of the response in cases of large-scale cyber incidents and cyber crisis in Albania are:

1. **Detection of the incident and activation of the response team**
   - When a potential large-scale cyber incident is identified, the emergency response team, CERT, is immediately activated to assess the incident and to draft the action plan that must be taken to prevent the spread and minimize the damage.
2. **Coordination** with national and international actors
   - Coordination with national security structures to prevent the further spread of the threat.
   - Cooperation with international cybersecurity partners, for information exchange and seeking assistance.
3. **Communication management**
   - Clearly defining messages for the public and stakeholders, to avoid panic and to ensure transparency regarding the measures being taken.
4. **Minimizing damage and system recovery**
   - After a full assessment has been carried out and the threat has been neutralized, the process of recovering lost or damaged data begins. This process must be conducted carefully and by ensuring that all systems are clean from any potential threats.
5. **Assessment and lessons learned**
   - After the incident response has concluded, it is essential to conduct a thorough analysis of the incident to understand how it occurred and how it can be prevented in the future. This includes an in-depth investigation of the causes of the incident and the improvement of policies and procedures for incident response.
   - After the incident, it is important to identify gaps in security measures and to take steps to increase cybersecurity capacities in the future. This may include continuous staff training, strengthening infrastructure, and improving security policies.

4.3 National resources and capacities for responding to large-scale incident situations and cyber crisis in Albania

Dealing with cyber crises requires genuine 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 to ensure an effective response to cyber crises.

4.3.1 Responsible entities

1. Council of Ministers;
2. Prime Minister;
3. Interministerial Committee of Cybersecurity;
4. Ministers;
5. National Cybersecurity Authority/ National CSIRT;

6. CERT/ Emergency Response Team, Cyber Crisis;
7. Head of the Institution;
8. Sectoral CSIRT;
9. CSIRT at the operator level;
10. Commissioner for the Right to Information and Protection of Personal Data.
11. State Police.

4.3.2 Public information

Public information in the first phase of a cyber crisis is a key element to minimize damage and maintain public trust. In this phase, the emphasis is placed on fast, clear, and transparent communication. To ensure effective information, a cyber crisis communication plan must be established with well-defined protocols for public information as well as the establishment of a communication team, and it is important to:

- Identify the audience, including the interested public, affected citizens, businesses, employees, the media, and other interested parties;
- Use appropriate communication channels, such as social media, official websites, dedicated applications, and television;
- Ensure transparency, clarity, as well as a commitment to further information;
- Provide concrete instructions, such as changing passwords, closing compromised accounts, or reporting incidents;
- Avoid panic, as well as focusing on public safety and resolving the situation;
- Monitor public response to track public perception and the spread of disinformation.

4.3. 3 Reporting

Reporting is an essential element of communication and coordination during large-scale incident response and cyber crises. It is carried out in accordance with the responsible cyber security structures as per the current legislation on cyber security. To ensure a standardized process, designated forms and procedures are used, which help in the efficient collection and sharing of information.

The method of reporting will be conducted according to the deadlines and standard formats approved by the National Cyber Security Authority, pursuant to the regulation on the categorization of cyber security incidents. The obligation to report applies to all operators of information infrastructures at the moment a cyber security incident is identified.

4.3. 4 Post action reviews

Post action reviews are an important step following the occurrence of a large-scale incident and cyber crisis. This process helps to assess how the incident was managed and identifies opportunities to improve response and prevent similar events in the future. The post action review includes a detailed analysis of all phases of the incident and the response to it, focusing on lessons learned and possible improvements. Some key elements of the post-action review are as follows:

1. **Incident management analysis**
   - It is assessed how quickly and efficiently the structures responsible for cybersecurity were activated. Were they activated in a timely manner?

- It is examined how communication was managed by the relevant structures and users. Was there any problem in conveying information in real time? Were the appropriate tools used for communication?

2. Assessment of the effectiveness of the measures taken

- It is analysed how effective the measures taken have been to stop the spread of the incident. Have protocols for the protection of data and systems been implemented?
- The efficiency of the measures taken to restore services and systems to normality is assessed. How long did the recovery take?

3. Identification of vulnerabilities

- It is examined which vulnerabilities in systems, procedures, or policies allowed the incident to occur or spread. Was there any non-compliance with best security practices? Were advanced technologies used for protection?
- Are the security protocols and plans updated and adapted to current threats? Are they sufficient to deal with a similar incident in the future?

4. Lessons learned and adaptation of the security plan

- The main lessons learned from handling the incident are identified. What can be done better to prevent similar events in the future? Which weaknesses require improvement?
- Based on the lessons learned, institutions and information infrastructures must improve their security plans and protocols. This may include updating incident response policies, staff training, and strengthening protective measures.

5. Assessment of recommendations and preventive measures

- After reviewing the incident, recommendations are identified for improving information infrastructure and security.
- Increasing the training and education of employees to prepare them to recognize and respond to cyber security threats.

6. Documentation and reporting after the incident

- A detailed post incident report should include a thorough analysis of the event, including the cause, consequences, and the measures that have been undertaken to address it. This report should be detailed and provide recommendations for future actions.
- Post incident documentation helps to create a basis for future investigations and to develop better strategies for managing similar events.

4.3.5 Review

The review following a large-scale incident and cyber crisis is an important process aimed at assessing incident management and identifying opportunities to improve response and protection in the future. This review is essential to understand how policies, procedures, and security measures have been implemented, as well as to learn from the event to prevent other incidents. This review should include all actors including those involved in cyber crisis management and to analyse how the planned measures have been implemented, as well as to suggest actions for improving preparedness and the effectiveness of the response in the future. This process should assist in identifying the weaknesses and strengths of the structures that responded to the cyber crisis.

Review and improvement consist of:

1. Improving preparedness measures: Based on the findings of the review, improvements may be recommended for preventive and mitigating measures, as well as for strengthening response capacities to cyber incidents.

2. Reviewing communication procedures: Adapting communication protocols to ensure that sensitive information remains secure and is distributed quickly and efficiently.
3. Strengthening inter-institutional and international cooperation: Increasing the level of cooperation with international agencies and the private sector to improve the response to cyber crises.
4. Training and simulations: Organizing regular trainings and simulations to test response procedures and to improve the preparedness of teams for cyber crisis.

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

1. **Council of Ministers** in its capacity as a collegial body, upon the proposal of the Prime Minister, makes the decision for:

a. The declaration of a cyber crisis for a period of 7 days.
b. Extension of the crisis period, but not more than 30 days.

2. The Prime Minister in the capacity of the principal leader, leads and coordinates all institutional and inter-institutional state actions for the coordination of all ministries and institutions as provided in article 11, letter "a"/i-ix of law no. 25/2024 "On Cyber Security" in the case of a cyber crisis and submits to the Council of Ministers the proposal for:

a. The declaration of a cyber crisis for a period of 7 days.
b. Extension of the crisis period, but not more than 30 days.

3. Interministerial Committee on Cyber Security, in its capacity as a consultative body for cyber security issues, which is chaired by the Deputy Prime Minister of the country, in the event of a crisis coordinates the work between ministries, institutions, members of the Interministerial Committee, as well as ensures consultation and coordination in cases of incidents/cyber crisis.

4. The Minister in its capacity as the individual body, plays a leading and coordinating role for the subordinate institution/institutions in cases of cyber incidents/crisis and reports to the Prime Minister. It also makes important decisions.

5. **National Cyber Security Authority**/ National CSIRT/ CERT (Emergency and Cyber Crisis Response Team) is an Authority with regulatory and coordinating competences, the Incident Response Team, Cyber Crisis, and exercises the following roles and responsibilities:

a. Proposes to the Prime Minister, in coordination with security and defence Institutions as provided in article 11, letter "a" of law no. 25/2024 "On Cyber Security", the declaration of the state of cyber security crisis and the emergency measures for resolving the situation;
b. Activates the ad-hoc CERT structure;
c. Coordinates crisis management;
ç. Issues decisions of a general nature or takes protection measures of a general nature;

6. CERT, The Emergency and Cyber Security Crisis Response Team
It is an ad-hoc structure that acts as the first line of defence for handling emergencies and the cyber security crisis.
Main duties:

a. Coordination and rapid intervention for handling large-scale incidents and cyber crises.

b. Drafting the emergency measures plan.
c. Emergency management and resolution.
ç. Supports in drafting recommendations to restore information systems and networks in information infrastructures following a large-scale incident or a state of cyber emergency and crisis

7. **The head of the institution** in the capacity of the head of the institution:
   a. Leads the institution in coordinating the necessary processes for managing the internal situation;
   b. Officially informs about the cyber situation of the affected services in their institution, accompanied by the financial, social, health, and environmental effects because of the cyber attack:
      i. The National CSIRT;
      ii. The respective Sectoral CSIRT;
      iii. State Police;
      iv. The Commissioner for the Protection of Personal Data;
      v. The Minister in charge (optional);
      vi. Secret service institutions (optional);
      vii. Law enforcement institutions (optional);
   c. Coordinates with the National CSIRT, the Sectoral CSIRT, and other parties involved in the process;
   ç. Coordinates with the media for providing information regarding the situation.

8. **Sectoral CSIRT**, in its capacity as the cybersecurity incident response team for the respective sector:
a. Reports to the National CSIRT any cyber incident occurring in the information infrastructures of the respective sector;
b. Coordinates with the CSIRTs at the operators to respond to the situation.

9. **CSIRT at the operator** level, in the capacity of the incident response team for the respective operator:
   a. Reports any incident occurring in the operator's information infrastructures to the National CSIRT and the Sectorial CSIRT;
   b. Coordinates with the National CSIRT and the Sectoral CSIRT in order to respond to the situation.

10. **The Commissioner for the Right to Information and Protection of Personal Data** in the capacity of the institution responsible for drafting policies for the protection of individuals' personal data, monitors the implementation of the relevant legislation in the case of incidents and cyber crisis:
   a. Handles, controls, and monitors the implementation of the legislation in force on the protection of personal data.

11. **State Police** in the capacity of the institution responsible for investigating cybercrime and implementing criminal legislation, performs the following actions:
   a. Carries out the necessary operational actions within the framework of the implementation of the criminal legislation.
   b. Cooperates with the National CSIRT and the CSIRT at the operator for the analysis and investigation of the cyber incident.
   c. Carries out procedural actions within the framework of the implementation of criminal legislation.

Section 5 Recovery

Recovery of services after large-scale incidents and cyber crisis it is an essential process that helps infrastructures return to normality after a severe cyber event. This process is divided into several phases and requires a coordinated and well-structured approach to ensure that services are restored in a safe and rapid manner, and to significantly minimize the long-term impacts of the large scale cyber incident and crises.

5.1. Recovery of services after large-scale incidents and cyber crisis

Recovery in cases of large-scale incidents is an important process that aims to restore operations and infrastructure functions to a stable state after a large-scale cyber incident. This process is closely linked to ensuring business continuity and restoring security to minimize the long-term impacts of the cyber incident. Recovery is not a single step, but a series of coordinated actions that help restore systems, services, and infrastructure, as well as improve preparedness for future incidents.

1. **Recovery of systems and infrastructure**

- After identifying the large scale cyber incidents and taking measures to stop the spread of impacts, the first step is the recovery of critical systems. This may include:
  - Restoring data from backup.
  - Restoring affected services.
  - Improving the integrity of security systems.
  - After the restoring systems and services, it is important to carry out checks and tests to ensure that they are operating normally and that issues are not repeated in the future.

2. **Security testing and verification**

After the restoration of systems, it is important to conduct security testing, including the verification of all protective measures and their update if necessary. This testing may include:

- Testing of firewalls and monitoring systems.
- Security testing to detect any possible vulnerabilities.
- Verification of protection against new threats, such as viruses, DDoS attacks, etc.

3. Communication and information management

- After the incident, it is important to maintain communication to inform everyone about the status of recovery and any new developments. This communication should be prompt and coordinated, especially for those who are part of the crisis management and cyber incident response team.
- Communication must be transparent and include clear information about the measures that have been taken, as well as the timelines for service restoration.

4. Analysis of consequences and damage assessment

- After the completion of recovery, it is important to conduct a thorough assessment of the consequences of the cyber incident. This process helps to understand how severe the damage was, the scale of it, and how short-term and long-term damages will be addressed.
- The assessment of consequences is important for planning and improving readiness for future incidents.

5. Improvement of readiness for future incidents

- After the completion of recovery, the business continuity plan for the infrastructure must be reviewed and updated. This plan must be kept up to date to reflect the lessons learned from the cyber incident and to address any identified weaknesses.
- Address and improve weaknesses to prevent similar incidents in the future.
- Exercises and simulations are important for preparing infrastructures for future incidents. After a large-scale cyber incident, it is important to conduct new readiness tests to ensure and prepare for the management of other events.

5.2 Roles and responsibilities of entities responsible for cybersecurity during the recovery phase

To manage cyber incidents at the national level, the roles and responsibilities of each actor in the recovery phase must be defined, starting from the highest management levels, including:

1. National Cyber Security Authority / National CSIRT;
2. Head of the Institution;
3. Sectoral CSIRT;
4. CSIRT at the operator level;
5. The Commissioner for the Right to Information and Protection of Personal Data.

1. **National Cyber Security Authority**/ National CSIRT, the Emergency Response Team, is an Authority with regulatory and coordinating competences, and exercises the following roles and responsibilities:

a. Supports the operator of information infrastructure in restoring services and data to their normal state and guides the use of tools and techniques to eliminate threats and repair the damages caused, as well as isolating affected end devices and systems to prevent further damage.
b. Supports the operator of information infrastructure in cleaning up cyber incident components on affected systems, such as deleting malicious files, deactivating user accounts, etc., according to the category of the cyber incident.
c. Supports the operator of information infrastructure in eliminating cyber threats by deactivating infected systems, scanning for malware, and addressing vulnerabilities;
ç. Supports the operator in restoring to their pre-compromise state by using clean backups. Also requires the operator of the information infrastructure to monitor for suspicious activities and to implement security patches to address the vulnerabilities that caused the breach.

2. The head of the institution:

a. Leads the institution for the coordination of the necessary processes during the recovery phase;
b. Ensures the execution of activities in cooperation with the National CSIRT to restore services and data to their normal state.

3. Sectoral CSIRT, in their capacity as the cyber security incident response team of the relevant sector:

a. Supports the operator of the information infrastructure of the relevant sector to restore services and data to their normal state and guides the use of tools and techniques to

exclude threats and repair the damages caused, as well as the isolation of end devices and affected systems to prevent further damage.

4. CSIRT at the operator level in their capacity as the cyber security incident response team of the relevant operator:

a. Works to restore services and data to their normal state by using tools and techniques to exclude threats and repair the damages caused, as well as isolating end devices and affected systems to prevent further damage.

b. Works to clean up the cyber incident components in the affected systems, such as deleting malicious files, deactivating user accounts, etc., according to the category of the cyber incident.

c. Works to eliminate cyber threats by deactivating infected systems by scanning for malware and addressing vulnerabilities;

ç. Works to restore systems to their pre-compromise state by using clean backup copies. Also requests the operator to carry out monitoring for suspicious activities and security patches are applied to address the vulnerabilities that caused the intrusion;

d. Works to address the vulnerabilities that caused the intrusion in the restored systems;

dh. Monitor the restored systems for suspicious activity.

5. Commissioner for the Right to Information and Protection of Personal Data in its capacity as the institution responsible for drafting policies for the protection of individuals' personal data, monitors the implementation of the relevant legislation in the case of large scale cyber incidents and cyber crisis:

a. Handles, controls, and monitors the implementation of the applicable legislation on the protection of personal data.