



**REPUBLIC OF ALBANIA**  
**NATIONAL AUTHORITY ON ELECTRONIC CERTIFICATION AND CYBER SECURITY**

**REPORT**  
**CYBERSECURITY GOVERNANCE IN ALBANIA**

**YEAR 2023**

<b>I.</b>	<b>INTRODUCTION.....</b>	<b>3</b>
<b>II.</b>	<b>LEGAL AND REGULATORY FRAMEWORK .....</b>	<b>4</b>
<b>III.</b>	<b>CYBER SECURITY POLICY AND STRATEGIES .....</b>	<b>4</b>
	<b>NATIONAL CYBER SECURITY STRATEGY 2020-2025.....</b>	<b>5</b>
	<b>RESPONSIBLE INSTITUTIONS FOR CYBER SECURITY .....</b>	<b>6</b>
	<b>    Roles and responsibilities of NAECCS.....</b>	<b>6</b>
<b>IV.</b>	<b>CYBER SECURITY GOVERNANCE .....</b>	<b>10</b>
	<b>CYBER SECURITY GOVERNANCE BY SECTORS .....</b>	<b>12</b>
<b>1.</b>	<b>DEVELOPMENT OF TECHNOLOGY AND INFRASTRUCTURE.....</b>	<b>15</b>
<b>2.</b>	<b>OVERSIGHT OF CYBER SECURITY GOVERNANCE IMPLEMENTATION .....</b>	<b>20</b>
<b>3.</b>	<b>DETERMINATION OF CYBER SECURITY MEASURES AND CONTROL OF THEIR IMPLEMENTATION.....</b>	<b>27</b>
<b>4.</b>	<b>PROMOTING A SUSTAINABLE CYBER CULTURE / HUMAN RESOURCES AND AWARENESS .....</b>	<b>29</b>
<b>5.</b>	<b>NATIONAL AND INTERNATIONAL COOPERATION .....</b>	<b>30</b>
<b>V.</b>	<b>KNOWN CASES OF CYBER ATTACKS.....</b>	<b>33</b>
<b>VI.</b>	<b>OVERALL ASSESSMENT: CONCLUSIONS AND RECOMMENDATIONS .....</b>	<b>35</b>
	<b>CONCLUSIONS.....</b>	<b>35</b>
	<b>RECOMMENDATIONS .....</b>	<b>37</b>

## I. INTRODUCTION

This report describes the situation of cyber security governance in the Republic of Albania during the year 2023. To present the situation of cyber security governance, it is important to understand the complexity and context of the development of this field as well as its importance for society and the economy. With the global technological developments of recent years, cyber security has become a priority for the Albanian government. The development of this field has taken on special importance for society and the economy, considering the high number of services that are offered online today and other important issues as follows.

### **Development of the necessary infrastructure in the field of information and communication technology:**

Albania has given importance to the modernization and development of the necessary infrastructure in the field of information and communication technology, including the use of advanced information technologies.

Digitization of public services with the aim of efficiency and quality of service delivery and interaction between government, citizens, and business is one of the most important processes that happened in the country. These developments have increased exposure to various cyber threats, bringing the urgent need to take concrete measures to secure information infrastructures.

### **Cyber threats:**

As in many other countries, Albania is facing a high number of cyber threats. These threats include attacks on critical information infrastructures targeting government institutions and private companies.

Due to the need to protect personal data and guarantee the proper functioning of information systems and networks, cyber security has taken on a special importance, being closely related to national security.

### **Identification of Critical and Important Information Infrastructures:**

The identification of critical and important information infrastructures is an important step for cyber security and the protection of systems that store and process data (Crown Jewels), the malfunction of which can cause serious consequences on national level.

In Albania, **289** critical information infrastructures have been identified in the sectors: banking, financial, energy, transport, health, digital infrastructures, and water supply.

Also, NAECCS is in the process of identifying new critical information infrastructures, including security and defense institutions.

### **Importance in the economy and society:**

Cyber security plays an important role in the economy as many sectors use information and communication technologies to provide their services. Possible cyber-attacks can cause great economic damage, as they can affect critical sectors such as banking, financial, energy, transport, health, digital infrastructures, water supply, or other important companies.

Public awareness and education about ways to protect cyber security have a significant impact on reducing cyber security issue.

### **Cyber Defense:**

Cyber defense is a global issue that is becoming increasingly important and includes taking measures to protect information systems and networks in critical and important infrastructures as well as guaranteeing the security of sensitive data from attacks and different cyber threats.

Albania is developing technical and human capacities in the field of cyber security, preparing for the challenges of the new digital age.

## II. LEGAL AND REGULATORY FRAMEWORK

NAECCS was created with DCM No. 141, dated 22.2.2017, and has the responsibility of supervising the implementation of Law No. 9880/2008, "On Electronic Signature", Law No. 107/2015, "On Electronic Identification and Trusted Services" as well as Law No. 2/2017, "On Cyber Security" and by-laws issued in their implementation.

The creation of NAECCS was an important step to address cyber security challenges at the national level and to help coordinate responsibilities and actions in this area.

**Law No. 2/2017, "On Cyber Security"**, is the first law adopted in the country covering cyber security issues partially transposed by the *EU Directive NIS 1*.

The purpose of this law is to achieve a high level of cyber security, by defining security measures, rights, and obligations, as well as cooperation between entities operating in the field of cyber security.

The by-laws issued under Law No. 2/2017, "On cyber security", are:

- DCM No. 141, dated 22.2.2017, "On the organization and operation of the National Authority on Electronic Certification and Cyber Security", amended, which defines the functions and responsibilities of the Authority.
- DCM No. 553, dated 15.07.2020, "On the approval of the List of Critical Information Infrastructures and the List of Important Information Infrastructures", amended.
- Regulation "On the content and manner of documenting security measures", approved by (Version 2.0)
- Regulation "On Categories of Cyber Incidents as well as the format and elements of the report"
- Guideline "On the Methodology of the Organization and Functioning of CSIRTs at National Level"
- DCM No. 1084, dated 24.12.2020, "On the approval of the National Cyber Security Strategy and Action Plan 2020-2025."

Currently, **the new Law** on cyber security has been approved in full compliance with the EU Directive, "*Regarding measures for a common high level of security of networks and information systems throughout the European Union*" (NIS 2), this obligation is also within the National European Integration Plan of the Republic of Albania 2022-2025.

Considering that EU member states have until October 2024 to transpose and implement this directive into the relevant national legislation, Albania has taken steps forward in integrating the provisions of the NIS2 directive into the national legal framework through the adoption of this Law.

## III. CYBER SECURITY POLICY AND STRATEGIES

The purpose of the Cybersecurity Policy is to review and coordinate the obligations arising from the commitments made for secure cyberspace at the national level to ensure the fulfillment of responsibilities by all actors.

The main objectives of cyber security policies are based on three main pillars:

1. **Human Resources:** Increase cybersecurity awareness and capability across the organization to ensure all users know safe practices, identify cyber threats and report suspicious behavior. This means regular training, and simulations of cyber-attacks, as well as clear instructions on security standards, increasing professional skills to implement cyber security measures and respond effectively to cyber-attacks.
2. **Processes:** Implementing clear policies and procedures for data protection, detecting and responding to cyber incidents, and regularly reviewing these processes to adapt to new threats. This includes creating a cyber incident response plan and regular checks for compliance with security standards.

3. **Technology:** Implementation of secure technologies for data protection, detection of cyber threats and reduction of exposure to risks. This means the use of monitoring systems, advanced authentication, data encryption and devices dedicated to preventing cyber-attacks.

After the sophisticated cyber-attack that occurred in 2022, against critical information infrastructures in Albania, NAECCS was reorganized to fulfill the vision of the Albanian government to achieve a high level of cyber security in the country. This reorganization was accompanied by an increase in the number of employees from 24 to 85, giving NAECCS the necessary technological and human capacities to address cyber security challenges.

## **NATIONAL CYBER SECURITY STRATEGY 2020-2025**

To strengthen cyber security at national level and guarantee a safe and stable cyber ecosystem in Albania, the Albanian Government has approved the Decision of the Council of Ministers No. 1084, dated 24.12.2020, the National Cyber Security Strategy and Action Plan 2020-2025.

The strategy is based on four main pillars:

1. **Guaranteeing** cyber security at national level, through the protection of information infrastructures, strengthening technological and legal means.
2. **Building** a safe cyber environment, educating and raising awareness of society in raising professional capacities in the field of information security.
3. **Creating** the necessary mechanisms for children's safety in cyberspace, while simultaneously preparing the new generation, capable of taking advantages of information technology and facing the challenges of development.
4. **Increasing** national and international cooperation in the field of cyber security with strategic partners.

To achieve the strategic objectives, Albania works for the expansion of bilateral and multilateral agreements in the field of cyber security with international partners, as well as being involved in international activities and partnerships to share information and best practices in the field of cyber security.

The National Strategy for Cyber Security 2020-2025 foresees the need to review the Action Plan every two years, based on the dynamics of the development of the cyber security sector. NAECCS worked intensively on the revision of the 2020-2025 Action Plan and drafted the 2024-2025 Action Plan, identifying priorities and needs as well as coordinating with the responsible institutions regarding its implementation.

In the revised Action Plan for the period 2024-2025, concrete measures have been defined that will make it possible to address needs, priorities and accelerate progress for cyber security.

The Action Plan 2024-2025 will contribute to achieve the following results also targeted by the National Cyber Security Strategy 2020-2025:

- **Improving the political and legal framework**, including laws, strategic policies, regulations, methodologies and procedures, through the implementation of EU cybersecurity policies and standards as well.
- **Strengthening cyber security structures and infrastructures** in relation to technical and professional capacities as well as their respective procedures. This was achieved through the establishment of the National Cyber Security Operational Center (SOC) for monitoring and handling cyber security incidents, the establishment of laboratories for analyzing malicious programs (malware), cyber investigation and simulation of cyber incidents, increasing technical and professional capacities, technological analysis of the environment of critical infrastructures,

improvement of incident handling and management procedures and others, which are foreseen in the action plan.

- **Raising awareness and education**, as well as improving preventive and protective measures regarding cyber security threats, cybercrime and illegal online content, child safety and protection online, and violent extremism and radicalization in cyberspace.
- **Increasing professional capacities in cyber security** through the organization of trainings and certifications, in cooperation with national and international partners.
- **Strengthening national and international cooperation**, where several activities are planned, such as: the creation of a forum with public and private institutions in Albania and international agencies, the creation of a cyber diplomacy structure in the Ministry for Europe and Foreign Affairs in coordination with NAECCS, drafting and signing of bilateral and multilateral agreements in the field of cyber security, promotion and implementation of international law, norms and confidence-building measures regarding the responsible behavior of the state in cyberspace, active participation in the UN, NATO, OSCE, EU and other international organizations, regional cyber exercises, participation in international projects, etc.

The 2024-2025 Action Plan also contributes to Albania's European integration process, as it foresees activities related to the improvement of the current legal and policy framework through the implementation of EU policies, cyber security standards and best practices. as well as international cooperation with strategic partners.

## **RESPONSIBLE INSTITUTIONS FOR CYBER SECURITY**

NAECCS, as the responsible and supervisory institution for the implementation of legislation in force on cyber security in Albania, plays a key role in the design, management and implementation of cyber security policies.

### **Roles and responsibilities of NAECCS:**

- Acts in the capacity of the National Security Incident Response Team (National CSIRT).
- Acts as a central point of contact on national level for operators of critical and important information infrastructures and coordinates the work to resolve cyber security incidents.
- Manages the National Security Operations Center (SOC) which monitors malicious activities on critical and important information infrastructures and handles cyber incidents.
- Drafts strategic policies, regulations, plans and procedures to strengthen cyber security at the national level and monitors their implementation.
- Exercises the role of coordinator at national level in cooperation with all relevant institutions for the implementation and monitoring of the "National Cyber Security Strategy".
- Identifies and classifies critical and important information infrastructures and ensures their protection.
- Defines cyber security measures and supervises/controls their implementation.
- Coordinates the actions of all structures responsible for solving cyber crisis situations.
- Develops specific programs and policies to increase cyber security awareness at national level.
- Cooperates with international organizations and partners in the field of cyber security in order to exchange best practices and expertise, build capacities, exchange information and implement joint projects.

Also, the other institutions responsible for the implementation of the revised National Cyber Security Strategy Action Plan 2024-2025 are as follows:

- Ministry of Education and Sports
- Ministry of Health and Social Protection
- Coordination Center against Violent Extremism
- Ministry of Infrastructure and Energy
- National Agency of Information Society
- General Directorate of the State Police
- National Authority for the Security of Classified Information
- The Electronic and Postal Communications Authority (AKEP): AKEP has a role in monitoring and regulating the telecommunications sector and supervising cyber security in this sector.
- Ministry for Europe and Foreign Affairs.

The main objectives that will be supported by NAECCS and the institutions responsible for the implementation of the revised National Cyber Security Strategy Action Plan 2024-2025 are as follows:

Specific Objective	Sub-objectives	Responsible institution
<b>Specific Objective A</b> - Improving the legal framework that regulates the field of cyber security in the country, as well as its harmonization with the directives and regulations of the European Union.	<b>A.1</b> Improving the regulatory framework for cyber security aligned with sectoral laws to properly address issues and resolve them including but not limited to: Cloud computing, ICT, 5G technology, Artificial Intelligence.	NAECCS/ MIE/AKEP/ MD/MB/SP
	<b>A.2.</b> Continuous adaptation of standards and rules according to developments in the cyber security field.	
	<b>A.3.</b> Fulfilling the commitments made as a country of the North Atlantic Alliance, for cyberspace.	SP/ NAECCS
	<b>A.4.</b> Defining a national procedure for cases of emergency situations created by cyber crises, with the aim of taking concrete measures to resolve the situation in real time.	NAECCS
<b>Specific Objective B</b> - Establishment and operation of CSIRTs in all industry sectors at national level	<b>B.1.</b> The establishment of the National CSIRT and new sectoral CSIRTs, in the critical and important information infrastructures, as well as the strengthening of the existing ones	NAECCS/ NAIS/ SP/ MIE/AKEP/ AKESK
	<b>B.2.</b> Creating optimal working conditions for the operation of CSIRTs, in fulfilling its duties, to guarantee cyber security in critical and important information infrastructures.	NAECCS/ NAIS/ SP/ MIE/AKEP
	<b>B.3.</b> Capacity building of CSIRTs, through training and cyber exercises.	NAECCS/ NAIS/ SP/ MIE/ AKEP
	<b>C.1.</b> The use of advanced hardware and software solutions for the identification, prevention, and management of cyber incidents.	NAECCS/ NAIS/SP
	<b>C.2.</b> Analysis of critical and important information infrastructures for risk assessment and management in them.	NAECCS/ NAIS
	<b>C.3.</b> Drafting of strategic plans for the protection of cyberspace from possible incidents.	NAECCS
	<b>C.4</b> Realization of self-assessments in critical and important information infrastructures for measuring the level of maturity of cyber security.	NAECCS
	<b>Specific Objective D</b>	<b>D.1.</b> Monitoring and prevention of phenomena that promote violent extremism and radicalization in vulnerable groups in space CYBER

- Improving information infrastructures to fight cybercrime, radicalism and violent extremism	<b>D.2</b> Continuous identification of contaminating elements circulating on the Internet, which compromise cyber security in the country	SP/ NAECCS
	<b>D.3</b> The establishment of mechanisms for the regulation of safe Internet in public premises, certified by the regulatory authority in the field of cyber security	NAECCS
	<b>D.4</b> Raising the capacities of the responsible authorities against cybercrime.	NAECCS/ SP/ NAIS
	<b>D.5</b> Increasing regional cooperation in the fight against cybercrime	SP
<b>Specific Objective A</b> - Increasing professional capacities in the field of information security through the revision of educational curricula	<b>A.1</b> - Designing study programs in higher education in the field of cyber security, with the aim of creating a new generation of cyber security experts	NAECCS
	<b>A.2.</b> Drawing up recommendations for the integration of information about the Safe Internet into university curricula.	NAECCS/ MAS
	<b>A.3.</b> Increasing research and innovation capacities in the field of cyber security	NAECCS/ MES/ UNIVERSITIES
<b>Specific Objective B</b> - Increasing the awareness and professional skills of public and private institutions for cyber security.	<b>B.1.</b> Periodic trainings, for the deepening of knowledge in cyber security, according to the dynamics of the field, for the administrative staff at the central and local level	NAECCS
	<b>B.2.</b> Growth and support of research capacities and business innovations by promoting the establishment of scientific research centers in the field of cyber security	NAECCS
	<b>B.3.</b> Increasing the capacities of CSIRTs at national level and the executive level of the public administration through training and cyber exercises	NAECCS/ NAIS
<b>Specific Objective C</b> - Increasing society's awareness of cyber security and cyber threats.	<b>C.1</b> Increasing society's awareness of cyber security, using the appropriate spaces for their realization, including audiovisual or social media	NAECCS
	<b>C.2</b> The creation of an online educational platform, for cyber security, to increase awareness in different age groups of society, for the use of safe Internet and digital infrastructure	NAECCS/ ASHMDF/ MES/ NAIS/ SP/AKEP etc.
<b>Specific Objective A</b> - Strengthening the legal framework for increasing the safety of children on the Internet.	<b>A.1</b> Drafting of a specific guideline (and accompanying regulation) for data collection of reported incidents of violence, bullying and online abuse of children in schools.	MES/ NAECCS
	<b>A.2.</b> Improving the regulatory framework to bring it in line with international legislation on the protection of children from sexual abuse on the Internet	MES/ ASHDMF/ SP
	<b>A.3.</b> Complementing and clarifying legislation regarding the notification, removal and blocking of illegal online material	NAECCS/ SP/ AKEP
<b>Specific Objective B</b> - Preventing sexual abuse of children on the Internet by raising awareness and creating safe spaces for surfing the Internet	<b>B.1.</b> Integration of the "Peer Educators for Online Safety" program into the educational system	MAS
	<b>B.2.</b> Creation and support of the online network of ICT teachers to promote the issue of child protection on the Internet	MAS/NAECCS
	<b>B.3</b> Creating public spaces with safe internet for children and families through the 'Friendly Wi-Fi' initiative in 5 municipalities of the country, offering not only free internet access but also filtered information to protect children and young people from abusive content online.	NAECCS
	<b>B.4</b> Application of filters in public and private schools to prevent children's access to inappropriate and illegal sites, as well as ongoing information of ICT teachers to report incidents.	MAS/NAECCS
	<b>B.5</b> Identifying, supporting and promoting talent to create technical solutions that help protect online security.	MAS/NAECCS/MSH RF



<b>Specific Objective C</b> - Effective investigation and prosecution of perpetrators of cybercrimes against children, with a focus on sexual abuse and exploitation	<b>C.1.</b> Provision of technical tools that help the police and relevant bodies in analyzing and detecting cases of online violence, especially related to images of sexual abuse of children	NAECCS/ ASHDMF/ SP/AKEP/MSHMS/ ASHDM
	<b>C.2.</b> Creation of training programs for judicial, prosecution and police personnel regarding the protection of children on the Internet and cyber security, including evidence of digital use and mutual legal assistance	NAECCS/ SP
	<b>C.3.</b> Creation of training programs for the personnel of the judiciary, prosecution and police regarding the protection of children on the Internet and cyber security, including evidence of the creation of a system of courses at the School of Magistrates and the Academy of Security in relation to issues related to the most crimes against children online and ways to protect them on the Internet.	NAECCS
	<b>C.4</b> Creation of mechanisms for the standardization of the work of analyzing digital evidence by the State Police.	SP
	<b>C.5</b> Establishing a working group together with industry to solve problems of investigation and identification of persons suspected of online child abuse, with special focus on identification of end users through IP addresses.	SP/ ASHDMF/ NAECCS/ AKEP
<b>Specific Objective D</b> - Raising awareness and educating all segments of society about the safe use of the Internet by children	<b>D.1</b> Awareness campaign with parents and educators about the dangers and problems that children face on the Internet	NAECCS/ ASHDMF/ MAS/ZVA
	<b>D.2</b> Developing training programs with ICT teachers on safe internet issues	NAECCS/ MAS
	<b>D.3</b> Development of training programs for Child Protection Workers related to the handling of cases of children in need of protection where the risk of violence, abuse, exploitation or neglect is related to the Internet and information technologies	NAECCS/ MSHMS/ ASHDMF
<b>Specific Objective E</b> - Strengthening cross-sectoral cooperation for the protection of children on the Internet.	<b>E.1.</b> Promotion through cooperation with all ISPs of existing mechanisms applied in their platforms for the safety of children on the Internet.	NAECCS/ AKEP/ ISP/ ASHDMF
	<b>E.2</b> Integration by all ISPs into their platforms of the IWF List (Internet watch Foundation Hash List) that prohibits any individual from posting, downloading or viewing images or videos of child sexual abuse	NAECCS
	<b>E.3</b> Establishment of a Technical Advisory Committee for Children's Safety on the Internet, at the National Council for Children's Rights and Protection	MSHMS
<b>Specific Objective A</b> - Strengthening institutional cooperation at national level	<b>A.1.</b> Increasing cooperation and coordination between state institutions to ensure security at national level in cyberspace	MEFA/ NAECCS
	<b>A.2.</b> Creation of an instrument for the exchange of information through the contact points dedicated by the relevant institutions, in cases of cyber threats.	NAECCS
	<b>A.3.</b> Establishing a flexible structure with the best cyber security experts in the country, in order to support in cases of cyber crises, testing and evaluating the level of cyber security on national level	NAECCS
<b>Specific Objective B</b> - Strengthening international cooperation in the field of cyber security and defense and the fight against extremism	<b>B.1.</b> Development of efficient mechanisms and procedures for international cooperation in case of cyber incidents, attacks and crises, according to internationally established principles.	MEFA/ NAECCS
	<b>B.2.</b> Strengthening cooperation and exchange of information with NATO / OSCE and other international organizations / forums	NAECCS, MEFA etc.

These institutions are coordinated and cooperate to take measures to strengthen cyber security in the country. Of particular importance is the close cooperation between these institutions and the sharing of information and experiences to face cyber security challenges effectively.

## IV. CYBER SECURITY GOVERNANCE

Cyber security policies include the use of cyber governance as an important instrument for improving governance and providing public services in a more efficient, transparent and secure manner.

The use of information technology in public administration has the potential to improve economic sustainability as well as the quality of life of citizens in Albania. However, it is essential to ensure that these platforms are secure and protected from cyber threats to guarantee the integrity and confidentiality of government and personal data of citizens.

**The national cyber risk policy** will enable cyber risk assessment by identifying and prioritizing threats and vulnerabilities to cyber security to reduce risk, take preventive and reactive measures in time, as well as guarantee cyber resilience.

**Performance evaluation and monitoring policies** will make it possible to define the appropriate political framework for monitoring and evaluating the level and stability of cyber security in critical and important information infrastructures to ensure that they are as protected as possible and invulnerable to potential threats from malicious actors.

**The cyber crisis policy**, as a comprehensive framework designed to define the cyber crisis management procedure and response at national level to cyber incidents that could escalate into national crises, serves to strengthen the preparation, effective management and recovery from such incidents.

**The communication policy** defines how communication should be carried out on national level regarding cyber threats, incidents, awareness and cooperation, including internal communication, public communication, crisis communication, and communication related to national and international cooperation.

**The policy for increasing the capacities of institutions for cyber security** is aimed at addressing the challenges in terms of technical and human capacities of public and private institutions on national level, providing for the measures that must be taken to increase human capacities, technical capacities, as well as for creating the necessary mechanisms and increasing cooperation national and international, in order to raise and strengthen capacities, in order to strengthen cyber security.

**The public-private partnership policy** is a strategic approach that facilitates cooperation between institutions, organizations and private sector entities to strengthen national cyber security in the country. This cooperation and gaining trust between the institution and private entities can be realized through the establishment of a formal platform for continuous communication and cooperation in the field of cyber security. This cooperation can also be strengthened through the development of projects in areas such as critical infrastructure protection, research and development, or awareness campaigns, joint expert training programs and exercises to build skills and expertise in cyber security. Encouraging the adoption of national and international cybersecurity standards and best practices in incident response and recovery plans to manage and mitigate the impact of cyber incidents and to have a more coordinated response to cyber threats in the private sector.

**The incident management policy** is a policy framework designed to enable the effective handling of incidents which includes the objectives and measures to be implemented for the successful management of the incident to minimize the impact as much as possible and prevent further escalation.

**The policy for the protection of children in cyberspace** is a policy that provides the objectives and measures necessary to educate, inform and protect children from online risks, with the aim of guaranteeing a safe cyberspace for children in Albania.

**The policy for the protection of critical and important information infrastructures** is a policy that includes the steps and measures that must be taken starting from the process of identifying them, assessing the cyber risk, determining the cyber security standards that must be applied to these infrastructures, up to plans for increasing the technical and human capacities of their operators in the field of cyber security.

**The cyber security awareness policy** aims to create a cyber security aware society in Albania, including all actors in every sector and define measures that make it possible to increase awareness of cyber security threats and ways of protection to potential dangers on the Internet.

These policies will contribute to strengthen cyber security in Albania by strengthening preventive, management and response measures related to cyber threats.

**Gender balance policy** is important to ensure equality and diversity in the workplace. It includes policies that encourage and support both genders at all levels. This includes equal access to recruitment, equal pay and work, training and development program.

## CYBER SECURITY GOVERNANCE BY SECTORS

The assessment of cyber security governance at national level is based on the following principles:

### ROLES AND RESPONSIBILITIES

To achieve effective cyber security governance, it is necessary to clearly define the roles and responsibilities of each person or sector for cyber security matters. This ensures that each person or team is aware through an approved procedure of their duties and responsibilities and works towards meeting the overall cyber security objectives of the institution they belong to.

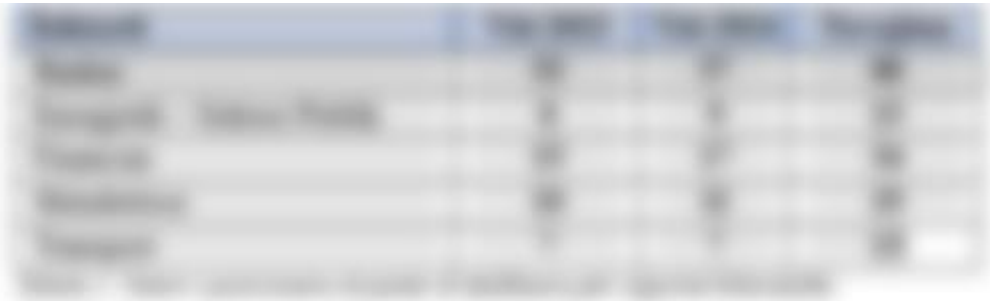
Some important steps to achieve this are:

1. **Defining cyber security roles:** Any entity or institution that administers critical or important information infrastructures must identify specific roles for cyber security. This includes the role of chief information security officer, information security officer, data protection officer, information systems administrator, etc.
2. **Creation of an organizational structure dedicated to cyber security:** This special structure includes specialized departments or sectors of cyber security (Sectoral CSIRT)
3. **Definition of duties and responsibilities:** Define the specific duties and responsibilities of each cyber security role, including monitoring, detection, prevention and management of cyber incidents.
4. **Communication and awareness:** It is of particular importance that all personnel understand their duties and responsibilities in the field of cyber security, as each one contributes to the protection of information systems and networks of which they are a part.
5. **Improving policies and regulations:** Cyber security policies and regulations are reviewed periodically, based on changes in defined roles and responsibilities.
6. **Audit and management review:** Audits and management review to assess the effectiveness of cyber security roles and responsibilities as well as the effectiveness of the information security management system.
7. **Training and human capacity building:** Continuous training and professional development for cyber security personnel to further enhance their skills.

In smaller entities, several cybersecurity roles may be included in a single person's job. In such cases, it is even more important for senior management to ensure that cybersecurity duties are clearly understood and well communicated. Everyone in the organization must understand their role in supporting effective cyber security.

NAECCS, in order to help the operators of critical and important information infrastructures for the creation of sectoral CSIRTs, has approved with Order No. 55, dated 31.07.2018, the Instruction "On the Methodology of the Organization and Functioning of the CSIRTs at National Level".

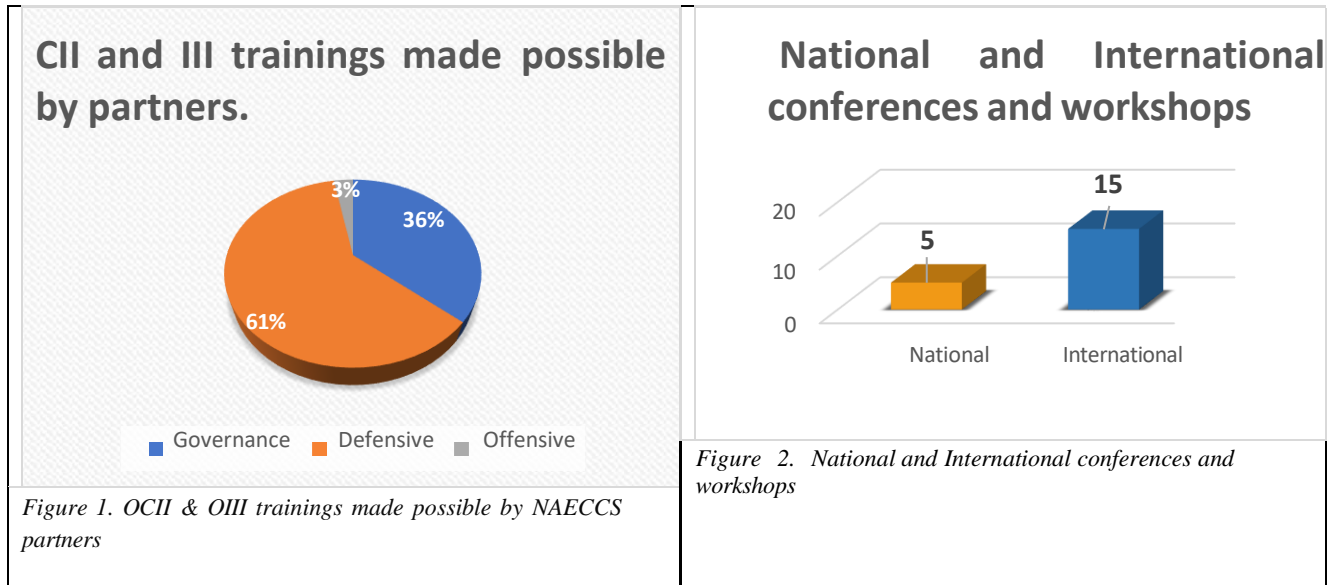
According to self-reported critical and important information infrastructures, there is a small increase in terms of dedicated cybersecurity job positions for each sector, indicating an effort to increase human capacity to defend against cyberattacks.



Also, NAECCS, in cooperation with partners, has undertaken a series of very important training initiatives to strengthen capacities in the field of cyber security. These trainings are designed and structured to address the challenges in cyber security, which range from the protection of critical and important information infrastructures to incident management and threat analysis and aim to improve the knowledge and skills of professionals in the field of cyber security. Through these programs, supported by the expertise of partners, NAECCS aims to raise awareness of current cyber risks as well as build a stronger resilience against potential attacks. These efforts reflect a commitment of clearly for raising cyber security standards and professional development, preparing them to deal effectively with potential cyber-attacks.

Training category	Number
<i>Governance</i>	25
<i>Defensive</i>	42
<i>Offensive</i>	2

Table 2. OCII & OIII trainings made possible by NAECCS partners.



During the year 2023, NAECCS has organized trainings and workshops for Operators of Critical and Important Information Infrastructures according to sectors with the aim of presenting Security Policies and Measures that every operator must implement, as well as improving the response to cyber incidents by developing Tabletop Exercises (TTX), Capture the Flag (CTF), as well as real Cyber Drill simulations.

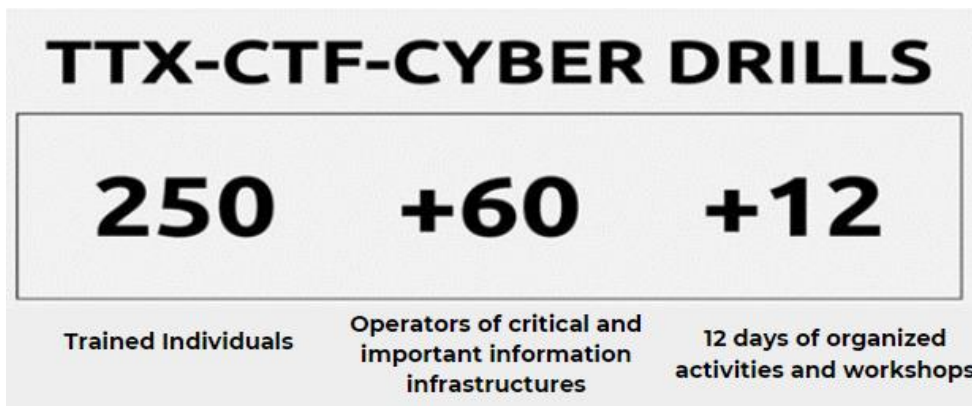


Figure 3. Trainings organized by NAECCS.

## 1. DEVELOPMENT OF TECHNOLOGY AND INFRASTRUCTURE

Technologies in the field of cyber security are diverse and are constantly evolving to meet the increased threats in the cyber environment. Starting from the cyber security situation in the country, NAECCS has approved some main technical measures (Baseline) which must be implemented by all critical and important information infrastructures in the country, which include:

- To install network perimeter devices that perform deep traffic analysis based not only on access list rules but also on its behavior (Firewalls).
- To consider "High-Availability" schemes in "core-network" devices at the perimeter level (firewall), at the routing level (L3) and packet switching (L2) and at the level of physical lines (L1).
- To take measures for the use of data mirroring techniques (RAID 1/5/6/10) to avoid the loss of sensitive data.
- To take measures to avoid "Single Point of Failure" in your critical and important services.
- Apply traffic filters in the case of remote access to hosts (employees/third parties/customers).
- Implement solutions that filter, monitor and block malicious traffic between Web applications and the Internet, Web Application Firewall (WAF).
- Conduct traffic analysis at the "behavior" level for end devices.
- To design the "Identity Access Management" user access management solution to control the identity and privileges of users in real time according to the "zero-trust" principle.
- To implement an automated system for managing and filtering logs in order to identify alerts in real time.
- If you have a development department, perform software development testing (staging) in an isolated environment separated from the production environment.
- Take measures to implement a system that controls the security parameters of an end system, not allowing the latter to be part of your network if these parameters are below the "Baseline" level previously given by you? (System which checks the lack of patches, Anti-Virus updates, etc.).
- To isolate logically, (in different VLANs) Database and Web services (if they are hosted in your environment).
- To take measures to raise DNS\_SEC to avoid DNS Amplification attack and DNS Poisoning attack.
- To implement and test the Disaster Recovery Site for the most important and critical services.
- Take measures to replace or isolate "End of Life" systems installed in your equipment.
- To take measures for the identification and effective management of assets and to carry out a risk assessment, documenting:

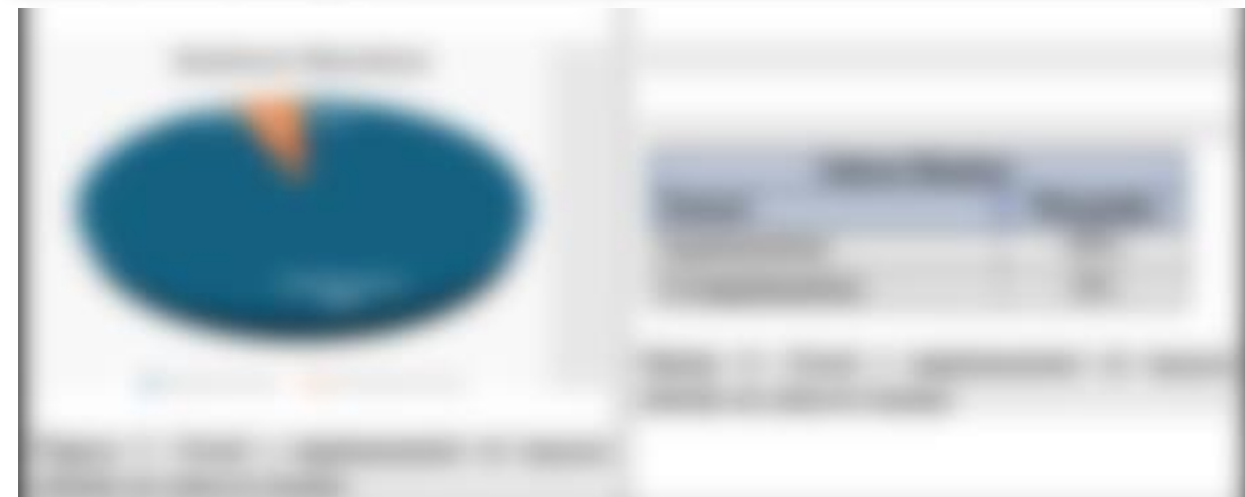
- Antiquity
- Affecting of C/I/A (Confidentiality/Integrity/Availability)
- Identified Vulnerabilities (CVEs)
- To draw up detailed plans and procedures for the management of cyber incidents.
- Take measures to isolate the wireless network from the rest of the network.
- Conduct employee awareness campaigns regarding cyber security and the most frequent attacks such as Phishing etc.
- Conduct tests for assessing the security of applications and networks (penetration test) and draw up a plan for dealing with identified problems.
- Conduct internal or third-party checks/audits for information security in your infrastructures.
- Check if the Email system does not have anti-spoofing features configured: DMARC/SPF/DKIM.
- To check if there is a Web Service that operates on the http protocol.
- To check if there is a Whitelist of allowed IP addresses set up in the firewall.
- To use random password policy for local users/administrators (e.g. as Microsoft's LAPS).
- Use the Data Leakage Prevention platform to prevent information leakage.
- To use the protection technique against DoS/DDoS attack.
- To use the technique of Port Security on Switches where the maximum number of MAC Addresses is 1 for simple users and a limited number for IT or Cyber Security experts.

These are just some of the main measures in the field of cyber security, and it is important for operators of critical and important information infrastructures to rigorously meet these technical measures as well as follow the latest developments to protect systems and networks their information from various cyber threats.

NAECCS, based on the baseline of cyber security measures, the controls exercised, as well as the follow-up of critical and important infrastructures, has carried out the evaluation of their implementation at the infrastructure level, as well as at the sectoral level.

Below is a summary of the level of implementation of technical security measures by critical and important information infrastructures at the sector level:





<p>Percentage of ...</p>  <p>50% Orange, 50% Blue</p>	<p>Percentage of ...</p>  <p>50% Orange, 50% Blue</p>
<p>Percentage of ...</p>  <p>25% Orange, 75% Blue</p>	<p>Percentage of ...</p>  <p>25% Orange, 75% Blue</p>
<p>Percentage of ...</p>  <p>75% Orange, 25% Blue</p>	<p>Percentage of ...</p>  <p>75% Orange, 25% Blue</p>

Also, in the framework of cyber security good governance, analyzes were carried out in cooperation with critical and important information infrastructures on the budgets dedicated to cyber security for 2023 and 2024, as well as investments in cyber security for 2023.

From the data collected by the operators of critical and important information infrastructures, it results that the budget, as well as planning for projects in the field of cyber security has a significant increase over the years, pointing out the awareness of the infrastructures for concrete investments in the field of cyber security.

The dedicated budget and investments for cyber security are summarized below at the sector level.



Sector	2023 Budget	2024 Budget	2023 Investments
Energy	150000000	200000000	100000000
Health	80000000	100000000	50000000
Finance	50000000	60000000	30000000
Transport	30000000	40000000	20000000
Government	20000000	30000000	15000000



## 2. OVERSIGHT OF CYBER SECURITY GOVERNANCE IMPLEMENTATION

### Identification of critical and important information infrastructures

NAECCS has approved the "Methodology for the identification and classification of critical infrastructures and important information infrastructures" (transposed from ENISA Guidelines and EU best practices). The list of critical and important infrastructures is updated at least once every two years.

The factors that were applied in the identification of critical and important infrastructures are:

- a) **Financial effect** - the financial impact caused when the infrastructure is out of order.
- b) **Geographic distribution** - the number of individuals who may be affected by not receiving service due to infrastructure malfunction.
- c) **Time effect** - defines the time interval, when a service cannot be provided because the infrastructure is out of order.

### The sectors identified as critical sectors are:

- Energy Sector
- Transport Sector
- Banking Sector
- Financial Sector
- Health Sector
- Digital Infrastructure Sector
- Water Supply Sector

Currently, NAECCS is in the process of drafting and approving the new methodology for identifying critical and important information infrastructures.

Below you find the number of critical and important information infrastructures identified over the year.

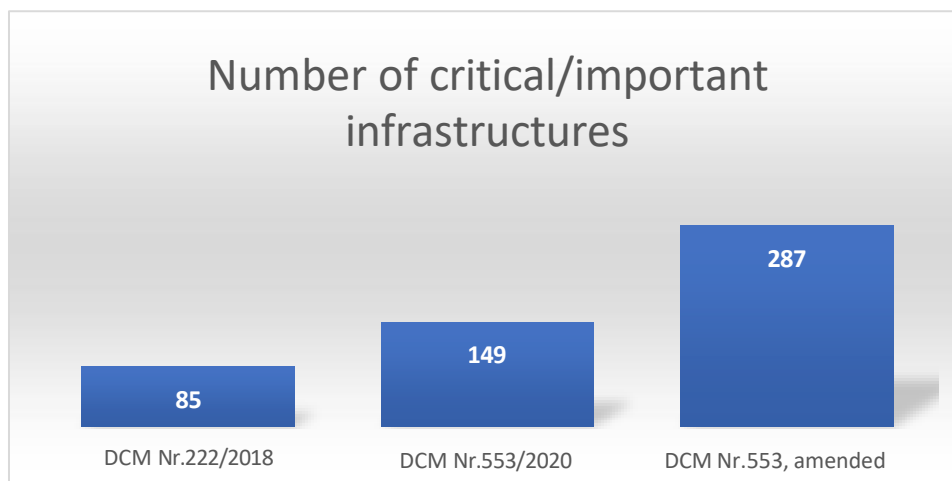


Figure 11: Critical and important information infrastructures identified over the years.

Based on DCM No. 553 dated 15.07.2020, amended, 145 Critical and Important Information Infrastructure Operators (14 of which are both critical and important), who administer 287 systems and 41 networks for providing services, have been identified.

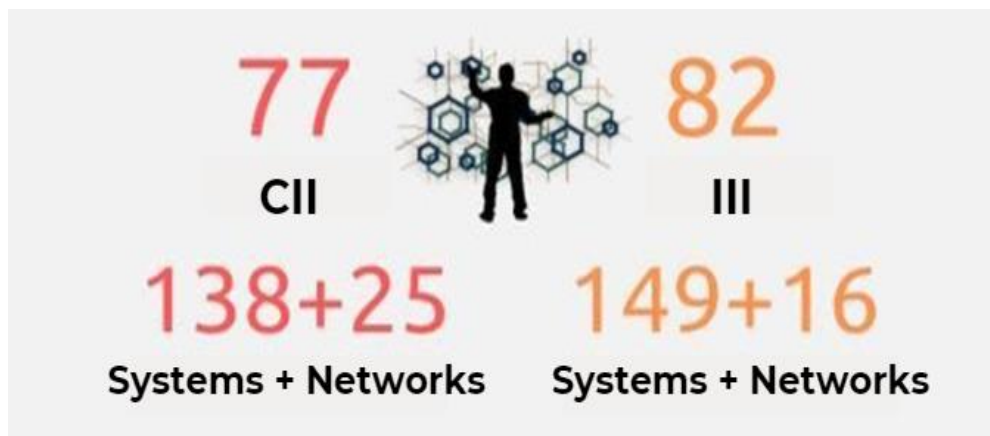


Figure 12. Infrastructure operators, systems and networks according to DCM No. 553/2020, amended.

In the framework of the ongoing work to improve the process of identification and classification of information infrastructures in accordance with the latest guidelines and standards of the EU, NAECCS has worked on the review and design of the new methodology for the identification and classification of critical infrastructures and important information, as well as continuing the commitment to identify new infrastructures.

### Management of cyber incidents, as well as analysis of identified vulnerabilities in the field of cyber security

Throughout 2023, NAECCS has determined the frequency and category of reported incidents according to the relevant sectors. The most frequent incidents were reported by the Banking sector in the amount of 36% of the total incidents reported, making it the sector most affected by incidents and potential cyber-attacks, followed by 31% of the incidents reported by the Infrastructure Digital Sector, 12% Energy sector, 7% Transport sector, 7% Financial sector, 5% Health sector, as well as 2% Telecommunication sector.

SECTOR	No. Incidents
Banking	15
Digital infrastructure	13
Energy	5
Transport	3
Financial	3
Health	2
Telecommunication	1

Table 11. Number of reported incidents by sector

## Number of Incidents

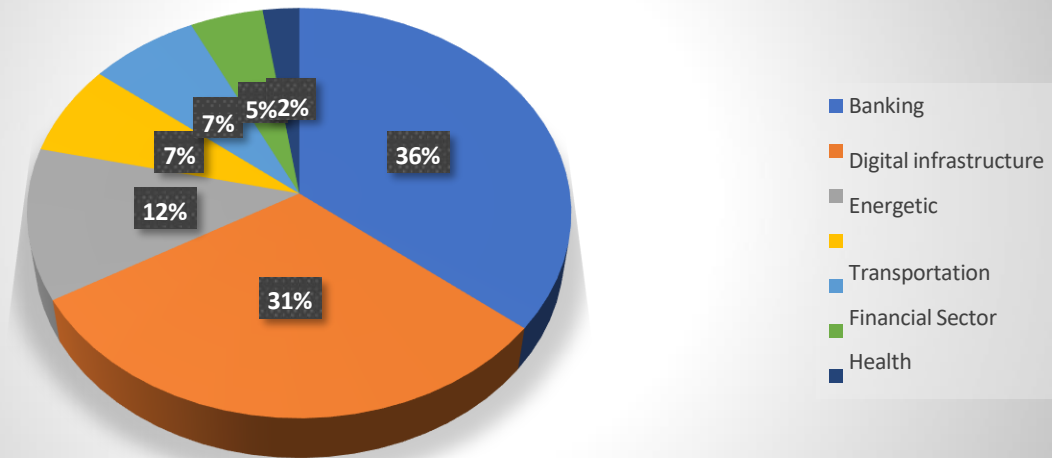


Figure 13. Number of reported incidents by sector

### Banking Sector

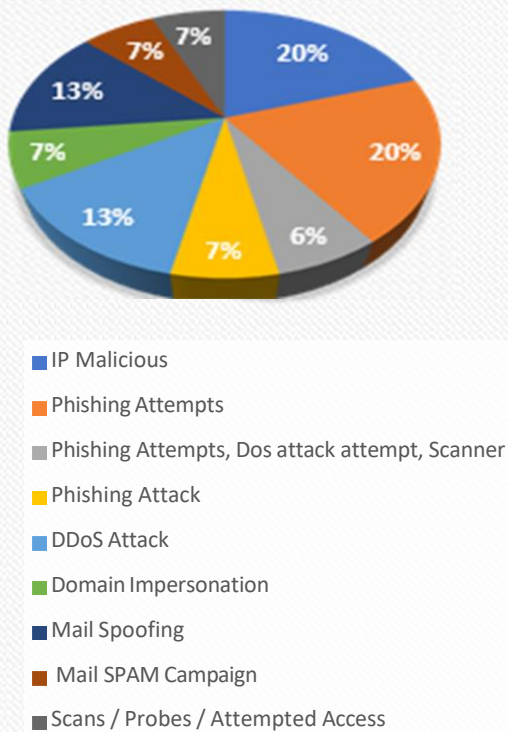


Figure 14. Categories of incidents reported in the banking sector

### Digital infrastructure

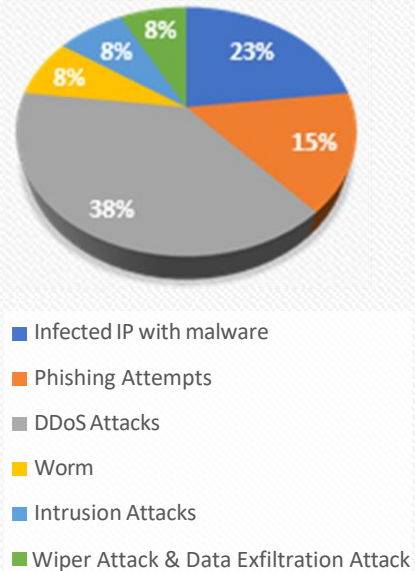


Figure 15. Categories of reported incidents in the digital infrastructure

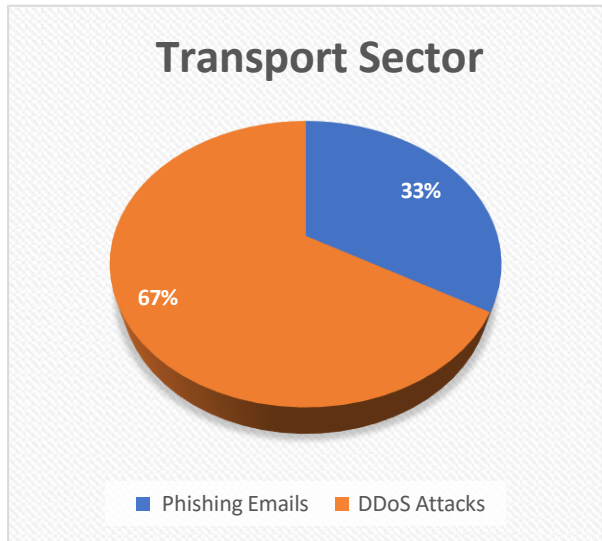


Figure 17. Categories of incidents reported in the transport sector

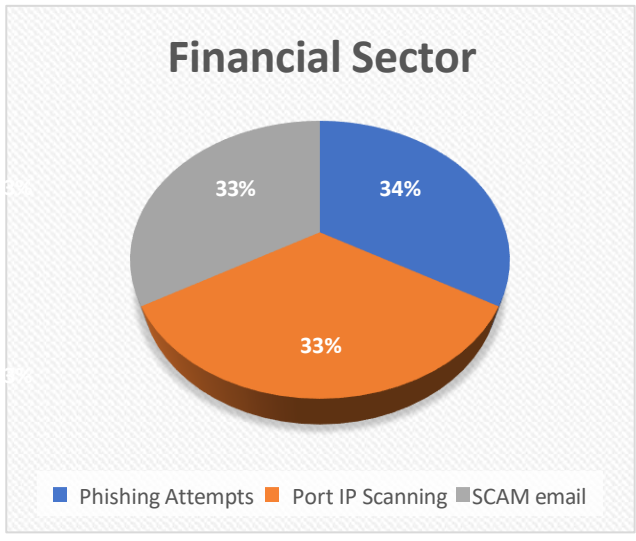


Figure 18. Categories of reported incidents in the financial sector

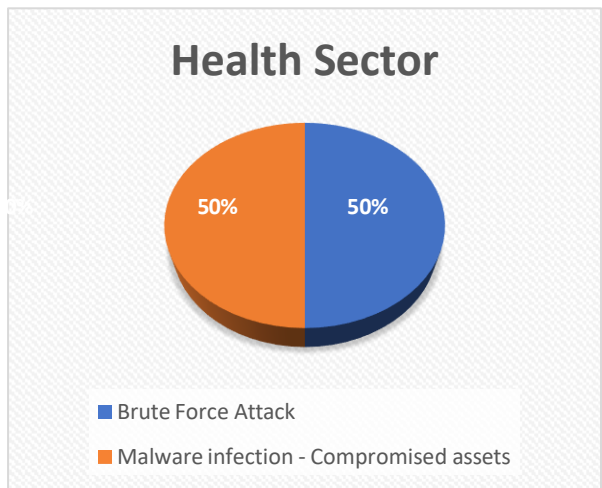


Figure 19. Categories of reported incidents in the health sector

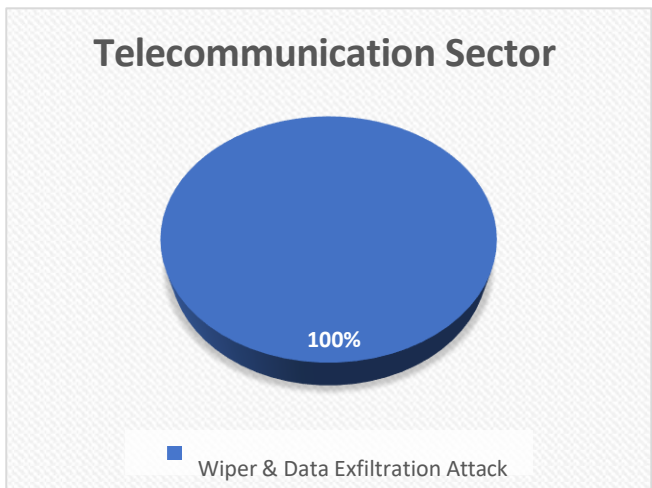


Figure 20. Categories of reported incidents in the telecommunications sector

Analysis of cyber incidents for 2023 shows a different picture of cyber security in critical sectors. These incidents reflect current challenges and trends in the field of cyber security, as well as provide a basis for strategic security improvement developments.

The high number of incidents in the banking sector shows that the critical and important infrastructures of this sector are high targets for cyber-attacks. Malicious actors are interested in stealing sensitive information, denial of services, image damage, economic instability. During 2023, a significant increase in phishing attempts towards the banking sector was observed. Therefore, a special focus should be given to the drafting and implementation of security policies, the continuous monitoring of critical information systems, as well as the implementation of the recommendations given by NAECCS.

Incidents in digital infrastructures, especially those sponsored by countries such as Iran, Russia, which include attempts to disrupt services, theft of sensitive data, economic and political instability, require a coordinated

response. In this context, interagency cooperation and the use of advanced technologies become essential to maintain national security and the integrity of government information.

In the *energy sector*, the number of incidents indicates a significant risk to infrastructure, highlighting the need for a major focus on the security of networks and systems built on Internet-related technologies.

In the *transport sector*, incidents are caused by attempts to disrupt service in critical and important information systems. These attempts at service interruptions in ICT systems signal a critical need to improve IT security. This key sector requires constant attention to prevent harmful interference.

Incidents in the *health sector* highlight the importance of patient data security and the uninterrupted operation of medical systems. Strengthening security and protecting critical infrastructure is essential to the integrity of patient data.

In general, incidents in different sectors indicate an increased need for strengthening cyber security in critical or important systems. To address this challenge, the importance of investments in staff training, improvement of security infrastructures, and proactive monitoring of cyber risks is emphasized. These actions are key to raising the level of cyber defense in various sectors, guaranteeing a safer environment at the national and international level.

The significant increase in cyber-attacks in the second half of 2021 and 2022 has marked a turning point in cyber warfare, particularly influenced by the Russia-Ukraine crisis. This period has increased awareness of the role and impact of cyber warfare in global conflicts, highlighting the need to review international norms in cyberspace and address challenges arising from state sponsorship of cyber-attacks and the targeting of critical civilian infrastructures.

The geo-political dynamics of our country make Albania an attractive place for sophisticated cyber-attacks.

International cooperation in the field of cyber security is essential for Albania, especially through NATO and EU initiatives. These collaborations provide access to resources and knowledge to deal with cyber threats through the sharing of best practices. In addition, the role of the government and the private sector in building a secure information infrastructure has been emphasized, focusing on the importance of preparing human and technological resources.

Future challenges for addressing these risks include the need to strengthen regional and global cooperation, investments in new technologies, updating legislation to reflect changes in the field of cyber security while ensuring that geopolitical interactions and policy decisions are considered a direct impact on a country's cyber security.

The threats of 2023 in the Western Balkans were characterized by the main "*Advanced Persistent Threat*" (APT) attacker groups linked to the state of Iran as well as groups originating from Russia. Their main attacks have been *ransomware* (a type of malicious software that blocks access to a computer system or user data until a ransom is paid), *malware* (any malicious software that infects or damages a computer or network), *social engineering* (manipulation of individuals to gain access to sensitive information), *wiper* (type of malware that aims to erase a system's data, destroying the user's data without the possibility of recovery). Trends in state-sponsored groups include exploiting known vulnerabilities, targeting legitimate individuals, devices and applications, and disrupting public services and critical information infrastructures.



NAECCS has carried out continuous monitoring of networks and information systems, sending warning notices and countermeasures case by case, and coordinating with the operator, to increase the level of security at national level. The use of monitoring platforms towards a variety of networks and systems of information infrastructures in Albania 24/7 is a proof of NAECCS's commitment to ensure a safer cyber environment.

To face the challenges and risks in the field of cyber security, NAECCS has emphasized the importance of investments in staff training, improving information security infrastructures, and proactive monitoring of cyber risks. These actions are key to raising the level of cyber defense in various sectors.

NAECCS's role in monitoring, following and recommending best practices in the management of cyber incidents during 2023 has been essential to address challenges and risks in cyber security in Albania.

### **Assessment of cyber security at the sectoral level**

NAECCS has carried out an assessment of the level of security of critical sectors, which is based on the following 3 components:

- The risk component of compromised systems,
- The due diligence component,
- User behavior component.

These three pillars are analyzed for each infrastructure and then averaged to determine the level of security, where a high rating indicates a high level of security and a lower cyber risk, while a low rating indicates high risk. Averaging at the sector level helps in the overall safety assessment.

The analysis of the data related to the assessment of the level of security represents a consistent improvement in all critical sectors. The increase in the level of security results from the implementation of the corrective security measures evidenced in the control reports, the increase of human capacities through specialized training and the increase of awareness on security issues, as well as the improvement of technological capacities and security systems. These measures have contributed to an increase in the overall level of safety in all critical sectors, proving the importance of a comprehensive and continuous approach to risk management and safety improvement.



### 3. DETERMINATION OF CYBER SECURITY MEASURES AND CONTROL OF THEIR IMPLEMENTATION

The regulation "**On the content and method of documenting security measures** (V. 2.0, approved by Order No. 10/2022)" defines the security measures that must be implemented by operators of critical and important information infrastructures.

NAECCS conducts continuous cyber security checks near critical and important information infrastructures, to supervise the fulfillment of security measures, through the method of self-declaration and on-site inspection. Through 2023, the number of on-site checks on critical and important information infrastructures **quadrupled**. This shows the high focus that NAECCS has on the implementation of security measures from critical and important information infrastructures.

Below is a summary of the cyber security checks carried out by NAECCS, for the year 2023.

	Checked	Self-declaration
Operators of Critical Information Infrastructures	26	32
Operators of Important Information Infrastructures	23	22
Total Infrastructure Operators	49	54

Table 12. Cyber security controls

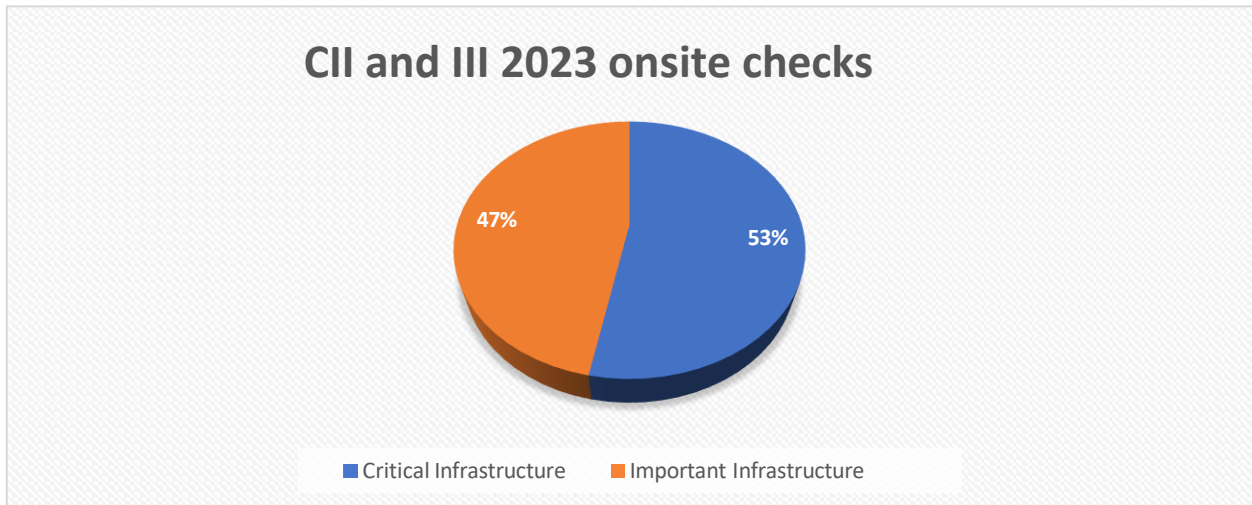


Figure 24. On-site controls for operators of critical and important information infrastructures.

## **Vulnerability Assessment through active scans on operators of critical and important information infrastructures**

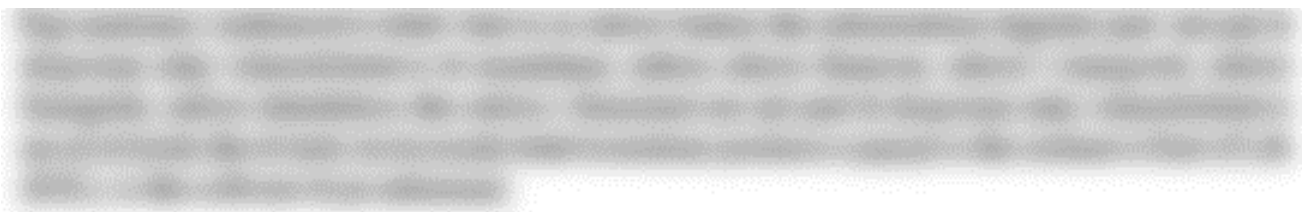
NAECCS, before starting the control process near the operators of critical and important information infrastructures, performs a preliminary assessment of possible vulnerabilities for the IP addresses made available by the information infrastructures themselves.

NAECCS uses various scanning sources that help identify and deal with problems.

NAECCS, for the year 2023, has carried out a total of 27 *Vulnerability Assessments* for the operators of critical and important information infrastructures defined in DCM No. 553, dated 15.7.2020 "On the approval of the list of critical information infrastructures and the list of important information infrastructures", amended.

After completing the vulnerability assessment process, a report with relevant findings is drawn up, which includes:

1. The results of the scanning process for available IPs and the duration of this process.
2. Assessment of the level of risk that may have an impact on critical or important information systems:
  - Info risk level **(0)**
  - Low risk level **(0.1 – 3.9)**
  - Medium risk level **(4.0 – 6.9)**
  - High risk level **(7.0 – 8.9)**
  - Critical risk level **(9.0 – 10.0)**
3. For the identified vulnerabilities, the level of risk, the description of the vulnerabilities and the way in which their mitigation can be carried out is determined.
4. Recommendations based on the findings of the scanning process. These results cannot be considered as a final measure of safety for critical and important infrastructures. Taking the proposed solutions into consideration in the mitigation process helps to reduce the level of risk to the infrastructure. NAECCS recommends applying all necessary updates based on the mitigation process section to each of the vulnerabilities explained above and considering recommendations for all additional findings.



To minimize the risk from possible cyber-attacks, NAECCS has given recommendations for the replacement of End of Life (EOL) equipment and systems, as well as periodic software and system updates.

**4. PROMOTING A SUSTAINABLE CYBER CULTURE / HUMAN RESOURCES AND AWARENESS**

Promoting a sustainable cyber culture is a long-term process and requires continuous commitment to raise awareness of cyber security risks in society, as well as efforts to improve protection by developing and raising the necessary human capacities in the field of security.

NAECCS has implemented training and awareness programs in the field of cyber security to educate children, young people, parents and teachers as well as social workers about the risks that can be encountered in the digital world, methods of protection as well as institutions where cases of cyber threats can be reported.

Also, NAECCS distributes educational materials, as well as daily announcements/news on possible cyber threats, cyber incidents (such as bulletins) on the official website of the Authority<sup>1</sup>, as well as on social networks.

<sup>1</sup> NAECCS official website: [www.cesk.gov.al](http://www.cesk.gov.al)

NAECCS has carried out awareness campaigns and trainings for raising professional capacities in the field of cyber security, with CII and III, such as table exercises, seminars, and cyber training.

Raising human capacities in the field of cyber security is a key element of the National Cyber Security Strategy and Action Plan 2020-2025.

NAECCS has given priority to the training and preparation of experts in this field, in order to improve the ability to prevent, detect and deal with cyber-attacks.

Specifically, during 2023, trainings were organized for experts of security and defense institutions, as well as CII and III on the following topics:

- CompTIA Security+,
- Certified Information Systems Security Professional (CISSP),
- Certified Information Security Manager (CISM),
- SIM 3 Auditor Training,
- Risk Assessment Training,
- Hacker Fundamentals,
- Secure Coding,
- Industrial Control Systems (ICS) Live training,
- Industrial Control Systems (ICS) Cybersecurity Evaluation (401),
- Threat hunting,
- ISO 27001.

Also, NAECCS in cooperation with the International Telecommunication Union, within the piloting of the ITU Global Project, "Creating a Safe and Prosperous Cyberspace for Children", have organized awareness campaigns to educate, empower and advise children, child protection workers and parents about the threats they may face online. NAECCS in cooperation with the State Agency for Children's Rights and Protection (ASHDMF), has carried out several trainings on the topic "Protection of children on the Internet and cyber hygiene", where the employees of the Child Protection Units in various municipalities of country were trained. Compared to previous years, the number of trainings has increased, and the topics have been increasingly advanced, in line with the latest developments in cyber security.

## **5. NATIONAL AND INTERNATIONAL COOPERATION**

Cyber risks are impossible to be addressed efficiently by a single institution or country alone. Therefore, the National Authority on Electronic Certification and Cybersecurity cooperates with public and private institutions at national level in order to prevent, treat and protect against cyber threats. Also, the Albanian government has cooperated with international organizations as well as with other homologous institutions, to share information, experiences, as well as to address cyber risks.

## **National cooperation**

The National Authority for Electronic Certification and Cyber Security, in the role of the coordinating institution in the field of cyber security in the country, has signed a Memorandum of Understanding for further cooperation in the field of cyber security with institutions and infrastructure operators such as:

- Albanian Association of Banks (2023),
- Academy of the Armed Forces (2023),
- The Assembly of the Republic of Albania (2023),
- Albanian Post (2023),
- Electricity Distribution Operator (2023),
- Transmission System Operator (2023),
- First Investment Bank (2023),
- Union Bank (2023),
- Raiffeisen Bank (2023),
- Tirana Bank (2023),
- Risi Albania Project (2023),
- State police,
- Audiovisual Media Authority and Coordination Center Against Violent Extremism (2021),
- Electronic and Postal Communications Authority (2019),
- Academy of Political Studies (2019).

## **International Cooperation**

**Cooperation with NATO and OSCE:** Albania is a member of NATO and OSCE and is involved in their cyber security activities and programs. This cooperation has improved the sharing of information, the exchange of experiences and the building of capacities in the field of cyber security in the region and beyond.

**Cooperation with the European Union:** Albania, within the framework of membership in the European Union, is engaged in harmonizing local legislation with EU directives, regulations and standards in the field of cyber security.

The National Authority on Electronic Certification and Cyber Security has signed a Memorandum of Understanding for the exchange of information in the field of cyber security with:

- United Arab Emirates (2023),
- Israel (2023),
- 4IG (2023),
- Romania (CERT-RO),
- North Macedonia (MKD-CIRT),
- Kosovo (KOS-CERT).

Also, Albania is a member of international forums such as ITU, FIRST, FESA, TF-CSIRT, TRUSTED INTRODUCER and CRI.

NAECCS has also continued communication with various cyber security agencies of the EU member states in order to establish and strengthen cooperation in the field of cyber security to achieve common objectives and European standards regarding cyber security.

International cooperation in the field of cyber security is important, to address the increased challenges of this field. Albania is actively involved in this process and works together with international partners to strengthen cyber security and improve its capacities to prevent and deal with cyber-attacks.

### **Cyber Security Diplomacy**

The Republic of Albania, as a member country of the OSCE, has committed to the implementation of confidence-building measures (CBM 15) in the field of cyber security in order to create a secure cyber environment through strengthening cooperation.

Also, as a member country in the United Nations (UN), Albania has a role and responsibility in cyber security issues in this international organization. The Republic of Albania has the right to take action and play an active role in cyber security diplomacy within the UN, NATO, OSCE and other international forums where it is a member, and above all, within of national interests in cyberspace and national foreign policy and security policy objectives.

On March 6 - 10, 2023, NAECCS was part of the work of the IV session of the *"Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies"* at the United Nations. The focus of this session was global cyber security threats, confidence building measures, capacity building, as well as norms of responsible behavior of states in cyberspace. In Albania's statement, the progress in harmonizing the legal framework with the framework of the European Union was emphasized, as well as the achievements related to the establishment of the National CSIRT; trainings for increasing the capacities of sectoral CSIRTs; consolidating capacities for cyber diplomacy and cyber governance; trainings and awareness campaigns for public administration, industry, children and young people; as well as addressing cyber security topics in educational curricula.

Cyber security policies are adapted to current cyber security challenges given the rapid developments in technology and the growth of cyber risks. The aim of these policies is to achieve a high level of cyber security, defining security measures, rights, obligations, as well as cooperation between entities operating in the field of cyber security, to promote a safe environment for development of economy and information society in Albania.



The following figure graphically presents the national and international cooperation agreements for the year 2023:



Figure 2c. Cooperation agreements for 2023

## V. KNOWN CASES OF CYBER ATTACKS

### *Known Cases: A brief analysis of known cases of cyber-attacks in Albania and their impact.*

Until 2021, Albania was not a target for large and well-known cyber-attacks. One of the most sophisticated cyberattacks against Albanian government systems was the one in 2022, originating from the Islamic State of Iran, where the goal of the malicious was to wipe all government systems and their data. Immediately after the ransomware attack was identified, lockdowns were initiated to prevent further spread, and by correctly implementing backup and disaster recovery policies, services were back up and running within the first week.

However, as in many other countries, cyber-attacks have now become a potential risk and their impact can affect:

**Critical and important information infrastructures:** Attacks on critical and important information infrastructures can cause disruption of services and serious impact on the economy and stability of the country. Potential cyber-attacks can affect:

1. **The energy sector:** Attacks on electricity and gas systems can cause interruptions in the supply of electricity and heating. These attacks can damage infrastructure and bring serious consequences to citizens' lives and economic activities.

2. **Transport Sector:** Cyber-attacks against transport systems can damage the road, air, and sea infrastructure causing traffic disruptions and major impacts on the movement of people and goods.

3. **Health Sector:** Systems in the health sector are important for the storage of medical data and the operation of health services. Attacks on them can damage medical records, doctors' access to patient information, as well as medical services in general.

4. **Banking/Financial Sector:** Banking/microfinance institutions are often targets for cyber-attacks, credit card data theft, bank account theft, and ransomware threats. These attacks can harm customers, cause huge financial losses, as well as loss of reputation.

5. **The sector of digital infrastructures:** Cyber-attacks against government institutions can have serious impacts. If a cyber-attack succeeds, it can compromise sensitive government data and information, including citizen data.

**Individuals and businesses:** Cyber-attacks on individuals and businesses are common. This includes attempts to steal personal data, or ransomware attacks that can block access to data. Some common types of cyber-attacks encountered in Albania against individuals and businesses include:

- ❖ **Phishing,**
- ❖ **Ransomware,**
- ❖ **Malware,**
- ❖ **Social engineering.**

## **Preparation of Albania against cyber attacks**

Albania has taken steps to prevent cyber-attacks by raising human capacities in the field of cyber security, as well as promoting awareness about potential cyber risks.

To protect critical and important information infrastructures, NAECCS has defined cyber security measures that must be implemented by CII and III, as well as performs periodic checks to verify their implementation.

Also, NAECCS performs continuous security monitoring of CII and III, performing vulnerability testing to prevent and detect potential attacks. International cooperation in this regard is important to address common cyber threats.

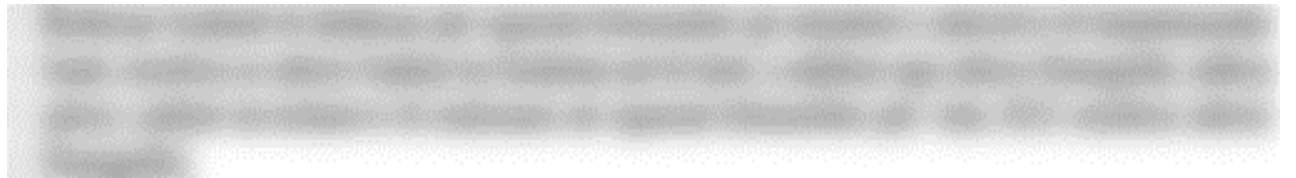
In order to protect the business from cyber-attacks, NAECCS has drafted manuals, instructions on the best practices of cyber security, which includes the use of complex passwords, updating computer programs and systems, raising employees' awareness of potential cyber risks. Also, NAECCS constantly recommends businesses to draw up a plan for managing cyber incidents in the event of a cyber-attack.

## VI. OVERALL ASSESSMENT: CONCLUSIONS AND RECOMMENDATIONS

### CONCLUSIONS

Cybersecurity is a great challenge in the digital age and is of great importance for the future, not only in Albania, but also internationally. From the analysis of aspects of cyber security governance, the following conclusions are reached:

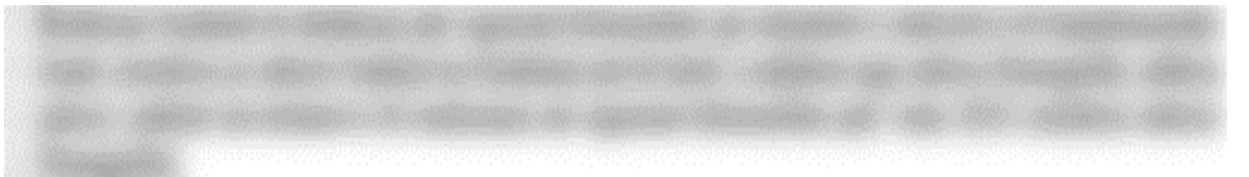
- Albania has made progress in terms of strategic policies, drafting policies in accordance with EU standards and continuously updating existing ones such as the National Cyber Security Strategy Action Plan which has been revised to address current challenges and priorities of cyber security at national level.
- Regarding the legislation, Albania has adopted the new law in accordance with the EU Directive NIS 2 and is working on the drafting of by-laws in its implementation.
- From the analysis of cyber security governance by sectors, it is concluded that sectors should give more priority to cyber security in terms of increasing human and technical capacities to cover the needs that may appear from cyber threats.



- Regarding the development of technology and infrastructure in critical sectors, NAECCS has defined several technical cyber security measures, which also include the implementation of various technological solutions to increase cyber security.



- In order to have an effective cyber security governance, budget planning and the implementation of dedicated projects in the field of cyber security have a key role.



- NAECCS has been working on the identification and classification of critical and important information infrastructures continuously, where of the 85 critical and important infrastructures that were in 2018, with DCM No. 553, dated 15.07.2020, amended, the number went to 287, and the process for the approval of the new Draft Decision is currently underway, which will increase the number of identified and classified information infrastructures.



- In order to increase the security of critical and important information infrastructures, Albania has identified "Crown jewels", which may be exposed to cyber-attacks, including the energy sector, transport, banking, financial, health, digital infrastructure, and the supply of water. Their identification allows to further strengthen the relevant cyber security measures for the stable operation of these systems.
- Albania has taken steps to protect itself and prepare to respond to cyber-attacks by raising technical and human capacities in the field of cyber security, as well as promoting awareness about potential cyber risks.
- Capacity building activities as well as awareness campaigns have increased, influencing the improvement of technical skills of cyber security experts of public institutions as well as all operators of critical and important information infrastructures, and contributing to the increase of awareness of the entire society on cyber risks and preventive measures.

Albania has made positive steps in the field of cyber security, but there are still big challenges ahead. To fulfill the goal of increasing the level of cyber security in the country, special importance should be given to improving human capacities in this field, investing in the technology and infrastructure necessary in the field of cyber security, increasing cooperation with the private sector and international organizations.

**From this report, some strong points and weak points can be identified, which are explained below:**

### **The strong points**

- **Completion of the legal framework, strategy, and policies in the field of cyber security:** Albania has completed the necessary legal framework, has approved the national strategy for cyber security, and has developed important policies in the field of cyber security in accordance with the best directives and practices goods of the EU. This is a strong point to better prepare the country and coordinate efforts in this area.
- **Creation and strengthening of the capacities of the National Authority on Electronic Certification and Cyber Security:** This is an important step to effectively coordinate the work to increase cyber security through the creation, strengthening and implementation of cyber

security policies and measures at national level, as well as to help prevent cyber-attacks and respond quickly to incidents.

- **Increasing the level of "Implementation of cyber security measures in critical and important information infrastructures"**, according to the recommendations and measures left by the controls carried out by NAECCS in various sectors during 2023.
- **Establishing a National Security Operations Center (SOC)** that serves to deal with cyber incidents, as well as aiding in discovering the source of attacks.
- **International cooperation:** Albania is involved in international cooperation in the field of cyber security with various international organizations and forums such as: NATO, OSCE, UN, ITU, FIRST, FESA, TF-CSIRT, TRUSTED INTRODUCER, CRI, as in the future it aims to create new memberships and collaborations.

### Weak points / Weaknesses

- **Security investments in critical and important information infrastructures:** Although efforts have been made over the last year to improve the security of networks and information systems, there is still a need for further investments to ensure a stronger, more reliable and safe infrastructure.

### RECOMMENDATIONS

From the above analysis, recommendations for possible actions to improve cyber governance in Albania emerge as follows:

- **Legislation and Policies:** Drafting of the sub-legal framework to implement the new law, including all the elements that are missing in the existing legislation. This option would guarantee the proper legal basis in the field of cyber security, establishing clear rules for all entities involved.
- **Approval of the updated Action Plan of the National Cyber Security Strategy:** The Government should review and approve the revised Action Plan for the period 2024-2025 in accordance with the latest developments in this field.
- **Investments in cybersecurity technology** to improve the security and resilience of critical systems.

- **Cooperation with the private sector:** The Authority should work to build close relations with the private sector. The cooperation will help share information on cyber threats and coordinate security measures.

- **International Cooperation:** The level of cooperation with civil society organizations and international partners should be increased to meet cyber security objectives.
- **Education and training in the field of cyber security:** All public administration personnel must receive regular training in cyber security. Also, the awareness of network users should be promoted.
- **Protecting children online:** Protecting children in the online environment, through awareness programs and collaboration with organizations and partners aimed at children's online safety.
- **Stimulating investment:** Encouraging investment in advanced technologies and innovation in cyber security to strengthen defenses and prevent cyber-attacks.
- **Monitoring the use of new technologies:** Monitoring the use of new technologies, such as artificial intelligence and machine learning, to ensure that they are used safely and comply with cybersecurity rules and standards.
- **Raising awareness in the field of IoT:** Raising awareness of the security risks of the Internet of Things (IoT) and the advantages of cyber security in the field, by providing training and education to professionals and users.
- **Strengthening CSIRTs:** Strengthening and improving Cyber Incident Response Centers (CSIRTs) at national level to ensure effective response to cyber incidents.
- **Critical Network Monitoring:** Improve network and systems monitoring to detect and prevent cyber-attacks in time and minimize potential damage.
- **Increasing Trust and Transparency:** Increasing transparency and accountability in the field of cyber security to build public and private sector trust.