REPUBLIKA E SHQIPËRISË

National Cyber Security Authority

No. ____ Prot. Tirana on, ____ .____. 2024

MONITORING REPORT
OF
THE NATIONAL CYBER SECURITY STRATEGY
2020-2025

General Director

Igli Tafa

2023

TABLE OF CONTENT

1. INTRODUCTION

Cyber security in the Republic of Albania has taken on a special importance within the national security agenda in recent years, being clearly reflected in the government's commitments to address and face cyber security challenges. In the context of the international and national strategic environment, a rapid digitization of services and not only, as well as the growing cyber-attacks targeting critical and important information infrastructures, during 2023, the Albanian government has worked with maximum commitment to strengthen cyber security, in line with the National Cyber Security Strategy 2020-2025. Considering the growing threats and the needs to guarantee a safe and stable cyber ecosystem, the National Authority on Electronic Certification and Cyber Security has worked on revising the Action Plan of the National Cyber Security Strategy for the period 2024-2025. In this context, a new strategic plan has been drawn up, in consultation with all the actors involved, which foresees measures for the modernization of cyber security policies and technological infrastructure in accordance with international standards, increasing awareness and online security for citizens and with a focus especially children and young people, as well as strengthening national and international cooperation.

As part of the work to improve the political and legal framework, as well as the process of aligning legislation with the European Union acquis, the Albanian government has worked on drafting a new law that regulates the field of cybersecurity by transposing Directive (EU) No. 2022/2555 (NIS 2).

Furthermore, significant progress has been made in strengthening the technological and professional capacities of the National Security Operational Center (National SOC) and the Cyber Security Incident Response Team at the Authority (National CSIRT) to ensure national cybersecurity through the protection of information infrastructures.

Likewise, the education and awareness-raising of society, as well as the increase of professional capacities in the field of information security in the public and private sector have been the focus of NAECCS 's work during 2023, with the aim of creating a culture of cyber security in society and preparing a generation of professionals capable of addressing cybersecurity challenges. A significant progress has been made in the framework of strengthening national and international cooperation in the field of cyber security and defense with strategic partners, where a series of cooperation agreements have been signed, and work continues to expand this cooperation.

In this context, the monitoring report for the year 2023 provides a detailed overview of the progress achieved in the realization of the strategic objectives of cyber security. The report documents the realization of the planned activities, evaluates the efficiency of the measures taken and identifies the areas where further efforts are needed. With a clear focus on long-term cybersecurity and resilience, the Albanian government is committed to continuing its work to be a model in the Balkan region and beyond in managing challenges in the field of cybersecurity, thus contributing to a safer cyberspace at a global level.

The Monitoring Report was prepared by examining the level of implementation of all measures outlined in the National Cyber Security Strategy. The National Cyber Security Strategy 2020-

2025, approved by Decision No. 1034, dated 24.12.2020, of the Council of Ministers, constitutes a key instrument for enhancing the security of networks and information systems at the national level, considering cybersecurity as a priority for the Albanian government.

This strategy aims to guarantee cyber security in the Republic of Albania through the establishment and operation of cooperative institutional mechanisms, legal and technical instruments, as essential elements of protection in cyberspace for information infrastructures, transactions and electronic communications; through raising professional capacities, increasing nationwide awareness, as well as strengthening national and international collaborations for a safe digital environment.

The strategy is based on the following fundamental principles:

- Applying the same core values in both the physical and digital worlds;
- Protecting fundamental rights, freedom of expression, personal data, and privacy;
- Access for all;
- Democratic and efficient governance;
- Shared responsibility in ensuring cybersecurity.

The actors involved in the Action Plan of the National Cyber Security Strategy 2020-2025 are:

- The National Authority on Electronic Certification and Cyber Security (NAECCS);
- The State Police;
- The National Authority for Classified Information Security;
- The Center for Coordination against Violent Extremism;
- The National Agency for Information Society;
- The Ministry of Health and Social Protection;
- The Ministry of Education and Sports.

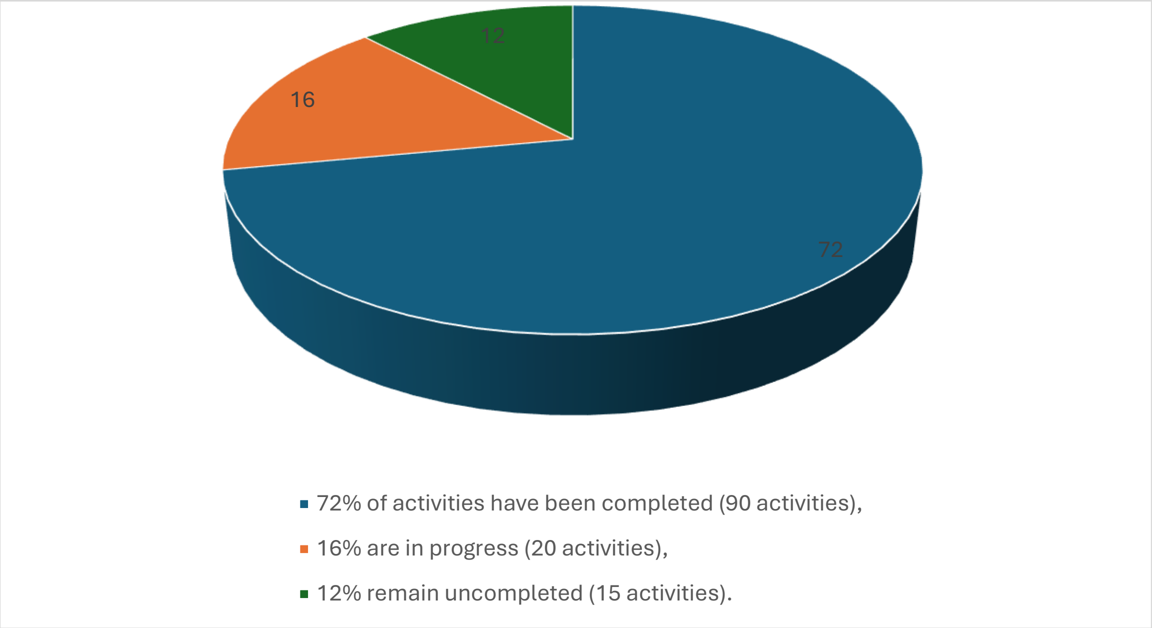
Implementation of the Action Plan Activities

Regarding the implementation of the Action Plan, by 2023, the completion rate of activities is as follows:

- 72% of activities have been completed (90 activities);
- 16% are in progress (20 activities);
- 12% remain uncompleted (15 activities).

Based on this data, it can be concluded that the most progress has been made in achieving Policy Goal 1 and Policy Goal 3 concerning the results achieved and activities implemented.

The implementation of activities in total:



2. MONITORING METHODOLOGY

The assessment of the achievement of the objectives of the National Cyber Security Strategy 2020-2025 will be conducted through the periodic tracking of the implementation of the planned activities for the period as well as the progress of the key monitoring indicators.

The analysis of this report is primarily based on monitoring the implementation of the activities outlined in the action plan covering the period from January to December 2023.

The monitoring of the Strategy has consisted of the following main phases: a) Reporting by institutions on the implementation of measures to achieve the results for which they are responsible; and b) Monitoring measurable indicators for the National Cyber Security Strategy.

To achieve the above, the following steps have been taken:

- A preliminary analysis of the action plan's activities has been carried out according to each strategic objective;
- Responsible institutions for their implementation have been identified;
- Communication was conducted in writing with each institution, and coordination was continuously maintained with the contact points for reporting the implementation status according to the methodology.

3. STRATEGY POLICIES

3.1 POLICY GOAL 1: ENSURING CYBERSECURITY AT THE NATIONAL LEVEL THROUGH THE PROTECTION OF INFORMATION INFRASTRUCTURES BY STRENGTHENING TECHNOLOGICAL AND LEGAL TOOLS.

The priority objectives focus on:

- Improvement of the legal framework that governs and regulates the field of cybersecurity in the country, as well as its harmonization with the directives and regulations of the European Union;
- Establishment and functioning of Computer Security Incident Response Teams (CSIRTs) across all sectors of the industry at the national level;
- Strengthening and implementation of security measures for critical and important information infrastructures;
- Enhancement of information infrastructures to combat cybercrime, radicalization, and violent extremism.

For the achievement of the objectives of the first strategic priority, the institutions involved in the implementation of the Action Plan, based on their reports, have achieved the following results:

3.1.1 NATIONAL AUTHORITY ON ELECTRONIC CERTIFICATION AND CYBER SECURITY (NAECCS)

The National Authority on Electronic Certification and Cyber Security (NAECCS) has worked on the analysis of the cybersecurity legislation and the legal and institutional gaps regarding the directives and regulations of the EU that regulate the field of cybersecurity. Within the framework of the analytical review process (screening) as one of the phases of the European integration process, NAECCS has analysed the EU acquis in the field of cybersecurity for chapters 10, 20, 31, and 24, as well as made comparisons with Albanian legislation, identifying the EU acts that need to be implemented. Additionally, in the context of this process, NAECCS has analysed institutional and administrative capacities to assess the current level and the needs for capacity building in the future. Following this analysis, NAECCS has contributed to the preparation of presentations for the chapters of the acquis where it is part of the inter-institutional working groups, which were held in bilateral meetings with the European Commission, presenting the current situation and future commitments in this field.

To align the existing legal framework in the field of electronic identification, trusted services, and cybersecurity with EU legislation, the Authority has worked on the process of harmonization with the acquis as follows:

- EU Regulation No. 910/2014 eIDAS, for the complete alignment of the draft law "On electronic identification and trusted services" with this regulation;
- NIS1 Directive to align the draft law "On cyber security" with this directive, where the Authority initially drafted a law, fully aligning it with this Directive.

With the entry into force of the NIS2 Directive in December 2022 (Directive No. 2022/2555 of the European Parliament and Council, dated December 14, 2022 "On measures for a high common level of cybersecurity across the European Union, amending Regulation (EU) No. 910/2014 and Directive (EU) No. 2018/1972, and repealing Directive (EU) No. 2016/1148), considering the innovations brought by the latter and since this Directive repealed Directive NIS 1, the Authority began the process of studying and aligning with this directive.

Upon completion of the initial draft, in accordance with Law No. 146/2014, "On public notification and consultation," the draft law "On cybersecurity" was published in the Electronic Registry for Public Notifications and Consultations (ERPNC) from April 26, 2023, to May 24, 2023. The Authority held consultation sessions with interested parties, including critical and important infrastructure entities, who were invited to participate and provide input through comments and suggestions.

After completing the public consultation phase and receiving relevant comments and suggestions, the Authority continued its work for the comprehensive transposition of the provisions of Directive (EU) No. 2022/2555 (NIS 2). This process also included the evaluation and reflection of relevant comments received from institutions, interest groups, as well as the preparation of the complete package of the draft law.

For 2023, the drafting process of the final draft of the law "On cyber security" and its accompanying package was completed, which was sent to the Prime Minister in December of this year for further procedures.

The draft law then went through the necessary procedures for approval in the Assembly of the Republic of Albania. The new law 25/2024 "On Cybersecurity" entered into force on May 3, 2024. The level of transposition of Directive NIS2 consists of a high level of compliance with Directive NIS 2.

Regarding the draft law "On electronic identification and trusted services," in May 2023, the final draft of the law and its accompanying package was completed, fully aligned with EU Regulation No. 910/2014, eIDAS, which has been sent to the Prime Minister for further procedures. Due to the reengineering of services, the draft law was returned for a comprehensive review.

Throughout 2023, the Authority studied the best practices of developed countries regarding the establishment of a national procedure for cases of emergency situations created by cybersecurity crises, with the aim of processing and selecting the best model for defining this procedure pursuant to sub-legal acts of the draft law on cybersecurity.

Considering the growing cyber security threats and attacks on Albania's critical information infrastructures, the Albanian government has increased its efforts to achieve a high level of cyber security at the national level. The National Cyber Security Strategy 2020-2025 foresees the need to revise the respective Action Plan every two years, based on the dynamics of the development of the cyber security sector.

In this context, the National Authority on Electronic Certification and Cyber Security (NAECCS) has reviewed the Action Plan of the National Cyber Security Strategy for the period 2024-2025, drafting a new strategic plan in accordance with the policy goals and specific objectives of the National Cyber Security Strategy 2020-2025. This action plan, in addition to NAECCS, also includes several other institutions such as the State Police, the National Agency for the Information Society, the Ministry of Education and Sports, the Ministry of Health and Social Protection, the National Authority for Classified Information Security, the Ministry of Infrastructure and Energy, the Electronic and Postal Communications Authority, the Coordination Center Against Violent Extremism, the State Agency for Child Rights and Protection, and the Ministry of Europe and Foreign Affairs, which will be responsible for its implementation.

The review process has involved coordination and periodic consultations with all responsible institutions and interest groups regarding the preliminary draft of the new action plan, through meetings and ongoing email communications to seek opinions and suggestions, as well as integrate relevant comments from all parties involved in accordance with strategic objectives. After integrating the comments and suggestions of the involved parties, the Action Plan 2024-2025 was also consulted with experts from the Regional School of Public Administration to carry out a forecast and analysis as accurately as possible regarding the necessary budget, leading to the preparation of the final version of this plan.

The Action Plan 2024-2025 of the National Cyber Security Strategy is an ambitious strategic plan, and its implementation will contribute to the government's efforts to guarantee cybersecurity at the national level by protecting critical and important information infrastructures, increasing capacities and awareness, creating the necessary mechanisms for the security of citizens in cyberspace, focusing on children and youth, and enhancing national and international cooperation with strategic partners in the field of cybersecurity.

This new action plan addresses the priorities, needs, and challenges concerning cybersecurity at the national level, by forecasting the necessary activities in accordance with the respective goals and specific objectives. These activities aim to improve policies and procedures, enhance technical and human capacities, strengthen cybersecurity structures and infrastructures, prevent and reduce phenomena such as cybercrime and illegal content online that threaten the security of citizens in cyberspace, as well as strengthen national and international cooperation, aiming to increase Albania's preparedness and resilience in the field of cybersecurity. The Action Plan

2024-2025 will contribute to achieving the targeted outcomes also outlined in the National Cyber Security Strategy 2020-2025.

Improvement of the political and legal framework, including laws, strategic policies, regulations, methodologies and procedures through the implementation of EU cybersecurity policies and standards;

- Strengthening cybersecurity structures and infrastructures in terms of technical and professional capacities as well as their respective procedures. This is planned to be achieved through activities such as: improving the capabilities of the National Security Operational Center (National SOC) for monitoring and addressing cybersecurity incidents, establishing laboratories for the analysis of malicious software (malware) and simulating cyber incidents, enhancing technical and professional capacities, conducting technological analysis of critical infrastructure environments, optimizing security infrastructure, improving incident handling and management procedures, among others, as anticipated in the action plan;
- Increasing awareness and education, as well as improving preventive and protective measures concerning cybersecurity threats, cybercrime, and illegal online content, internet safety, and protection of children online, as well as violent extremism and radicalization in cyberspace;
- Enhancing professional capacities in cybersecurity through educational programs. To achieve this, the revised action plan anticipates the development of new study programs and the updating of existing higher education curricula in the field of cybersecurity, enabling online courses, training programs, and cybersecurity drills for cybersecurity experts from institutions, operators of critical information infrastructure (OIKI), and operators of important information infrastructure (OIRI);
- Strengthening national and international cooperation, where several activities are planned, such as: creating a forum with public and private institutions in Albania and international agencies, establishing a structure for cybersecurity diplomacy within the Ministry for Europe and Foreign Affairs in coordination with NAECCS drafting and signing bilateral and multilateral agreements in the field of cybersecurity, promoting and implementing international law, norms, and measures for building trust regarding responsible state behaviour in cyberspace, active participation in the UN, NATO, OSCE, EU, and other international organizations, conducting regional cybersecurity exercises, participating in international projects, etc.

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

Considering the National Cyber Security Strategy, the establishment and strengthening of the National CSIRT has been and remains a key priority. Since the beginning of this initiative, significant steps have been taken to ensure that the National CSIRT is equipped with the necessary technical and human procedures and capacities to tackle cybersecurity challenges.

During 2023, a procedure for incidents management (version 1.0) was developed and approved containing detailed measures for identifying, assessing, and effectively managing cybersecurity incidents. This procedure ensures a structured and coordinated approach to minimize the impact of incidents on critical systems and data, contributing to strengthening national cybersecurity.

To enhance the capabilities of the Cybersecurity Incident Response Team at the Authority (National CSIRT), the technological infrastructure has been modernized, ensuring that the CSIRT is equipped with the most advanced tools and technologies to detect, prevent, and combat cybersecurity threats.

To further reinforce the capabilities of the National CSIRT, NAECCS has worked on staffing the planned structure with new personnel, with the recruitment process ongoing. In this context, a priority for the Authority has been attracting talent and professionals in the field of cybersecurity, who will contribute to developing preventive strategies and strengthening incident response.

NAECCS, in fulfilling its duties, has worked to provide a functional and efficient working environment for the National Security Operational Center (National SOC) to ensure cybersecurity in critical and important information infrastructures.

The National SOC has made significant strides in addressing cybersecurity challenges. The SOC plays a key role in monitoring, analyzing and responding to cybersecurity incidents in critical information infrastructures. In this process, a key aspect has been creating optimal working conditions, which include developing technical infrastructure, increasing human capacities, and strengthening strategic cooperation.

In terms of infrastructure development, the National SOC has undergone a significant transformation, including the implementation of advanced security monitoring and analysis tools that enable proactive identification and management of cybersecurity threats. Through strategic partnerships and investments, technologies and tools have been secured that align with the specific needs of information infrastructures.

A key element has been the strengthening of human capacities through ongoing training and professional development programs. SOC personnel have participated in training sessions and workshops, focusing not only on technical aspects but also on crisis management and effective communication during incidents. Additionally, a mentoring program has been established to aid in the rapid development of the skills of new staff.

The National Authority on Electronic Certification and Cyber Security has also worked to enhance the capacities of CSIRTs across all industrial sectors at the national level through cybersecurity training and exercises, surpassing the established objective of a minimum of four cybersecurity drills and exercises per year. In 2023, approximately 12 cybersecurity drills were organized. This result reflects NAECCS's commitment to improving and strengthening national cybersecurity.

In 2023, progress was made regarding the strengthening and implementation of security measures in critical and important information infrastructures, as well as the analysis of critical and important information infrastructures for risk assessment and management.

In fulfilment of its functional duties and in accordance with Law No. 2/2017, "On Cybersecurity," the Decision of the Council of Ministers No. 553, dated July 15, 2020, "On the Approval of the List of Critical Information Infrastructures and the List of Important Information Infrastructures," as amended, and the regulation "On the Content and Method of Documenting Security Measures" (Version 2.0, approved by Order No. 10/2022), the National Authority on Electronic Certification and Cyber Security conducted continuous physical cybersecurity audits (onsite) at the operators' facilities in relation to the implementation of minimum security measures during the period from January to December 2023. As a result of intensive work, the number of onsite audits at critical and important information infrastructures quadrupled in 2023.

Based on the current cybersecurity situation and the need to increase security levels in information infrastructures, additional technical measures (Baseline) were developed and approved as an integral part of the "Regulation on the Content and Method of Documenting Security Measures." The Baseline contains 28 mandatory minimum technical cybersecurity measures to be implemented by OIRI and OIKI.

NAECCS has also organized consultative meetings with operators of critical and important information infrastructures on the importance of implementing additional technical cybersecurity measures (Baseline) within the specified deadlines. NAECCS has assessed the implementation of these measures at both the infrastructure and sectoral levels.

Specifically, during 2023, NAECCS has inspected the implementation of cybersecurity measures:

- 26 Operators of Critical Information Infrastructures in the Health, Financial (Banking, Microfinance), and Energy sectors (using the onsite inspection method);
- 32 Operators of Critical Information Infrastructures (using the self-declaration method);
- 23 Operators of Important Information Infrastructures in the Energy, Transportation, Health, and Financial (Insurance Market) sectors, as well as Water Supply (using the onsite inspection method);
- 22 Operators of Important Information Infrastructures (using the self-declaration method).

The assessment of technical security measures was based on emergency measures as well as the New Program for assessing cybersecurity vulnerabilities (GAP Analysis).

Also, through the self-declaration method, during 2023, the assessment of the implementation of cybersecurity measures for security and defense institutions, which are not part of critical and important information infrastructures, has been carried out for:

1. Ministry of Defense;
2. General Directorate of State Police;
3. Police Supervisory Agency;
4. Directorate for the Security of Classified Information;
5. High Judicial Council;
6. High Council of Prosecutors;
7. Assembly of the Republic of Albania;
8. Institution of the President of the Republic;
9. High Inspectorate of Declaration and Audit of Assets and Conflict of Interest;
10. General Prosecutor's Office;
11. Central Election Commission.

In order to automate the process of auditing the level of implementation of security measures, the National Authority on Electronic Certification and Cyber Security has implemented the CISA CSET TOOL. This platform served for the digitalization of the audit process as well as for the creation of an electronic database for the audits carried out, the level of implementation of measures, and the security level for each evaluated institution.

Some of the main functionalities of the CSET TOOL include:

- Effective control of the implementation of security measures by OIKI and OIRI;

- Analysis of cybersecurity vulnerabilities of OIKI and OIRI;

- Assessment of cybersecurity resilience, as well as risk evaluation of OIKI and OIRI;

- Creation of dedicated profiles for all critical and important information infrastructures, according to specific sectors;

- Generation of reports (in statistical/graphical form) on the cybersecurity level of infrastructures;

- Recommendations for improving the vulnerabilities identified during audits.

In order to ensure good governance of cybersecurity at the national level, investments in cybersecurity in the public and private sectors play a crucial role. To gain an overview of the investment situation in cybersecurity, in cooperation with operators of critical and important information infrastructures, an analysis was conducted on the budgets dedicated to cybersecurity for 2023 and 2024, as well as investments in cybersecurity for 2023.

During the year 2023, NAECCS also drafted the guideline *"Guideline for the Methodology of Determining Administrative Penalties in the Process of Controlling Critical and Important Information Infrastructures"* approved by the General Director under No. 179 Prot., dated 03.03.2023.

After completing the control process "On the Evasion of Implementing Recommendations and Corrective Measures as well as the Verification of the Implementation of Some Technical

Measures, the following were sanctioned with fines:

Infrastructure	**Number**	**Revenue for the state budget from fines**
Critical Information Infrastructure	4	3 600 000 LEKË
Important Information Infrastructures	2	

In the context of ongoing commitments to strengthen cooperation and information sharing in the field of cybersecurity, experts from NAECCS have participated in a series of important meetings organized by NATO. Some of these meetings include:

- MISP User Meeting – May 2023
  This meeting focused on sharing experiences and best practices in using the MISP (Malware Information Sharing Platform), thereby enhancing our capabilities in managing and sharing data on cyber threats.
- Cyber Coalition 2023
  This is one of NATO's largest exercises in the field of cybersecurity, aimed at improving interaction and coordination among member states and partners in the event of a cyber attack, held in Tallinn, November 27 – December 1, 2023. This activity included training and practical exercises, focusing on preparing and equipping our teams to address current and future challenges in cybersecurity.

As a result, NAECCS has made significant progress in harmonizing cybersecurity legislation and practices with European Union standards. During this process, NAECCS has assessed and worked to transpose EU directives and regulations and has committed to enhancing its capacities as well as those of critical and important information infrastructures, reflecting the government's profound commitment to achieving a high level of cybersecurity in accordance with the objectives of the National Cyber Security Strategy 2020-2025 and integration with best international practices.

3.1.2 STATE POLICE (SP)

As reported by the State Police, concerning the specific objective of improving the legal framework that regulates the field of cybersecurity in the country and harmonizing it with the directives and regulations of the European Union, the Minister of Interior's order No. 494, dated December 30, 2020, approved the "Strategy for Investigating Cyber Crimes and the Action Plan 2021-2025." Additionally, by order No. 60, dated January 15, 2021, the General Director of the State Police approved the "Work Program of the Special Task Force for Implementing the Strategy for Investigating Cyber Crimes" and the "Action Plan 2021-2025." Subsequently, an inter-institutional working group was established for amendments to the penal code. Also, pursuant to international conventions and due to their functioning, it has been proposed to transfer certain criminal offenses from other structures to the Cyber Crime Investigation structures.

Based on order No. 974, dated June 29, 2023, from the General Director of the State Police, criminal offenses have been defined, subject to work within the State Police structures, aiming for internal division of labor among the central and local levels. By order No. 47, dated April 14, 2024, from the Minister of Interior “For the approval of the structure and organization at the central, local, and special structures of the State Police,” the Directorate for Investigating Cyber Crimes has been established at both central and local levels.

Regarding the specific objective of improving information infrastructures to combat cybercrime, radicalization, and violent extremism, following the order No. 47, dated April 14, 2024, from the Minister of Interior “For the approval of the structure and organization at the central, local, and special structures of the State Police,” in order to enhance existing cyber defense capabilities, the Directorate for Investigating Cyber Crimes has been created at both central and local levels.

The State Police has worked to strengthen the capacities of this structure, extending throughout the territory of the country, increasing training capacities, and enhancing relevant training in the field of cybercrime, as well as increasing the logistical capacities of the Cyber Crime Investigation structures. Efforts will continue in this direction throughout 2024.

Regarding international cooperation, the enhancement of cooperation among cybercrime investigation structures with law enforcement partners is part of the ongoing work of the State Police, where the establishment of this structure will receive even more priority.

3.1.3 NATIONAL AGENCY FOR THE INFORMATION SOCIETY (NAIS)

Based on written reports, the National Agency for the Information Society (NAIS) has worked on optimizing security infrastructures, improving security procedures and regulations, and enhancing cybersecurity systems and hardware structures.

NAIS has optimized security infrastructures by expanding the current infrastructure thanks to the installation of security agents in institutions that have sought NAIS's assistance for monitoring and responding to cyber incidents. Additionally, technical expansion has been carried out through integration with various platforms, such as threat intelligence and sandbox environments. The organization, subject of efficiency in operational responsiveness by using artificial intelligence and machine learning, has enabled automation without requiring human interaction.

As part of the modernization and functioning of the government CSIRT, NAIS is currently certified with International Standards ISO and is also following the SIM3 model, maturing its CSIRT governance, performance assessment, and documentation. It is worth noting that collaboration with the Microsoft SIM3 responsible team highlights Albania among the few European countries following this model. Moreover, NAIS GCSIRT (designated as government CIRT) is in the listing process, aspiring to achieve the certified level of Trusted Introducer, thus ranking the government CSIRT as a partner among CSIRTs in the European Union.

In collaboration with Microsoft, the Information Security Regulation document has been improved by integrating best security practices. Based on the guidelines of this document, NAIS personnel in institutions, economic operators, and staff of institutions have been required to rigorously implement it.

Additionally, NAIS has followed guidelines for managing and mitigating vulnerabilities and various information regarding recorded activities, as well as conducting monitoring of their implementation with the assistance of security agents that analyze the posture of end-user computers, technical components, and abnormal user behaviors.

Currently, the NAIS Security Operations Center and the Cyber Incident Response Team monitor and respond to incidents in the governmental cyberspace. The implemented philosophy, Defense in Depth, provides a multi-layered defense. The ultimate goal is the implementation of the Zero Trust principle. Regarding the objective of improving hardware structures and establishing access control systems on the Gov Net network, NAIS has taken measures, achieving a realization rate of 90%.

Furthermore, NAIS has conducted research to strengthen national priorities as a basis for forecasting investments in the development of cybersecurity. In this context, various scientific papers have been published based on scientific research related to the current cyber posture and the investments needed to build a sustainable ecosystem. These papers have been presented at national and international scientific conferences, such as the Security and Defense Innovation Center and the Faculty of Economics at the University of Tirana.

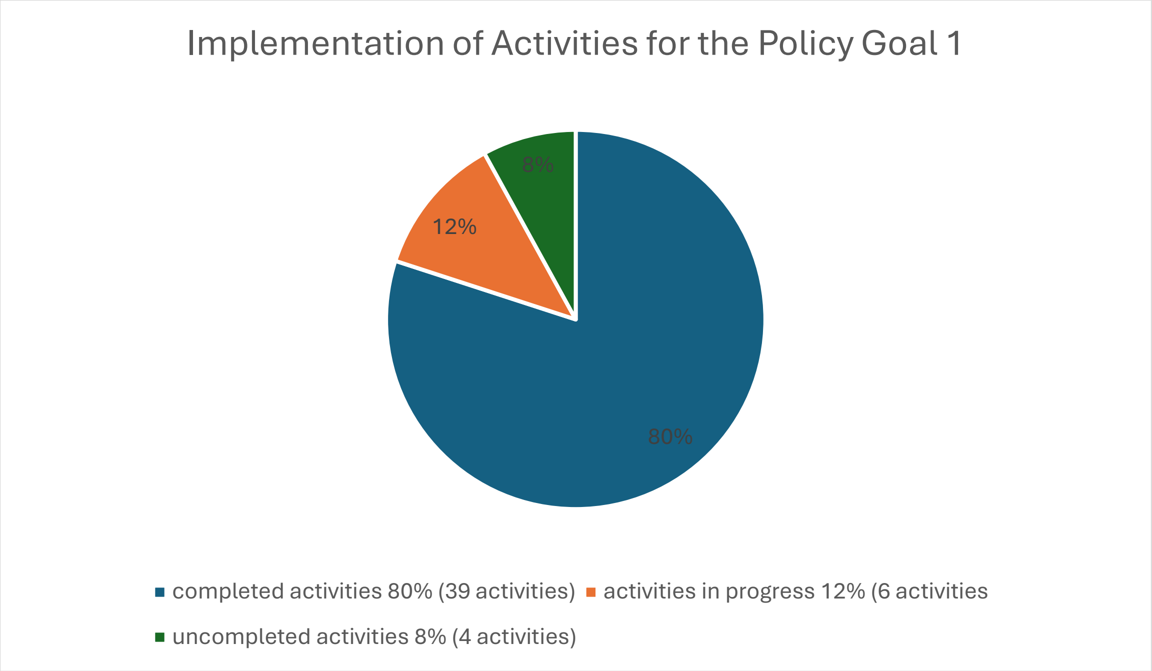
Regarding some of the objectives of the National Cyber Security Strategy that NAIS is working to fulfil, the agreement signed between the Council of Ministers and Microsoft also contributes to their realization.

Summary of Policy 1

Referring to the progress of Albanian government institutions concerning Policy 1, marked during 2023, it is clear that Albania is making positive strides in harmonizing its legislation and cybersecurity practices with European Union standards. Improving capacities and implementing security measures in critical infrastructures are essential to addressing cybersecurity challenges, and NAECCS has achieved high results in this regard. These efforts demonstrate a sustained and clear commitment to ensuring a secure cyber environment for all citizens, which not only enhances national security but also strengthens Albania's position on the international stage as a reliable partner in addressing cyber threats.

Implementation of Activities for the Policy Goal 1

For Policy 1, it is reported that by 2023, the level of activity implementation is as follows: completed activities 80% (39 activities), activities in progress 12% (6 activities), and uncompleted activities 8% (4 activities)



POLICY GOAL 2: BUILDING A SECURE CYBER ENVIRONMENT BY EDUCATING AND RAISING AWARENESS IN SOCIETY TO ENHANCE PROFESSIONAL CAPACITIES IN THE FIELD OF INFORMATION SECURITY.

The priority objectives focus on:

- Increasing professional capacities in the field of information security through the revision of educational curricula;
- Enhancing the awareness and professional skills of public and private institutions regarding cybersecurity;
- Raising societal awareness about cybersecurity and cyber threats

For the achievement of the objectives of Policy 2, the institutions involved in the implementation of the Action Plan report as follows:

3.2.1 NATIONAL AUTHORITY ON ELECTRONIC CERTIFICATION AND CYBER SECURITY (NAECCS)

National Authority on Electronic Certification and Cyber Security has committed to developing and promoting a sustainable cybersecurity culture by raising awareness of cyber risks and improving cyber defenses through the development of necessary human capacities in the field of cybersecurity.

In this context, NAECCS has carried out training sessions and awareness campaigns related to online safety, cyber hygiene, as well as cyber security issues for operators of critical information infrastructures and operators of important information infrastructures (OIKI and OIRI), including public and private institutions.

NAECCS has taken important steps in the framework of achieving the objectives for increasing professional capacities in the field of cyber security through the review of educational curricula, such as the agreement signed with the Academy of the Armed Forces on 30.11.2023 on education, research and training of students and academic staff in the field of cyber security. In the framework of this agreement, in January 2024, a joint working group was established between NAECCS and the Academy of the Armed Forces to work on the improvement of curricula in the field of cyber security. Specifically, NAECCS is committed to improving the curriculum related to the teaching program of the second cycle of Professional Master studies "Cybersecurity in the field of defense".

NAECCS, in cooperation with the Armed Forces Academy, has carried out the analysis of the current situation of critical and important information infrastructures of the public and private sector, identifying the needs for further improvements in terms of human capacities and investments in the field of cyber security. Through a questionnaire designed and sent to 52 (fifty-two) subjects, data was collected about human resources and the necessary skills in cyber security, in order to assess the needs and the possibility of improving the Professional Master's program in Cyber Security in the field of Defense at the Armed Forces Academy (AFA)[1].

NAECCS has implemented training and awareness programs in the field of cybersecurity to educate children, young people, parents and teachers as well as social workers on the risks that may be encountered in cyberspace, protection methods, and the institutions where cases of harmful and illegal content can be reported.

Additionally, during the year 2023, NAECCS distributed educational materials as well as daily notifications/news regarding potential cyber threats and cyber incidents (such as bulletins) on the official website of the Authority and on social media.

Enhancing human capacities in the field of cybersecurity is a key element of the National Cyber Security Strategy and the Action Plan 2020-2025. NAECCS has prioritized training and preparation of experts in this field to improve the ability to prevent, detect, and respond to cyber attacks. NAECCS has worked to increase the professional capacities of its staff as well as the staff responsible for cybersecurity at critical and important information infrastructure operators.

NAECCS has carried out awareness campaigns and training with critical information infrastructure operators (OIKI) and important information infrastructure operators (OIRI), including table exercises, seminars, and cybersecurity drills. During the year 2023, 250

[1] Marreveshje-bashkepunimi-1.pdf (aksk.gov.al)

individuals from 60 critical and important information infrastructure operators were trained in activities organized by NAECCS. NAECCS, in collaboration with partners, has also engaged in a series of significant training initiatives to increase capacities in cybersecurity. These programs include staff participation in various training sessions both domestically and internationally, designed to address a range of challenges in this field. The focus of the trainings has been on protecting critical information infrastructures, incident management, and threat analysis. The primary goal of these trainings has been to improve the knowledge and skills of professionals, while raising awareness and building resilience against cyber attacks remain top priorities for NAECCS, supported by the expertise of partners.

For the above, specialized trainings have been conducted to strengthen the capacities of NAECCS staff as follows:

- CompTIA Security+
- TAIEX workshop on Cybersecurity incident (case ID ETT 81753)
- KPMG – Hacker Fundamentals
- KPMG – Secure Coding
- Threat Hunting Exercise
- Cybexer Technologies – Technical Cybersecurity Threat Hunting Exercise - Cybersecurity Capacity Building Exercises for Albania, Montenegro, and North Macedonia
- Cyber Incident Response (CIR) training for Albanian critical Infrastructure Operators and Government Agencies, supported by Catalisto LLC
- Workshop "Governing Cyber Crisis"
- Cyber Tech Europe 2023
- Security Operations Concepts and Practices Course, supported by SEI
- Cyber Defense Planning Engagement from the U.S. Institute for Security Governance.

NAECCS has also conducted dedicated training with operators of critical information infrastructures and important information infrastructures, identified for the first time in Decision No. 761, dated December 12, 2022.

The focus of the training was on the following issues:

- Familiarization with the legal framework for cybersecurity in the Republic of Albania;
- The new Cybersecurity Strategic Plan;
- Management of the CSIRT lifecycle;
- Benefits of establishing a CSIRT;

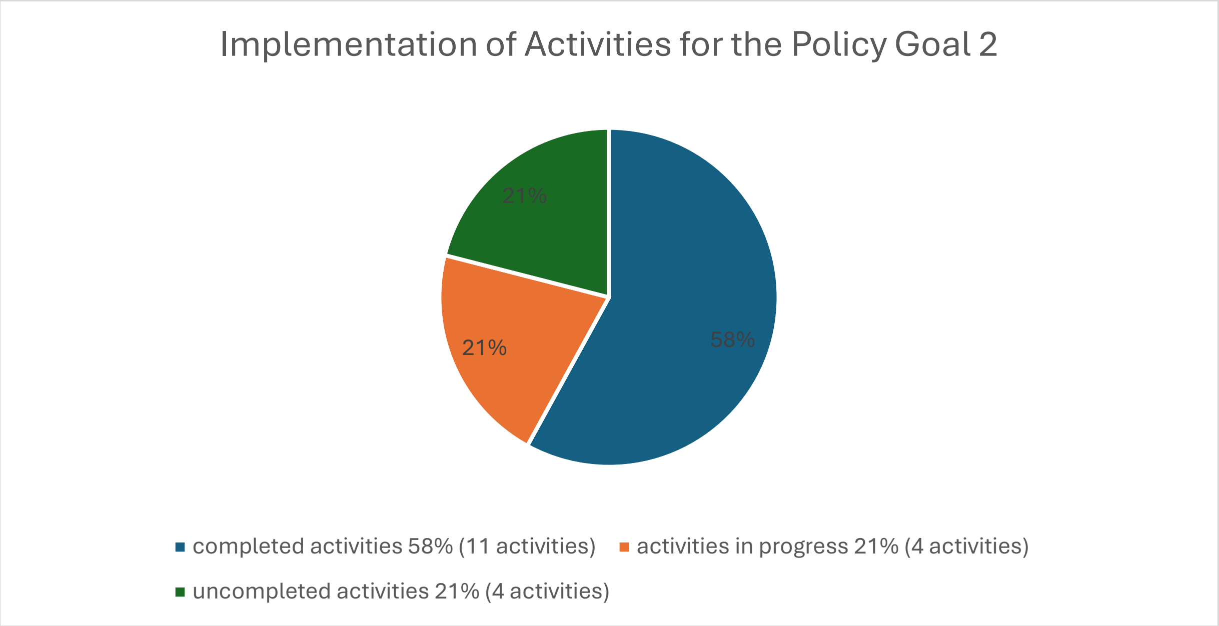
- Categorization of cybersecurity incidents;
- Organizational and technical security measures to be implemented by OIRI and OIKI;
- Cybersecurity controls.

Summary of Policy 2

The work carried out by the National Authority on Electronic Certification and Cyber Security within the framework of Policy 2 of the National Cyber Security Strategy demonstrates a clear and continuous commitment to strengthening cybersecurity at all levels of society. From specific training for the protection of children online to improving academic curricula and implementing awareness campaigns, **NAECCS** has managed to build a strong knowledge base that is essential for a safer digital environment. These efforts not only increase professional capacities but also strengthen the country's cybersecurity resilience, ensuring that all users, from children to professionals, are more adept at cyber threats.

Implementation of Activities for the Policy Goal 2

For Policy 2, it is reported that by the year 2023, the degree of activity implementation is as follows: completed activities 58% (11 activities), activities in progress 21% (4 activities), and uncompleted activities 21% (4 activities)



POLICY GOAL 3: ESTABLISHING NECESSARY MECHANISMS FOR CHILDREN'S SAFETY IN CYBERSPACE, WHILE SIMULTANEOUSLY PREPARING A NEW GENERATION CAPABLE OF BENEFITING FROM INFORMATION TECHNOLOGY ADVANCEMENTS AND FACING DEVELOPMENT CHALLENGES

The objectives of the priority focus on:

- Strengthening the legal framework for enhancing the safety of children online;
- Preventing child sexual abuse online through increased awareness and the creation of safe spaces for internet navigation;
- Effective investigation and prosecution of cybercrime perpetrators against children, focusing on abuse and sexual exploitation;
- Raising awareness and educating all segments of society about the safe use of the internet by children;
- Strengthening intersectoral cooperation for the protection of children online

For the achievement of the objectives of Policy 3, the institutions involved in the implementation of the Action Plan report as follows:

3.3.1 NATIONAL AUTHORITY ON ELECTRONIC CERTIFICATION AND CYBER SECURITY (NAECCS)

The National Authority on Electronic Certification and Cyber Security has continuously worked in collaboration with the responsible institutions to establish inter-institutional interactive mechanisms and organize awareness campaigns and training for the online safety of children and youth, as a functional duty of the institution and in fulfilment of Policy Goal 3, with well-defined objectives in the Action Plan of the National Cyber Security Strategy 2020-2025.

Starting in 2021, Albania, through NAECCS as the responsible institution for protecting children and raising awareness about potential online risks, committed to becoming the first pilot country to implement the project “Creating a Safe and Prosperous Cyber Space for Children” in collaboration with the International Telecommunication Union (ITU).

The project began implementation in September 2021 and concluded in December 2023. In this context, NAECCS, with the support of ITU, has prepared and published the National Guidelines on Child Online Protection (COP), organized training and workshops, prepared additional materials, and conducted awareness campaigns aimed at enhancing the capacity and awareness at the national level of all responsible actors for the protection of children and youth, including parents, teachers, social protection workers in schools, school security officers, and representatives from businesses.

During the year 2023, NAECCS in cooperation with the International Telecommunication Union (ITU), within the piloting of the Global Project "Creating a Safe Cyberspace for

Children", has continued the implementation of 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 Child Rights and Protection (ASHDMF), carried out several online trainings on the topic "Protection of children on the internet and cyber hygiene", where employees from Child Protection Units in the municipalities of Dibër, Klos, Tirana, and Lushnje were trained. These trainings were carried out respectively on March 9, 10 and 13, 2023.

NAECCS is part of the reporting institutions for Albania for the implementation of the United Nations Convention on the Rights of the Child, where during the proceedings of the 94th session of the Committee on the Rights of the Child, held in Geneva, September 2023, reported on the concrete steps taken to create a safe cyber ecosystem for children and young people. NAECCS, in this report, emphasized the need for awareness and ways of protection against the increased and continuous threats that children and young people face on the internet, as well as the continuous need for inter-institutional cooperation.

The concluding workshop for the joint project with ITU, titled "A Decade of Awareness for Children's Online Safety," was held December 6, 2023, where the main goal was to raise awareness among interest groups and industry sector entities for the creation of a safe cyberspace for children and young people.

During the workshop, NAECCS presented the results of the project and the activities developed for the implementation of this project throughout the country. Participants included state institutions focused on the protection of children and youth, such as the Ministry of Education and Sports, the State Agency for Child Rights and Protection, the Electronic and Postal Communications Authority, the Center for the Prevention of Crimes against Minors and Youth, the State Police, representatives from Internet Service Providers (ISPs), and non-governmental organizations representing civil society.

During the discussions, representatives from institutions, civil society, and businesses showcased their ongoing efforts to protect children, raised issues regarding legal gaps, and emphasized the need for amendments to existing legislation. They also committed to creating potential bridges for collaboration and the development of ongoing projects in the future.

Based on the above, it can be concluded that the work and commitments of the National Authority on Electronic Certification and Cyber Security (**NAECCS**) and its partners have brought concrete positive results in the field of online safety for children and youth in Albania. Through completed projects and developed trainings, NAECCS has contributed to raising awareness and enhancing cybersecurity capacities at the national level, involving a wide range of actors from both the public and private sectors. The continuous commitment to protect and educate vulnerable groups, especially children and youth, in facing cyber challenges marks a significant step towards the security of the country’s cyber space. The work done so far serves as a foundation for future initiatives and the continuous improvement of safeguarding policies and practices.

3.3.2 MINISTRY OF EDUCATION AND SPORTS (MES)

Based on the report regarding the monitoring process of the implementation of the measures provided for in the Action Plan of the National Strategy for Cyber Security 2020-2025, the Ministry of Education and Sports has worked on strengthening the legal framework for increasing the safety of children on the internet by engaging in the drafting of manuals and guidelines for safe internet use.

In the framework of the realization of the objectives of the work plan for 2023, the Agency for the Assurance of the Quality of Pre-University Education (ASCAP) has drawn up the Internet Safety Manual, a material that provides a package of guidelines and advice related to promoting the safe and effective use of the internet by students and teachers. The purpose of this manual is to recognize the main services of the Internet, as well as the main challenges and risks that come from using it in an unsafe manner. The manual deals in detail with the main risks that children may encounter while using the Internet, such as: cyberbullying, sexual harassment, hacking of personal data, addiction to online games, etc. This material has been published on the official ASCAP website and has been shared with teachers and network administrators.

Additionally, regarding the cybersecurity of students and their protection from illegal and harmful content in pre-university educational institutions, the following acts are being implemented:

1. Joint Guidance between the Ministry of Education, Sports and Youth (MESY, now MES) and the Ministry of Health and Social Protection (MHSP) No. 658, dated September 23, 2019 "On the procedures and actions undertaken by educational structures, in cooperation with child protection structures, in cases where it is found that a child is accessing illegal and/or harmful content on the internet within the premises of pre-university educational institutions."
2. Guidance No. 34, dated 16.11.2018, "On the prohibition of mobile phones in pre-university educational institutions, both by teachers and students."
3. Order no. 493, dated 30.07.2018, "On the prohibition of the use of mobile phones during the teaching process in schools." [2]

Based on point 15 of Article 33 of the Regulation "On the operation of pre-university educational institutions in the Republic of Albania," security officers currently document their work according to the document "Working Practice of Security Officers in Schools" and prepare periodic reports as follows:

1. https://qbz.gov.al/eli/udhezim/2019/09/23/658/bc47bc07-8bcc-4337-a1d6-856d66877dab
2. https://arsimi.gov.al/udhezim-nr-34-date-16-11-2018-per-ndalimin-e-telefonit-celular-ne-institucionet-arsimore-parauniversitare/
3. https://www.ascap.edu.al/udhezuesi-per-praktiken-e-punes-se-oficereve-te-sigurise/
4. https://www.ascap.edu.al/praktika-e-punes-se-sherbimit-psiko-social-shkollor/
5. https://www.ascap.edu.al/parimet-per-etiken-profesionale-te-sherbimit-psiko-social-shkollor/

1. Incident/problem report;
2. Weekly report;
3. Annual report.

These reports also highlight the problems and cases related to the main risks that children may encounter while using the internet, such as cyberbullying, sexual harassment, hacking of personal data, and addiction to online games.

In schools, a network of cooperation has been established with parents and the Child Protection Unit (CPU) to protect minors against cyber violence.

Regarding the methodology for collecting incident cases in schools, the approved document for security officers in schools to perform their functional duties and collect incident cases is the "Working Practice of Security Officers in Schools."

For the psycho-social service (PSS), the following documents have been approved: "Working Practice of the Psycho-Social Service" and "General Ethical Principles of the Psycho-Social Service," which address situations of violence, bullying, and online abuse in schools.

The methodology for collecting cases includes:

1. Informative training sessions with students and parents conducted by the psycho-social service about the risks of uncontrolled internet use;
2. Creation of brochures and awareness materials to inform students, parents, and the community regarding cybersecurity;
3. Development of questionnaires by the psycho-social service regarding the time spent on social networks and the forms of bullying that may occur on them;
4. Handling informative discussions with students/teachers/parents about the safe use of the internet;
5. Awareness-raising training, primarily with students in grades VII-IX, on the themes of violent extremism;
6. Roundtables with the participation of various actors such as teachers, students, parents, representatives from the community, the State Police, etc., on the topic: “Preventing the sexual abuse of children online through raising awareness and creating safe spaces for internet navigation”;
7. Partnership with parents to enhance communication and support on bullying issues, where the information and assistance of parents has been particularly important in addressing this topic with their children;
8. Observations in collaboration with the supervising teacher and the psycho-social service of the schools;
9. Questionnaires with students;
10. Individual and group counselling;
11. Focus groups.

Regarding the reports of the local educational institutions responsible for pre-university education, the Ministry of Education and Sports reports that during the year 2023, informative reports were prepared by the Security Officer and the psycho-social service for the prevention of negative phenomena by identifying and taking steps in cooperation with the teaching staff and the parents.

In the framework of the educational work in institutions and the plan of activities against violent extremism, school psychologists in cooperation with the coordinator teacher of the plan against violent extremism at school have organized awareness-raising activities on the safety issue with students and teachers on the topic: "The use of Internet, the risks of extremist behaviours on the internet".

Informative discussions were also held on the topic: “Safe children online and protection from virtual violence,” carried out with students of lower secondary education, with the participation of representatives from the Child Protection Unit, the Coordinator for Domestic Violence, and institution’s psychologists. The main goal of these discussions has been to inform about the legal necessity of respecting children's rights and protecting them from all forms of violence.

Since the 2021-2022 school year, a professional network of ICT teachers has been established and is functioning, along with a group of school coordinators, for conducting the cyber security evaluation report. Within the framework of the implementation of the cooperation project between ASCAP and the Albanian Media Institute, 10 schools and around 150 teachers have been trained in 2023 on media education and information of lower secondary and upper secondary education. In addition to the knowledge gained about the world of media and information, important issues related to the challenges and risks in the virtual world were discussed. Teachers were introduced to codes of conduct, privacy rules, and some of the main risks that may be encountered during internet use. Furthermore, teachers were encouraged to use basic teaching methods and tools to help students use the internet responsibly and to make them aware of the challenges and risks associated with its use. Additionally, during 2023, this project was piloted with leaders of social sciences and biology-chemistry networks, where 120 network leaders participated in these trainings. The meeting of the professional network of ICT teachers is held twice a month (one in-person meeting, one online) where teachers discuss, share experiences, and assess needs.

Educational institutions in the country apply filters to prevent children from accessing inappropriate and illegal websites, where the verification of filters will continue even during 2024. The group of coordinators for the evaluation report on cyber security has also been set up in schools. Additionally, periodic incident reports are prepared by security officers or psycho-social service staff and reported according to the relevant work documents. Closed meetings are organized in schools to address the issue of social media bullying in a safe and trusting environment, encouraging students to speak freely and seek help.

The Ministry of Education and Sports has worked on identifying, supporting, and promoting talents to create technical solutions that help in online protection and security.

The applied methodology consists of the following steps:

1. Identification of students in schools by ICT teachers regarding their tendencies in using the internet and computers.
2. Development of contests and projects on the topic "Internet Safety". Assignments of high difficulty levels.
3. Development of a national Olympiad every year in ICT, as a means of discovering talents in the field.

As reported by the Ministry of Education and Sports, for monitoring the application of the above methodology, the following are considered:

1. The realization of the distribution of awareness raising posters regarding the risks that may arise from unsafe internet use.
2. Students who are inclined towards technology have trained their peers on how to protect themselves from cyber attacks;
3. Identification of participating and winning students in the national Olympiad for ICT for each phase.

As part of the commitment to increasing cyber security and protecting children online, the Ministry of Education and Sports, in collaboration with other relevant institutions, has implemented significant legal and practical measures. The development of Internet Security Manuals and the implementation of guidelines in educational environments are part of efforts to build a safer online environment for children and young people. Through trainings, raising awareness of internet risks, and promoting responsible use of technology, this commitment aims to protect children from harmful content and encourage safe and effective technology use. This comprehensive and coordinated approach supports the development of a new generation that is educated and equipped to face security challenges in cyberspace, thereby contributing to a more sustainable and secure digital society.

3.3.3 STATE POLICE (SP)

The State Police has worked on providing the technical tools that help the structure of the investigation of cybercrimes in the State Police in analyzing and detecting cases of online violence, especially related to images of sexual abuse of children, as well as on creating a working group from the structure of cybercrime investigation together with industry to solve the problems of investigating and identifying persons suspected of online child abuse, with a special focus on identifying end users through IP addresses.

Currently, with the implementation of order no. 47, dated April 14, 2023, from the Minister of the Interior “For the approval of the structure and organization at the central, local, and special structures of the State Police”, the Directorate for Cybercrime Investigation has been created. This structure includes the Sector for Investigating Child Pornography at the centre, the Unit for Investigating Child Pornography at the Local Police Directorate in Tirana, and sections in all counties of the country where cases related to cybercrime can be reported.

Since December 2020, the Cybercrime Structure has been part of NCMEC (National Center for Missing and Exploited Children), which provides daily reports and information on suspected criminal acts related to child pornography occurring in our country.

Moreover, as part of the ongoing procedures followed by the State Police, efforts are being made to implement the AMBER system. The “AMBER Alert” system is activated for serious cases of child abductions, missing children, etc., and serves to encourage/galvanize the community to help in the search for lost/missing children. Work on investigating and identifying perpetrators of cybercrime against children is always ongoing.

In 2023, the Cybercrime Investigation structures participated in awareness-raising meetings in schools and roundtables, collaborating with NGOs and other governmental organizations focused on child safety, to prevent online sexual abuse of children, bullying, data protection, etc.

As for the creation of a working group together with industry, work continues and is still in progress. In this regard, initiatives have been taken for cooperation with ISPs regarding the exchange of information. At the same time, initiatives have been undertaken for cooperation with public and private institutions in the field of child protection.

The efforts of the State Police to combat cybercrime, especially those involving sexual abuse of children on the internet, have resulted in the creation of specialized structures and the implementation of advanced technologies for detecting and handling these cases. Commitment to improving cooperation between cyber investigation structures and industry, as well as involvement in national and international initiatives show a clear will to address these challenges seriously and efficiently. These actions not only increase the capacity to detect and prosecute the perpetrators of these crimes, but also contribute to building a safer environment for children in cyberspace, prioritizing their protection from cyber threats.

3.3.4 MINISTRY OF HEALTH AND SOCIAL PROTECTION (MHSP)

As the State Agency for Child Rights and Protection reports, in terms of strengthening cross-sectoral cooperation for the protection of children on the internet, in the framework of the implementation of the National Agenda for the Protection of Children's Rights 2021-2026, a monitoring report has been prepared for the years 2021-2022 in coordination with line ministries, independent institutions and the participation of 120 children, who were part of the process and contributed to the design of this project.

The findings and results of this report were presented and discussed at the meeting of the National Council for the Protection of Children's Rights, which took place on November 2, 2023. Nineteen children participated in the meeting, where one of the discussed issues was online protection and security during internet navigation.

At the national level, there are 241 child protection workers in all municipalities (61). Child protection workers in all municipalities have managed 1413 cases of children for protection during the period January - September 2023.

During the period January - December 2023, from the National Line ALO 116 111, 1155 children received online counseling and 386 cases were referred to public institutions responsible for treatment and follow-up. Additionally, counseling and referrals for treatment in responsible institutions were provided for about 60 cases of children abused in the digital environment.

In the framework of cooperation for addressing the needs of children and guaranteeing their rights, the State Agency for Child Rights and Protection and NAECCS, in cooperation with the organization "ARSIS Initiative", are implementing the program "A Safer Cyberspace" for children and young people", in 4 municipalities of the country, Tirana, Durrës, Elbasan and Krujë. The program aims to promote children's rights in the digital world, making public actors in these municipalities aware of a safer environment in Internet browsing.

During November-December 2023, meetings were held in the aforementioned four municipalities, attended by 80 workers from NJMF/PMF administrative units, social workers, school psychologists, teachers, school security officers, police officers, prosecutors, and police personnel from the cybercrime sector.

On November 20, 2023, as part of International Children's Day, the Ministry of Health and Social Protection, the Minister of the Interior, the Minister of Education and Sports, the Minister of State for Youth and Children, and representatives of civil society signed the "National Pact against Sexual Violence against Children in Albania," a document aimed at the special protection of children from sexual violence originating from the internet as well as in daily life.

Simultaneously, in the framework of the International Children's Day on November 20, 2023, the Ministry of Health and Social Protection in cooperation with the State Agency for Child Rights and Protection, the State Minister for Youth and Children, NAECCS, the State Social Service, national and international partners, organized an awareness activity for children's rights. In this activity organized in the premises of the "TUMO" center, at Piramida, the children presented the innovative projects that they attend at the center, giving messages to other children about their rights.

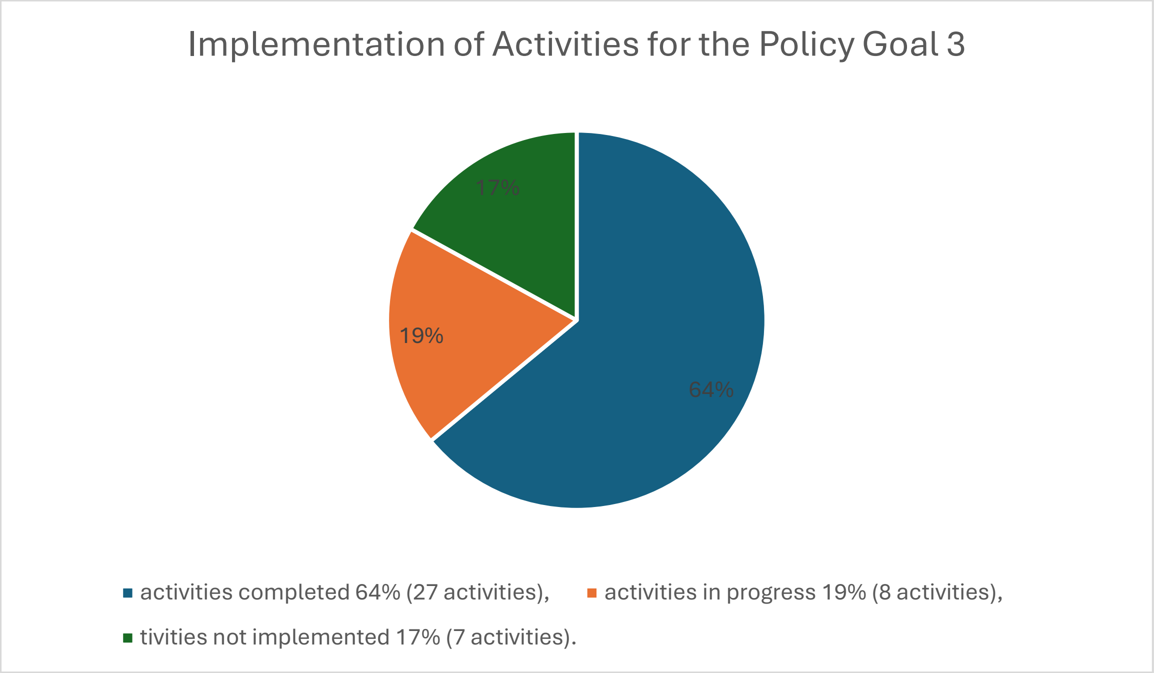
The work of the State Agency for Child Rights and Protection, in cooperation with various institutions and international organizations, shows a consistent commitment to the protection of children in the online and physical environment.

Summary of Policy 3

The initiatives undertaken by the National Authority on Electronic Certification and Cyber Security and other institutional partners in the framework of the implementation of policy goal 3 have contributed to the creation of a safer cyber environment for children and young people in Albania. Joint efforts to increase awareness and protective capacities against online challenges, through training, guidance, and awareness campaigns, have created a strong foundation to protect the most vulnerable groups of society.

Implementation of Activities for the Policy Goal 3

For the Policy Goal3, it has been reported that by 2023, the completion rate of activities is as follows: activities completed 64% (27 activities), activities in progress 19% (8 activities), and activities not implemented 17% (7 activities).



POLICY GOAL 4. Increasing National and International Cooperation in the Field of Cybersecurity with Strategic Partners

The objectives of the priority consist of:

- Strengthening institutional cooperation at the national level;
- Strengthening international cooperation in the field of cybersecurity and the fight against violent extremism and radicalization..

To achieve the objectives of Policy 4, the institution responsible for implementing the Action Plan reports as follows:

3.4.1 NATIONAL AUTHORITY ON ELECTRONIC CERTIFICATION AND CYBER SECURITY (NAECCS)

NAECCS, as the authority responsible for cybersecurity at the national level, and in fulfillment of the legal obligations and vision of the Republic of Albania for the development of information and communication technology, has identified partners at the national and international level with whom the Authority can cooperate within the framework of strengthening cyber security and has developed dialogue processes with the aim of strengthening cooperation.

Aiming to strengthen cooperation at the national level and create synergies in order to address and protect against cyber risks, the Authority has drawn up and signed a series of agreements with both public and private institutions within the country.

The agreements signed during the year 2023 are as follows:

- Cooperation Agreement with the Albanian Banking Association (dated 06/02/2023);
- Cooperation Agreement with the Academy of Armed Forces (dated 07/12/2023);
- Confidentiality Agreement with the General Directorate of Albanian Post (dated 06/07/2023);
- Cooperation and Confidentiality Agreement with the Transmission System Operator (dated 11/07/2023);
- Confidentiality Agreement with the Assembly of the Republic of Albania (dated 16/10/2023);
- Confidentiality Agreement with the First Investment Bank (dated 23/11/2023);
- Confidentiality Agreement with Tirana Bank (dated 12/12/2023);
- Confidentiality Agreement with Union Bank (dated 19/07/2023);
- Confidentiality Agreement with the Electricity Distribution Operator (OSHEE) (dated 13/07/2023);
- Cooperation Agreement with Raiffeisen Bank (dated 03/11/2023).

NAECCS has cooperated with the Tirana Chamber of Commerce and Industry for the organization of periodic meetings with the operators of critical and important information infrastructures.

Special importance has been given to cooperation with civil society such as the Academy of Political Studies (ASP) with which NAECCS organized the joint project related to violent extremism and illegal content on the internet according to the relevant national and international legal framework.

Within the framework of national cooperation to strengthen cybersecurity, NAECCS has worked to strengthen communication and trust between public and private CERT and CSIRT teams through dedicated communication platforms. In this framework, the Cyber Incident Management and Reporting System has been implemented. This advanced system provides a common communication platform that facilitates cooperation in cases of cyber incidents and strengthens trust between NAECCS and operators of critical and important information infrastructures that report cyber incidents.

Implementing this system not only improves the efficiency and effectiveness of responding to cyber incidents, but also helps build a safer and more reliable ecosystem for all stakeholders. The Authority continues to share information on security updates and Indicators of Compromise through the Incident Management and Reporting System, a system established since 2019 to facilitate continuous communication between the National CSIRT and operators of critical and important information infrastructures.

The Incident Management and Reporting System is a classified system that contains appropriate security elements for information exchanges. Another step taken is the establishment of the Malicious Activities Information Sharing Platform (MISP), which, at the national level, aims to share, store and link Indicators of Compromise (IoCs) of potential cyber-attacks and threats, information related to cyber threat actors, attack vectors, etc.

NAECCS, to guarantee a higher level of security at the national level in cyberspace, is committed to the successful fulfillment of strategic objectives also in terms of increasing international cooperation.

Throughout 2023, NAECCS has initiated meetings with representatives of counterpart authorities in Europe with the aim of establishing contacts for information exchange, sharing best practices and the possibility of concluding agreements. In this context, online meetings were held with Italy, Switzerland, Norway and Latvia.

To create a communication network for the exchange of information and best practices, the Authority has signed agreements with well-known international institutions such as:

- Memorandum of Understanding with 4IG (dated 20/01/2023);
- Cooperation Agreement with the National Cyber Security Directorate of Israel (dated 01/02/2023);
- Memorandum of Understanding with the Security Council of the United Arab Emirates (dated 06/04/2023).

The Authority has also implemented initiatives focused primarily on increasing capacities by integrating national and international cooperation. Initiatives and activities such as conferences, meetings, and training at the national and regional levels have served as communication bridges for collaboration and strengthening trust with operators of information infrastructures, both public and private, as well as the academic community. In this regard, NAECCS has collaborated with international partners that focus on cybersecurity as follows:

- International Telecommunication Union (ITU);
- MITRE Corporation;
- Electronic Governance Academy (EGA);
- Geneva Centre for Security Sector Governance (DCAF);
- Global Forum on Cyber Expertise (GFCE), where throughout 2023, NAECCS followed the membership procedures as a full member of this organization;

- Counter Ransomware Initiative (CRI), where at the Global “RSA Conference” in April 2023, NAECCS expressed interest in joining CRI, becoming the 36th country in the world to be a member;
- Regional School of Public Administration (ReSPA)

The Authority has been actively engaged both domestically and internationally in activities of NATO, OSCE, UN, EU, and FIRST, participating in both political and diplomatic level meetings as well as in activities such as conferences, cyber exercises, and training.

Specifically, 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. Albania's statement highlighted the progress in harmonizing the legal framework with the European Union framework 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.

In particular, active participation in NATO meetings for the implementation of international standards and regulations in the framework of cyber security is a key component for improving cyber defense. In this context, meetings were held in Brussels and Mons where the use of the MISP platform (Malware Information Sharing Platform) for the exchange of information on cyber threats and incidents was discussed and demonstrated. These meetings have helped to increase cooperation and information sharing among NATO member countries, improving the response to cyber threats and overall cybersecurity. This enables NAECCS, in the role of the National CSIRT, to inform and raise awareness of the information infrastructures in real time about the incidents that have occurred and have been reported. In addition, the cooperation of all relevant actors in the process of development and unification of security standards, standardization of cooperation, as well as the definition and establishment of the mandatory level of protection of entities that manage cyber incidents has been realized.

Regarding membership and participation in various international activities and initiatives in the field of cybersecurity, representatives of NAECCS have participated in the following events:

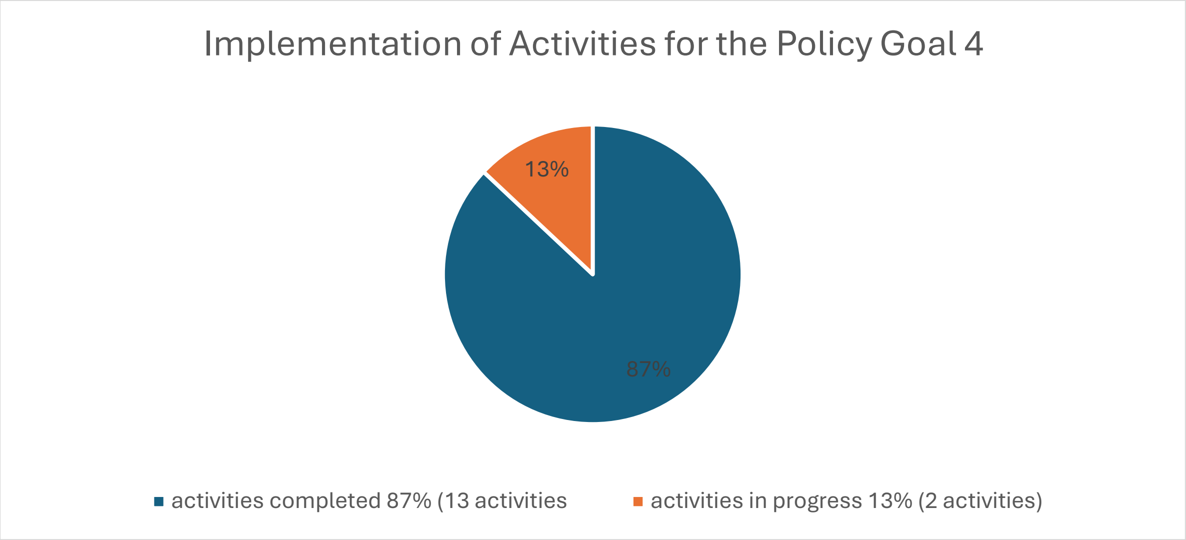
- FIRST/DCAF Technical Colloquium | Balkan Cybersecurity Days 2023 - Ohrid, MK;
- TF-CSIRT Meeting & 2023 FIRST Regional Symposium for Europe - Bilbao, ES

Summary of Policy 4

NAECCS has strengthened cooperation and increased information exchange at both the national and international levels by drafting and signing various agreements aimed at improving cybersecurity. This collaboration enables the exchange of valuable knowledge and experiences, as well as the establishment of a secure cybersecurity environment. Through active engagement in international meetings and conferences, as well as implementation of international standards, advanced technologies, and security measures, NAECCS contributes to a more efficient and coordinated response to cybersecurity incidents, making Albania a state that is fully committed to cybersecurity at both the national and international levels.

Implementation of Activities for the Policy Goal4

For the Policy Goal4, it is reported that by 2023, the level of activity implementation is as follows: activities completed 87% (13 activities), activities in progress 13% (2 activities), and activities not implemented 0% (0 activities).



4. RECOMMENDATIONS

✓ **Increasing Investments in Technology and Infrastructure**

- Enhancing investments in the latest cybersecurity technologies to better protect critical and important information infrastructures.
- Strengthening the capacities of the National Security Operational Center (SOC) to include advanced monitoring and incident response capabilities, covering all critical and important infrastructures at the national level.
- Creating optimal working conditions for the functioning of CSIRTs (Computer Security Incident Response Teams) to facilitate the effective fulfillment of their duties, with the aim of ensuring cybersecurity in critical and important information infrastructures.

✓ **Improvement of the Legal and Regulatory Framework in Line with the European Union Acquis**

- Adoption of the draft law "On Electronic Identification and Trusted Services."
- Drafting and adoption of secondary legislation for the implementation of the new law no. 25/2024 "On Cybersecurity," which transposes the NIS2 Directive.
- Further harmonization of national legislation with European Union directives and standards.

- Drafting and adoption of regulations for providing secure internet in public and broader spaces.

✓ **Approval and Implementation of the 2024-2025 Action Plan of the National Cyber Security Strategy**

- Approval of the Action Plan drafted to respond to the dynamics of cyber threats and technological developments, as well as the implementation of the new measures foreseen for the 2024-2025 period.

✓ **Continuous Awareness and Education**

- Expanding awareness programs for the general public on the importance of cybersecurity and protective measures that individuals can take.
- Integrating cybersecurity curricula into educational systems, from basic to university education.

✓ **Development of Professional Capacities and Training**

- Increasing training programs for the development of cybersecurity skills at all levels of public and private institutions.
- Recruiting and training new talents in the field of cybersecurity through scholarships and specialized programs.

✓ **Incident Response and Management**

- Developing and implementing a comprehensive and coordinated plan for managing cyber incidents involving all key national and international actors.
- Enhancing rapid and effective response capacities to incidents to prevent and minimize their impact.

✓ **Strengthening International Cooperation**

- Strengthening and promoting cross-sectoral cooperation in cybersecurity to ensure the full implementation of the National Cyber Security Strategy.
- Expanding cooperation agreements with international organizations and other countries to exchange knowledge, technology, and best practices.
- More active participation in international forums and initiatives to promote responsible state behavior in cyberspace, contribute to defining norms and confidence-building measures, and enhance the ability to respond to transnational threats.