AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Monitoring of National Cybersecurity Strategy 2020-2025

Tirana, 2023

Table of Contents

1. INTRODUCTION

Cyber security is currently more than ever a priority of the Albanian government. The cyber-attacks that Albania faced last year showed the importance of cyber security to have a solid national security, as well as pointed out the need for strengthening national and international cooperation and increasing investments and capacities in terms of cyber protection. Although much has been done to increase the level of cyber security in the country, no country in the world is immune to cyber-attacks, and especially countries like Albania, which have achieved a high level of digitization of public services, thus becoming more exposed in this regard. To ensure that Albania is prepared for potential cyber threats, resisting, and responding to them in a sustainable manner, the Albanian government is working to improve current policies as well as to implement new initiatives and projects that contribute to create a secure cyber ecosystem. There are various malicious individuals and groups in cyberspace who influence the well-being and functioning of states. Privacy intrusions and identity theft are a growing concern for society. Albania, aiming to increase well-being and improve public services, is investing in digital infrastructure. This, together with the benefits, also brings problems in cyber security. Cyber threats are on the rise targeting the security of information systems. The current challenges consist of building a digitally developed society but at the same time cyber-protected. Along with developments in information technology, the legal framework on cyber security is also improved.

The main goal of the government's work and initiatives in this field has been to guarantee cyber security at the national level, through the protection of information infrastructures, by strengthening technological and legal means. Likewise, the government has also worked for the education and awareness of society, as well as for raising professional capacities in the field of information security, committing to prepare a new generation capable of benefitting from the advantages of information technology and to meet the challenges of technological development. Special importance has also been given to addressing cyber threats that target young people and children online, where work has been done to create the necessary mechanisms for their safety in cyberspace. Important steps have been taken in the framework of increasing national and international cooperation in cyber security and defense with strategic partners, where a series of cooperation agreements have been signed, and work continues to expand this cooperation.

The National Cybersecurity Strategy 2020-2025 was approved by Decision no. 1034 dated 24.12.2020, of the Council of Ministers as a key instrument for increasing the security of networks and information systems at the national level as a priority of the Albanian Government.

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

The strategy is based on main principles as below:

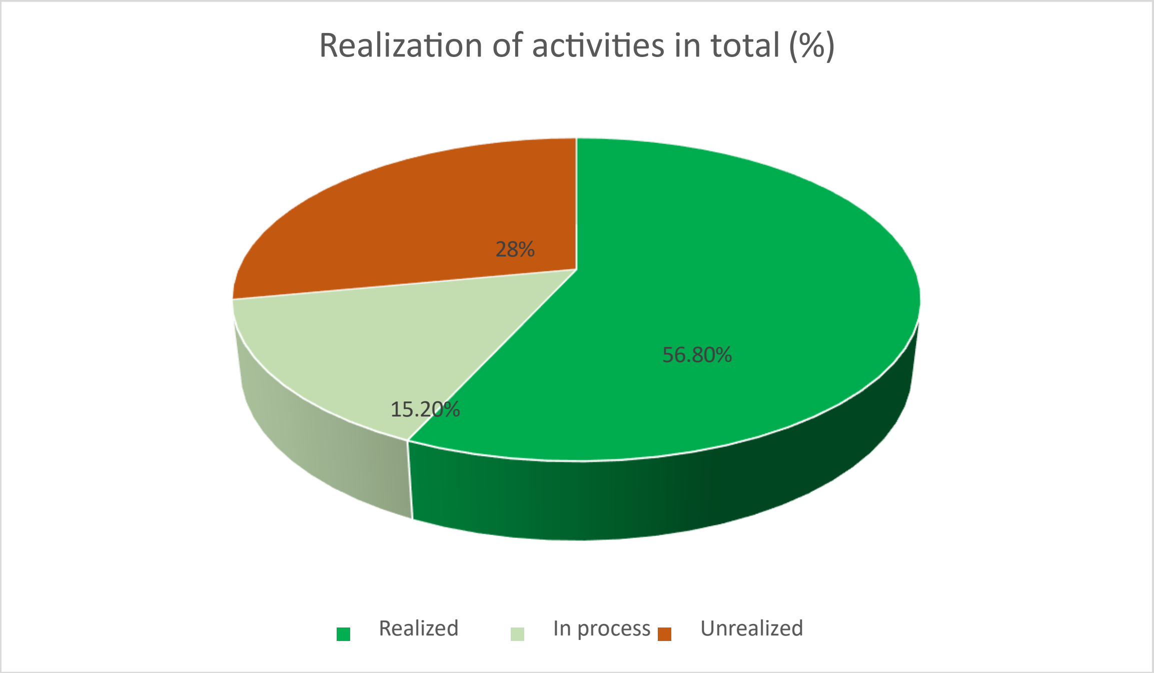
- applying the same basic values in the physical and digital world;
- protection of fundamental rights, freedom of expression, personal data and privacy;
- access for all;
- democratic and efficient governance;
- joint responsibility in guaranteeing cyber security.

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

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

The implementation of Action Plan's activities

As for the implementation of the Action Plan, it results that until 2022, the rate of realization of activities in % is: realized activities 56.8% (71 activities), activities in process 15.2% (19 activities) and unrealized activities 28% (35 activities). Based on these data, it is concluded that in terms of the results achieved and the activities implemented, there has been more progress in the realization of the purpose of Policy 1 and Policy 4.



2. MONITORING METHODOLOGY

The evaluation of the achievement of the objectives of the National Cyber Security Strategy 2020-2025 will be done periodically following the implementation of the plan of activities foreseen as well as the progress of the main monitoring indicators.

The analysis of this report is mainly based on the monitoring of the implementation of the activities foreseen in the action plan that includes the period January - December 2022.

Monitoring of the Strategy has consisted of the following main stages:

a) Reporting of institutions on the implementation of the Measures for which they are responsible, and

b) Monitoring measurable indicators for the National Cyber Security Strategy

To achieve the above, the analysis of the activities of the action plan according to each strategic priority was carried out in advance; the institutions responsible for their implementation have been identified; has been communicated in writing with each institution and continuously coordinated with the contact points for the reporting of the implementation status according to the methodology[1].

[1] *Note: The monitoring of the implementation of the activities of the Action Plan for 2022 is finalized on March 23, 2023 and continued with the drafting of the report. For the activities that were in process during 2022 and were realized at the beginning of 2023, before the ending of monitoring, information was provided about their realization, but they were not counted as realized activities in this report.*

3. STRATEGY POLICIES

The purpose of the policy 1. Guaranteeing cyber security at the national level, through the protection of information infrastructures, strengthening technological and legal tools.

Priority objectives focus on:

- Improving the legal framework that regulates the cybersecurity in the country, as well as its harmonization with the directives and regulations of the European Union.
- Establishment and operation of CSIRTs in all industry sectors at the national level
- Strengthening and implementing security measures in critical and important information infrastructures
- Improving information infrastructures to combat cybercrime, radicalization, and violent extremism.

For the realization of the objectives of the first strategic priority, the institutions involved in the realization of the Action Plan report as follows:

National Authority on Electronic Certification and Cyber Security (NAECCS)

NAECCS has worked intensively for the complete alignment of policies and legislation with the respective policies of the European Union, in accordance with the priorities and needs at the national level. Also, the policies of the Albanian government are in line with NATO's policies regarding cyber security. The authority, which also acts in the capacity of the National CSIRT, has drawn up and approved procedures for the operation and exercise of its activity. Although it was not approved in 2022, although all the preparatory work was done in this calendar year, it is worth mentioning that the new structure of NAECCS, which provided for the increase of the institution's employees from 24 to 85, was approved by the Prime Minister's Order no. 32, dated 16.03.2023.

The analysis of the legal and institutional gap for EU Directives and Regulations on cyber security has been carried out.

The draft law for the transposition of the European Regulation eIDAS "On electronic identification and trusted services for electronic transactions in the internal market" has been drafted and the public consultation process has been completed (date 07.12.2022 - 10.01.2023), the comments have been reflected and it is sent reworked to the Prime Minister to continue with further legal procedures.

Furthermore, NAECCS has completed the draft law "On cyber security", transposing Directive NIS 2016/1148 of the European Parliament " Concerning measures for a high common level of security of network and information systems across the Union " and including some elements from Directive NIS 2022/2555.

Pursuant to Law no. 2/2017 "On Cyber Security" and based on the European Directive of Networks and Information Systems 2016/1148, of the European Parliament " Concerning measures for a high common level of security of network and information systems across the Union ", the updated list of critical and important information infrastructures was approved with the Decision of the Council of Ministers no. 761, dated 12.12.2022 "On the approval of the list of critical information infrastructures and the list of important information infrastructures".

The Authority has approved procedures for reducing and managing risks in cyberspace, including the regulation on the content and manner of documenting security measures, Version 2.0, approved by Order No. 10, dated 14.02.2022. Also, the procedures, policies and plans for the protection of cyber space from cyber incidents have been drawn up and approved and in this context the Action Plan of the National Cyber Security Strategy 2020-2025 is in the process of revision since October 2022.

On 9.12.2022, Normative Act no. 18, "On some amendments and additions to law no. 9880, dated 25.2.2008, "On the electronic signature", amended, which brought such changes to make possible the necessary changes in the structure of the institution based on the functional activity and meeting the needs for qualified staff in a shorter time.

NAECCS is the coordinating institution in the Republic of Albania, which carries out the organization and interaction with the national security and defense institutions in the country, to participate in the cyber exercise Cyber Coalition of NATO. Cyber Coalition is NATO's main annual cyber defense exercise. The Cyber Coalition, which is held annually since 2008, brings together a cyber coalition of NATO bodies, NATO Allies, and partners to strengthen the Alliance's ability to deter and defend against threats in and through cyberspace in support of NATO's main tasks. Cyber Coalition training is executed through the Estonian Cybersecurity Training and Exercise Center, or 'CR14'. The training audience and local trainers participate from their respective Nations and entities through virtual networks and a group of participants gathers in Estonia to execute the exercise.

NAECCS has set up a Cyber Incident Reporting System. This system serves not only for the reporting of security incident events in the Operators of Important Information Infrastructures (*OIII*) and in the Operators of Critical Information Infrastructures (*OCII*), but also for reporting and information from NAECCS of possible vulnerabilities or attacks, together with the relevant recommendations for their prevention. This system is currently undergoing upgrade.

Currently, the reporting of incidents by OIII and OCII is increased, considering the increase in the number of cyber-attacks and the awareness of the need to report incidents for a better coordination at the national level.

NAECCS has cooperated with international partners such as: EATM CERT, CISA, Lithuanian Cyber Defense Center, Shadowserver, Arctic-Hub, Bitsight. Recommendations and identified vulnerabilities of ICT systems have been produced and published.

These update reports have been sent to OCII and OIII through the Incident Monitoring and Management System and through the institution's official e-mail for those operators who have encountered problems accessing the system.

NAECCS, in the capacity of the responsible institution for the implementation of the sub-objective on analyzing critical and important information infrastructures, carries out risk assessment and management in them. The procedure that is followed for the reduction and management of risks is to send to all Critical and Important Infrastructures a questionnaire which is posted on the official website of the Authority.

In the framework of the protection of cyberspace and the increase of the level of cybersecurity in critical infrastructures, NAECCS in implementation of law no. 2/2017 "On Cyber Security", has approved the "Regulation on the content and method of documenting security measures", mandatory to be implemented by the Critical and Important Information Infrastructures in the Republic of Albania by order no. 10, dated 14.02.2022. The Methodology for the Identification and Classification of Critical Infrastructures and Important Information Infrastructures has also been approved by order of the General Director no. 9, dated 14.02.2022.

NAECCS conducts self-assessment reports from Critical and Important Information Infrastructures for the level of Cyber Security maturity. In the framework of assessing the level of cyber security in critical and important information infrastructures, NAECCS, in fulfillment of its functional tasks, performs controls of critical and important information infrastructures for the implementation of minimum measures on information security. Controls of critical and important infrastructures are performed through the self-declaration and the onsite method.

In addition, the Authority has organized activities and trainings with the responsible teams near the operators of critical and important information infrastructures within the Authority's activity for the development and increase of the assessment and monitoring capacities of the sectorial CSIRTs.

NAECCS organized the in-depth training for "Cyber Incident Management", two days in a row on December 22-23, 2022, with all Critical Information Infrastructures divided by sector, in fulfillment of the objectives of the National Strategy for Cyber Security 2020-2025. The aim of the training was to increase the professional capacities needed for operators of critical infrastructures in Albania, as one of the Authority's main goals. Also, cyber exercises were organized with different scenarios based on best practices.

On December 21, 2022, the General Director of NAECCS, at the same time the National Coordinator for Cyber Security, held the meeting on the topic "Security of financial information, current priority of NAECCS", with the participation of the highest security leaders in the banking and financial sectors. The purpose of the meeting was to address the need to apply additional security measures for the protection and provision of citizens' financial information, as a focus of the Albanian government and a current priority of NAECCS.

The general director of NAECCS, following the meetings aimed at increasing the level of security and cooperation, held a meeting with the "health sector, microfinance and insurance companies" on December 7, 2022. The purpose of this meeting was to analyze the current situation of cyber security as well as to create opportunities for strengthening cooperation, for increasing security in critical infrastructures, within the framework of the implementation of the new strategy and vision for cyber security.

In the context of current developments in the field of cyber security, NAECCS on November 23, 2022, held the meeting on "Cyber security in the banking sector". This meeting was attended by the highest security managers in the banking sector.

On November 16, 2022, a meeting was held with high representatives from the defense and security institutions in the country. The purpose of this meeting was to increase institutional interaction to increase the level of cyber security in the country.

The National Authority on Electronic Certification and Cyber Security has been conducting continuous cyber exercises at the national level during 2022.

NAECCS in cooperation with the Geneva Center for Security Governance (DCAF), OSCE, Regional Cooperation Council (RCC), the American Chamber of Commerce in Albania, the Albanian Microfinance Association, and One Telecommunications organized on April 19-21, 2022, the innovative workshop "Regional Cyber Camp Albania". The purpose of this three-day workshop was to develop practical skills for cooperation and information exchange between CSIRTs, the State Police and other regional institutions responsible for cyber security, as well as to increase the capacities of young people on cyber security. During the 3 days of the workshop, about 100 young people and 50 professionals from Albania, Kosovo, Serbia, Bosnia and Herzegovina, North Macedonia and Montenegro, deepened their knowledge and exchanged the best national practices in the field of cyber security.

Additionally, NAECCS participated in the "CRDF Global Cross Cyber Drill" workshop on July 7-8, 2022, as well as in NATO's online activity for increasing capacities on the MISP platform.

National Authority on Classified Information Security (NACIS)

The Directorate for the Security of Classified Information (DCIS), has changed its name based on Article 63 of Law No. 10/2023, dated 02.02.2023 "On Classified Information", now being named as the National Authority on Classified Information Security (NACIS).

NACIS, called DCIS throughout the year 2022, for the development of defense in the field of cybercrime near their structure has recruited a new employee since 2021, who continues to be engaged in the systems where information classified as "state secret" is handled "based on Decision of Council of Ministers no. 542 dated 25.07.2019 "On the approval of the regulation "On the provision of classified information that is handled in the communication and information systems (SKI)". In the framework of the completion of the Cyber Defense structure set up in NACIS, during the year 2022 the procedure for filling vacancies in this sector was published twice on the official website of the Department of Public Administration and there were no interested candidates. NACIS, to attract expert candidates to these positions, has increased the salaries with an allowance for special nature of work. The procedure has been postponed again to December 2022.

NACIS has organized working meetings with its counterparts in Spain and Italy to obtain the best experiences related to testing procedures, evaluation of systems classified "State Secret" as well as cyber protection policies developed by these countries. NACIS personnel participated in the training organized by NAECCS, provided by Cyber Diplomacy Academy.

National Agency of Information Society (NAIS)

NAIS within Policy 1 of the National Cyber Security Strategy has achieved the following results:

• Optimization and expansion of security infrastructures and procedures for the operation of the governmental CSIRT.

Beyond the planning and commitments made in the National Cyber Security Strategy, the cyber-attack accelerated the unification transition to Microsoft security solutions by expanding the security infrastructure. These solutions were added to current ones such as Rapid7, Imperva, Bitsight etc.

The NAIS's Security Operations Center, now up and running, conducts 24/7 monitoring of governmental cyberspace and the Security Incident Response Sector handles incidents through Microsoft tools.

The transition has been completed by providing complete visibility over the infrastructure, monitoring, and control of all suspicious or malicious activities and a clear panorama on the correlation traces of threat actors who may be present or attempt to gain access to the government cyberspace.

Some of the tools that are used and have expanded security infrastructures are:

- Microsoft Sentinel - SIEM solution, correlates all activities generated by integrated logs and analyzes them through artificial intelligence and machine learning.

- Microsoft Defender for Endpoint - EDR/XDR solution, detects, prevents, and handles all incidents.

- Microsoft Defender for Identity - Solution which analyzes the behavior of users, identifying the anomalies they may present.

• Improvement of hardware structures and establishment of the access control system

The improvement of the hardware structures was realized by replacing the existing hardware firewall devices with new generation devices and higher technical parameters, as well as the establishment of the control system thanks to the implementation of the solution for remote access with MFA in GOV-NET.

• Conducting research to strengthen national priorities as a basis for the development of cyber security and analyzing the current capacities of the authorities.

The level of the cyber-attack and the threat actors, who tried to delete the government e-GOV systems and infrastructures, clearly showed that now, the challenges of the Albanian cyberspace are not only at the regional level, but also at the global level.

Analysis of current capacities, identification of gaps and conducting research to strengthen national cyber security priorities were conducted by various partners who assisted in the investigation and recovery from the cyber-attack.

Creating a cyber defense system includes threat response and mitigation, test center of malicious programs, staff training and monitoring of sensitive information.

The staff of the Monitoring and Cyber Defense Directorate for e-GOV Systems and Infrastructures have been and are in continuous training by Microsoft teams. Their support consists of risk analysis, vulnerability reduction and response to identified threats.

The "honeypot" system to draw attention from the real target of various attacks is implemented using the Rapid7 solution, and testing for malicious programs is performed in the Microsoft Defender for Endpoint console.

The monitoring of sensitive information on the Dark Web is carried out by the Incident Response Sector, which, through the indicators and traces of the threat actors they identify, analyzes whether they have a presence in the government network.

The Coordination Center for Countering Violent Extremism (CVE)

CVE is the responsible institution for the implementation of the sub-objective on the monitoring and prevention of phenomena that promote violent extremism and radicalization in vulnerable layers in cyberspace.

Within the framework of fulfilling the objectives of the strategy, CVE has organized sensitization campaigns in schools and with access to the community against radicalization and violent online extremism. CVE has coordinated the project "Support of CVE in the spread of strategic communication for the prevention and opposition of violent extremism through capacity building and research" in cooperation with the organization "Center for the Study of Democracy and Governance" (CSDG Albania) and with the support of the Embassy of the USA in Albania, has developed three trainings. In implementation of this project, in cooperation with representatives of the General Directorate of Prisons, the Ministry of Education and Sports (MES) and the Ministry of Health and Social Protection (MHSP), workshops were held to increase the capacities of the employees of the ministries who have in the field of action the prevention of violent extremism and strategic communication.

As part of this project, CVE has coordinated the work with the organization CSDG Albania for the development of training for the key personnel of institutions that are involved in the reintegration processes of citizens repatriated from conflict countries with a focus on the prevention of violent extremism and strategic communication.

CVE and CSDG Albania co-organized a workshop within the project "Strengthening of inter-institutional cooperation and strategic communication mechanisms in order to prevent/fight against violent extremism".

This workshop was attended by representatives from the Ministry of Interior and the Ministry of Justice, as well as teachers, psychologists, and social workers. Through this workshop, frontline workers have been equipped with the necessary knowledge to identify the early signs of radicalism that leads to violent extremism, increasing awareness for combating this phenomenon.

During the year 2022, the Albanian Public Radio Television (RTSH), with the coordination and cooperation of CVE, broadcast Episodes 4, 5, 6, 7, 8 and 9 of the cycle of reports carried out by the Active Media Center, on the evidence of cooperation against the phenomenon of violent extremism between Albanian state institutions, civil society, and religious communities.

During 2022, CVE coordinated and conducted two interviews with individuals returned from conflict areas, who are following rehabilitation/re-integration programs in the community, supported by CVE. CVE gave its contribution through an interview on the show "Education Auditor" on Albanian Radio Television (RTSH), where information was conveyed on the interventions carried out during these years by CVE in cooperation with the Ministry of Education and Sports (MES) in the pre-university system and university for the identification, prevention and opposition of violent extremism as well as related to the re-integration of children returned from conflict zones in school and community.

During October, CVE gave its contribution through an interview on the show "31 Minutes- Life after hell in Al Haul" on A2CNN television, during which the government's plans for the process of re-integration of mothers and children returned from conflict zones into school and community were discussed.

CVE has contributed to the trainings organized by IDM during 2022 in pre-university education schools with topics such as: Safe Internet, Cyber Bullying, Internet Safety, The Other Side of the Internet, and Safe Internet Day. The fight against violent extremism and radicalism in the online space and community by promoting the exchange of information and cooperation between partner institutions remains the focus of CVE.

State Police

The State Police has worked to strengthen and implement security measures in critical and important information infrastructures, as well as strengthening capacities for cybercrime investigation, undertaking several initiatives within the implementation of the National Cyber Security Strategy.

To strengthen capacities, to increase security parameters, DTI has forwarded to NAIS as the authority that will negotiate the agreement at the national level with Microsoft some requests for the implementation of systems such as: Microsoft Intune and Microsoft Sentinel. Investments from the state budget are foreseen in 2023 for projects within the framework of strengthening network security capacities, where we mention the following projects:

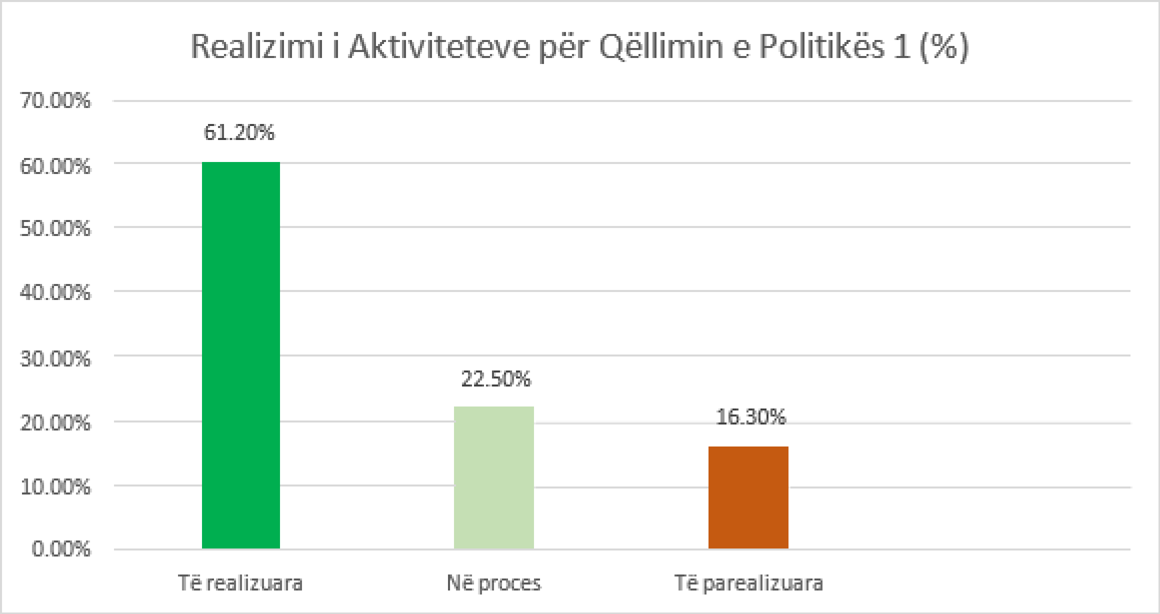
- Increasing cyber security in the Police infrastructure and

- Audit of IT systems for security.

Also, work has been done on the project "Elevation of the DRC infrastructure for State Police systems" with a 2-year financial commitment (2023-2024).

Realization of Activities for the Purpose of Policy 1

For Purpose of Policy 1, it results that until 2022, the rate of realization of activities is: activities realized 61.2% (30 activities), activities in process 22.5% (11 activities) and unrealized activities 16.3% (8 activities).



The purpose of policy 2. Building a safe cyber environment by educating and raising awareness of society in raising professional capacities in the field of information security.

Priority objectives focus on:

- Increasing professional capacities in the field of information security through the revision of educational curricula.
- Increasing awareness and professional skills of public and private institutions for cyber security
- Increasing society's awareness of cyber security and cyber threats.

For the realization of the objectives of the purpose of policy 2, the institutions involved in the realization of the AP report as follows:

National Authority on Electronic Certification and Cyber Security (NAECCS)

To raise awareness in different age groups of the society, for the use of safe internet and digital infrastructure NAECCS has conducted periodic trainings for the deepening of knowledge in cyber security, according to the newest development, for the administrative staff at the central and local level.

The National Authority on Electronic Certification and Cyber Security to increase the capacities of CSIRTs at the national level and the executive level of the public administration has organized cyber exercises such as "Regional Cyber Camp Albania" in April 2022. This activity enabled the development of the practical skills of the public administration employees who participated, such as the State Police, the Ministry of Education, the Ministry of Defense, the Commissioner for the Right to Information and the Protection of Personal Data, AKEP, etc. This activity was organized by NAECCS in cooperation with the Geneva Center for Security Sector Governance (DCAF), the Organization for Security and Cooperation in Europe (OSCE), the Regional Cooperation Council (RCC), the American Chamber of Commerce in Albania, the Albanian Microfinance Association, and the One Telecommunications company on April 19-21, 2022.

NAECCS, in the framework of increasing capacities, has organized a two-day training for deepening knowledge in cyber security on December 22-23, 2022, with all critical information infrastructures divided by sector, where employees from the public sector at the central level are also included. This activity fulfills several objectives of the strategy in the field of cyber security. To increase the capacities of the executive level of the public administration and not only, during this training, cyber training was developed for the participants.

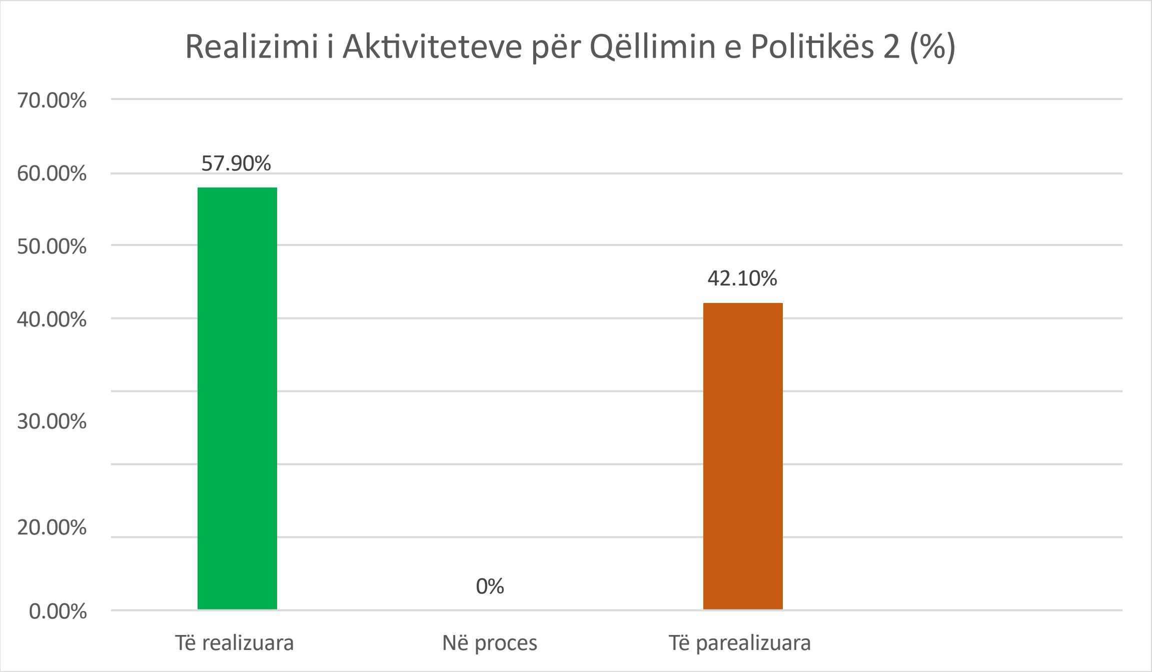
The authority has worked to increase society's awareness of cyber security, using the appropriate spaces for their realization, including audiovisual media and social media. In this line, awareness materials have been drafted and awareness campaigns have been organized.

Within the framework of the implementation of the Action Plan of the National Cyber Security Strategy 2020-2025, NAECCS has continued to organize awareness campaigns online and physically, with participants from public and private institutions, parents, teachers, young people and children in different districts of Albania. Also, the cyber security bulletin is published every month with news and the main events organized or developed by the Authority.

In September 2021, NAECCS committed to become the first pilot country in the world for the ITU2 Global Project. The project is planned to last until March 2023. In this context, an online educational platform for cyber security has been created, to increase awareness in different age groups of society, for the use of safe internet and digital infrastructure. On this page there are published joint initiatives in all relevant sectors to guarantee digital safety in the online environment for children and young people in Albania, as well as a series of activities developed and implemented within the framework of the Global Project, with the aim of act as a reference framework for other countries of the Europe Region that would be interested in becoming a beneficiary country for the implementation of Child Online Protection (COP) funded by the Global Project.

Realization of Activities for the Purpose of Policy 2

For the purpose of policy 2, it results that until 2022, the degree of realization of activities is: realized activities 57.9% (11 activities), and unrealized activities 42.1% (8 activities).



The purpose of policy 3. Designing of necessary mechanisms for the safety of children in cyberspace, while preparing the new generation benefitting from the advantages of information technology and facing the challenges of development.

Priority objectives focus on:

- Strengthening the legal framework for increasing the safety of children on the Internet.
- Preventing sexual abuse of children on the Internet by increasing awareness and creating safe spaces for surfing on the Internet.
- Effective investigation and prosecution of perpetrators of cybercrimes against children, with a focus on sexual abuse and exploitation.
- Raising awareness and educating all segments of society about the safe use of the Internet by children
- Strengthening cross-sectoral cooperation for the protection of children on the Internet.

For the realization of the objectives of the purpose of policy 3, the institutions involved in the realization of the AP report as follows:

Ministry of Education, Sports and Youth (MESY)

The Ministry of Education and Sports (MAS) has worked to strengthen the legal framework for increasing the safety of children online, especially in terms of online bullying and abuse, and protecting children from harmful content.

With the aim of protecting children online, questionnaires have been developed by the psycho-social service regarding the perception of bullying and violence at school by students, as well as informational materials have been distributed to students about online abuse and bullying in schools.

Of particular importance is the familiarization of students with the topic of cybercrime and its consequences, as well as ways to identify cyber risks. As part of the International Day of Internet Safety, awareness-raising video messages were developed by school senates, which were distributed on their official websites, as well as awareness-raising activities and exhibitions with awareness-raising paintings and posters. MAS has also carried out activities in schools on the topic "Using the Internet in a safe way" in order to learn about the consequences of giving the passwords of their addresses to third parties, as well as the different forms of emotional, psychological, cyber and sexual violence .

Throughout 2022, the training of ICT network leaders and network members continued. During this period, the training of ICT teachers was carried out related to various topics on the work and organization of professional networks, including the use of ICT in the implementation of the curriculum and student assessment. Also, the trainings aimed at the professional development of ICT teachers for the use of online platforms in a safe and efficient way in the learning process have continued. In the framework of the implementation of the cooperation project between the Quality Assurance Agency of Pre-university Education and the Albanian Institute of Media, about 250 teachers of the cycle of Lower Secondary Education (AMU) and Higher Secondary Education (AML) have been trained, regarding with media and information education. In addition to the knowledge gained about the world of media and information, important issues related to challenges and risks in the virtual world were discussed.

Teachers are familiar with codes of conduct, privacy rules and some of the main risks that can be encountered when using the Internet. Teachers are encouraged to use basic teaching methods and tools to help students use the Internet responsibly and safely, and make them aware of the challenges and risks that come with using it. Communication groups have been created on different platforms where at least once a month live or online meetings are organized, where teachers discuss, share experience and assess needs.

The psycho-social service and the school directorates have held information sessions for the recognition and publication of the column "Report illegal content", which is connected to the online portal of NAECCS[2], for closing access to internet pages with illegal content, which helps children, persons exercising parental responsibility and young people to report illegal content encountered while surfing the Internet.

MES monitors the application of the designed methodology with practical activities with students of classes V-IX and X-XII, for protective measures and cyber security. Through the schools, practical activities were also developed with the students on protective measures and cyber security. These activities include discussion of experiences with staff and groups of students, creation of posters and essays by students themselves about cyber risks and online security, and implementation of projects in this field in the educational institutions of AMU[3] and AML[4], as well as by cooperating organizations/associations. with MES.

In order to identify, support and promote talents to create technical solutions that help in online protection and security, MES has developed competitions, projects on the topic "Internet Security", the National Olympiad in the subject of ICT with AML students , and other extra activities for students who show inclination in ICT.

MES in cooperation with NAECCS have implemented the application of filters in public and private schools to prevent children's access to inappropriate and illegal sites, as well as the subsequent informing of ICT teachers about reporting incidents. Also, the "Report illegal content" column has been put into operation on the official website of MAS, DPAP, DRAPs, ZVAPs and IAPs, which is linked to the online portal www.cesk.gov.al of NAECCS , to block access to websites with illegal content, which helps children, persons exercising parental

[2] www.cesk.gov.al

[3] Abbreviation for Lower Secondary Education

[4] Abbreviation for Higher Secondary Education

responsibility and young people to report illegal content encountered while browsing the Internet.

National Authority on Electronic Certification and Cyber Security (NAECCS)

NAECCS has coordinated the work for the realization of the activities within the joint project with UNICEF Albania "Development of the necessary mechanisms for the internet safety of children and young people in Albania" during February - September 2022.

The results of this project are:

- ✓ 6 documents drafted in the form of inter-institutional protocol, guide, analytical report
- ✓ 518 trained parents and teachers in 12 units / cities of Albania: Babrru, Vorë, Kavajë, Dibër, Klos, Kukës, Has, Laknas, Burrel, Bulqizë, Fushë Arrëz, Pukë, Vau Dejës, Shkodër, Tropojë, Kamëz and Paskuqan.
- ✓ An awareness manual drafted for parents and teachers, containing advice on protecting children online, with a focus on online trafficking.

The drafted documents are:

- Report on the analysis and identification of illegal content reporting mechanisms.

- Inter-institutional protocol for cooperation between law enforcement agencies, internet service providers and NAECCS.

- Report on the analysis and identification of the legal gap in the protection of children online from sexual abuse, including the necessary recommendations.

- Report on the analysis of the technical functionalities of the Portal for Blocking Pages with Illegal Content, along with recommendations for improving the functionalities in order to increase efficiency.

- Report on the analysis of existing initiatives of Internet Service Providers for the protection of children on the Internet.

- Guidance on the integration of the Internet Watch Foundation Hash List into the services of Internet Service Providers.

Additionally, NAECCS has coordinated the work for the implementation of activities within the piloting of the global project with the International Telecommunication Union (ITU) "Creating a safe and empowering digital environment for children" for the period January-December 2022.

The results of this project are:

- ✓ Drafting of 2 awareness manuals:

    o Child-friendly manual – dedicated to the protection of children on the Internet o Train of Trainers (ToT) Manual – dedicated to parents, to increase children's safety

✓ 37 trainings for children and young people, parents and teachers, industry representatives
o 12 trainings for children and young people
o 15 trainings for parents and teachers
o 10 trainings for industry representatives

✓ 750 training participants
o 190 children and young people
o 460 parents and teachers
o 100 industry representatives

✓ 1 unified message published in physical stores and social media of Internet Service Providers.
✓ 1 poster with advice from the ITU Guidelines.

Within the framework of the implementation of the Action Plan of the National Cyber Security Strategy 2020-2025, NAECCS has continued to organize awareness campaigns online and physically, with participants from public and private institutions, parents, teachers and young people and children, in circles of various of Albania.

The trainings carried out included the following group:

- Child Protection Units in the district of Tirana, Dibra, Shkodra and Kukës

- Internet Service Providers that operate in the Republic of Albania

- 4,500 unique online users in the online awareness campaign.

As part of Cyber Security Awareness Month, from October 19 to November 2, 2022, NAECCS held meetings with children, parents, teachers, psychologists and social workers in schools to increase community awareness of cyber threats. The information sessions, held in Korçë, Pogradec, Shkodër Malësi e Madhe, Rrëshen and Lezhë, also aimed to help young people protect themselves online, while threats to technology and personal data become more and more common. NAECCS organized these information sessions in partnership with the OSCE Presence in Albania.

During the year 2022, in implementation of the communication plan of the sector, the realization and publication on the social networks of the National Authority for Electronic Certification and Cyber Security of three promotional videos for the awareness of the community for increasing the level of cyber security, which have achieved more than 6000 views on social media (the following videos can be accessed by clicking on the corresponding youtube links).

- Video "**Safety of children on the Internet"**

- Video **"Advice for parents and educators on children's safety on the Internet"**

- Video **"Instructions for the child protection industry on the Internet"**

Based on the analysis of the current situation of ICT and cyber security, news and articles are periodically published on the official social media communication channels of the Authority. Here we can also mention the "Cyber Security News Bulletin" publications from January 2022, every month, until December 2022.

Ministry of Health and Social Protection (MHSP)

MHSP coordinates and monitors the National Agenda for Children's Rights 2021-2026 approved by VKM No. 659, dated 3.11.2021, a strategic document of a cross-sectoral nature that includes goals, objectives and measures, which aim to engage all public and non-public actors to effectively and fairly provide the highest quality services for children. At the same time, this is done by following child-friendly principles and standards, with the aim of education in the function of protecting children online, thus guaranteeing the well-being and a better future for children.

In the framework of the protection of children from all forms of violence, as one of the main pillars of this Agenda, objectives related to specialized and integrated mechanisms and services for addressing severe forms of violence, including sexual abuse, have been foreseen and online abuse and exploitation. A special chapter is the "Strategic goal for the promotion of children's rights in the digital world", which includes ensuring access and inclusion of children in the digital environment in full compliance with objective 5 of the European Union Strategy for Children's Rights. Learning and creativity in the digital environment through the development of digital competences through ICT has been seen as a priority and important goal for children, evaluating as important in this process the highest interest of the child, by all institutions that contribute to the digital environment.

The State Agency for Children's Rights and Protection (ASHDMF) monitors and is in permanent contact with child protection structures throughout the country, providing technical support for case management, coordinating institutional interventions for the protection of each case of violated, abused or neglected children, to ensure that the children receive the necessary services and specialized psychological treatment.

Cases of violence and abuse of children on social media and websites are reported to ASHDMF through the Alo116 111 Advice Line and the isigurt.al platform. These pages are then reported by ASHDMF to the portal administered by the National Authority for Electronic Certification and Cyber Security (AKCESK). For the year 2022, 6 web pages with inappropriate content for children were reported near the AKCESK portal.

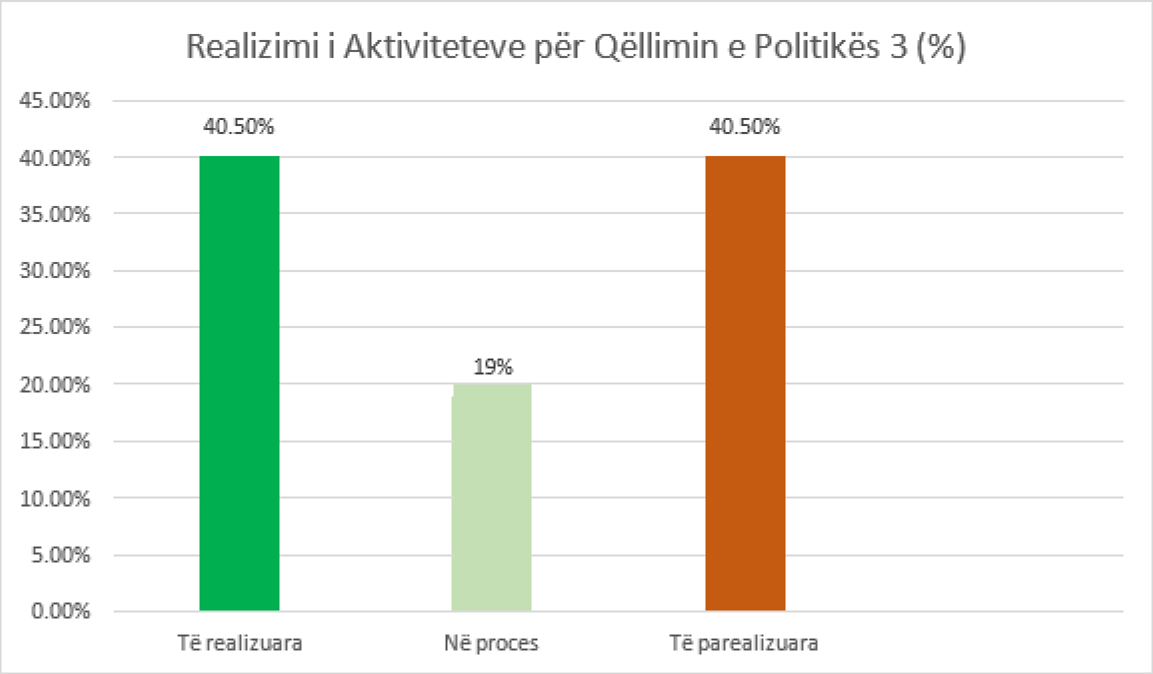
MSHMS supports the National Advice Line ALO 116 111, which offers psychosocial counseling for cases of online abuse or bullying, and has referred cases to the bodies responsible for their treatment. For the cases handled in the period January-December 2022, we have a number of 28,812 phone calls, which include cases of children in need of protection, of which counseling was given for 1727 cases, as well as 439 cases were referred to public institutions for treatment. In relation to online security, 50 cases have been reported.

MHSP in cooperation with NAECCS in the framework of the implementation of the activities of the National Cyber Security Strategy 2020-2025 and the National Agenda for Children's Rights 2021-2026, has carried out trainings related to the safety of children in the cyber environment. Currently, workshops have been held with the participation of 31 child protection workers and other actors at the local level in the municipalities of Tirana, Kavajë, Kamëz, Vorë and Rrogozhinë.

In the month of February every year, awareness raising activities are organized within the framework of "Safer Internet Day". In this context, in 2022, an awareness-raising activity was organized with students from 9-year and secondary schools, parents and teachers, invited to the COD Center in the Prime Minister. At the same time, ASHDMF in cooperation with child protection workers has organized awareness meetings in the framework of child protection in the digital environment in various schools in the municipalities of Tirana, Durrës, Bulqizë, Kukës, Fier and Burrel.

Realization of Activities for the Purpose of Policy 3

For Policy Goal 3, it results that until 2022, the degree of realization of activities is: realized activities 40.5% (17 activities), activities in process 19% (8 activities) and unrealized activities 40.5% (17 activities).



The purpose of policy 4. Increasing national and international cooperation with strategic partners in the field of cyber security.

Priority objectives focus on:

- ➢ Strengthening institutional cooperation at the national level
- ➢ Strengthening international cooperation in cyber security and defense and the fight against violent extremism and radicalization

For the realization of the objectives of the purpose of policy 4, the institutions involved in the realization of the AP report as follows:

National Authority on Electronic Certification and Cyber Security (NAECCS)

NAECCS within the framework of growth, cooperation and coordination between state institutions to guarantee security at the national level in cyber space has drawn up and signed inter-institutional agreements thus creating a network of contact points. The agreements we can mention are:

- Memorandum of Understanding with the Audiovisual Media Authority
- Memorandum of Understanding with the Cyber Security Policy Institute
- Memorandum of Understanding with 4Ig (signed on January 2023)
- Memorandum of Understanding with Raiffeisen Bank Albania
- Memorandum of Understanding with CERT-Romania to be renewed (process started in 2022, to be signed in 2023)
- Memorandum of Understanding with the Association of Banks in Albania (process started in 2022, signed in early 2023)
- Memorandum of Understanding with National Cyber Directorate of the State of Israel (process started in 2022, to be signed in early 2023)
- Memorandum of Understanding with CSIRT Italy (process started in 2022, to be signed in early 2023)

Meetings and trainings at local and regional level have contributed as a communication bridge for cooperation and confidence building with other public and private CERT and CSIRT teams, and academic communities. Experts in the field of cyber security have worked to create an instrument for the exchange of information through contact points dedicated by the relevant institutions, in cases of cyber threats.

In order to carry out the exchange of information, knowledge and experience in the public sector, defense and cyber security institutions and the private sector, NAECCS has taken several steps in order to ensure safe communication routes.

One of the steps taken by NAECCS is the improvement and further development of existing mechanisms such as the Incident Reporting Management System, a system established in 2019, which serves to report incidents that occurred in critical and important infrastructures of information, the continuous communication between the National CSIRT and the infrastructures for the reports of the attacks that have occurred and their analysis, produced by the responsible team of the National CSIRT. Also, this system communicates with infrastructures related to vulnerabilities and confidential information that may affect information infrastructures at the national and international level. The Incident Reporting Management 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. Currently, a platform has been set up at the National CSIRT, which will continue to interact directly with critical information infrastructures.

NAECCS, within the framework of strengthening international cooperation in the field of security and cyber protection and the fight against violent extremism and radicalization, has had active participation in NATO meetings for the implementation of international standards and regulations in the framework of cyber security.

NAECCS also has an important role in strengthening cooperation and information exchange with NATO, OSCE and other international organizations/forums.

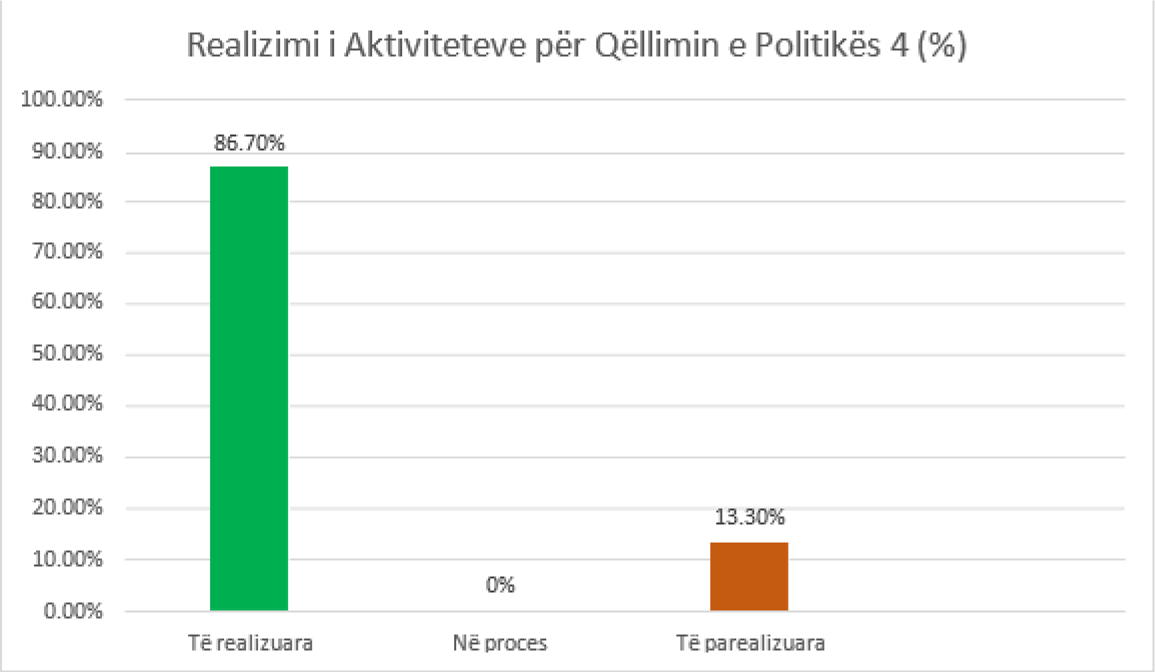
Due to its interaction and cooperation with NATO, NAECCS has managed to be part of and use the NATO-MISP platform, made available by NATO for Albania, which interacts with international organizations for reporting incidents and Indicators of Compromise, occurring in information infrastructures at the global level. This makes it possible for NAECCS, in the role of the National CSIRT, to inform and raise awareness in real time of the information infrastructures about the incidents that have occurred and reported.

The National Authority on Electronic Certification and Cyber Security has joined various international activities and initiatives in the field of cyber security (such as First, Trust Introducer).

In addition, the cooperation of all relevant actors in the process of development and unification of security norms, 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.

Realization of Activities for the Purpose of Policy 4

For the purpose of policy 4, it results that until 2022, the rate of realized activities is 86.7% (13 activities), and unrealized activities is 13.3% (2 activities).



4. THE PASSAPORT OF INDICATORS

The purpose of the "Passport" of the following indicators is to provide a detailed methodological description of the measurement for all the Indicators of the Result level that are included in the National Cyber Security Strategy 2020-2025.

The document covers only so-called Result (or Performance) level indicators, those that have been developed to measure progress against the defined objectives of the Strategy.

For each indicator, the following elements are included:

- The source of information (data), which serves as a basis for measuring the indicator;

- The institution responsible for gathering data for measuring the indicator (and providing information for reporting / monitoring purposes). This specific responsibility also includes responsibility for the validity / quality of the data;

- Frequency of data publication (and/or data gathering);

- A methodological description of the measurement method, allowing for an external control and better understanding of how certain values of the indicators have developed;

- Core and target values

The information included in the Passport of the indicators below, which is found in ANNEX 1, has been developed in full cooperation with the responsible institutions, based on the information provided by the responsible institutions, and their wording has the full consent of all the responsible institutions.

List of indicators:

1. Legislation aligned with EU Directives and Regulations in cyber security
2. Establishment and operation of CSIRTs in all industry sectors at the national level
3. Raising the capacities of professionals in the field
4. Cyber security awareness campaign
5. Completed legal framework (for children's online safety)
6. Trained children aware in the use of online materials
7. Strengthening cooperation at the national level to ensure cyber security in the country
8. International cooperation

5. RECOMMENDATIONS

- ✓ Improving the regulatory framework for cyber security aligned with the EU acquis, to address issues and resolve them including, but not limited to: Cloud computing, IoT, 5G technology, Artificial IntelligenceDrafting of the procedure for the management of cyber crises.
- ✓ Drafting and approval of the regulation for providing secure internet in public spaces
- ✓ Determining a national procedure for emergency situations designed by cyber crises, with the aim of taking concrete measures to resolve the situation in real time
- ✓ Drafting and approval of the methodology for risk assessment at the national level
- ✓ Creating optimal working conditions for the operation of CSIRTs, to facilitate the fulfillment of their tasks effectively, in order to guarantee cyber security in critical and important information infrastructures
- ✓ Development and implementation of study programs in higher education in the field of cyber security, with the aim of growing a new generation of cyber security experts
- ✓ Raising the capacities of the responsible authorities against cybercrime.
- ✓ Establishing a research-scientific center in the field of cyber security and participating in national and international research projects and activities related to cyber security.
- ✓ Increase and support research capacities and business innovations by promoting the establishment of scientific research centers in the field of cyber security
- ✓ Drafting of a special instruction and accompanying regulation for data collection of reported incidents of violence, bullying and online abuse of children in schools.
- ✓ Finalization of training programs for judicial, prosecutorial and police personnel in relation to child protection on the Internet and cyber security, including mutual legal assistance
- ✓ Setting up a system of courses at the School of Magistracy and Security Academy regarding issues related to crimes against children online and ways to protect them online.

- ✓ Setting up a flexible structure with the best cyber security experts, in order to support in cases of cyber crises, testing and evaluating the level of cyber security at the national level
- ✓ Review of the Action Plan of the National Cyber Security Strategy, ensuring the continuous involvement of stakeholders
- ✓ Strengthening and promoting cross-sector cooperation in cyber security to ensure full implementation of cyber security programs
- ✓ Continuing with the organization of periodic trainings for the employees of NAECCS and Critical Infrastructures
- ✓ Improving the national cyber incident response escalation procedure detailing coordination with Critical and Important Information Infrastructures.
- ✓ Realization of ENISA's Critical and Important Information Infrastructure Maturity Self-Assessment Survey based on the SIM3 model to gain further knowledge on NAECCS's maturity and capabilities.

ANEX 1

Indicator no. 2

Name of the indicator	**Legislation aligned with EU Directives and Regulations in cybersecurity**
Type of indicator	Score indicator
No, Dt, Name of the document	“National Cybersecurity Strategy 2020-2025”
Relation with NSDI[5] (No. of pilar)	Pilar no. 2 Good governance, democracy and rule of law
Purpose/Strategic Goal of NSDI	Strategic Goal of NSDI: "Consolidation of social protection"
The purpose of the corresponding policy	“Guaranteeing cyber security at the national level, through the protection of information infrastructures, strengthening technological and legal tools"
The Specific Objective to which the indicator/indicator is related	Improving the regulatory framework for cyber security aligned with sectoral laws to properly address and resolve issues including but not limited to: Cloud computing, IoT, 5G technology, Artificial Intelligence
Relevance of the Indicator	Policy Framework
Link to Acquis Communautaire	NIS Directive 2016
Data source for performance monitoring indicator	Acts approved by the Council of Ministers
Institutions responsible for data collection	NAECCS
	NAIS / Ministry of Interior / etc
Description of the Methodology	1) The strategic regulatory framework drawn up versus the approved regulatory framework 2) The implemented strategic framework, the average level of the implementation report

[5] Abbreviation for National Strategy

Measurement Frequency	Annual	
Nature of Indicator: Cumulative/Incremental	Cumulative	
Direct or Composite Input	Composite	
Calculation formula	1) Planned framework versus the approved strategic framework 2) average report of the individual reports of the implementation of each strategic document, through the monitoring of the relevant action plan.	
Data sharing (for composite indicators)	First level	
	Second level	
	Third level	
Emphasize the direction of change / trend (tendency) of progress	Cumulative	
Core Values	2019	
	1 policy document and 1 law	
Target value/Target	2020	1 Decision of Council of Ministers
	2021	1 Law
	2022	2 draft laws
	2023	
	2024	
	2025	full alignment
Target Value/Revised Target	2025	100%
Current Base Value:		
SDG - Title of the Sustainable	N/A	N/A

Development Goal according to the UN		
Target value of the SDG indicator	N/A	N/A

Indicator no. 2

Name of the indicator	**Establishment and operation of CSIRTs in all industry sectors at national level**
Type of indicator	Score indicator
No, Dt, Name of the document	“National Cybersecurity Strategy 2020-2025”
Relation with NSDI (No. of pilar)	Pilar no. 2 Good governance, democracy and rule of law
Purpose/Strategic Goal of NSDI	Strategic Goal of NSDI: "Consolidation of social protection"
The purpose of the corresponding policy	"Guaranteeing cyber security at the national level, through the protection of information infrastructures, strengthening technological and legal tools"
The Specific Objective to which the indicator is related	Establishment and operation of CSIRTs in all industry sectors at national level
Relevance of the Indicator	Implementation measures
Relation with Acquis Communautaire	NIS directive 2016
Data source for performance monitoring indicator	Annual evaluation reports
Institutions responsible for data collection	NAECCS
	Sectorial CSIRTs/ Government institutions

Description of the Methodology	According to the NAECCS’s regulation on control	
Measurement Frequency	Annual	
Nature of Indicator: Cumulative/Increasing	Increasing	
Direct or Composite Input	Direct	
Calculation formula		
Data sharing (for composite indicators)	First level	
	Second level	
	Third level	
Emphasize the direction of change / trend (tendency) of progress	Increasing	
Core Values	Statistics are missing	
Target value/Target	2021-	1- national operational CSIRT
	2022-	Sectorial CSIRT
	2023-	
	2024-	
	2025-	CSIRTs up and running
Target Value/Revised Target	2025	100%
Current Base Value:		
SDG - Title of the Sustainable Development Goal according to the UN	N/A	N/A
Target value of the SDG indicator	N/A	N/A

Indicator no. 3

Name of the indicator	**Raising the capacities of professionals in the field**
Type of indicator	Score indicator
No, Dt, Name of the document	“National Cybersecurity Strategy 2020-2025”
Relation with NSDI (No. of pilar)	Pilar no. 5 INVESTMENT IN HUMAN CAPITAL AND SOCIAL COHESION
Purpose/Strategic Goal of NSDI	Strategic Goal of NSDI: "Consolidation of social protection"
The purpose of the corresponding policy	"Building a safe cyber environment by educating and raising awareness of society in raising professional capacities in the field of information security"
The Specific Objective to which the indicator is related	Increasing professional capacities in the field of information security through the revision of educational curricula
Relevance of the Indicator	Implementation measures
Relation with Acquis Communautaire	NIS directive 2016/Law 2/2017
Data source for performance monitoring indicator	Annual evaluation reports
Institutions responsible for data collection	NAECCS
	Sectorial CSIRTs/ Government institutions
Description of the Methodology	Reporting based on annual monitoring
Measurement Frequency	Annual
Nature of Indicator: Cumulative/Increasing	Increasing

Direct or Composite Input	Direct	
Calculation formula		
Data sharing (for composite indicators)	No. of curricula	
	No. of Courses	
	No. of trainees	
Emphasize the direction of change / trend (tendency) of progress	Increasing	
Core Values		
Target value/Target	2021-	25 trained professionals in the financial sector and 20 professionals in the health sector
	2022-	66 professionals from critical infrastructure operators in Albania and 50 professionals from Albanian and regional public institutions
	2023-	
	2024-	
	2025-	
Target Value/Revised Target		
Current Base Value:		
SDG - Title of the Sustainable Development Goal according to the UN	N/A	N/A
Target value of the SDG indicator	N/A	N/A

Indicator no. 4

Name of the indicator	**Cyber Security Awareness Campaign**
Type of indicator	Score indicator
No, Dt, Name of the document	“National Cybersecurity Strategy 2020-2025”
Relation with NSDI (No. of pilar)	Pilar no. 2 Good governance, democracy and rule of law
Purpose/Strategic Goal of NSDI	Strategic Goal of NSDI: "Consolidation of social protection"
The purpose of the corresponding policy	"Building a safe cyber environment by educating and raising awareness of society in raising professional capacities in the field of information security"
The Specific Objective to which the indicator is related	Increasing society's awareness of cyber security and cyber threats.
Relevance of the Indicator	Implementation measures
Relation with Acquis Communautaire	NIS directive 2016/Law 2/2017
Data source for performance monitoring indicator	Annual evaluation reports
Institutions responsible for data collection	NAECCS
Description of the Methodology	Reporting based on annual monitoring
Measurement Frequency	Annual

Nature of Indicator: Cumulative/Increasing	Cumulative	
Direct or Composite Input	Direct	
Calculation formula		
Data sharing (for composite indicators)	No. of curricula	
	No. of Courses	
	No. of trainees	
Emphasize the direction of change / trend (tendency) of progress	Increasing	
Core Values	Statistics are missing	
Target value/Target	2020-	1
	2021-	1
	2022-	1
	2023-	1
	2024-	1
	2025-	
Target Value/Revised Target:		
Current Base Value:		
SDG - Title of the Sustainable Development Goal according to the UN	N/A	N/A
Target value of the SDG indicator	N/A	N/A

Indicator no.5

Name of the indicator	**Completed legal framework (for children' online safety)**
Type of indicator	Score indicator
No, Dt, Name of the document	“National Cybersecurity Strategy 2020-2025”
Relation with NSDI (No. of pilar)	Pilar no. 2 Good governance, democracy and rule of law
Purpose/Strategic Goal of NSDI	Strategic Goal of NSDI: "Consolidation of social protection"
The purpose of the corresponding policy	"Creating the necessary mechanisms for the safety of children in cyberspace, while preparing the new generation capable of taking advantage of information technology and facing the challenges of development"
The Specific Objective to which the indicator is related	Strengthening the legal framework for increasing the safety of children on the Internet.
Relevance of the Indicator	Policy framework
Relation with Acquis Communautaire	
Data source for performance monitoring indicator	Annual evaluation reports
Institutions responsible for data collection	UNICEF
Description of the Methodology	Reporting based on annual monitoring
Measurement Frequency	Annual

Nature of Indicator: Cumulative/Increasing	Cumulative	
Direct or Composite Input	Composite	
Calculation formula		
Data sharing (for composite indicators)	Revised legal acts	
	Approved regulation	
	Methodology	
Emphasize the direction of change / trend (tendency) of progress	Increasing	
Core Values		
Target Value/ Target:	2020-	10%
	2021-	
	2022-	50%
	2023-	
	2024-	
	2025-	100%
Target Value/Revised Target:		
Current Base Value:		
SDG - Title of the Sustainable Development Goal according to the UN	N/A	N/A
Target value of the SDG indicator	N/A	N/A

Indicator no. 6

Name of the indicator	**Aware trained children in the use of online materials**
Type of indicator	Score indicator
No, Dt, Name of the document	“National Cybersecurity Strategy 2020-2025”
Relation with NSDI (No. of pilar)	Pilar no. 5 INVESTMENT IN HUMAN CAPITAL AND SOCIAL COHESION
Purpose/Strategic Goal of NSDI	Strategic Goal of NSDI: "Consolidation of social protection"
The purpose of the corresponding policy	"Creating the necessary mechanisms for the safety of children in cyberspace, while preparing the new generation capable of taking advantage of information technology and facing the challenges of development"
The Specific Objective to which the indicator is related	Raising awareness and educating all segments of society about the safe use of the Internet by children
Relevance of the Indicator	Implementation measures
Relation with Acquis Communautaire	
Data source for performance monitoring indicator	Annual evaluation reports
Institutions responsible for data collection	UNICEF
Description of the Methodology	Reporting based on annual monitoring
Measurement Frequency	Annual
Nature of Indicator: Cumulative/Increasing	Cumulative
Direct or Composite Input	Direct

Calculation formula		
Data sharing (for composite indicators)	Trained students	
	Trained teachers	
	Trained magistrates	
Emphasize the direction of change / trend (tendency) of progress	Increasing	
Core Values	2019	
	13000 trained students	
Target Value/ Target:	2020-	1200
	2021-	1600
	2022-	2000
	2023-	2400
	2024-	2600
	2025-	3000
Target Value/Revised Target:		
Current Base Value:	2022	2000
SDG - Title of the Sustainable Development Goal according to the UN	N/A	N/A
Target value of the SDG indicator	N/A	N/A

Indicator no. 7

Name of the indicator	**Strengthening cooperation at the national level to guarantee cyber security in the country.**
Type of indicator	Score indicator
No, Dt, Name of the document	“National Cybersecurity Strategy 2020-2025”
Relation with NSDI (No. of pilar)	Pilar no. 2 Good governance, democracy and rule of law
Purpose/Strategic Goal of NSDI	Strategic Goal of NSDI: "Consolidation of social protection"
The purpose of the corresponding policy	" Increasing national and international cooperation with strategic partners in the field of cyber security "
The Specific Objective to which the indicator is related	Strengthening institutional cooperation at the national level
Relevance of the Indicator	Implementation measures
Relation with Acquis Communautaire	NIS directive
Data source for performance monitoring indicator	Annual evaluation reports
Institutions responsible for data collection	NAECCS
Description of the Methodology	Reporting based on annual monitoring
Measurement Frequency	Annual
Nature of Indicator: Cumulative/Increasing	Cumulative
Direct or Composite Input	Direct
Calculation formula	
Data sharing (for composite indicators)	

Emphasize the direction of change / trend (tendency) of progress	Cumulative	
Core Values	2019	
	2	
Target Value/ Target:	2020-	1
	2021-	1
	2022-	1
	2023-	1
	2024-	1
	2025-	1
Target Value/Revised Target:		
Current Base Value:	2022	2
SDG - Title of the Sustainable Development Goal according to the UN	N/A	N/A
Target value of the SDG indicator	N/A	N/A

Indicator no. 8

Name of the indicator	**International cooperation**
Type of indicator	Score indicator
No, Dt, Name of the document	"National Cybersecurity Strategy 2020-2025"
Relation with NSDI (No. of pilar)	Pilar no. 1 EU Membership

Purpose/Strategic Goal of NSDI	Strategic Goal of NSDI: "Consolidation of social protection"	
The purpose of the corresponding policy	" Increasing national and international cooperation with strategic partners in the field of cyber security "	
The Specific Objective to which the indicator is related	Strengthening international cooperation in the field of cyber security and defense and the fight against violent extremism and radicalization.	
Relevance of the Indicator	Implementation measures	
Relation with Acquis Communautaire	NIS directive	
Data source for performance monitoring indicator	Annual evaluation reports	
Institutions responsible for data collection	NAECCS	
Description of the Methodology	Reporting based on annual monitoring	
Measurement Frequency	Annual	
Nature of Indicator: Cumulative/Increasing	Cumulative	
Direct or Composite Input	Direct	
Calculation formula		
Data sharing (for composite indicators)		
Emphasize the direction of change / trend (tendency) of progress	Cumulative	
Core Values	2019	2
Target Value/ Target:	2020-	4
	2021-	5
	2022-	6
	2023-	7
	2024-	8

	2025-	9
Target Value/Revised Target:		
Current Base Value:	2022	1
SDG - Title of the Sustainable Development Goal according to the UN	N/A	N/A
Target value of the SDG indicator	N/A	N/A