NAECCS

NATIONAL AUTHORITY ON
ELECTRONIC CERTIFICATION
AND CYBER SECURITY

Monitoring of “National Cybersecurity Strategy 2020-2025”

Tirana, 2022

Table of Contents

1. INTRODUCTION……………………………………………………………..….3
2. MONITORING METHODOLOGY………………………………………...…5
3. STRATEGY POLICIES…………………………………………………………..6

   The purpose of policy 1. Guaranteeing cyber security at the national level, through the protection of information infrastructures, strengthening technological and legal tools..5

   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………………………………………………………………………. 14

   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…………………16

   The purpose of policy 4. Increasing national and international cooperation with strategic partners in the field of cyber security …………………………………………… ….22
4. THE PASSPORT OF INDICATORS……………………………...……….24
5. RECOMMENDATIONS…………………………………………………….…..25

ANEX 1…………………………………………………………………………...…27

1. INTRODUCTION

A free cyberspace makes possible communication between countries, communities, and citizens in the exchange of information worldwide. Recent developments in information and communication technology bring great benefits to the community and citizens as real-time information sharing is considered very important. All these developments along with the benefits also bring threats in different fields. In this perspective, cyber defense and security are considered the challenge of the future.

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 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 and 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:

- 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.

This is the first monitoring report, and it was prepared based on the reports made by the implementing institutions during the first year of the implementation of the strategy. The monitoring report aims to evaluate the progress of the implementation of this strategy according to the 4 policy goals and respective objectives for the period January - December 2021.

The Action Plan of the National Cyber Security Strategy 2020-2025 includes a total of 125 basic activities to be implemented throughout the years of implementation of the Strategy. 52% of these (65 activities) were fully realized during the first year 2021, while 42 % (52 activities) are expected to start during 2022 and beyond.

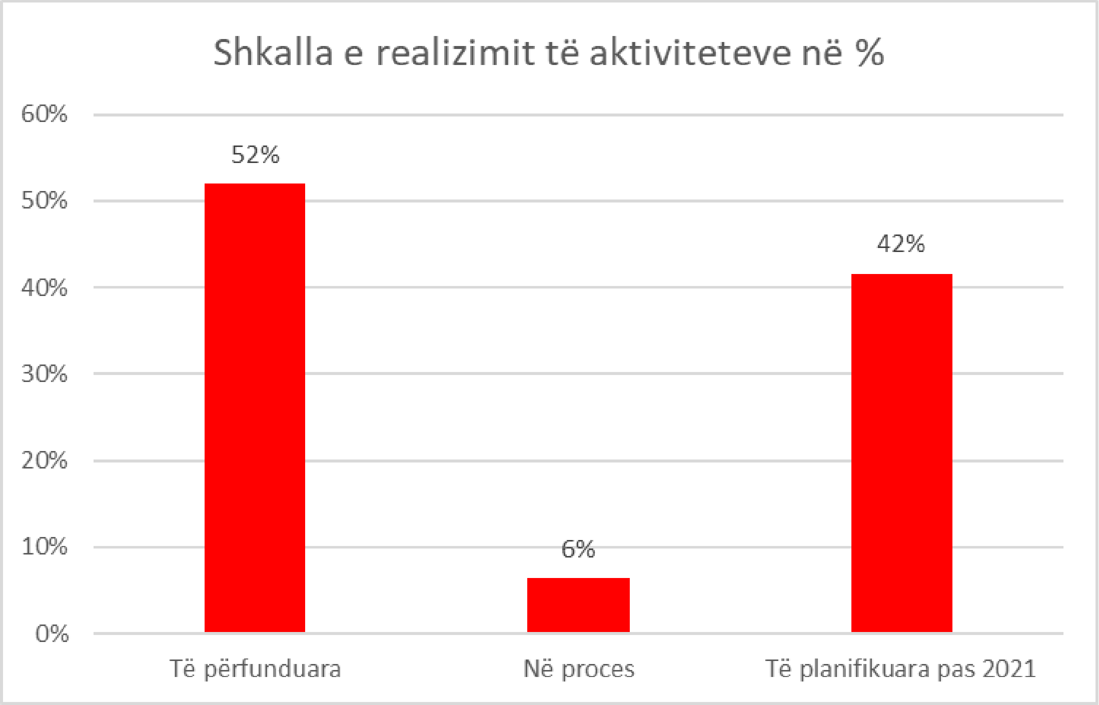


Figure 1 Percentage of realization of activities

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

• National Authority on Electronic Certification and Cyber Security,

•State police,

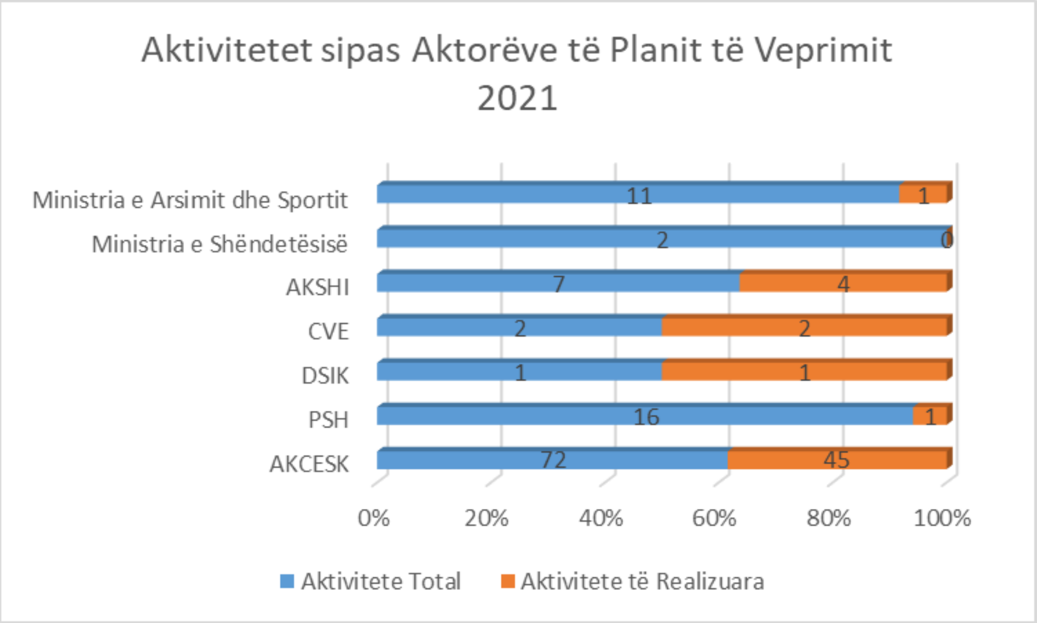
• Directorate of Classified Information Security,

• The Coordination Center for Countering Violent Extremism

• National Agency of Information Society,

•Ministry of Health

• Ministry of Education and Sports



There is progress in fulfilling the goal of the first policy on "Guaranteeing cyber security at the national level, through the protection of information infrastructures, strengthening technological and legal means." if the activities carried out and those in progress are considered.

In the realization of the objectives of this policy, 49 activities (39%) have been foreseen, 29 of which have been fully realized and 8 are in the process, as can be seen in the graph below:

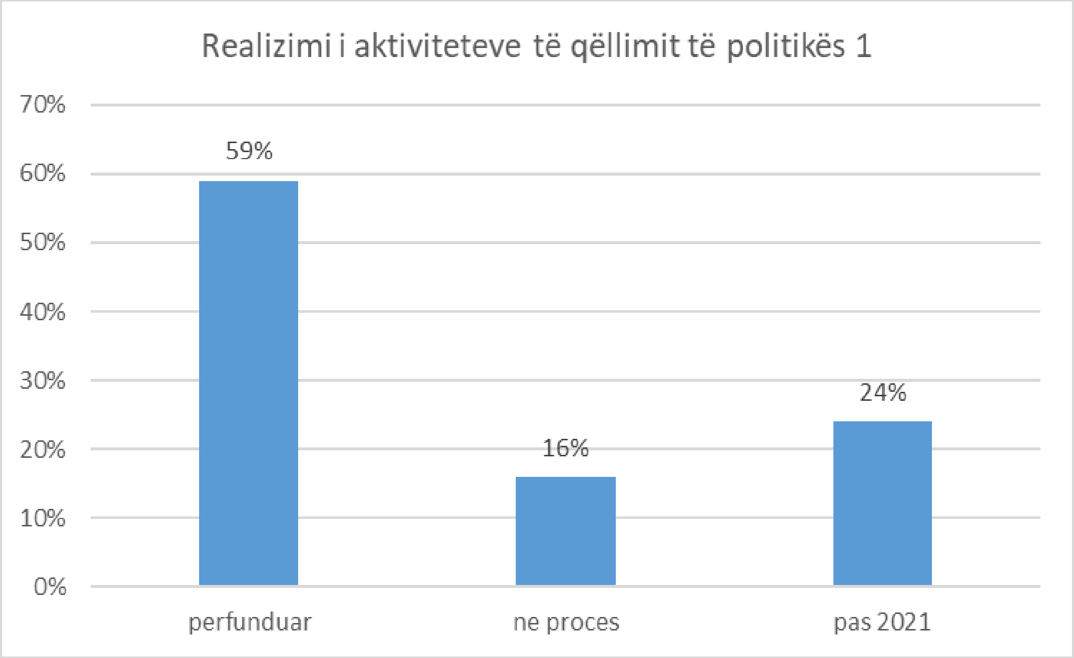


Figure 2 Realization of the activities of policy goal 1

In the realization of the objectives of the second policy goal, 19 activities (15%) have been foreseen, 8 of which have been fully realized and 11 have not yet started as seen in the graph.

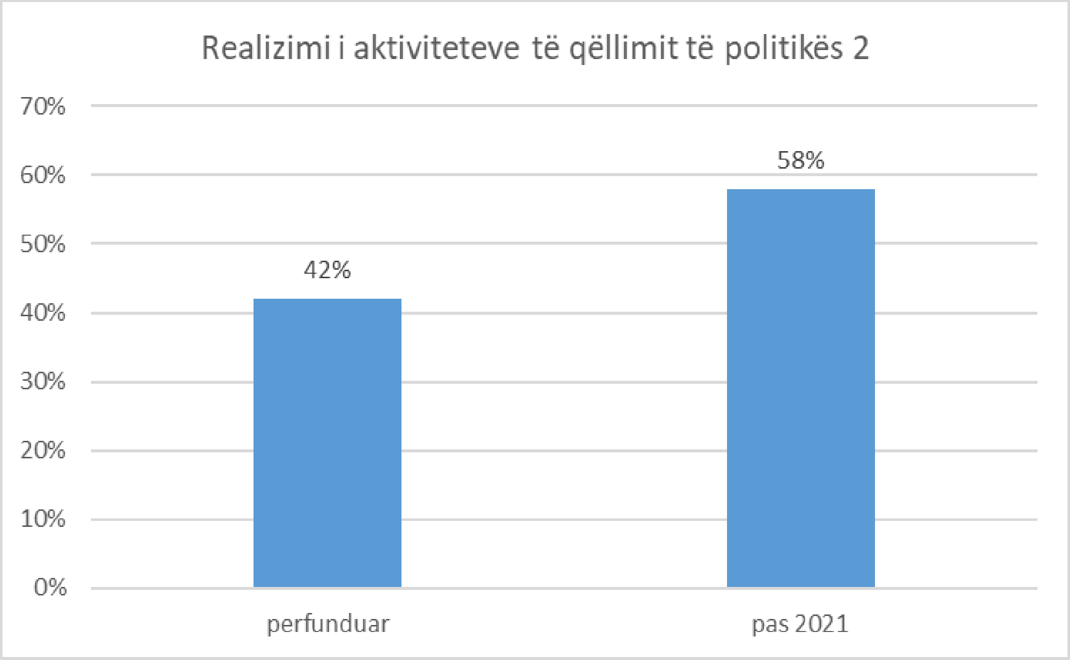


Figure 3 Realization of activities of policy goal 2

In the realization of the objectives of the third policy goal, 42 activities (34%) have been foreseen, 17 of which have been fully realized and 25 have not yet started as can be seen in the graph.

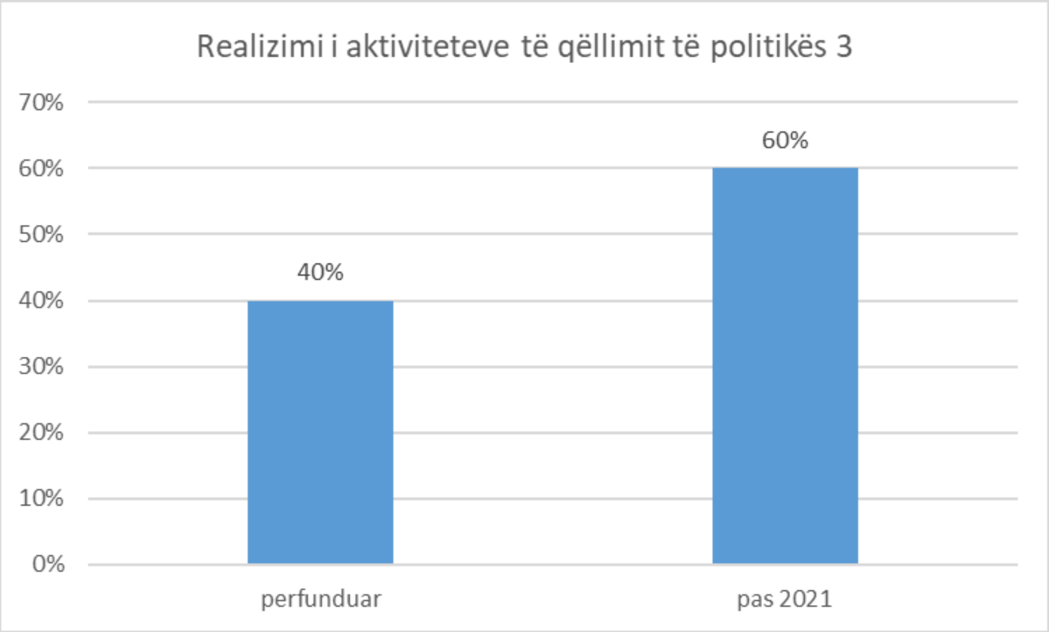


Figure 4 Realization of activities of policy goal 3

In the realization of the objectives of the fourth policy goal, 15 activities (12%) have been foreseen, 11 of which have been fully realized and 4 have not yet started as can be seen in the graph.

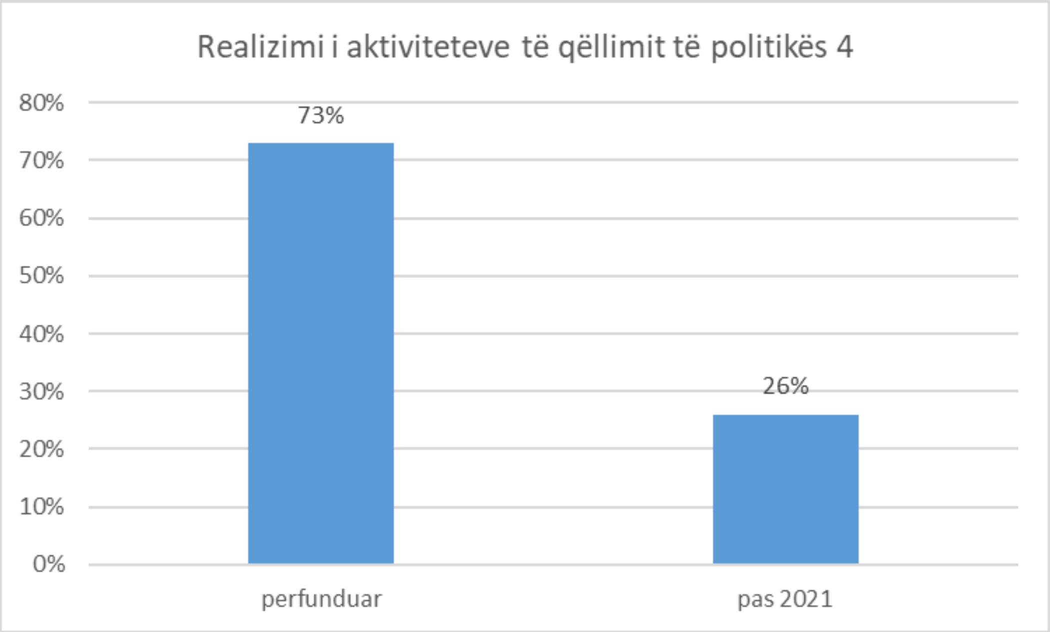


Figure 5 Realization of activities of policy goal 4

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 2021.

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.

3. STRATEGY POLICIES

The goal of the policy 1 is to guarantee cybersecurity at the national level, through the protection of information infrastructures, strengthening technological and legal means.

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 is in the process of fully aligning the regulatory legal framework of its field of activity. The draft law for the transposition of the European eIDAS Regulation "On electronic identification and trusted services for electronic transactions in the internal market" is in the final drafting process and is ready for the public consultation process. Also, NAECCS is finalizing the transposed legislation on cyber security based on 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."

In the execution of Law no. 2/2017 on Cyber Security, the updated list of critical and important information infrastructures has been approved by the Decision of the Council of Ministers no. 553 dated 15.07.2020 "For the approval of the list of critical information infrastructures and the list of important information infrastructures". Currently, the updated package has been sent to the Council of Ministers for the approval of the updated list of critical and important information infrastructures, 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 ".

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. Currently, the reporting of incidents by OIII and OCII is low, not only due to the need to strengthen trust in the confidentiality of reported data, but also because the implementation of many levels and layers of security to Critical and Important Infrastructures makes the information more immune to potential incidents.

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.

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 the control 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.

The National Authority on Electronic Certification and Cyber Security, with the aim of increasing the capacities of CSIRTs, through training and cyber exercises, has produced, in cooperation with RISI Albania, 4 brochures for which training, and capacity building were carried out with interest groups for each brochure.

1. Cybersecurity in the Energy Sector

2. Cybersecurity in the Financial Sector

3. Cybersecurity in small and medium enterprises

4. Cybersecurity in health

The National Authority on Electronic Certification and Cybersecurity has conducted exercises at the national level during 2021.

NAECCS in cooperation with the US Embassy in Tirana, Tirana Bank, Union Bank, Albsig Sh.a., Iute Credit, DCAF, Silensec International Telecommunication Unit, Carnegie Mellon University, organized on June 21-25, 2021, the fifth edition of the Albanian Cyber Academy (ACA5). ACA5 aimed to increase capacities and deepen knowledge in the field of cybersecurity for final year students of ICT and operators of critical information infrastructures. The fifth edition of the Albanian Cyber Academy invited 10 international speakers and 11 national experts: Dan Cimpean, Vilma Tomco, Ogerta Koruti, Almerindo Graziano, Volha Litvinets, JustinNovak, Stefan Tanase, Andrei Bozeanu, Dorin Nedelcu, Laura Thaqi, Eralda Caushaj, Paweł Srokosz, Naim Isufi, Hergis Jica, Lawrence Rogers, Fatjon Kadillari, Rexhion Qafa, Saimir Kapllani, Lorin Baxhaku, Ergis Gaxho, Klorenta Pashaj, who shared their expertise with 300+ online participants and more than 70 unique participants per day.

NAECCS organized the 5-day activity "Cyber Health" with about 20 representatives of the public and private health sectors. The purpose of this activity is to raise awareness for building a digitally developed society, cyber protected and equipped with the necessary knowledge to maximize benefits and minimize risks.

NAECCS, in fulfillment of the functional tasks and objectives of the "National Cyber Security Strategy", in cooperation with the Albanian Association of Banks (AAB), organized the 2-day activity, on the 17th-18th November 2021, "Financial Cyber Drill", attended by approximately 25 participants. The purpose of the activity was to raise the capacities of the financial sector, as one of the most sensitive sectors at the national level.

Directorate of Classified Information Security (DCIS)

DCIS for the development of defense in the field of cybercrime near their structure have recruited a new employee in 2021, who is engaged in the systems where information classified as "state secret" is handled based on the Decision of Council of Ministers no. 542 dated 25.07.2019 " For the approval of the regulation "On the provision of classified information that is handled in the communication and information systems (SKI)". DCIS has also developed trainings for raising the capacities of employees in its structure.

National Agency of Information Society (NAIS)

NAIS within Policy 1 of the National Cybersecurity Strategy for the optimization and expansion of security infrastructures has implemented the Project "Improvement with advanced techniques of cybersecurity in the governmental network gov-net and the governmental data center" with a total cost of 413,588,880 lek.

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.

The Coordination Center for Countering Violent Extremism has completed the Moonshot CVE project, aimed at countering Violent Extremism in Albania, which targets individuals at risk of VE with tailored services that reduce their vulnerability to radicalization. This project was piloted with an Albania-specific methodology, combining Moonshot CVE's data-driven approach to engaging cyber-vulnerable individuals with sustainable interventions to be delivered by local service providers. Moonshot CVE used quantitative and qualitative research methods to identify key violent extremist narratives circulating online, relevant local services, potential avenues for technical targeting and engagement, and opportunities for synergy with existing CVE programming.

The Coordination Center for Countering Violent Extremism has organized sensibilization campaigns in schools and with access to the community "Against online radicalization and violent extremism" with different target groups according to the profile and portfolio of Line Ministries, dependent institutions, and local government.

The National Authority on Electronic Certification and Cyber Security (NAECCS) has signed a cooperation agreement between the CVE Center and the Audiovisual Media Authority (AMA).

APS and CVE have organized an activity for the "Presentation of the unique portal for reporting websites with illegal content".

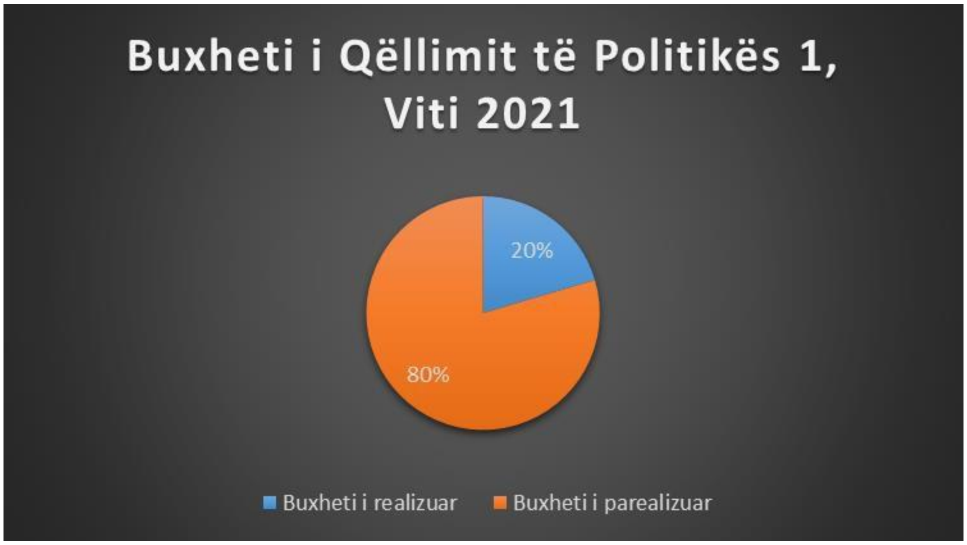
IKTD in cooperation and under the coordination of the CVE Center is implementing the project "Building safe and stable communities against the phenomena of radicalization and violent extremism ONLINE, in the peripheral areas of Tirana". (In process)

The CVE Center in collaboration with the Active Media Center have conducted a series of interviews with front-line actors engaged in the fight against violent extremism, as part of 5 reports that aim to highlight the cooperation between the institutions of the Albanian state, civil society, and religious communities in efforts to combat violent extremism on online platforms.

After a fruitful collaboration of more than a year with the Center for the Study of Democracy and Governance (CSDG), the study "Exploring the development of a strategic communication in P/CVE in Albania - Research-based approach" was finalized.

In fulfillment of the goal of the first policy on "Guaranteeing cybersecurity at the national level, through the protection of information infrastructures, strengthening technological and legal means." both realized and unrealized budgets are considered.

In the realization of the objectives of this policy, a budget of 327,799,008 ALL has been provided, of which 66,957,408 ALL (20%) has been realized and 260,841,600 ALL (80%) has not yet been realized as seen in the graph below:



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

The purpose of policy 2 is to build 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 Policy Goal 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 dynamics of the field, for the administrative staff at the central and local level. These trainings were conducted based on the brochures prepared by NAECCS regarding Cyber Security in the Energy, Financial, Small and Medium Enterprises and Health Sectors.

The National Authority on Electronic Certification and Cyber Security in order to increase the capacities of CSIRTs at the national level and the executive level of the public administration has organized cyber training during the implementation of activities such as the Albanian Cyber Academy, "Cyber Health", "Financial Cyber Drill" and "Cyber Camp Albania".

The National Authority on Electronic Certification and Cyber Security in cooperation with the US Embassy in Tirana, Tirana Bank, Union Bank, Albsig Sh.a., Iute Credit, DCAF, Silensec International Telecommunication Unit, Carnegie Mellon University, organized on 21- June 25, 2021, the fifth edition of **Albanian Cyber Academy**. ACA5 aimed to increase capacities and deepen knowledge in the field of cyber security for final year students of ICT and operators of critical information infrastructures. The fifth edition of the Albanian Cyber Academy invited 10 international speakers and 11 national experts, who shared their expertise with 300+ online participants and more than 70 unique participants per day.

NAECCS organized the 5-day activity **"Cyber Health"** with about 20 representatives of the public and private health sectors. The purpose of this activity is to raise awareness for building a digitally developed society, cyber protected and equipped with the necessary knowledge to maximize benefits and minimize risks.

NAECCS, in fulfillment of the functional tasks and objectives of the "National Cyber Security Strategy", in cooperation with the Albanian Association of Banks (AAB), organized the 2-day activity, on the 17th-18th November 2021, **"Financial Cyber Drill",** attended by approximately 25 participants. The purpose of the activity was to raise the capacities of the financial sector, as one of the most sensitive sectors at the national level.

NAECCS in cooperation with the Council of Europe, Raiffeisen Invest and Catholic University "Our Lady of Good Counsel" organize on December 6-8 the innovative activity "**Cyber Camp Albania**" near Movenpick Hotel, Lalzi Bay. The goal of Cyber Camp is to create a safe environment for children and young people, through close institutional cooperation, awareness and raising professional and technical capacities.

NAECCS with the aim of increasing society's awareness of cyber security, using the appropriate spaces for their realization, including audiovisual and social media, has drafted awareness materials. Throughout 2021, in implementation of the Authority's communication plan, 4 promotional videos were made and published for community awareness for increasing the level of cyber security under the motto **#ThinkCyber:**

a) Monitor your child's access to the Internet

b) Apply CYBER INSURANCE

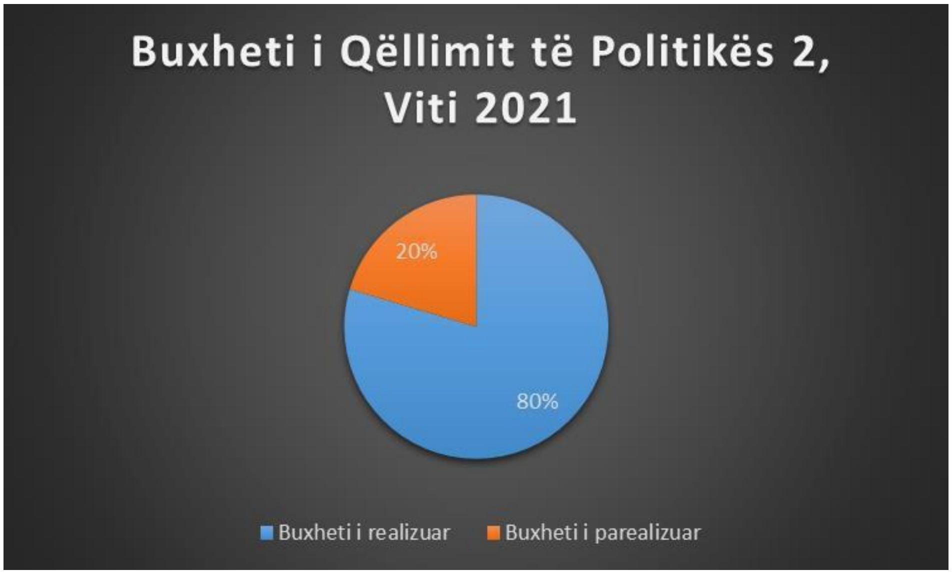
c) Protect your online privacy

d) Guidelines for the Child Protection Industry on the Internet

Cyber security bulletin is published every month with news and main events developed or organized by the Authority.

NAECCS has cooperated with international partners such as: Qualys, EATM Cert, Shadowserver and 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 as well as through the institution's official e-mail for those operators who have encountered problems accessing the system.

In the realization of the objectives of this policy, a budget of 5,256,000 ALL has been provided, of which 4,183,200 ALL (80%) has been realized and 1,072,800 ALL (20%) has not yet been realized as seen in the graph below:



The purpose of policy 3. Creation of the necessary mechanisms for the safety of children in cyberspace, while preparing the new generation on taking advantage of information technology and facing the challenges of development.

The goal of policy 3 is to create the necessary mechanisms for the safety of children in cyberspace, while preparing the new generation on taking advantage 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 Policy Goal 3, the institutions involved in the realization of the AP report as follows:

Ministry of Education, Sports and Youth (MESY)

MESY, within the scope of policy 1 and sub-objective 1, has taken concrete steps on the drafting of a special instruction (and accompanying regulation) for the collection of data on reported incidents of violence, bullying and online abuse of children in schools.

Based on the document "European framework for the digital competence of teachers, DigComEdu1", in the ICT competence framework for teachers (ICT CFT, version 3) from UNESCO, ASCAP has drafted:

a) Modules and materials for teacher training.

b) Digital citizenship and online security in digital environments.

ASCAP has developed the document "Professional standards of the teacher for the use of information and communication technology", which aims to understand the basic principles of cyber security, media and information literacy.

MESY in cooperation with NAECCS have organized activities such as "Internet Safety" at school, with the aim of sensibilizing the school community on Internet safety, rights, risks and responsibilities through artistic performance, drawings, essays, poems. Activities have been organized in the classroom, where students talk to each other, the teacher and the psycho-social service about the use of the Internet, cyberbullying (leaflets) and school violence. During these activities, questionnaires were developed regarding the perception of bullying and violence at school by students. In addition, the distribution of informational materials to parents and students about online abuse and bullying in schools has been done.

The Ministry of Education, Sports and Youth has drafted an accompanying regulation in schools for gathering of data on reported incidents of online violence, bullying and abuse. This regulation, carried out by the Environment, Health and Safety group in collaboration with the Community Policing on Cybercrime Strategy, facilitates the identification of cases of school and online bullying from the beginning, and their prevention.

MESY has also designed a methodology for collecting incident cases in schools by introducing students to the topic of cybercrime and its consequences:

- How is cybercrime identified?

- Why is it necessary to ask for help if you are attacked?

- The legal way according to the Criminal Code of the Republic of Albania?

- Awareness video on bullying and cybercrime, was made to help pupils by preventing any incidents between them, creating security and peace even in home conditions.

MESY collects the reports of local educational institutions responsible for pre-university education and drafts a final report on the situation in schools and how it can be improved.

MESY, within the framework of preventing sexual abuse of children on the Internet by increasing awareness and creating safe spaces for surfing the Internet, has drawn up procedures for the integration of the "Peer Educators for Online Safety" program in 9-year-old schools. This program includes:

- discussions in the 8th and 9th grades on the topic "Using the Internet in a safe way" in order to learn about the consequences of sharing passwords, friends' addresses, different forms of emotional and psychological violence up to in the consequences of sexual violence and cyber violence.

- activity "Recognizing the rights and responsibilities of children on the Internet", to equip them with values, attitudes and behaviors as citizens of our country in social media through artistic performance, drawings, essays and various creations.

The Ministry of Education, Sports and Youth has supported the creation of an online network of ICT teachers to promote the issue of protecting children on the Internet. The network of online ICT teachers affects the establishment and operation of professional networks for the 2021-2022 school year. Meetings of ICT professional networks are organized every month. There are currently 1200 ICT teachers in professional networks, who have been continuously trained by ASCAP specialists, for the network operation guide, for planning the annual work of the networks, for the way of reporting, as well as for content topics such as: training for ICT teachers; violent extremism.

Throughout this period, the training of ICT teachers continued regarding various topics on the work and organization of professional networks, including the use of ICT in the implementation of the curriculum and in student assessment. The trainings aimed at the professional development of ICT teachers for the safe and efficient use of online platforms in the learning process have also continued. School teachers are prepared to increase children's safety through:

a) drawing up school rules to increase the safety of children in school premises;

b) creation of videos by students regarding cyber security awareness;

c) creating discussion networks for cyber-bullying;

d) creating forums to help children who may be victims of any kind of violence.

Within the implementation of the cooperation project between the Agency for Quality Assurance of Pre-university Education and the Albanian Media Institute, 123 teachers were trained on Media Education and Information. In the framework of this training, 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 while using the Internet. Teachers are encouraged to use basic teaching methods and tools to help students use the Internet responsibly and make them aware of the challenges and risks that come from using it.

MESY 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 MES, DPAP[1], DRAPs[2], ZVAPs[3] and IAPs[4], which is connected to the online portal www.cesk.gov.al of NAECCS, to block access to websites with illegal content, which helps children, persons exercising their parental responsibility and young people to report illegal content encountered while browsing the Internet.

In order to identify, support and promote talents to create technical solutions that help in online protection and security, MESY has developed competitions, projects on the topic of "Internet Security", extra activities for students who show a tendency in ICT, the development of the National Olympiad in the ICT subject, with AML[5] students.

MESY also monitors the application of the methodology with practical activities with pupils of first grade, V-IX and X-XII on safeguards and cyber security. Discussion on experiences with staff and student groups. Creating posters and essays by students about cyber risks and online safety. Implementation of projects, in the educational institutions of AMU and AML, by organizations/associations that have cooperation with MES.

Ministry of Health (MH)

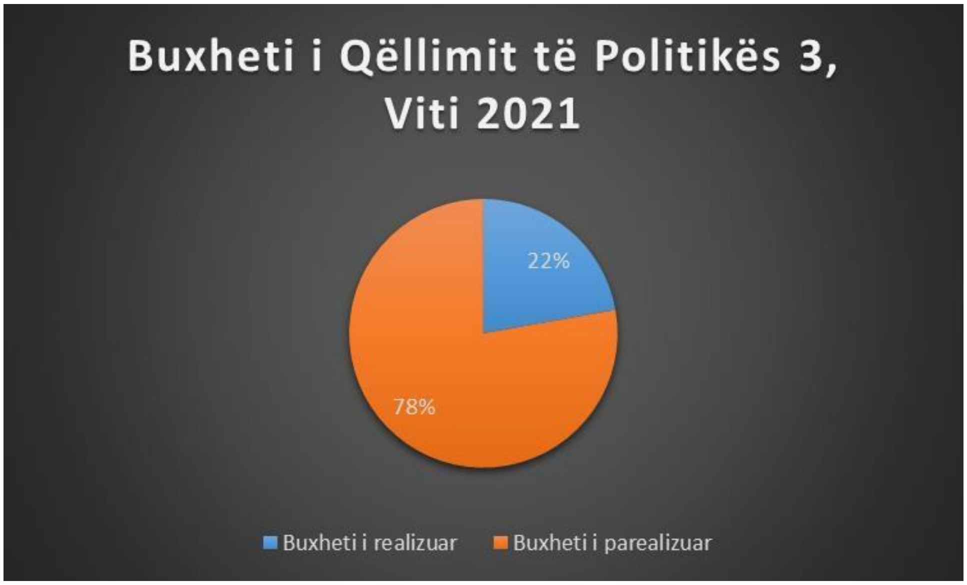
The Ministry of Health, in order to strengthen cross-sectoral cooperation for the protection of children on the Internet, has established a Technical Advisory Committee for Children's Safety on the Internet, at the National Council for the Rights and Protection of Children (Ministry of Health).

Decision of the Council of Ministers No. 659, dated 3.11.2021 "National Agenda for Children's Rights, 2021-2026". This document aims to:

- To influence the lives of children, improving the quality of services at all levels.
- To promote a culture of children's rights in Albania
- To enable protection from all forms of violence.
- To provide quality data to improve the policies and programs designed for them.
- To provide education regarding online protection of children, thus guaranteeing the well-being and a better future for children.

[1] Abbreviation for General Directorate of Pre-University Education
[2] Abbreviation for Regional Directorate of Pre-University Education
[3] Abbreviation for Local Office of Pre-University Education
[4] Abbreviation for Institutions of Pre-University Education
[5] Abbreviation for Higher Secondary Education

In the realization of the objectives of this policy, a budget of 3,858,000 ALL has been provided, of which 856,400 ALL (22%) has been realized and 3,001,600 ALL (78%) has not yet been realized as seen in the graph below:



The purpose of policy 4. Increasing national and international cooperation with strategic partners in cybersecurity

The purpose of policy 4 is to increase national and international cooperation with strategic partners in 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 Policy Goal 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:

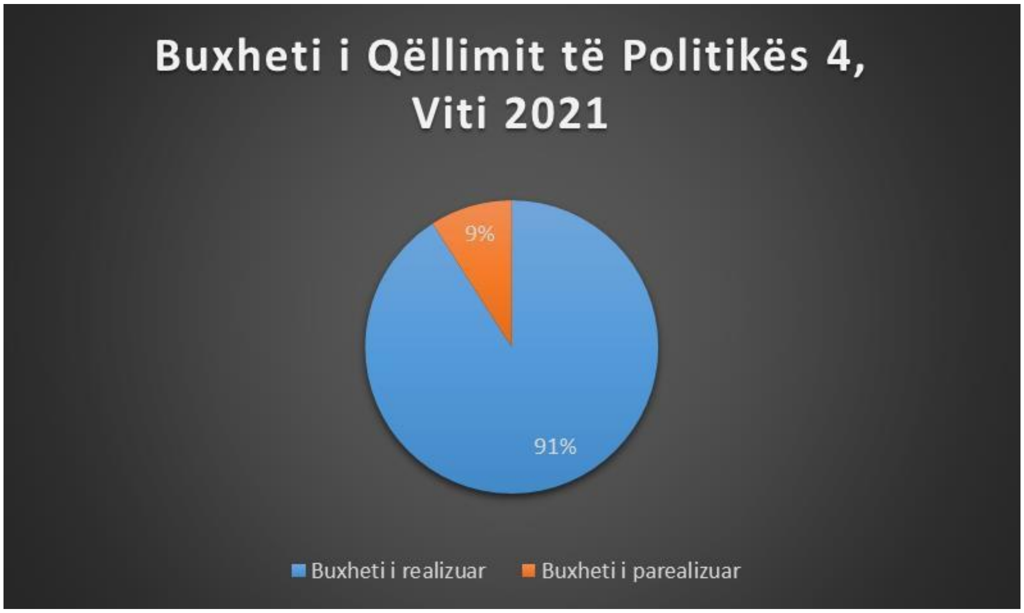
- Cooperation Agreement with the Audiovisual Media Authority and The Coordination Center for Countering Violent Extremism
- Cooperation Agreement with Macedonia (MKD-CIRT)
- Cooperation Agreement with Kosovo (KOS-CERT)
- Cooperation Agreement with Romania (CERT-RO)
- Cooperation Agreement with AKEP[6]

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.

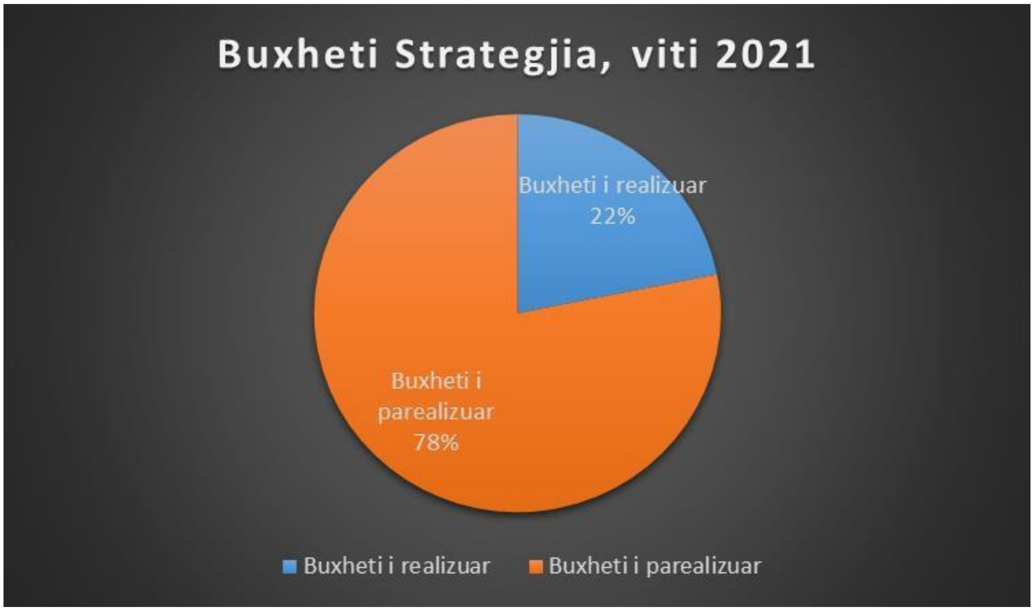
NAECCS, within the framework of strengthening international cooperation in the field of security and cyber protection and the fight against violent extremism and radicalization, has actively participated in NATO meetings for the implementation of international standards and regulations in the context of cyber security. NAECCS also has an important role in strengthening cooperation and information exchange with NATO / OSCE and other international organizations / forums. The National Authority on Electronic Certification and Cyber Security has joined various international activities and initiatives in cyber security (such as First, Trust Introducer).

In the realization of the objectives of this policy, a budget of 2,408,400 ALL has been provided, of which 2,190,000 ALL (91%) has been realized and 218,400 ALL (9%) has not yet been realized as seen in the graph below:

[6] Abbreviation for The Electronic and Postal Communications Authority



The Action Plan of the National Cyber Security Strategy 2020-2025 has foreseen a total budget for the year 2021 of about ALL 339,321,408. During the monitoring period of the Strategy by the National Authority on Electronic Certification and Cyber Security, the budget realized during 2021 is ALL 74,187,008 (22%) as in the graph below:



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. Aligned legislation 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 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

- ✓ Drafting the methodology regarding the national cyber risk assessment.
- ✓ Drafting of the procedure for the management of cyber crises.
- ✓ Review of the National Cyber Security Strategy, ensuring continued involvement of stakeholders.
- ✓ Establishing an expert forum on cyber security at the national level.
- ✓ Strengthening and promoting cross-sectoral cooperation in cyber security to ensure full implementation of cyber security programs.
- ✓ Organization of periodic trainings for employees of NAECCS and Critical Infrastructures.
- ✓ Improvement of the national escalation procedure for response to cyber incidents by detailing coordination with Critical and Important Information Infrastructures.
- ✓ Conducting ENISA's Critical and Important Information Infrastructure Maturity Self-Assessment Survey based on the SIM3 model to gain further insight into NAECCS's maturity and capabilities.

ANEX 1

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[7] (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" III
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
Measurement Frequency	Annual

[7] Abbreviation for National Strategy

Nature of Indicator: Cumulative/Incremental	Cumulative	
Direct or Composite Input	Composite	
Calculation formula	1) Planned framework versus the approved strategic framework	
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 Laws
	2023	
	2024	
	2025	full aligment
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

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-	
	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

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

Name of the indicator	Completed legal framework (for children's 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

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:	2021	1600
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

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:		
SDG - Title of the Sustainable Development Goal according to the UN	N/A	
Target value of the SDG indicator	N/A	

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:	2021	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