DECISION
No. 1084, dated 24.12.2020

ON ADOPTING THE NATIONAL CYBERSECURITY STRATEGY AND ITS ACTION PLAN 2020-2025

According to Article 100 of the Constitution upon the proposal of the Deputy Prime Minister, the Council of Ministers

DECIDED:

1. To adopt the National Cybersecurity Strategy and its Action Plan 2020–2025, according to the text herein attached, which is its constituent part.
2. The National Electronic Certification and Cybersecurity Authority, the ministries, and other institutions responsible as provided in the strategy and the action plan shall be charged with the implementation of this decision.

This decision shall enter into force upon publication in the Official Gazette.

DEPUTY PRIME MINISTER
Erion Braçe

NATIONAL CYBERSECURITY STRATEGY

The National Cybersecurity Strategy, which should have been attached to decision No. 1084, dated 24.12.2020 of the Council of Ministers "On adopting the National Cybersecurity Strategy and its Action Plan 2020-2025", and published in the Official Gazette no. 233, dated 30.12.2020.

TABLE OF CONTENTS

PART I: STRATEGIC CONTEXT

1. INTRODUCTION

The development of the internet and technology innovation changes over the recent decades have resulted in fundamental changes and challenges in every society worldwide. Our daily lives, human rights, economies, and social interaction are deeply impacted by information and communication technologies. A common and

open cyberspace promotes social and political engagement, breaks down communication barriers between countries, communities, and citizens, and ensures transparency, allowing interaction with and exchange of information and ideas in real-time worldwide. All the developments and growing use of information and communication technologies have brought great benefits, but also threats, which makes cyber defense and security-critical.

Various groups and individuals with malicious interests perpetuate continuous efforts in the cyberspace, which impact the progress and functioning of states. Privacy breaches and identity theft are also increasing and highly concerning problem for society at large.

On the one hand, the government is increasingly investing in digital infrastructure to provide digital services to citizens. On the other hand, the public is increasingly using the internet because of the advantages it offers.

As a developing country, Albania relies on information technology as well, intending to improve the quality of life and public services. Alongside the advantages of using new digital technologies, internet use also has its issues related to cybersecurity. Cyberthreats are on the rise, taking advantage of technological weaknesses or lack of knowledge inadequately using these tools, thus threatening information systems security.

One of the current and ongoing challenges in many countries is the building of a developed digital society, which is cybernetically protected, equipped with the required knowledge and skills to maximize benefits and manage risks.

Under the "National Security Strategy 2014-2020" and the "Cybersecurity Policy Paper 2014-2017", Albania has taken important steps to improve its cybersecurity situation. Alongside the developments in the technology and information field, and the public services digitalization revolution, the legal framework on cybersecurity was completed and improved upon. Due to this progress, Albania has improved its rank in the Global Cybersecurity Index compared to 2017 from 89th to 62nd globally and top 36th in Europe.

However, this process has not yet reached the change scale and pace required to stay ahead of the fast-moving evolution of the various cyber threats. Cybercrime is undoubtedly one of the major threats to modern global security and for this reason, cybersecurity has become an important part of national security. For this reason, the National Cybersecurity Strategy 2020-2025 development is a necessity for the establishment of the relevant institutional mechanisms that will improve the cybersecurity level in the country.

This strategy will be based on the following core principles to meet government commitments and to be incomplete coherence with the strategic developments in developed countries:

- application of the same core values in both the physical and digital worlds;
- fundamental rights, freedom of expression, personal information, and privacy protection;
- access for all;
- democratic and effective governance;
- joint responsibility in guaranteeing cybersecurity.

2. ASSESSMENT OF THE CURRENT SITUATION IN ALBANIA

The current cybersecurity situation in Albania was evaluated in cooperation with the relevant institutions and is based on the following 4 pillars:

1. Cybersecurity situation;
2. Cybersecurity legal framework;
3. Safe internet for children;
4. Education, research, and training on cybersecurity

2.1. Cybersecurity situation

2.1.1 Critical information infrastructure

The "National Security Strategy" adopted in 2014 has provided the national framework and pillars to increase security in the country. Being a developing country without the necessary cybersecurity legal infrastructure, this field has only been developing in the last two years in Albania, over which critical and

important information infrastructure has been identified in the public and private sectors. , besides, minimum security measures to be implemented for better cybersecurity in this infrastructure have been developed along with the development of a methodological mechanism for sector CSIRT establishment and operation at the national level.

The legal framework on electronic communication security is completed with legal provisions on the security and integrity of electronic communication networks and telecommunication networks covered by Law No. 9918, dated 19.5.2008 "On electronic communication in the Republic of Albania" as amended, which has transposed EU directives on electronic communication.

The cybersecurity legal framework has also designated the National Electronic Certification and Cybersecurity Authority (NAECCS), as the authority responsible for overseeing the implementation of the law.

As a result, after the implementation of the law on security, the current critical information infrastructure situation in the **banking sector** has improved compared to two years ago. Considerable security measures, approved by NAECCS have been applied in this infrastructure, and sector CSIRT shas been established, creating a safe cyberspace.

In the **financial sector**, cybersecurity is divided into two pillars, the public and the private, and the current situation is as follows:

Security measures according to the applicable legislation and in compliance with the ISO 27001 standard are applied in critical government information infrastructure used by public institutions, allocated in the government data center, and managed by the National Agency on Information Society. NAIS is a government sector CSRIT and was certified in 2018 for this standard, and ISO 27001 standard policies are applied to any government infrastructure managed by NAIS.

Critical infrastructure managed by private operators is currently being identified and in some cases, the investment to develop them is also being identified.

In the health sector, which is also divided into the public and private pillars, the cybersecurity situation is as follows:

Measures approved according to the law on security have been applied in critical infrastructure managed by public operators/institutions, which has led to improved cybersecurity levels. Besides, groups responsible for managing and addressing incidents, which did not exist when the legal framework was absent, have also been established.

The private operator managed information infrastructure, considered to be critical infrastructure as defined by the European Commission legal framework on information networks and infrastructure, have not been identified and the situation study conducted by the relevant authority found that they do not meet security elements that critical infrastructure should guarantee.

Energy Sector Currently, all generation, transmission, and distribution energy system operators are implementing innovative technologies based on computer systems and data transmission networks, to manage and optimize their technological processes. SCADA systems are implemented or are planned for implementation in all three sectors of the energy system, and they have their operation, computer system, and data transmission centers. Along with reading and analyzing energy system data remotely, operation modules automating processes that are currently completed manually by operators are planned for implementation in the near future. Transitioning to independent systems that operate automatically will certainly require the implementation of security measures and policies, since the impact of cyber-incidents would be great. This will certainly require energy operators to pay special attention to system security and to develop internal procedures and human capacities for cybersecurity when planning ICT projects and automation.

In the transport sector, which is composed of three pillars, the situation is as follows:

Critical information infrastructure related to *air transport* meets minimum security rules obligations and sector CSIRT has been established in the relevant sector.

Critical information infrastructure in *road transport* does not meet any minimum-security rules obligations, including the establishment of the relevant CSIRT.

Information infrastructure in maritime transport, which is considered critical infrastructure in the meaning of the legal framework adopted by the European Commission on networks and infrastructure is yet to be identified.

Besides, critical information infrastructure in the water supply sector, which is managed by local governance, has yet to be identified as such in the meaning of the applicable legislation on cybersecurity and no security measures are applied in this regard.

Considering that the majority of cyber threats and cyberattacks are perpetrated through electronic communication networks, cybersecurity issues in the digital infrastructure and electronic communication networks and/or services are covered and are under the responsibility of the Electronic and Post Communication Authority (AKEP). According to article 122 of Law No. 9918, dated 19.5.2008 "On Electronic Communication in the Republic of Albania" and Regulation No. 37 dated 29.10.2015 "On Technical and Organization Measures to guarantee Electronic Communication Network and/or Services Integrity", AKEP requires adequate technical and organizational measures to be put in place by all electronic communication entities operating under the General Authorization Regime to guarantee electronic communication networks and/or services security and integrity for all services they provide to their subscribers, including DNS services. AKEP has conducted and continues to periodically conduct inspections and audits in entities, to verify the establishment and implementation of the relevant technical and organizational security measures, and in cooperation with NAECCS it follows up on security incidents reported by electronic communication businesses. AKEP is the ".al" domain administrator and has authorized 8 businesses as accredited registries to provide *domain name* registration services under the .al domain (*TLD name registries*).

With the inclusion of this service in the critical and important information infrastructure list, the registries accredited by AKEP to provide .al domain name registration services will also be subject to the provisions of regulation No. 37 "On Technical and Organization Measures to guarantee Electronic Communication Network and/or Services Integrity".

Internet penetration in Albania is still ongoing and the country currently has mid-level internet use. Some 67% of the population and some 40% of households had internet access in 2019.

2.1.2 Cybercrime

Similar to other countries, Albania is often a victim of malicious cyber activity perpetrated by criminal actors, including state and non-state actors that can use network infrastructure in the country and abroad. Alongside the improvement of internet services, Albania has also experienced the rise of various forms of cybercrime. The most common forms of cybercrime dominating in Albania include fraud-related to internet banking such as *phishing and spam*. Even when those responsible for cybercrime against the Republic of Albania are identified, it is often difficult for law enforcement agencies in the Republic of Albania and international organizations to persecute when they are located in restricted jurisdictions.

Currently, there is a lack of necessary tools to obtain general cyber intelligence, using human and logistical resources available for law enforcement activities.

For this reason, it is fundamental to increase capacities to address cyber challenges, which in turn requires a change in structures, approach, technical and logistical capacities, etc.

An important step forward in legislation development and measures were taken against cybercrime will also be the first national cybercrime strategy, which will be

developed by the relevant authorities and will be put into action in a relatively short time. This document will define the methods for combating cybercrime in the cyberspace and will provide more adequate tools for this fight.

Cybersecurity legal framework

A comprehensive national approach to cybersecurity cannot be achieved through the use of technologies and services alone, and it should be accompanied by a proper and current legal framework focusing on the dynamic nature of the ICT space and the evolving nature of cyberthreats.

Various national and international structures have organized awareness-raising campaigns for various stakeholders on protecting from threats resulting from cybercrime and other attacks against internet safety.

A legal and regulatory framework protecting from various forms of electronic crime and abuse is fundamental to the establishment of a reliable environment for electronic communication and transactions.

The main laws related to cybercrime are the following:

Law No. 7895, dated 27.1.1995, "Criminal Code of the Republic of Albania", as amended;

Law No. 2/2017, "On cybersecurity";

- Law No. 9918 dated 19.5.2014, "On Electronic Communications in the Republic of Albania", as amended;

Law No. 9887, dated 10.3.2008, "On Personal Data Protection", as amended;

- Law No. 8457, dated 11.2.1999, "On Classified Information", as amended;

Law No. 9880, dated 25.02.2008 "On the Electronic Signature", as amended;

- Law No. 107 dated 15.10.2015, "On Electronic Identification and Trusted Services," as amended.

Regarding the above, legislation in the cybersecurity field should be harmonized with EU legislation, thus creating

a complete and codified mechanism to adequately address and resolve issues.

Besides, where possible, international internet security mechanisms should be accessed, signed, ratified, and implemented, including the allocation of sufficient resources based on national priorities and considering technological developments and applying the neutral technology principles.

Safe internet for children

The increasing use of the internet by children is the greatest issue regarding their online safety, not only in Albania. Child online safety is one of the priorities for Albania and all institutions focusing on this issue in their activity.

In 2018-2019, the government's main and strategic partner in child protection and rights, UNICEF Albania conducted a study on **"Children's experiences of internet use in Albania"**[79], which surveyed 1000 children between the ages of 9 and 18 and their parents, and its preliminary results found the following:

Surveyed children accessed the internet for the first time at 9 years of age, with 37% stating that they used the internet at 8 years of age or even earlier. 51% of children interviewed have permanent access to the internet (whenever they wish).

In general, children interviewed use the internet more and have more online technological skills than their parents. This creates an obstacle for parents in effectively overseeing child experiences on the internet, not only as regards controlling access but also to help children in developing a critical judgment of their online experiences and content.

The study found that during their time online, children have had upsetting situations. Namely, 14% of children interviewed have had upsetting experiences online, especially those between 15 and 17 years of age. 1 in 10 children reported at least one unwanted sexual experience through the internet.

The statistics of this research show that children are exposed to harmful content online, such as images of violence or abuse (1 in 5 children),

79 The "Children's experiences of internet use in Albania" will be published in 2019 by *UNICEF Albania*. Its preliminary findings were presented in the "VIRAL" Summit, organized by *UNICEF Albania* in November 2018: https://www.unicef.org/albania/viral-summit-better-Internet-children-and-adolescents-albania

content discussing physical violence (17% of children) or content discussing suicide (1 in 10 children). 1 in 5 children has been subjected to denigrating and hate messages, which is also an indicator of possible online bullying situations.

Besides, the study shows that children find it difficult to distinguish the difficult situations they experience and to ask for help: 1 in 5 children never told anyone about what upset them, while 75% of children interviewed asked their peers and not adults for help and support.

Over 20% of children interviewed accept all friend requests on social networks, while 25% of children say they have interacted online with someone they don't know, and 16% of them have met in real life someone they only knew online. Parents are aware of only 9% of the abovementioned cases.

Children interviewed note they are under no control or supervision from their parents when watching videos online (78%), when using social networks (58%), when using texting apps (57%), or when using the computer or telephone web camera (56%).

As the study notes, the uncontrolled use of the internet by children is at a very high level. Often this results in grave consequences. Lack of parental information regarding the risks of unsafe internet is also at high levels.

Even though some internet service providers offer the technical possibility to apply parental controls, they are not applied. Besides, a study of the situation in 7 regions of the country, using information from awareness-raising campaigns with some 12,000 middle school children, found that the majority of children confirm that their parents do not have clear information on the risks of unsafe internet use by children.

Another study conducted in 2019 by UNICEF Albania entitled "WebFactor"80 has found a series of legal and institutional gaps, which hamper the efficient guarantee of child safety online.

The study found that even though the Albanian legislation is overall in line with relevant international standards on child sexual abuse, it is often fragmented and lacking very important definitions related to child sexual abuse, their engagement, and coercion to participate in sexual and other improper acts. The principle of protection from harmful and illegal content online is hindered by two factors: 1. The definition for harmful material is very general and leaves much space for individual judgment; and 2. The lack of clear definitions for child exploitation in sexual acts makes the identification of illegal acts difficult.

Another important finding is related to the Albanian legislation regulating the operation of internet service providers, which is unclear concerning charging of administrative authorities the competencies to block or delete specific materials. This does not allow these authorities to clearly understand their role and functions, and to have appropriate mechanisms to exercise them. Clear legislation on the exact administrative authorities' competencies and procedures is necessary for this field.

When considering criminal investigation and prosecution for cases of online sexual abuse with children, the study notes that neither the police nor the prosecution is fully equipped with the adequate infrastructure to effectively investigate online child abuse cases. The cybercrime investigation unit of the State Police lacks the resources to undertake active online surveillance, thus hampering their ability to start *ex officio* and proactive investigations. The failure of internet service providers to quickly react to the requests of the prosecution, and difficulties in identifying alleged perpetrator IP addresses, gravely impact the overall quality and efficiency of the investigation, and

80 UNICEF Albania, 2019, WebFactor: Assessment of the legal framework and institutional readiness to address child sexual exploitation and abuse online in Albania https://www.unicef.org/albania/sq/deklarata-shtypi/faktoriweb-vler%C3%ABsimi-i-kuadrit-ligjor-dhe-gatishm%C3%ABris%C3%AB-institucionale-p%C3%ABr

consequently, the possibility to bring perpetrators to justice.

The study shows that Child Protection Units and other professionals dealing with child protection online need capacity development and support in handling online child abuse. Besides, there are no specific online child abuse data that have been collected or published.

2.4. Education, research, and training in the field of cybersecurity

In developing countries, human resources with adequate skills and qualifications in cybersecurity have proven to be one of the most difficult challenges as regards the implementation of a national level CSIRT and the improvement of the overall national cybersecurity situation. Ensuring an adequate level of education, research, and training on online safety, and supporting the internal needs of professionals regarding cybersecurity is critical.

Several study programs in the field of cybersecurity are offered by higher education institutions, but they are in their first steps and more effort is required to reach an adequate level. Besides, no cybersecurity research initiatives have been undertaken in Albania. The knowledge gained by students in universities is insufficient to meet labor market requirements in this field. Furthermore, even academic staff has its issues in covering the entire range of this field.

As a result, developing appropriate cybersecurity curricula and enhancing academic staff knowledge is an immediate necessity to meet market demand.

On the other hand, human resources capacity development through dedicated training in the cybersecurity field in the public administration and all other public sectors is another necessity that public institutions should consider.

Besides, a common approach is required for the education of the government staff and the public regarding safer practices on cybersecurity awareness.

3. STRATEGY VISION

Vision

Guaranteeing cybersecurity in the Republic of Albania through the establishment and operation of interactive institutional mechanisms, legal and technical instruments, and critical cyberspace protection elements for digital infrastructure, transactions, and electronic communication; through the development of professional capacities, nationwide awareness, and strengthened national and international cooperation for a safer digital space.

Impact indicators and outcome indicators

The National Cybersecurity Strategy will be monitored by measuring core indicators defined in the indicator Passport annex. The core indicators, which will serve as a road map for the Strategy implementation monitoring, were developed to track the achievement of specific objectives translated into a detailed action plan.

The indicators were developed to be understandable, measurable, and easily compared over the monitoring periods. Two core indicators were developed for each specific objective, which can be simple or complex depending on the sub-objectives they are measuring.

PART II
POLICY GOAL AND STRATEGY SPECIFIC OBJECTIVES

The Government of the Republic of Albania will achieve the following goals to improve the cybersecurity level in the country:

Guaranteeing cybersecurity at a national level through the protection of information infrastructure, while strengthening technological and legal tools.

Establishing a safe cyberspace, raising awareness in society, and developing professional capacities.

Developing mechanisms required for child safety in cyberspace, while at the same time preparing the younger generation to benefit from the advantages of information technology and overcome development challenges.

Improving national and international cooperation with strategic partners in the cybersecurity field.

4. Policy goal 1. Ensuring cybersecurity at the national level through the protection of information infrastructure and strengthening technological and legal tools. The rapid developments across the sectors of the economy, heavily based on technological innovation as well, makes it difficult for decision-makers to understand and mitigate risks related to the use of information and communication technology. These risks are a common global responsibility and include national and international perspectives.

Domestically, the common responsibility included the industry, and the administration, and the citizens.

Development and implementation of policies and tools to establish a safe communication space, is the most valuable component for cybersecurity incident management and secure electronic transactions in the domestic market, intending to guarantee safe electronic interaction between public authorities, citizens, and businesses, thus improving the effectiveness of online public and private services, and electronic business and commerce.

The digital space is sensitive: information systems and networks may be impacted by security incidents, such as human error, natural causes, technical faults, or attacks. These situations are increasing in number and are becoming ever more complex and may lead to great financial losses and impact the wellbeing of the society overall.

Establishing trust in the online environment is the key to economic and social development. Lack of trust, especially because of the perceived lack of cybersecurity leads consumers to hesitate in using electronic transactions.

Specific objective 1: Improving the legal framework providing norms and regulating cybersecurity in the country and aligning this framework with European Union directives and regulation.

Security authorities in the country have developed the legal basis for their activity. However, even though even though laws, secondary legislation, regulations, and standards have been developed, the analysis conducted and the evaluation of the cybersecurity maturity level in the country, found the need to revise the entire legal and regulatory framework achieve complete alignment with European Union directives, and to achieve domestic institutional coordination.

This specific objective aims at harmonizing the Albanian legislation on cybersecurity with the EU legislation. Besides, a national procedure will be developed for action in case of extraordinary situations created by cyber crises.

Sub Objectives:

Improving cybersecurity regulatory framework in line with sector laws, to appropriately address and resolve issues including, but not limited to IoT, 5G technology, artificial intelligence.

Continuously adapting standards and rules to the developments of the cybersecurity field.

Meeting engagements undertaken regarding cyberspace as a member country of the North Atlantic Treaty Organization.

Defining a national procedure for extraordinary situations created by cyber crises, taking concrete measures to resolve the situation in real-time.

Specific objective 2: Establishing and operation of CSIRTs in all industry sectors nationally

According to the law "On cybersecurity" and the obligations provided therein, and to guarantee information and communication system security, there is an obligation to dynamically identify critical and important information infrastructure and then establish incident response teams (CSIRT). Currently, the initial measures for the establishment of these teams in some of the infrastructure defined by a relevant decision have been taken, but this is a continuous process monitored by NAECCS.

Achievement of this policy 1 objective will be measured with the number of established CSIRTs. All critical and important information infrastructure operators should have their relevant CSIRT, which should meet minimum requirements and be audited by NAECCS.

Sub Objectives:

Creating optimal work conditions for CSIRT operation, in line with the duties to guarantee cybersecurity in critical and important information infrastructure.

Building CSIRT capacities through training and cyber drills.

Specific objective 3: Strengthening and implementing security measures in critical and important information infrastructure

Based on the assessments made in 2018 to 2019 by the authority responsible for cybersecurity, a major task for critical and important information infrastructure remains increasing and strengthening the implementation of security measures. Public and private organizations should improve their procedures and develop cyber defense strategic plans against cybercrime or cyberattacks, and risk management plans in case of such attacks. The objective of this Strategy is to stimulate and obligate all critical and important information infrastructure to develop strategic plans in case of cyberattacks and to take measures to withstand these attacks and to recover the damages or eliminate these attacks.

The achievement of this specific objective will require all critical and important information infrastructure operators that have their CSIRTs, to implement specialized systems for the identification, prevention, analysis, and damage recovery of cyberattacks, and to learn lessons for the future. Besides, operators should conduct risk management analyses and self-assessments on the level of cybersecurity maturity in the infrastructure they manage.

Sub Objectives:

Using advanced hardware and software solutions to identify, prevent and manage cyber incidents.

Analyzing critical and important information infrastructure to assess their risk management.

Developing strategic plans to protect cyberspace from potential incidents.

Conducting critical and important information infrastructure self-assessments to measure cybersecurity maturity levels.

Specific objective 4: Enhancing information infrastructure to combat cybercrime, radicalization, and violent extremism.

On the one hand, the internet leads to the development of society and facilitates quick procedures and access to data, but on the other, it is a tool for malicious individuals/groups to perpetrate cybercrime or to radicalize individuals from vulnerable or marginalized groups for extremist purposes and to commit punishable offenses. Concerning this, public and private organizations should take a series of measures to combat, control, and minimize these activities.

To achieve this, the development of mechanisms to regulate and provide safe internet in public spaces is aimed. Besides, the aim is to cooperate with civil society organizations and businesses to control and identify polluting elements circulating online and threatening cybersecurity in the country. In this context, mechanisms to monitor the abovementioned phenomena will be developed.

Sub Objectives:

Monitoring and preventing phenomena that stimulate violent extremism and radicalization among vulnerable groups in cyberspace.

Continuously identifying polluting elements circulating online and threatening cybersecurity in the country.

Developing mechanisms to regulate safe internet in public spaces, certified by the regulatory entity for the cybersecurity field.

Developing the capacities of the authorities responsible for fighting cybercrime.

Increasing regional cooperation in the fight against cybercrime.

5. Policy goal 2: Developing a safe cyber space educating and raising awareness in the society regarding professional capacity building in the information security field

Ensuring professional skills and capacities to respond to and manage cybersecurity incidents is no longer just an option in our times.

Building capacities in the cybersecurity field aims at responding as effectively as possible against cybercrime. This is an integral component of the international cooperation that could improve harmonization with the EU vision for a global, open, free, and safe cyberspace for all, ensuring respect for human rights.

The methods used to develop capacities and raise the awareness of the society are fundamental in determining the effectiveness of establishing a safe space.

Specific objective 1: Professional capacity building in the information security field through revision of education curricula.

Sub Objectives:

Developing higher education study programs in the cybersecurity field, to developsa new generation of cybersecurity experts.

Developing recommendations for the integration of safe internet related information into university curricula.

Improving research and innovation capacities in the cybersecurity field.

Specific objective 2: Awareness raising and professional skills building on cybersecurity in public and private institutions.

Sub Objectives:

Training for central and local level administrative staff to enhance knowledge on cybersecurity based on the field dynamics.

Business research and innovation capacity building and support through the establishment of cybersecurity scientific research centers.

Building CSIRT capacities at the national and executive public administration level through training and cyber drills.

5.3 Specific objective 3: Raising society awareness on cybersecurity and cyber threats.

Sub Objectives:

5.3.1 Awareness-raising campaigns on cybersecurity with various stakeholders, using adequate means of realizing them including audiovisual and social media, organized by the authority responsible for cybersecurity.

5.3.2 Establishing an online education platform on cybersecurity to raise awareness among various age groups in the society on safe internet use and digital infrastructure.

6. Policy goal 3: Developing mechanisms required for child safety in cyberspace, while preparing the younger generation to benefit from the advantages of information technology and overcome the challenges from the recent developments.

Providing safe internet for children and youth in Albania remains one of the strategic objectives of the Albanian government, as also stated in the National Agenda for the Child Rights 2017-2020. The internet, smartphones, and several other information technologies have become a part of the daily lives of a considerable number of children. The family (parents), peers and the school are three spaces where children socialize, while the digital space has become the fourth. For them, the distinction between online and offline is becoming increasingly blurred and they shift incessantly between the two spaces. Child protection online requires specific and articulated actions. At the same time, child protection should be proportional to the risks children face, and they should not restrict the use of information technology for child growth, education, and development. Government policies should create a digital space that is responsive to the needs of children while at the same time guaranteeing the protection and respect of their rights. Thus, taking immediate steps to create safe digital spaces is paramount, while also guaranteeing

the respect for their rights and the fulfillment of all children's development potential.

6.1 Specific objective 1: Strengthening the legal framework to improve child safety online

Sub Objectives:

6.1.1 Development of a dedicated legal framework on collecting incident data on reported cases of online violence, bullying, and abuse of children in schools.

6.1.2 Improvement of the Criminal Code, aligning it with the international legislation on child protection from online sexual abuse.

6.1.3 Amendment to the criminal procedure provisions in the Code of Criminal Procedure and adoption of regulatory acts providing for criminal acts related to child sexual abuse, and for relevant procedures and time frames to improve investigation effectiveness, case priority, and evidence analysis in connection to child sexual abuse cases online or through communication technologies.

6.1.4 Legislation completion and clarification regarding notice and take down procedures, and blocking of illegal materials online.

6.2 Specific objective 2: Preventing child sexual abuse online through awareness-raising and the creation of a safe online navigation space

Sub Objectives:

6.2.1 Developing and establishing programs for internet safety awareness-raising in the education system.

6.2.2 Establishing and supporting the ICT teachers' online network to promote children's protection online issues.

6.2.3 Establishing safe internet public spaces for children and their families through initiatives to provide both free access to and filtered information to protect children and youth from abusive content online.

6.2.4 Application of filters in public and private schools to prevent child access to harmful and illegal websites, and continuous information for ICT teachers on incident reporting.

6.2.5 Identification, support, and promotion of talents in developing technical solutions tackling online protection and safety.

6.3 Specific objective 3: Effective investigation and bringing perpetrators of cybercrime against children to justice, focusing on sexual abuse and exploitation

Sub Objectives:

6.3.1 Ensuring technical means to assist police and relevant bodies in analyzing and uncovering cases of online violence, especially those related to child sexual abuse materials with children

6.3.2 Establishing training programs for the judiciary, prosecution, and police officials regarding child protection online and cybersecurity, including evidence of digital use and mutual legal assistance.

6.3.3 Developing a courses system at the School of Magistrates and the Security Academy on cases related to crimes against children online and methods for protecting them online.

6.3.4 Developing standardization mechanisms for digital forensic evidence analysis work for the dedicated cybercrime structures at the Albanian State Police.

6.3.5 Establishing a working group with the participation of State Police cybercrime structures and industry to resolve issues of investigating and identifying persons suspected of abusing children online, focusing especially on the identification of end-users through IP addresses.

6.4 Specific objective 4: Awareness raising and education for all segments of the society regarding safe internet use for children

Sub Objectives:

6.4.1 Awareness-raising campaigns with parents and educators on the risks and issues children face online.

6.4.2 Developing training programs for ICT teachers regarding safe internet issues.

6.4.3 Developing training programs for Child Protection Workers regarding case management of children in need of protection in which the risk of violence, abuse, exploitation, or neglect is connected to the internet or information technology.

6.5 Specific objective 5: Strengthening cross-sector cooperation for the protection of children online

Sub Objectives:

6.5.1 In cooperation with ISPs, promoting existing mechanisms for child safety online, that are applied in their platforms.

6.5.2 Integration of the IWF (Internet Watch Foundation Hash List) List, which prevents anyone from uploading, downloading, or viewing child sexual abuse images or videos in all Internet Service Providers platforms, and providing access to this list for State Police cybercrime investigation structures.

6.5.3 Establishing a Technical Advisory Committee for Child Safety Online, within the National Council for Child Rights and Protection.

7. Policy goal 4: Improving national and international cooperation with strategic partners in the cybersecurity field

Coordination and cooperation among all actors are the core element to guarantee success. Cooperation with the private sector should be strengthened because of the Information and Communication Technology (ICT) rapid development dynamic. ICT security and development in the state administration can only be enhanced with close cooperation and in coherence with technology developments and trends. Increased cooperation and coordination between state institutions will be strengthened to guarantee interaction and coordination in strengthening security and minimizing damages from cyber-attacks.

Albanian endorses and will be a part of international initiatives aimed at improving and strengthening security. Cooperation with NATO and the EU will be specially strengthened by becoming part of common cybersecurity initiatives. Albania's membership in internationally recognized cybersecurity organizations and forums and improved cooperation are priorities.

In the quality of NATO member country, Albania recognizes cyberspace as the fifth domain of warfare, along with land, sea, air, and space. Cyberspace presents challenges and security in this domain is only achieved by thinking globally and working closely at the international level.

Specific objective 1: Strengthening institutional cooperation at the national level

Sub Objectives:

Increasing cooperation and coordination among state institutions to guarantee cyberspace security at the national level.

Establishing a tool for information exchange between dedicated contact points in relevant institutions, in case of cyberthreats.

Establishing a flexible structure with the best cybersecurity experts in the country to provide support in case of cyber crises, and national level cybersecurity level testing and assessment.

7.2 Specific objective 2: Strengthening international cooperation in the cybersecurity and cyber defense field and countering violent extremism and radicalization

Sub Objectives:

7.2.1 Developing effective mechanisms and procedures for international cooperation in case of cyber incidents, attacks, and crises, based on internationally defined principles.

7.2.3 Strengthening cooperation and information exchange with NATO/OSCE and other international organizations/forums.

PART IV IMPLEMENTATION, INSTITUTIONAL RESPONSIBILITY, ACCOUNTABILITY

The development of the National Cybersecurity Strategy 2020-2025 is based on the European Union Cybersecurity Strategy and is a continuation of the Cybersecurity Policy Paper 2015-2017.

- A participatory and comprehensive methodology with all public institutions contributing to cybersecurity in the country was used, providing a large number of stakeholders with the opportunity to contribute.

- The strategy was based on EU and other international organization commitments and standards, and on the two assessments conducted by ITU and the Oxford University with the support of the World Bank.

- The engagement of public and private organizations allows this Strategy to be objective and implementable. The inter-institutional working group and all the stakeholders involved in the consultation process provided valid comments leading to a series of draft revisions, intending to adopt a comprehensive strategy where everyone takes ownership and contributes to guaranteeing cybersecurity in the country.

- This Strategy is not just for the institutions but is also a strategy that stimulates and supports cyber protection for individuals, citizens, and especially children as the future of this country. It also identifies measures to not only fight cybercrime, but also incitement of terrorism and violent extremism through the cyberspace.

The action plan accompanying the National Cybersecurity Strategy 2020-2025 was developed based on the following:

a) findings and recommendations of the Cybersecurity Policy Paper 2015–2017 implementation assessment report;

b) findings and recommendations from the ITU[81] and Oxford University[82] assessment reports;

c) Public institutions budget plans for the 2020 to 2022 period.

As provided in the specific objectives and main activities proposed in this Strategy and the Action Plan, the coordinating role should be taken by the National Electronic Certification and Cybersecurity Authority in cooperation with the National Agency for Information Society.

Besides, this document considers the obligations stemming from the European integration process, the recommendations made in this regard by the NIS Directive and the EU adaptations for ENISA as EU CERT, and the relevant commitments as a NATO member country.

[81] https://cesk.gov.al/Publikime/2019/Albania_Assessment_ReportITU.pdf

[82] https://cesk.gov.al/Publikime/2019/AlbaniaCMMReport.pdf

After having been assessed and completed by the inter-institutional working group responsible for developing the Strategy, all proposed measures/activities were further detailed during the review of financial effects resulting from the implementation of this National Strategy and its Action Plan 2020-2025, establishing the need to review biannually based on the sector development dynamics.

Any institution responsible for activities should plan for their realization guaranteeing earmarked budgets, human resources, and technical capacities for their implementation.

An annual assessment will be undertaken to review activity implementation and identified objectives achievement, based on indicators met. Institutions responsible for implementing activities and achieving results must report following reporting standards. The Strategy Coordinator should develop and publish the annual report.

PART V
ACTION PLAN AND FINANCIAL RESOURCES FOR IMPLEMENTATION

Activity costing methodology

The expenditures required for the NAP implementation have been determined through a costing of the activities in this action plan. The methodology used to develop these costs presents a combination of the methods that can be used in multi-actor strategies.

The main methodology used is the Activity-Based Costing – ABC, where the responsible institution and the sources for covering costs are identified for each activity, and resources are allocated for all products and services based on the actual consumption for each activity

The budget was developed based on the cost of each activity reflected in the action plan, the length and frequency of its implementation, and the number of beneficiaries per activity.

The following methodology has been used to estimate costs for the main activities:

- The estimation for human resources expenses is based on the estimated time required to implement the activity and an average daily wage for a given category of civil servants.

- Services expenses estimation.

Service costs in the relevant institutions based on adopted standards were considered for these activities.

- Costing of activities related to the development and review of legislation, monitoring, and functioning of permanent structures, etc.

Estimations for these activities consider running expenses incurred for example for salaries, Social Security contributions, international expertise (when planed), and consumables.

- Estimation of expenses for activities related to studies, awareness-raising campaigns, training programs, foreign expertise, etc., was based on specific similar initiates and the nature of activities and market costs for such services.

- In estimating training expenses, the training cost per person was considered. ASPA costs and/or costs applied to similar training in the past were used as cost units.

- For activities, information on which was not complete (such as projects or studies), an analogy method for costing is applied, meaning that expenses for similar activities included in previous budget programs were considered.

Budget and financial resources for action plan implementation

The Nation Cybersecurity Strategy will be implemented during the 2020-2025 period. The expenses required for each activity, specific objective and policy goal have been costed to enable the implementation of this strategy.

The overall budget for the implementation of the Strategy is reflected in various forms:

- The overall budget per year for each activity, specific objective, strategic goal and funding sources

- The Budget is detailed according to activity, financing source and institutions responsible.

Policy	Specific objective	Sub-Objective	Responsible institution	Results	Total cost	2021	2022	2023	2024	2025	Cost in ALL	Donors	Other	Gap
Policy Goal 1	**Specific Objective A** - Improving the legal framework providing norms and regulating cybersecurity in the country and aligning this framework with European Union directives and regulations.	**A.1** Improving cybersecurity regulatory framework in line with sector laws, to appropriately address and resolve issues including, but not limited to IoT, 5G technology, artificial intelligence.	NAECCS	A.1.1 DCM "On some Addenda and Amendments to DCM No. 69/2016 "On Approving the Regulation on Electronic Identification and Trusted Services", drafted and approved	78,000	62,400	15,600	-			78,000			-
			NAECCS	A.1.2 DCM "On some Addenda and Amendments to DCM No. 222, dated 26.04.2018, "On Approving Critical Information Infrastructure List and Important Information Infrastructure List", drafted and approved	78,000	62,400	15,600	-			78,000			-
			NAE CCS	A.1.3 Drafted and approved legal and sub-legal acts on cybercrime, considering the applicable legal framework in the Republic of Albania and the EU.	78,000	62,400	15,600	-			78,000			-
			NAE CCS	A.1.4 Analyzing the legal and institutional gap in EU Directives and Regulations regulating cybersecurity	61,200	61,200	-	-			61,200			-
			NAE CCS	A.1.5 Approved aligned legislation	140,400	46,800	46,800	46,800			140,400			-
				A.1.6 Regulation on providing safe internet in public spaces, drafted and approved	187,200	62,400	62,400	62,400			187,200			-
				Subtotal A.1	**622,800**	**337,800**	**136,000**	**109,200**	**-**	**-**	**622,800**	**0**	**0**	**-**
		A.2 Continuously adapting standards and rules to the developments of the cybersecurity field.	PA	A.2.1 Drafted procedures for cybercrime identification	-	-	-	-			-			-
			PA	A.2.2 Drafted procedures for cyber incidents identification	-	-	-	-			-			-
			PA	A.2.3 Periodic reports on measuring the adaptability and efficiency of the national regulation on cybercrime	-	-	-	-			-			-
			PA	A.2.4 Strategies and policies on cyber protection of classified systems, drafted and approved.	-	-	-	-			-			-
			PA	A.2.5 Technical procedures and policies on cyber protection of classified systems	-	-	-	-			-			-
				Subtotal A.2	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**0**	**0**	**-**
		A.3 Meeting engageme	PA	A.3.1 Aligning local and international cybercrime policies	-	-	-	-			-			-
			NAECCS	A.3.2 Aligning local and North Atlantic Treaty Organization cybercrime policies	244,800	81,600	81,600	81,600			244,800			-
			NAECCS	A.3.3 Actively partaking in periodic										

		nts undertaken regarding cyberspace as a member country of the North Atlantic Treaty Organization.		meetings of NATO initiatives, such as CDMB, MISP, etc.	2,925,000	975,000	975,000	975,000			2,925,000			-
			NAECCS	A.3.4 Partaking in joint cyber drills organized by NATO, coordinated with national security and protection institutions	3,412,500	1,137,500	1,137,500	1,137,500			3,412,500			-
				Subtotal A.3	**-**	**-**	**-**	**-**			**-**	**-**	**-**	**-**
		A.4 Defining a national procedure for extraordinary situations created by cyber crises, with the aim of taking concrete measures to resolve the situation in real-time.	NAECCS	A.4.1 Risk assessment methodology at the national level, drafted and approved.	244,800	81,600	81,600	81,600			244,800			-
				Subtotal A.4	**244,800**	**81,600**	**81,600**	**81,600**	**-**	**-**	**244,800**	**0**	**0**	**-**
		Subtotal A			867,600	439,200	237,600	190,800	-	-	867,600	-	-	-
	Specific Objective	B.1 Establishing the National CSIRT and new sector CSIRTs in critical and important information	CISD NAE CCS NAE CCS NAECCS NAE	B.1.1 Establishing a structure within CISD, which will play the role of the National Cyber Protection Authority for systems treating "state secret" classified information, according to DCM No. 542, dated 25.07.2019, "On Approving the Regulation "On Securing Classified Information handled in Information and Communication Systems (ICS)"	18,450,724	5,464,108	6,493,308	6,493,308	-	-	18,450,724			-
				B.1.2 Procedures on the functioning of the National CSIRT, drafted and approved	-	-	-	-						-
				B.1.3 Approved structure and responsibilities of the National CSIRT.	91,800	61,200	30,600	-			91,800			-
				B.1.4 Reporting system for security break events in IT systems, developed and operational		-	-	-			-			
				B.1.5 Assessment and monitoring	52,000	52,000	-	-			52,000			-

		infrastructures, and strengthening existing ones	CCS	sector CSIRT capacities, developed										
			NAIS	B.1.6 Upgrading and extending security infrastructures.	106,525,000	53,649,000	24,841,000			106,525,000			-	
			NAIS	B.1.7 Improving hardware structures. Establishing a control system for access to Gov NET. network.	107,880,000	29,389,000	53,649,000	24,842,000			107,880,000			-
				Subtotal B.1	**232,595,224**	**83,003,308**	**113,813,908**	**36,176,308**	**-**	**-**	**233,862,224**	**-**	**-**	**-**
		B.2 Creating optimal work conditions for CSIRT operation, in line with the duties to guarantee cybersecurity in critical and important information infrastructure.	NAIS	B.2.1 Procedures on operating the Government CSIRT, drafted	46,800	46,800	-	-			46,800			-
			NAECCS	B.2.2 Assessment and monitoring capacities for implementing the sector CSIRT methodology establishment, developed	61,200	61,200	-	-			61,200			-
				Subtotal B.2	**108,000**	108,000	-	-	-	-	108,000	-	-	-
		B.3 Building CSIRT capacities through training and cyber drills.	NAECCS	B.3.1 Study and training programs in cybersecurity, developed and implemented.	62,400	62,400	-	-			62,400			-
			NAECCS	B.3.2 Cyber drills at the national level, minimum 4 times a year	920,000	920,000	-	-			920,000			-
				Subtotal B.3	**982,400**	982,400	-	-	-	-	982,400	-	-	-
		Subtotal B			234,089,224	64,093,708	113,813,908	56,176,308	-	-	234,957,524	-	-	-
	Specific Objective C - Strengthening and implementing securit	C.1 Using advanced hardware and software solutions to identify, prevent and manage cyber incidents.	NAIS	C.1.1 researching strengthening national priorities as a basis to envisage cybersecurity development investments.	124,800	-	-	-			-			124,800
				Subtotal C.1	**-**	-	-	-	-	-	-	-	-	-
		C.2 Analyzing	NAECCS	C.2.1 Procedures for reducing and managing risks in cyberspace, drafted	124,800	62,400	62,400	-			124,800			-

	y measures in critical and important information infrastructure	critical and important information infrastructure to assess their risk management		and approved											
				Subtotal C.2	124,800	62,400	62,400	-	-	-	124,800	-	-	-	

		C.3 Developing strategic plans to protect cyber space from potential incidents.	NAEC CS NAEC CS	C.3.1 Procedures, policies and plans for protecting cyberspace from cyber incidents, drafted and approved.	187,200	62,400	62,400	62,400			187,200			-
				C.3.2 Drafting cooperation agreements through actors in the field, aiming at ensuring protection, testing and assessment of cyberspace security level.	140,400	46,800	46,800	46,800			140,400			-
				Subtotal C.3	327,600	109,200	109,200	109,200	-	-	327,600	-	-	-
		C.4 Conducting critical and important information infrastructure self-assessments to measure cybersecurity maturity levels.	NAECCS	C.4.1 Self-assessment in critical and important information infrastructure for measuring Cybersecurity maturity level.	187,200	62,400	62,400	62,400			187,200			-
				Subtotal C.4	187,200	62,400	62,400	62,400	-	-	187,200	-	-	-
		Subtotal C			639,600	234,000	234,000	171,600	-	-	639,600	-	-	-
		D.1. Monitoring and preventing phenomena that stimulate violent extremism and radicalization among vulnerable groups in cyber space	CVE	D.1.1. Developing and operating a software that absorbs key words generated from websites in Albanian language, aiming at detecting, analyzing and blocking content that disseminates/promotes violence, extremism, and hate through the internet.	-	-	-	-			-			-
			CVE	D.1.2 Organizing awareness raising campaigns in schools as community centers, titled: "Combating Online Radicalization and Violent Extremism" with different target groups, according to the profile and portfolio of line ministries, subordinate institutions, and the local government.	-	-	-	-			-			-
				Subtotal D.1	-	-	-	-	-	-	-	-	-	-
		D.2 Continuously identifying polluting elements circulating online and threatening cybersecurity in the country	PA	D.2.1. Existing identified cyber protection capacities	-	-	-	-			-			-
				Subtotal D.2	-	-	-	-	-	-	-	-	-	-
		D.3 Developing	NAECCS	D.3.1 Support mechanisms for Information and Communication Technology and	234,000	78,000	78,000	78,000			234,000			-

		mechanisms to regulate safe internet in public spaces, certified by the regulatory entity for the cybersecurity field		cybersecurity, drafted										
	Specific objective D - Enhancing information infrastructure to combat cybercrime, radicalization and violent extremism			**Subtotal D.3**	**234,000**	**78,000**	**78,000**	**78,000**	**-**	**-**	**234,000**	**-**	**-**	**-**
			NAIS	D.4.1 Analyzing current capacities and identifying gaps of responsible institutions	187,200	-	-	-			-			187,200
			NAIS	D.4.2 Preparing recommendations and monitoring their application for purposes of building the capacities of responsible authorities	187,200	-	-	-			-			187,200
			NAIS	D.4.2 Establishing a cyber protection system for critical information infrastructure of the government system.										-
				Establishing access control system in GovNet network	23,985,000	20,910,000	3,075	-	-	-				
				Risk assessment program + threat response and remediation	86,100,000	86,100,000	-	-	-	-				
				Designated Support Engineering Cybersecurity	13,530,000	13,530,000	-	-	-	-				
				Staff training	7,380,000	4,920,000	2,460,000	-	-	-				
				ISO 27001 Information security or review procedure	8,610,000	8,610,000		-	-	-				
		D.4 Developing the capacities of the authorities responsible for fighting cybercrime.		Monitoring service of sensitive information circulation on world wide web	60,885,000	40,590,000	20,295,000							
				Test Center of malicious programs and suspicious applications (Malware Testing Center MTC) developed and functional	6,150,000	6,150,000								
				HoneyPot Systems developed and operational for detecting, analyzing and preventing potential cyberattacks	79,950,000	79,950,000								
				Subtotal D.4	**286,964,400**	**260,760,000**	**22,758,075**	**-**	**-**	**-**	**-**	**-**	**-**	**374,400**
		D.5 Increasing regional cooperation in the fight against cybercrime	PA	D.5.1 Procedures of cooperation and information exchange in the field of cybercrime among relevant national entities and other security services, drafted and approved.	-	-	-	-			-			-
			PA	D.5.2 Drafting regional cooperation agreements among actors of the field in combating cybercrime.	-	-	-	-			-			-
				Subtotal D.5	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
		Subtotal D			287,198,400	260,838,000	22,836,075	78,000	-	-	234,000	-	-	374,400
	Total 1				**522,795,524**	**325,604,908**	**137,127,583**	**56,616,708**	**-**	**-**	**236,698**	**-**	**-**	**374,400**
											-			-

Policy Goal 2	Specific objective	Sub-Objective	Responsible institution	Results	Total cost	2021	2022	2023	2024	2025	Cost in ALL MTBP	Donors	Other	Gap
	A.1 -	Developing	NAECCS	A.1.1. Study programs drafted for the public administration servants.	187,200	62,400	62,400	62,400			187,200			-

		higher Education study programs												
	Specific Objective A - Professional capacity building in the information security field through revision of education curricula	in the cybersecurity field, with the aim of developing a new generation of cybersecurity experts	NAECCS	A.1.2 Study programs for the management staff in the public sector.	187,200	62,400	62,400	62,400			187,200			-
			NAECCS	A.1.3 Continuously training experts specialized in various cybersecurity aspects.	3,148,800	807,600	807,600	1,533,600			3,148,800			-
				Subtotal A.1	**3,523,200**	**932,400**	**932,400**	**1,658,400**	**-**	**-**	**3,523,200**	**-**	**-**	**-**
		A.2 Developing recommendations for the integration of safe internet related information into university curricula.	TBD (after 2022)	A.2.1. Establishing a scientific research center in the cybernetic security field.	-	-	-	-			-			-
			TBD (after 2022)	A.2.2 Partaking in national and international research projects and activities related to cybersecurity.	-	-	-	-			-			-
				Subtotal A.2	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
		A.3 Improving research and innovation capacities in the cybersecurity field	NAECCS	A.3.1 Conducting continuous training to ensure a high level of awareness and responsibility regarding protection and cybersecurity.	-	-	-	-			-			-
				Subtotal A.3	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**

		Subtotal A			3,523,200	932,400	932,400	1,658,400	-	-	3,523,200	-	-	-
	Specific Objective B - Awareness raising and professional skills building on cybersecurity in public and private institutions	B.1 Training for central and local level administrative staff to enhance knowledge on cybersecurity based on the field dynamics	NAECCS	B.1.1. Training curricula on cybersecurity, drafted	187,200	62,400	62,400	62,400			187,200			-
			NAECCS	B.1.2 Conducting trainings on cybersecurity with the administrative staff at the central level	4,238,400	1,412,800	1,412,800	1,412,800			4,238,400			-
			NAECCS	B.1.3 Conducting trainings on cybersecurity with the administrative staff at the local level	4,209,600	1,403,200	1,403,200	1,403,200			4,209,600			-
				Subtotal B.1	**8,635,200**	**2,878,400**	**2,878,400**	**2,878,400**	-	-	**8,635,200**	-	-	-
		B.2 Business research and innovation capacity building and support through the establishment of cybersecurity scientific research centers	NAECCS	B.2.1 Current situation analysis	234,000	78,000	78,000	78,000			234,000			-
			NAECCS	B.2.2 Developing business recommendations	187,200	62,400	62,400	62,400			187,200			-
			NAECCS	B.2.3 Monitoring and assessing the application of recommendations in business innovation	81,600	81,600	-	-			81,600			-
				Subtotal B.2	**502,800**	**222,000**	**140,400**	**140,400**	-	-	**502,800**	-	-	-
		B.3 Building CSIRT capacities at the national and executive public administration level through training and cyber drills	NAECCS	B.3.1 Developing training modules	124,800	62,400	62,400	-			124,800			-
			NAECCS	B.3.2 Organizing cyber drills	2,547,200	1,242,400	1,242,400	62,400			2,547,200			-
				Subtotal B.3	**2,672,000**	**1,304,800**	**1,304,800**	**62,400**	-	-	**2,672,000**	-	-	-
		Subtotal B			11,810,000	4,405,200	4,323,600	3,081,200	-	-	11,810,000	-	-	-
	Specific Objective C - Raising society awareness on cybersecurity and cyberthreats	C.1 Awareness raising campaigns on cybersecurity with various stakeholders, using adequate means of realizing them including audiovisual and social media	NAECCS	C.1.1 Developing awareness raising materials	-	-	-	-			-			-
			NAECCS	C.1.2 Organizing awareness raising campaigns	-	-	-	-			-			-
			NAECCS	C.1.3 Delivering awareness raising publicity campaigns/spots on audiovisual media	-	-	-	-			-			-
				Subtotal C.1	-	-	-	-	-	-	-	-	-	-
		C.2 Establishing an online education platform on cybersecurity to raise awareness among various age groups in the society on safe internet use and digital infrastructure	NAECCS	C.2.1 Developing platform materials	-	-	-	-			-			-
			NAECCS	C.2.2 Developed and operational platform	-	-	-	-			-			-
				Subtotal C.2	-	-	-	-	-	-	-	-	-	-
		Subtotal C			-	-	-	-	-	-	-	-	-	-
	Total 2				**589,730,000**	**527,013,600**	**50,928,150**	**4,895,600**	-	-	**15,801,200**	-	-	**748,800**

Policy Goal 3	**Specific objective**	**Sub-Objective**	**Responsible institution**	**Results**	**Total cost**						**Cost in ALL**			
						2021	**2022**	**2023**	**2024**	**2025**	**MTBP**	**Donors**	**Other**	**Gap**
	Specific Objective A - Strengthening the legal framework to improve child online safety	A.1 - Drafting a special guideline (and associated regulation) on collecting incident data on reported cases of online violence, bullying and abuse of children in schools.	MoESY	A.1.1. Guideline for collecting data on reported incidents of online abuse, bullying, and violence in schools, drafted and approved.	-	-	-	-			-			-
			MoESY	A.1.2 Associated regulation on collecting data on reported incidents of online abuse, bullying, and violence in schools, drafted and approved.	-	-	-	-			-			-
			MoESY	A.1.3 Methodology of collecting data on incidents in schools, drafted and approved	-	-	-	-			-			-
			MoESY	A.1.4 Reports of local educational institutions that are responsible for pre-university education	-	-	-	-			-			-
				Subtotal A.1	-	-	-	-	-	-	-	-	-	-
		A.2 Improving the regulatory framework, aligning it with the international legislation on child protection from online sexual abuse	NAECCS	A.2.1. Analyzing the national legal gap of children's protection from online sexual abuse	124,800	-	124,800	-			124,800			-
			NAECCS	A.2.2 Preparing recommendations on alignment with the international legislation.	62,400	-	62,400	-			62,400			-
			NAECCS	A.2.3 Drafted and approved legal acts	46,800	-	46,800	-			46,800			-
				Subtotal A.2	234,000	-	234,000	-	-	-	234,000	-	-	-
		A.3 Completing and clarifying the legislation regarding notices and removal and blocking of illegal material online	NAECCS	A.3.1. Analyzing and identifying gaps at the national level	124,800	124,800	-	-			124,800			-
			NAECCS	A.3.2 Drafting the necessary protocol for interinstitutional coordination	62,400	62,400	-	-			62,400			-
			NAECCS	A.3.3 Drafted and approved protocol	46,800	46,800	-	-			46,800			-
				Subtotal A.3	234,000	234,000	-	-	-	-	234,000	-	-	-
		Subtotal A			468,000	234,000	234,000	-	-	-	468,000	-	-	-
	Specific Objective B - Preventing child online sexual abuse through awareness raising and the creation of a safe online browsing space	B.1 Integrating the "Peer Educators for Online Safety" program in the educational system	MoESY	B.1.1. Drafting procedures for integrating the "Peer Educators for Online Safety" program in 9K schools	-	-	-	-			-			-
				Subtotal B.1	-	-	-	-	-	-	-	-	-	-
		B.2 Establishing and supporting the ICT online teachers' network to promote the online child protection issue	MoESY	B.2.1 Establishing an online ICT teachers' network	-	-	-	-			-			-
			MoESY	B.2.2 Developing a communication platform	-	-	-	-			-			-
				Subtotal B.2	-	-	-	-	-	-	-	-	-	-
		B.3 Creating safe internet public spaces for	NAECCS	B.3.1 Developing a guideline on safe internet in public spaces	182,000	78,000	78,000	26,000			182,000			-
			NAECCS	B.3.2 Monitoring the guideline application	31,200	31,200	-	-			31,200			-

		children and families through the "Friendly Wi-Fi" initiative in 5 municipalities of the country, to provide both free access to and filtered information to protect children and youth from abusive content online.		**Subtotal B.3**	**213,200**	**109,200**	**78,000**	**26,000**	-	-	**213,200**	-	-	-
		B.4 Applying filters in public and private schools to prevent child access to inadequate and illegal websites, and continuous information for ICT teachers on incident reporting.	MoSEY	B.4.1 Reports on the maintenance and control of filters validity	-	-	-	-			-			-
			MoSEY	B.4.2 Monthly and annual reports of children's online safety incidents by ICT teachers at local educational institutions that are responsible for pre-university education/MoESY.	-	-	-	-			-			-
				Subtotal B.4.	-	-	-	-	-	-	-	-	-	-
		B.5 Identifying, supporting and promoting talent in developing technical solutions helping online safety and protection	MoSEY	B.9.1 Developing methodologies for identifying new talents	-	-	-	-			-			-
			MoSEY	B.9.2 Monitoring the developed methodology application	-	-	-	-			-			-
				Subtotal B.5.	-	-	-	-	-	-	-	-	-	-
		Subtotal B			213,200	109,200	78,000	26,000	-	-	213,200	-	-	-
		C.1 Ensuring technical means to assist police and relevant bodies in analyzing and uncovering cases of online violence, especially those related to sexual abuse images with children	State Police	C.1.1 Current situation analysis in responding to cases of violence	-	-	-	-			-			-
			State Police	C.1.2 Preparing recommendations on the necessary means to effectively respond to reported cases	-	-	-	-			-			-
				Subtotal C.1	-	-	-	-	-	-	-	-	-	-
		C.2. Establishing training programs for judicial, prosecution and Police staff regarding child protection online and cyber security, including evidence of digital use and mutual legal assistance	MoI/NAECCS	C.2.1 Developing training curricula	124,800	62,400	62,400	-			124,800			-
			MoI/NAECCS	C.2.2 Organizing training programs	1,600,000	560,000	560,000	480,000			1,600,000			-
				Subtotal C.2	**1,724,800**	**622,400**	**622,400**	**480,000**	-	-	**1,724,800**	-	-	-
	Specific Objective C - Effectively investigating and bringing perpetrators to justice, focusing on sexual abuse and exploitation of children	C.3. Developing a courses system at the School of Magistrates and the Security Academy on cases related to crimes against children online and methods for protecting them online.	NAECCS	C.3.1 Developing training curricula	124,800	62,400	62,400	-			124,800			-
			NAECCS	C.3.2 Organizing training programs	1,600,000	560,000	560,000	480,000			1,600,000			-
				Subtotal C.3	**1,724,800**	**622,400**	**622,400**	**480,000**	-	-	**1,724,800**	-	-	-
		C.4 Developing standardization mechanisms for digital evidence analysis work for the State Police	PA	C.4.1 Current situation analysis on digital evidence testing mechanisms	124,800	62,400	62,400	-			124,800			-
			PA	C.4.2 Developing recommendations	62,400	62,400	-	-			62,400			-
			PA	C.4.3 Monitoring the applicability of established mechanisms	46,800	46,800	-	-			46,800			-
				Subtotal C.4	**234,000**	**171,600**	**62,400**	-	-	-	**234,000**	-	-	-
		C.5 Establishing a working group with the participation of the industry to resolve issues of investigating and identifying persons suspected of abusing children online, focusing especially on the identification of end users through IP addresses	PA	C.5.1 Developing an order on establishing the working group	-	-	-	-			-			-
			PA	C.5.2 Developing the working group cooperation methodology	-	-	-	-			-			-
				Subtotal C.5	-	-	-	-	-	-	-	-	-	-
		Subtotal C.			3,683,600	1,416,400	1,307,200	960,000	-	-	3,683,600	-	-	-
	Specific objective D - Raising awareness and educating all segments of the society on using safe internet for children	D.1 Awareness raising campaigns with parents and educators on the risks and issues children face online	NAECCS	D.1.1 Developing training curricula	124,800	62,400	62,400	-			124,800			-
			NAECCS	D.1.2 Organizing awareness raising campaigns	1,600,000	560,000	560,000	480,000			1,600,000			-
				Subtotal D.1	**1,724,800**	**622,400**	**622,400**	**480,000**	-	-	**1,724,800**	-	-	-
		D.2 Developing training programs for ICT teachers regarding safe internet issues	NAECCS	D.2.1 Developing training curricula	124,800	62,400	62,400	-			124,800			-
			NAECCS	D.2.2 Organizing training programs	1,600,000	560,000	560,000	480,000			1,600,000			-
				Subtotal D.2	**1,724,800**	**622,400**	**622,400**	**480,000**	-	-	**1,724,800**	-	-	-

		D.3 Developing training programs for Child Protection Workers regarding case treatment of children in need of protection in which the risk of violence, abuse, exploitation or neglect is connected to the internet or information technology	NAECCS	D.3.1 Developing training programs curricula	124,800	62,400	62,400	-			124,800			-
			NAECCS	D.3.2 Organizing training campaigns	1,600,000	560,000	560,000	480,000			1,600,000			-
				Subtotal D.3	**1,724,800**	**622,400**	**622,400**	**480,000**	-	-	**1,724,800**	-	-	-
		Subtotal D			5,174,400	1,867,200	1,867,200	1,440,000	-	-	5,174,400	-	-	-
	Specific Objective E - Strengthening cross-cutting cooperation for online children's protection	E.1 In cooperation with ISPs, promoting existing mechanisms for child safety online, that are applied in their platforms.	NAECCS	E.1.1 Organizing activities for promoting online child protection mechanisms	200,000	200,000	-	-			200,000			-
			NAECCS	E.1.2 Developing informative leaflets/materials with existing online child protection mechanisms	31,200	31,200	-	-			31,200			-
				Subtotal E.1	231,200	231,200	-	-	-	-	231,200	-	-	-
		E.2 Integration of the IWF (Internet Watch Foundation Hash List) List, which prevents anyone from uploading, downloading or viewing child sexual abuse images or videos	Proposal of the civil society (UNICEF)	E.2.1 Developing a guideline on integrating the IWF list in ISPs platforms	-	-	-	-			-			-
			Proposal of the civil society (UNICEF)	E.2.2 Monitoring the applicability of the drafted guideline	-	-	-	-			-			-
				Subtotal E.2	-	-	-	-	-	-	-	-	-	-
		E.3 Establishing a Technical Advisory Committee for Child Safety Online, within the National Council for Child Rights and Protection	MoHSP	E.3.1 Meetings of the Technical Advisory Committee for Children's Rights and Protection.	-	-	-	-			-			-
			MoHSP	E.3.2 Defining regulations on children's rights and protection	-	-	-	-			-			-
				Subtotal E.3	-	-	-	-	-	-	-	-	-	-
		Subtotal E			231,200	231,200	-	-	-	-	231,200	-	-	-
	Total 3				**9,770,400**	**3,858,000**	**3,486,400**	**2,426,000**	-	-	**9,770,400**	-	-	-

Policy Goal 4	Specific objective	Sub-Objective	Responsible institution	Results	Total cost						Cost in ALL			
						2021	2022	2023	2024	2025	MTBP	Donors	Other	Gap
	Specific Objective A - Strengthening institutional cooperation at the national level	A.1 Increasing cooperation and coordination among state institutions to guarantee cyber space security at the national level	NAECCS	A.1.1 Developing and signing interinstitutional agreements	140,400	46,800	46,800	46,800			140,400			-
			NAECCS	A.1.2 Establishing a network of focal points and drafting the network working methodology	140,400	46,800	46,800	46,800			140,400			-
			NAECCS	A.1.3 Establishing a joint communication platform for cooperating and strengthening trust among other public and private teams of CERT and CSIRT, and academic communities.	140,400	46,800	46,800	46,800			140,400			-
				Subtotal A.1.	421,200	140,400	140,400	140,400	-	-	421,200	-	-	-
		A.2 Establishing a tool for information exchange between dedicated contact points in relevant institutions, in case of cyberthreats.	NAECCS	A.2.1. Building trust among all relevant actors, including the development of a national platform/system for exchanging information on laws, incidents and immediate threats.	140,400	46,800	46,800	46,800			140,400			-
			NAECCS	A.2.2 Developing and implementing a system and programs for exchanging information, knowledge and experience among the public, protection and security in the field of cyber protection.	140,400	46,800	46,800	46,800			140,400			-
			NAECCS	A.2.3 Advancing existing and new mechanisms of cooperation and information exchange with private and civil sectors.	140,400	46,800	46,800	46,800			140,400			-
			NAECCS	A.2.4 Cooperation with all relevant actors in the process of developing and joining security norms, cooperation standardization, and definition and establishment of the mandatory level of protection for subjects that manage cyber incidents.	140,400	46,800	46,800	46,800			140,400			-
			NAECCS	A.2.5 Developing a unified format with awareness raising messages about online safety by ISPs, which will be displayed on sales points	62,400	62,400	-	-			62,400			-
				Subtotal A.2	**624,000**	**249,600**	**187,200**	**187,200**	-	-	**624,000**	-	-	-
		A.3 Establishing a flexible structure with the best cybersecurity experts in the country to provide support in case of cyber crises, and national level cybersecurity level testing and assessment	NAECCS	A.3.1 Setting up a tool for establishing the structure	124,800	62,400	62,400	-			124,800			-
			NAECCS	A.3.2 Developing the cooperation methodology	124,800	62,400	62,400	-			124,800			-
				Subtotal A.3	**249,600**	**124,800**	**124,800**	-	-	-	**249,600**	-	-	-
		Subtotal A			**1,294,800**	**514,800**	**452,400**	**327,600**	-	-	**1,294,800**	-	-	-
	Specific Objective B - Strengthening international cooperation in the cybersecurity and defense field and to counter violent	B.1. Developing effective mechanisms and procedures for international cooperation in case of cyber incidents, attacks, and crises, based on internationally defined principles	NAECCS	B.1.1 Becoming a member to international organizations, such as: ENISA, FIRST, etc., to be aligned with the latest developments of cybersecurity.	140,400	46,800	46,800	46,800			140,400			-
			NAECCS	B.1.2 Developing and signing bilateral and/or multilateral interinstitutional agreements for obtaining and disseminating information	140,400	46,800	46,800	46,800			140,400			-
				Subtotal B.1	**280,800**	**93,600**	**93,600**	**93,600**	-	-	**280,800**	-	-	-

	extremism and radicalization														

				TOTAL STRATEGY COST 374,400	**522,795,524**	**325,804,908**	**137,127,583**	**56,616,708**	-	-	236,698,724	-	-		
		B.2. Strengthening cooperation and information exchange with NATO/OSCE and other international organizations/forums	NAECCS	B.2.1 Actively partaking in NATO meetings for implementing international standards and regulations in the framework of cybersecurity	2,700,000	900,000	900,000	900,000			2,700,000			-
			NAECCS	B.2.2 Actively partaking and contributing to building skills at the global level for cybersecurity and trust building activities.	2,700,000	900,000	900,000	900,000			2,700,000			-
			NAECCS	B.2.3 Becoming a member and partaking in different international activities and in cybersecurity (FIRST, Trust Introducer)	-	-	-	-			-			-
				Subtotal B.2	**5,400,000**	**1,800,000**	**1,800,000**	**1,800,000**	-	-	**5,400,000**	-	-	-
		Subtotal B			**5,680,800**	**1,893,600**	**1,893,600**	**1,893,600**	-	-	**5,680,800**	-	-	-
	Total 4				**6,975,600**	**2,408,400**	**2,346,000**	**2,221,200**	-	-	**6,975,600**	-	-	-