NATIONAL CYBER SECURITY STRATEGY 2025 - 2030

Contents

PART I: STRATEGIC CONTEXT

1. Introduction

In a period where digital transformation is profoundly impacting all aspects of social, economic, and institutional life, cybersecurity has gained extraordinary importance everywhere in the world. Albania, as an inseparable part of the global information ecosystem, is committed to facing the challenges and embracing the opportunities offered by cyberspace, in order to ensure a safe and trustworthy digital environment for its citizens, businesses, and institutions.

National Cybersecurity Strategy 2025-2030 is an important document that reflects this commitment and sets out the strategic directions for the development and strengthening of cybersecurity in Albania.

The main objective of this strategy is to strengthen national capacities to identify, prevent, and manage cyber threats, including the protection of critical and important information infrastructures, the protection of sensitive data, and the guarantee of the continuity of digital services. It also aims to increase the necessary technical and professional capacities to address the ongoing challenges for the protection of the digital space and to promote international cooperation in order to improve the effectiveness and response to cyber incidents.

The strategy establishes a framework to increase the readiness and resilience of information systems and services in the country, ensuring that Albania meets international standards and best practices in this field. It reflects the harmonisation of cybersecurity policies with those of the European Union and international partners, to support the sustainable development of the country's information infrastructures and digital economy.

An important aspect of this strategy is the engagement of all actors such as: state institutions, the private sector, civil society, and higher education institutions, to create a coordinated and inclusive cybersecurity ecosystem. This will enable the sharing of information and resources, the development of common policies, and the increase of awareness about risks and security measures.

2. Assessment of the Current Situation in Albania

At a time when Albania is increasingly implementing information and communication technologies in every field of life, cyber security risks are also evolving rapidly. Global trends show an increase in cyber attacks, driven by state-sponsored actors, criminal organizations, and malicious groups. The state, economy, and Albanian government face ongoing cyber threats that require immediate attention to protect critical and important information infrastructure, public sector networks, and citizens' data.

In Albania, significant steps have been taken to strengthen cybersecurity. The drafting of the national cybersecurity strategy established a clear framework for the protection of critical and important information infrastructures and the management of cyber risks. The National Cybersecurity Authority has considerably strengthened and improved processes for monitoring, risk assessment, and threat management. Some of the most important achievements at the national level include the increase in the implementation of security measures in critical and important information infrastructures, as well as the enhancement of the technical capacities of experts through training and rigorous inspections.

Albania has significantly intensified cooperation with international organizations such as NATO and the European Union, ensuring compliance with international standards. In addition, steps have been taken to increase awareness and educate citizens and businesses on cyber security. Albania has harmonised its legislation with the directives of the European Union, thereby strengthening cyber protection at both the national and international level.

The cyber-attacks of recent years have highlighted the importance of improving standardized processes for incident response, strengthening network monitoring capacities, and developing centralized mechanisms for the effective sharing of information on threats.

Furthermore, in the Global Cybersecurity Index 2024, Albania has made remarkable progress, climbing 23 places in the global ranking, from 80th to 57th place, and advancing from 40th to 30th place in Europe, where it is ranked in the “Tier 2” group, which includes countries with rapid advancement in digital security.

In this regard, Albania is committed to building a secure and trustworthy digital space for citizens and businesses, strengthening the country's cyber resilience, accelerating the process of integration into the European Union, and positioning itself as a strong and reliable actor in the global digital era.

Despite the considerable progress that Albania has achieved in the field of cybersecurity, many tasks remain to be completed. Cybersecurity challenges become even greater as a result of the continuous increase in the number of cyberattacks, as well as the high and sophisticated level of these attacks, which exploit the most advanced technologies. The targets of these attacks are becoming increasingly broader, involving not only the public sector, but also vital services such as healthcare, finance, transport, and energy.

The use of the internet for spreading extremist ideologies and recruiting individuals for terrorist purposes is a growing threat, making the prevention of these activities increasingly complicated. In this context, the national security of Albania is closely linked to the ability to identify, prevent, and respond to cyber threats, including hybrid ones. A key aspect of this strategy is the development of intelligence structures specialized in monitoring and preventing extremist and terrorist activities in cyberspace. Within the framework of the fight against terrorism, an important focus is the prevention of extremist propaganda and online recruitment. This includes the use of advanced technologies to identify and shut down sites and content that promote violence and radicalization, as well as the establishment of cooperation mechanisms with international actors and online platforms.

Additionally, social factors are increasingly having an impact, including online bullying, the exploitation of children and vulnerable groups in society, as well as attacks against organizations and individuals with the purpose of disinformation and financial gain through the destruction of reputation, both at a personal and professional level.

3. Vision and Mission

3.1 Vision

The National Cybersecurity Strategy 2025-2030 has the vision of ensuring a secure, sustainable, and inclusive digital ecosystem that fosters trust, innovation, and the country’s economic progress.

By embracing digital transformation through the application of advanced technologies such as artificial intelligence, supercomputers, and blockchain, the strategy aims to strengthen Albania's position as a leader in cybersecurity in the region and integrate with the policies and legal and regulatory framework of the European Union.

Beyond technical protection, this vision reflects a broader commitment to support the political, social, and economic development of the country, promoting cooperation between institutions, the private sector, and international partners, by creating a unified approach for addressing new threats and opportunities in the digital era.

Through this strategy, Albania aims not only to protect its digital space, but also to create a culture of responsibility and awareness for cybersecurity. This comprehensive commitment will enhance the country's resilience to ongoing challenges, making Albania a model for advanced approaches to cybersecurity in the region and beyond.

3.2 Mission

The mission of the National Cybersecurity Strategy 2025-2030 is to create a strong and comprehensive shield to protect citizens, institutions, critical and important information infrastructures in the Republic of Albania from ongoing and evolving threats in cyberspace. This strategy aims to consolidate an advanced legal, technical, and organizational framework, aligned with European and international standards, to guarantee sustainable security and the development of the national digital ecosystem.

By building a secure digital environment, this strategy aims to empower citizens and create conditions for a society where technology serves as a catalyst for innovation and progress. By supporting sustainable economic and social development, the strategy not only protects national interests, but also promotes competition and Albania’s ability to play an important role in the digital transformation of the region and beyond. The mission also highlights the importance of inter-institutional and international cooperation in addressing the complex challenges of cybersecurity. It is based on a commitment to creating a culture of cyber responsibility, including increasing public awareness and building technical capacities and human resources. Through this strategy, Albania aims not only to face current cyber threats, but also to build a strong foundation for the protection and secure development of the digital space of the future by increasing cyber resilience at the national level.

PART II PURPOSE OF POLICIES AND SPECIFIC OBJECTIVES OF THE STRATEGY

The objectives of the National Cybersecurity Strategy 2025–2030 focus on strengthening the protection of critical and important information infrastructure in the country, by establishing a legal and technical framework that ensures the continuity of services and the stability of information systems.

The strategy aims to improve cooperation between the public sector, private sector and other actors to enhance defensive capacities and to enable the exchange of important information in the management of cyber incidents.

Another key objective is the development of technical and professional capacities to address cyber threats, by investing in skills development and advanced technologies.
Furthermore, the strategy promotes innovation and scientific research to enhance capabilities with the aim of anticipating, managing, and responding to cyberattacks, as well as increasing society's awareness and education on cybersecurity.
In this context, the strategy aims for compliance with the norms and directives of the European Union and the strengthening of cooperation with international partners to address sophisticated and hybrid threats that may endanger national security and the country's digital stability.

Policies

National Cybersecurity Strategy of Albania 2025-2030 is built upon five key policies, where ***Protection of Digital Infrastructure*** constitutes the core policy of the entire strategy. Developments in cybersecurity, which are closely connected to technological, economic, and geopolitical advances, the increase of international cooperation, as well as sophisticated cyber threats, require a national cybersecurity strategy that is dynamic and capable of adapting to rapid changes in the digital environment.

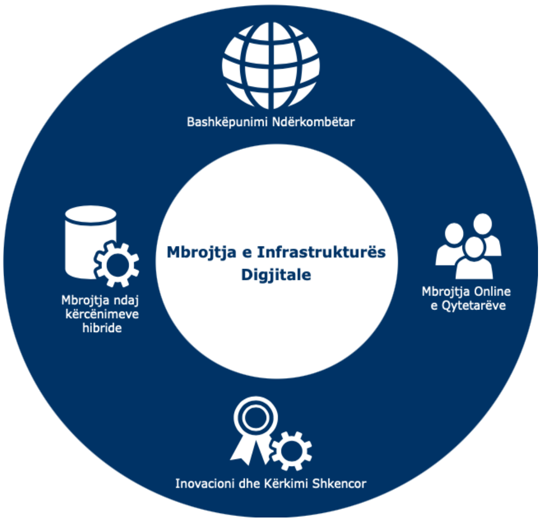
Bashkëpunimi Ndërkombëtar
Mbrojtja e Infrastrukturës Digjitale
Mbrojtja Online e Qytetarëve
Mbrojtja ndaj kërcënimeve hibride
Inovacioni dhe Kërkimi Shkencor

Figure 1. Strategy Policies

- The strategy is accompanied by an action plan that defines concrete activities for its implementation, aiming to achieve the specified objectives. This action plan specifies clear steps and deadlines for each phase of the process. *The purpose of the policy 1*: **Protection of Digital Infrastructure**: The basis of the National Cybersecurity Strategy is the protection of critical and important information infrastructures in the country, which includes the networks, systems, and services that support the functioning of the state and the daily lives of citizens. This policy aims to ensure the continuity of services and the protection of information systems that keep energy, transport, healthcare, finance, public administration, and other key sectors operating. Part of this policy are preventive and protective measures for identifying and minimizing risks, as well as the development of rapid response mechanisms in cases of cyber incidents in order to increase digital and cyber resilience.

- *Purpose of policy 2*: **Defence *online* of citizens and the promotion of cyber culture.** The creation and promotion of a culture of cybersecurity awareness across all groups of society are essential elements of this strategy. Awareness fosters shared responsibility. An informed citizen contributes to a safer chain in society, minimizing vulnerabilities that could be exploited by attackers. Public education and awareness is an ongoing process aimed at equipping citizens with knowledge and practical tools to address current challenges and make informed decisions. An informed society is able to contribute to public debate and to advocate for better policies. Likewise, it is important to promote cyber ethics and the observance of proper online conduct, as well as to prevent online radicalization, by promoting the use of respectful and responsible language.

  The National Cybersecurity Strategy 2025-2030 focuses on the creation of the necessary mechanisms for the online protection of citizens, particularly the protection of children and young people as well as underrepresented groups.
- *Purpose of policy 3:* **Strengthening International Cooperation**: Cybersecurity is an international challenge and a joint effort to address challenges related to threats and risks in the digital environment. The strategy promotes the strengthening of cooperation between institutions and international partners, encouraging the exchange of information, development of joint capacities, and the creation of unified standards, thus ensuring collective and more effective protection against cyber threats. In this context, Albania is committed to actively contributing to international initiatives and agreements, particularly the diligent implementation of existing obligations as a NATO member, thereby strengthening the resilience of the global digital environment.
- *The purpose of policy 4*: **Promotion of innovation and scientific research**: The National Cybersecurity Strategy embraces the use of the most advanced technologies, including artificial intelligence, *blockchain* and quantum computing, to strengthen cybersecurity and to address the complex challenges of an increasingly intricate digital environment. Innovation is an essential pillar that contributes to the improvement of advanced security protocols, early detection of threats, and ensuring the resilience of the digital ecosystem. Scientific research and the adoption of new technologies increase Albania's strategic capability to face cyber threats effectively, ensuring a trustworthy and sustainable digital environment.
- *Purpose of policy 5:* **Protection against hybrid threats**: To counter complex hybrid threats that exploit vulnerabilities in cyberspace, Albania is drafting a proactive, sustainable, and appropriate defense strategy. One of the key policies of this strategy is protection against hybrid threats. These threats include harmful activities that combine cyberattacks with other actions such as information manipulation, economic influence, political maneuvering, coercive diplomacy, and military threats. The objective of this policy is to identify and neutralize hybrid threats by strengthening defensive capacities, improving cooperation between institutions and international partners, and developing rapid response mechanisms, in order to preserve national security and the integrity of critical and important information infrastructures.

Objective of Policy 1: Protection of Digital Infrastructure

Protection of Digital Infrastructure It is the main policy of the National Cybersecurity Strategy of Albania 2025 - 2030. Securing information systems, communication networks, and critical and important information infrastructure assets is essential for national security, public safety, and economic stability.

The purpose of the protection of digital infrastructure aims to create a sustainable and effective model of joint protection that distributes responsibilities and manages risk by providing a high level of security and resilience for the digital ecosystem.

Addressing and handling cyber threats will only be successful if operators of critical and important information infrastructures have the necessary cooperation and awareness regarding the importance of implementing cyber security measures.

Pursuant to the main objective of of this pillar for the security and protection of information systems and communication networks through ensuring the availability, integrity, and confidentiality of data, Albania undertakes to take comprehensive and coordinated initiatives, which include addressing challenges in:

- Processes
- Technology
- Human Capacities

1. Processes

Processes play a key role in the National Cyber Security Strategy.

Processes include a series of interrelated and coordinated steps aimed at protecting digital assets, information systems, and communication networks from threats and cyber attacks. They define how a digital infrastructure interacts with all aspects of cybersecurity, including practices:

- clear and well-documented in the definition of roles and responsibilities;
- dynamics regarding hybrid threats;
- continuous and adaptive towards the maturity of the cybersecurity posture of the infrastructure.
-

Specific Objective 1.1: Drafting and implementation of the legal framework for Cybersecurity

This objective includes the process of harmonizing international standards and directives in the drafting of legislation and the regulatory framework that determine the manner of managing cybersecurity at the national level. The purpose of this objective is to ensure effective protection against cyber threats and attacks by aligning with security requirements and the needs for the development of new technologies.

Specific Objective 1.2: Improvement of Monitoring Capacities and Protection of Systems

This objective includes the continuous monitoring of information systems and communication networks, tracking suspicious activities, identifying vulnerabilities, developing secure software and hardware products, and ensuring a secure approach for users. The purpose of this objective is to minimize risks through the implementation of proactive measures and ensuring sustainable protection against cyber-attacks and threats, including the expansion of control and compliance activities for advanced technologies such as blockchain, cloud computing, AI, and other emerging technologies to ensure the protection of new systems and their integration into existing security ecosystems.

Specific objective 1.3: Cyber governance and Risk Management

This objective includes the ongoing assessment of cyber risks, including the identification, evaluation, analysis, and treatment of risks at the infrastructure, sector, and national level. The purpose of this objective focuses on cooperation with national and international partners to address cyber risks, as well as to create communication channels for the exchange of information.

Specific Objective 1.4: Development of response and incident management plans for cyber incidents

This objective covers the management and dissemination of information related to cyber incidents, threat intelligence, analysis of the causes of incidents, reporting to improve preventive measures, and timely response. The goal is to establish clear processes for handling incidents and prompt response to prevent and limit potential damage in a shorter period of time.

Specific Objective 1.5: Guaranteeing electronic transactions through Trusted Services

This objective aims to guarantee secure electronic transactions for businesses and citizens through the use of trusted services. Ensuring security in the use of electronic identification means and trusted services enables and facilitates safe participation in the digital society as well as the use of public and private services. *online*.

Specific Objective 1.6: Implementation of the Cybersecurity Certification Scheme

This objective aims at the creation of a reliable national mechanism for cyber security certification, harmonised with the legal framework of the European Union. Through the use of certified ICT products, services, and processes, trust in the digital market will be increased, a higher level of security for ICT products, services, and processes will be guaranteed, as well as the protection and resilience of critical and important information infrastructures will be strengthened.

2. Human capacities

The fulfilment of the vision and objective of the National Strategy requires the development of the appropriate skills, knowledge, and culture in the field of cybersecurity. Human capacity plays an important role in raising the level of cybersecurity by applying their expertise in the design and implementation of security measures. This process involves all actors such as policymakers, cybersecurity specialists, and users of digital systems, who must understand their roles and responsibilities to manage and mitigate risks and contribute to strengthening the resilience of cybersecurity. Education, training, and awareness programs are essential for reinforcing human capacities, enabling the creation of a secure digital environment.

Specific Objective 2.1: Promotion and Development of Cyber Culture

Strengthening the culture of cybersecurity is essential for the protection of networks and information systems, as users are often the weakest link in the security chain. This objective requires continuous training, awareness campaigns, and partnerships with the media and community organizations. The creation of proactive environments and the continuous improvement of practices are necessary to ensure digital and cyber resilience. Likewise, the involvement of all stakeholder groups and the implementation of security principles at all levels contribute to strengthening cybersecurity.

Specific Objective 2.2: Increasing Professional Capacities

The development of professional capacities through the integration of enhanced curricula in the education sector, specialized trainings, professional certifications, attraction and engagement of talents, inclusivity and cooperation with international organizations for best practices, aims to create an effective approach to addressing challenges and managing cybersecurity risks at the national level.

3. Technology

Technology plays an important role in the protection of digital infrastructure, as it provides the necessary tools and resources for implementing cybersecurity measures for the prevention and management of cyber threats. The advancement of technology increases the need for a rapid response to ever more sophisticated cyberattacks. This process involves a series of major challenges to ensure a sustainable and effective protection against these complex threats.

Specific objective 3.1: Use and integration of advanced technologies

The use and integration of advanced technologies, such as Artificial Intelligence (**AI**), intelligent computer programs (**LLM**), quantum computers, quantum cryptography, and decentralized technologies (**Blockchain**), will improve cybersecurity by enabling advanced threat identification and automated responses.

Specific Objective 3.2: Monitoring, detection, and cyber protection by utilizing advanced technologies

Albania undertakes to ensure a level of cyber resilience proportional to the risk, by expanding technological monitoring capacities to identify, prevent, and address cyber threats across all critical and important information infrastructures.

Specific Objective 3.3: Implementation of the 'secure by design' framework for digital infrastructures

The implementation of the principle *'secure by design'* to integrate cyber security measures at all stages of the lifecycle of digital systems and services, procurement and secure deactivation. This approach will ensure a continuous and interactive process for risk management, with the inclusion of security policies, procedures, and expertise at every stage of digital services development.

Specific Objective 3.4: Effective management of obsolete technologies

This approach will ensure effective management of outdated technologies at the national level through the development and implementation of comprehensive policies aimed at identifying, updating, isolating, or replacing them, thereby contributing to the strengthening of cyber protection, service resilience, and the increased reliability of critical and important information infrastructures.

Specific Objective 3.5: Use of Alternative Compensating Technologies for Cybersecurity

Albania will promote and implement alternative open-source technologies as a supporting measure to be applied in cases where closed-source technologies are not available or affordable for critical and important information infrastructures (OIKI/OIRI). This approach aims to ensure the continuity of cyber protection and the preservation of the operational resilience of these infrastructures, especially in technologically or financially constrained conditions.

Policy Goal 2: Protection *online of citizens* and the promotion of cyber culture

This policy aims to ensure a comprehensive approach to online protection and promote a sustainable cyber culture in Albania. It focuses on the suitability of the legal framework, ensuring that all citizens, including underrepresented groups, are protected and have equal opportunities to participate in cyberspace. To achieve this goal, roundtable discussions are organized, where representatives from public institutions, the private sector, non-profit organizations (NGOs), media, and civil society discuss challenges and solutions for cybersecurity. These dialogue platforms help in the creation of consensus-based policies and the addressing of diverse community needs. Additionally, activities and trainings to raise awareness and cyber skills are a priority, including awareness campaigns about online risks, educational programs for youth and underrepresented groups, as well as specific training for professionals and the general public. Interinstitutional and cross-sectoral cooperation plays an important role in the implementation of this policy. Public institutions, the private sector, NGOs, and media coordinate efforts to build a robust cybersecurity ecosystem, ensuring a comprehensive and sustainable approach to protecting and empowering citizens.

Specific Objective 1: Drafting and development of the National Citizen Awareness Plan (PKNQ)

This objective aims at drafting and implementing a comprehensive plan to raise citizens' awareness regarding the challenges and risks related to cybersecurity, as well as the benefits of being part of a secure digital environment. The PKNQ will include campaigns organized in education establishments, public institutions, and local communities, with the purpose of increasing awareness about best practices for security. *online*. In this context, educational programs will be developed aiming to equip citizens with the necessary skills to identify and avoid cyber threats, including protection from potential cybercrime such as fraud, identity theft, etc., creating a continuous educational chain for everyone.

Specific objective 2: Drafting of a legal framework for the comprehensive approach of citizens

This objective aims to create and adapt an advanced legal framework that ensures all citizens have equal access to the digital space. The legal framework will include mechanisms that regulate transparency, equality in access to digital services, and protection against discrimination. *online.* To achieve this, comprehensive consultations will be organized with citizens, public institutions, the private sector and NGOs, to ensure that everyone's voice is reflected in the relevant policies and legislation.

Specific Objective 3: Establishment of the necessary mechanisms for the online protection of children

Children constitute one of the most vulnerable categories in the digital ecosystem, therefore this objective aims at creating and implementing specific mechanisms to guarantee their safety *online.* In this context, dedicated platforms will be developed to offer educational and entertaining content in a safe and monitored environment, while advanced monitoring systems and joint interinstitutional plans will be implemented to support parents and guardians in the effective supervision of children's digital activities. As part of this objective, structured awareness campaigns and training programs will also be carried out, equipping them with the necessary skills to identify and address cyber risks. This comprehensive approach aims to create a safe and educational digital environment that promotes the well-being and development of children.

Specific Objective 4: Promotion of Gender Equality in the Digital Space

This objective aims to create an inclusive and safe digital environment for women and girls, focusing on their empowerment and the fight against any form of discrimination or cyber violence. The implementation of this objective is closely linked to addressing a number of challenges that affect the equal participation of women and girls in the digital sector, including:

- **Inequalities in access to and use of digital technologies**, where women and girls face limited opportunities compared to men and boys;
- **Gender segregation in the fields of education**, especially in science, technology, engineering and mathematics (STEM), where girls are less likely to pursue or be represented in these disciplines;
- **The low participation of women in the digital labor market**, including their limited representation in careers in the field of information and communication technologies (ICT);
- **Violence and online harassment**, including bullying and other forms of gender-based violence that limit the active participation of women and girls in the online environment;
- **The reinforcement of gender stereotypical roles and the promotion of harmful gender norms online**, which contribute to inequality;
- **The absence of data** administrative **separated by gender**, as well as gaps in interinstitutional coordination for the definition and monitoring of key gender indicators.

Through awareness campaigns, the active participation of women and girls in the technology and cybersecurity sector will be promoted. Activities will include training to empower them through digital skills, the creation of security platforms that address harassment *online,* as well as the development of support networks for women professionals in the field of technology. This objective will also aim at creating policies that encourage gender equality in every aspect of the digital space and promote a supportive culture for women and girls *online.*

Specific Objective 5: Establishment of appropriate mechanisms for the protection of SMEs online

Within the efforts to strengthen digital security and improve the cyber resilience of the private sector, particular focus has been devoted to promoting education in the field of technology and cyber security for Small and Medium Enterprises (SMEs). This initiative aims to raise awareness and strengthen the defensive capacities of SMEs, enabling them to better cope with the increasing challenges related to cyber threats. In this regard, practical guidelines will be drafted on the necessary cyber security measures, which will serve as guiding resources for SMEs in improving their digital infrastructure and implementing best practices for the protection of their data and systems. Furthermore, annual dedicated trainings will be organized for SME employees, with the aim of developing their practical skills in identifying and managing cyber risks. These trainings will provide specialized knowledge in key areas of digital security and will contribute to creating a stronger culture of security within the SME sector.

Specific Objective 6: Establishment of Necessary Mechanisms for the Protection and Empowerment of Underrepresented Groups

This objective aims to protect and empower underrepresented groups by creating inclusive platforms that address the specific needs of these groups, to guarantee equal access to digital tools and services. Through educational programs and training, these groups will be empowered to be more active and protected in the digital space. Additionally, policies and mechanisms that address discrimination will be implemented. *online* and ensure an equal and inclusive digital environment for all. This objective will be achieved through close cooperation with organizations supporting these groups, public institutions, and the private sector.

Policy objective 3: Strengthening International Cooperation

Cybersecurity is an international challenge and a joint effort to address the challenges related to threats and risks in the digital environment. The strategy promotes the strengthening of cooperation between institutions and international partners, fostering the exchange of information, the development of joint capacities, and the creation of unified standards, ensuring a collective and more effective protection against cyber threats. In this context, Albania is committed to actively contributing to international initiatives and agreements on cybersecurity, thus strengthening the resilience of the global digital environment.

Specific objective 1: Harmonisation of policies and legislation

The purpose of this objective is to ensure the compliance of Albania's cybersecurity legislation with international standards and regulations, by establishing a strong and sustainable legal framework. This harmonisation will enable a more efficient and coordinated response to cyber threats, enhancing the protection of the digital space and Albania's contribution at the global level. Cyber attacks are more complex and, given these conditions, their management, prevention, or recovery must be based on five very important elements: legal, technical, organisational, professional capacity, and cooperation. As the nature of these attacks has shown that they do not depend on borders between states, economic, political, or social situations, unified legislation or standards are a priority in the joint fight against ongoing cyber attacks.

Specific Objective 2: Strengthening regional (WB6) and international cooperation

To build a secure and sustainable digital ecosystem, you cannot act alone, as cyberattacks or hybrid attacks have shown that the best practice against them is cooperation. Even when a state is the main target of malicious actors, the consequences of cyberattacks extend beyond its borders, affecting the regional level and beyond. This makes international cooperation a necessity to face cyber threats and to undertake all measures to prevent their impact in the shared digital space. The development and strengthening of regional and international cooperation to address cyber threats can be achieved by improving the exchange of information and the coordination of responses to cyber incidents.

Specific Objective 3: Development of cyber diplomacy

The development of cyber diplomacy with the aim of creating clear diplomatic frameworks at the national and international level to effectively address cybersecurity issues, engaging states, international organizations, and other actors in the protection of digital infrastructures and information systems.

Objective of Policy 4: Promotion of Innovation and Scientific Research in Cybersecurity

Albania aims to develop a sustainable ecosystem through innovation and scientific research by emphasizing cooperation between higher education institutions, the private sector, and public institutions in increasing national capacities in the field of cybersecurity and the creation of new technological solutions. This approach strengthens the ability to face cyber challenges, but also helps in creating an innovative and secure digital environment for Albania.

Specific Objective 1: Establishment of the National Cybersecurity Center of Excellence

The establishment of the National Center of Excellence for Cybersecurity (QKESK) as an innovative center for technological research and development will enable close cooperation between higher education institutions, national and international research centers, as well as public and private institutions. It will promote scientific research, the identification of talents, and their training with the most advanced technologies. The focus will be on the development of innovative solutions, such as artificial intelligence, data analysis, and cryptography, for the prevention and detection of cyberattacks in real time, with the aim of strengthening national digital security and resilience.

Specific Objective 2: Support for Startups in the field of Cybersecurity

This objective aims to support the development of startups in the field of cybersecurity through the creation of an environment that fosters innovation and technological entrepreneurship. This includes facilitating access to research resources and technical expertise, providing specialized training and mentoring programs, as well as encouraging cooperation between the public sector, private sector, and higher education institutions. Special focus will be given to encouraging the participation of women and girls in the cybersecurity sector.

Specific Objective 3: Development of Funding Programs for Research and Innovation in Cybersecurity

To develop financing programs for research and innovation in cybersecurity. These programs will include the creation of specific funds, the promotion of gender equality in innovation and scientific research policies, the provision of fiscal incentives for businesses that invest in secure technologies, and the promotion of public-private partnerships for the co-financing of innovative projects.

Objective of Policy 5: Protection against hybrid threats

Hybrid threat involves the use of a plan or strategy in which various actors combine cyber threats with attacks in other domains, such as physical, economic, and informational, to achieve specific objectives. This type of threat is often exploited by states or non-state actors, taking advantage of vulnerabilities in the technological, infrastructural, political, and social systems of targeted objectives or goals.

To protect against hybrid threats, an integrated approach is needed that includes strengthening the security of critical infrastructure and important information, improvement of capacities for the detection and prevention of cyberattacks, as well as close inter-institutional and international cooperation, including NATO allied countries, to ensure a coordinated, rapid and effective response.

Specific Objective 1: Drafting the Legal Framework for Protection against Hybrid Cyber Threats

The drafting of an appropriate legal framework for protection against hybrid cyber threats will enable the prevention, identification, and management of threats. This legal framework will ensure close national and international inter-institutional cooperation, strengthening the protection of infrastructure against hybrid threats.

Specific Objective 2: Inter-institutional and International Coordination for Protection against Hybrid Threats

Interinstitutional and international cooperation and coordination will address hybrid threats and will optimize the sharing of information and resources. Close coordination ensures a rapid and efficient response to prevent and manage the consequences of hybrid threats.

Specific Objective 3: Establishment of Mechanisms for Protection against Hybrid Threats
For the development of an integrated and efficient structure for forecasting, identifying, and responding to hybrid threats, which include cyberattacks and disinformation, the use of modern tools and technologies is necessary. Platforms for information exchange, as well as increasing public awareness to ensure a quick and effective response to threats, preserve stability and national security.

Specific objective 4: Establishment of mechanisms for the prevention and investigation of Cybercrime
The prevention of cybercrime requires a proactive approach and the use of advanced technology that includes early detection and rapid response to threats. This objective aims at creating a safe and sustainable environment in the digital space, preventing and managing the possible effects of cybercrime.

Implementation, Institutional Responsibility, Accountability

The drafting of the National Cybersecurity Strategy 2025–2030 is based on Decision of the Council of Ministers No. 783, dated 18.12.2024, "Për organizimin dhe funksionimin e Autoritetit Kombëtar për Sigurinë Kibernetike", as well as on the commitments and standards of the EU and other international bodies.

- The involvement of public and private institutions gives this Strategy the opportunity to be objective and achievable. The inter-institutional working group, as well as all actors involved in the consultations, provided valuable comments, repeatedly reviewing the prepared draft in order to approve a comprehensive strategy, where everyone can find themselves and contribute to guaranteeing the country's cybersecurity.

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

The Action Plan accompanying the National Cybersecurity Strategy, 2025–2027 was prepared based on:

a) The National Strategy for Cyber Security 2025-2030 and its component Policies;

b) in the budget plans of public institutions.

As presented in the specific objectives and the main activities proposed in this Strategy and Action Plan, the coordinating role must be carried out by the National Authority for Cyber Security. Furthermore, this document takes into account the obligations arising from the

European integration process and alignment with the NIS2 and EIDAS2 directives, as well as the commitments as a NATO member country.

All proposed measures/activities, after being evaluated and further supplemented by the inter-institutional working group responsible for the drafting of the Strategy, were further detailed during the assessment of the financial effects for the implementation of this National Strategy and its Action Plan 2025–2027, with the need for periodic review based on the dynamics of developments in the field of cyber security.

Each responsible institution for the activities must plan their implementation by ensuring the planned budgets, human resources, and technical capacities for their realization. Every year, the assessment of the implementation of activities and the achievement of identified objectives will be conducted through the realization of indicators. The responsible institutions for the implementation of activities and achievement of results have the obligation to report according to reporting standards. The Strategy Coordinator must prepare the annual report and publish it.

Action Plan and Financial Resources for Implementation

Activity costing methodology

The necessary expenses for implementing the NAP have been determined by costing each of the activities of this action plan. The methodology applied for calculating costs presents a combination of methods that can be used in cases of strategies involving multiple actors. The main methodology used is activity-based costing (Activity Based Costing-ABC), where for each activity the responsible institution is identified, as well as the source of cost coverage, and resources are allocated for all products and services based on current consumption for each activity.

The budget was drafted based on the cost of each activity reflected in the action plan, its timeline and frequency of implementation, as well as the number of beneficiaries for specific activities. For calculating the expenses for the main activities, the following approach was used:

- The calculation of expenses for human resources is based on the estimated time required for carrying out the activity and an average daily wage for a specific category.
- Calculation of expenses for services. For these activities, the costs of services of the respective institutions are taken into account, based on the approved standards.
- The calculation of expenses for activities related to drafting and reviewing legislation, monitoring and functioning of permanent structures, etc. For these activities, ongoing expenses that will occur have been taken into account during the calculations, for example for salaries, social insurance contributions, foreign expertise (when foreseen in the plan), and consumables.
- Calculation of expenses for activities related to studies, awareness campaigns, training programs, foreign expertise, etc. The calculation of costs has been carried out based on similar specific initiatives, as well as according to the nature of the activities and the costs offered by the market for such services.

- - In calculating expenses for training, the cost of training per person has been taken into consideration. As the unit cost, the costs applied for similar trainings in the past have been used.
- For that part of the activities where the information is not complete (such as in the case of projects or studies), the method of assessment by analogy has been followed or expenditures made for similar activities included in previous budget plans have been taken into consideration.

Budget and financial resources for the implementation of the action plan

The National Cybersecurity Strategy will be implemented during the period 2025-2030. In order to enable its implementation, the necessary expenditures for the implementation of each activity, specific objective, and policy goal have been calculated. The overall budget for the implementation of the Strategy is reflected in several forms:

- The overall budget by year for each activity, specific objective, strategic goal, and sources of financing;

- The detailed budget by activities, sources of funding, and responsible institutions.