DECISION
No. 606, dated 23.10.2025
ON THE APPROVAL OF THE NATIONAL CYBERSECURITY STRATEGY 2025–2030 AND THE ACTION PLAN 2025–2027

Pursuant to Article 100 of the Constitution and paragraphs 4 and 5 of Article 6 of Law no. 25/2024, "On Cybersecurity", upon the proposal of the Prime Minister, the Council of Ministers

HERBEY DECIDED:

1. To approve the National Cybersecurity Strategy 2025 – 2030 and its Action Plan 2025–2027.

2. Decision no. 1084, dated 24.12.2020, of the Council of Ministers, "On the approval of the National Cybersecurity Strategy and the Action Plan 2020–2025", is hereby repealed.

3. The National Cybersecurity Authority, the ministries and other responsible institutions designated in the strategy and the action plan are tasked with the implementation of this decision.

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

DEPUTY PRIME MINISTER

Belinda Balluku

Policy	Specific Objective		Results	Responsible Institution	Spending Institution	Total Costs	PBA			Donators			GAP
							Year 2025	Year 2026	Year 2027	Year 2025	Year 2026	Year 2027	
	Specific Objective 0.1 Draft and implement the legal framework on Cybersecurity		1.0.1.1 Draft bylaws pursuant to Law No. 25/2024 'On Cybersecurity'.	NCSA	NCSA	2,365,164	788,388	788,388	788,388	-			-
			1.0.1.2 Harmonisation of the legal framework with the EU acquis.	NCSA	NCSA	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.0.1.3 Draft national and international agreements in the field of cybersecurity.	NCSA	NCSA	4,680,396	1,560,132	1,560,132	1,560,132	-			-
			1.0.1.4 Monitor the enforcement of law "On cybersecurity" by conducting periodic checks on CIIO/IIIO (Critical Information Infrastructure Operators/Important Information Infrastructure Operators).	NCSA	NCSA	2,787,330	929,110	929,110	929,110	-			-
					Subtotal Objective	**14,563,218**	**4,854,406**	**4,854,406**	**4,854,406**	**-**	**-**	**-**	**-**
	1.1. Processes	**1.1.2. Sub-Objective** Enhance Monitoring and Systems Protection Capacities	1.1.2.1 Improve and standardise procedures for monitoring networks and information systems, including real-time reporting and response to cybersecurity incidents.	NCSA/NAIS	NCSA/NAIS	12,643,452	4,214,484	4,214,484	4,214,484	-			-
			1.1.2.2 Monitor cyber threats in Albania's digital space through cyber threat intelligence.	NCSA/NAIS/MOD/APS/SIS	NCSA	11,533,860	3,844,620	3,844,620	3,844,620	-			-
			1.1.2.3 Update security measures and check their implementation by CIIO/IIIO in order to reflect changes in legislation, technology and standards.	NCSA	NCSA	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.1.2.4 Draft security guidelines and protocols for CIIO/IIIOs.	NCSA	NCSA	12,419,568	4,139,856	4,139,856	4,139,856	-			-
			1.1.2.5 Revise periodically security policies and procedures based on evolution of threats and technology.	NCSA	NCSA	7,095,492	2,365,164	2,365,164	2,365,164	-			-
			1.1.2.6 Revise cybersecurity measures, and their inclusion a secure cloud environment (PaaS, SaaS, IaaS, etc.).	NCSA	NCSA	-	-	-	-	-			-
			1.1.2.7. Improve procedures concerning the assessment and testing of information technology networks and systems.	NCSA	NCSA	-	-	-	-	-			-
			1.1.2.8 Draft procedures for the secure use of IoT, OT, ICS, SCADA and advanced technologies.	NCSA	NCSA	-	-	-	-	-			-
					Subtotal Sub-Objective	**48,422,700**	**16,140,900**	**16,140,900**	**16,140,900**	**-**	**-**	**-**	**-**
		Specific Sub-Objective 1.1.3 (Processes) Cyber Governance and Risk Management	1.1.3.1 Implementat and revise periodically the methodology for an assessment of cyber risks for all systems and networks operated by CIIOs and IIIOs.	NCSA	NCSA	3,120,264	1,040,088	1,040,088	1,040,088	-			-
			1.1.3.2 Assess cyber risks on a six-monthly basis by identifying vulnerabilities, technological and geopolitical threats, as well as potential opportunities for cyber attacks.	NCSA	NCSA	6,240,528	2,080,176	2,080,176	2,080,176	-			-
			1.1.3.3 Establish mechanisms for cyber risk information sharing with public institutions and CIIO/IIIOs.	NCSA/NAIS	NCSA	150,000,000	150,000,000	-	-	-			-
			1.1.3.4 Assess cybersecurity at both sectorial and national levels.	NCSA	NCSA	6,290,132	520,044	520,044	5,250,044	-			-
					Subtotal Sub-Objective	**165,650,924**	**153,640,308**	**3,640,308**	**8,370,308**	**-**	**-**	**-**	**-**
		Specific Sub-Objective 1.1.4 (Processes) Develop Cyber Incident Response and Management Plans	1.1.4.1 Review and improve cyber incident response and management plans at a national and sectorial level.	NCSA	NCSA	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.1.4.2 Review and update the national cyber incident response and management plan after each incident affecting CIIOs/IIIOs.	NCSA	NCSA	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.1.4.3 Review and improve communication procedures in cases of cyber incidents.	NCSA	NCSA	3,570,804	1,190,268	1,190,268	1,190,268	-			-
			1.1.4.4 Update the national procedure for cyber crisis management .	NCSA	NCSA	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.1.4.5 Implement advanced mechanisms for detecting and tracking cyber attacks via forensic analysis and incident data correlation.	NCSA/ NAIS/ MOD	NCSA/ NAIS/ MOD	305,643,656				61,128,731	122,257,462	122,257,462	
			1.1.4.6 Draw up a report on the in-depth investigation of cyber attacks targeting data storage systems.	NCSA/APS	NCSA	9,460,656	3,153,552	3,153,552	3,153,552	-			-
					Subtotal Sub-Objective	**332,866,100**	**9,074,148**	**9,074,148**	**9,074,148**	**61,128,731**	**122,257,462**	**122,257,462**	**-**
		Specific Sub-Objective 1.1.5 (Processes) **Guarantee electronic transactions via trust services**	1.1.5.1 Align domestic legislation on electronic identification, trust services, and the Digital Identity Wallet with the EU regulatory framework established under eIDAS 1.0 and eIDAS 2.0.	NCSA	NCSA	7,095,492	2,365,164	2,365,164	2,365,164	-			-
			1.1.5.2 Draw up bylaws in the field of electronic identification, trust services, and the Digital Identity Wallet.	NCSA	NCSA	9,460,656	3,153,552	3,153,552	3,153,552	-			-
			1.1.5.3 Sign agreements with Western Balkan countries on mutual recognition of trust services.	NCSA	NCSA	7,095,492	2,365,164	2,365,164	2,365,164	-			-
			1.1.5.4 Monitor the activity of qualified trust service providers to ensure full compliance with the legal requirements in force.	NCSA	NCSA	3,570,804	1,190,268	1,190,268	1,190,268	-			-
					Subtotal Sub-Objective	**27,222,444**	**9,074,148**	**9,074,148**	**9,074,148**	**-**	**-**	**-**	**-**
			1.1.6.1 Draft Cybersecurity Certification Scheme.	NCSA	NCSA	-	-	-	-	-			-

Policy	Specific Objective		Results	Responsible Institution	Spending Institution	Total Costs	PBA			Donators			GAP
							Year 2025	Year 2026	Year 2027	Year 2025	Year 2026	Year 2027	
Policy 1:Protection of Digital Infrastructure (Processes, Human Capacities and Technology)		**Specific Sub-Objective 1.1.6** Implement Cybersecurity Certification Scheme	1.1.6.2. Accredit Conformity Assessment Bodies (CABs).	DPA	DPA	-	-	-	-	-			-
			1.1.6.3.Authorise and register Conformity Assessment Bodies (CABs).	NCSA	NCSA	-	-	-	-	-			-
					Subtotal Sub-Objective	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
					Subtotal Objective	**574,162,168**	**187,929,504**	**37,929,504**	**42,659,504**	**61,128,731**	**122,257,462**	**122,257,462**	**-**
	1.2. Human Capacities	**Specific Sub-Objective. 1.2.1** (Human Capacities): Promote and develop Cybersecurity Culture	1.2.1.1. Draft and implement national awareness-raising campaigns on cyber hygiene and security best practices, with a specific focus on employees of CIIO and IIIO(Operators of Critical/Important Information Infrastructure).	NCSA/ NAIS	NCSA	9,460,656	3,153,552	3,153,552	3,153,552	-			-
			1.2.1.2. Develop awareness-raising campaigns aimed at promoting the use of trust services.	NCSA	NCSA	1,190,268	396,756	396,756	396,756	-			-
			1.2.1.3. Develop a dedicated training plan on cybersecurity.	NCSA	NCSA	396,756	132,252	132,252	132,252	-			-
			1.2.1.4. Cybersecurity training programmes for employees of CIIOs and IIIOs.	NCSA	NCSA	1,069,108,872	170,000,000	-	-	179,821,774	359,643,549	359,643,549	
					Subtotal Sub-Objective	**1,080,156,552**	**173,682,560**	**3,682,560**	**3,682,560**	**179,821,774**	**359,643,549**	**359,643,549**	**-**
		Specific Sub-Objective. 1.2.2 (Human Capacities): Strengthen Professional Capacities	1.2.2.1 Revise and integrate cybersecurity into pre-university education curricula.	MOE/NCSA	NCSA	6,307,104	2,102,368	2,102,368	2,102,368	-			-
			1.2.2.2 Enhance technical competencies and practical expertise of cybersecurity professionals via structured participation in periodic technical trainings, international cooperation initiatives, and cyber competitions including real-world threats and incidents.	NCSA/NAIS	NCSA	5,770,000	5,770,000	-	-	-			-
			1.2.2.3 Identify, recruit and develop new cybersecurity talents via structured training programmes, mentoring schemes, and career development opportunities.	NCSA/NAIS	NCSA	12,643,452	4,214,484	4,214,484	4,214,484	-			-
			1.2.2.4 Create dedicated cybersecurity laboratories (cyber ranges) to enable hands-on training, practical exercises, and real-life incident simulations.	NCSA	NCSA	360,820,856	37,088,600			64,746,451	129,492,902	129,492,902	
			1.2.2.5 Build capacities for school staff and implementat school-based awareness campaigns "Against online radicalization and violent extremism".	CVE / MOE/ SAPCR	CVE	185,859	61,953	61,953	61,953	-			-
			1.2.2.6 Develop and disseminate counter-narratives aimed at fostering tolerance and counter online hate speech linked to radicalization and violent extremism.	CVE / MOE	CVE	371,721	123,907	123,907	123,907	-			-
					Subtotal Sub-Objective	**386,098,992**	**49,361,312**	**6,502,712**	**6,502,712**	**64,746,451**	**129,492,902**	**129,492,902**	**-**
					Subtotal Objective	**1,466,255,544**	**223,043,872**	**10,185,272**	**10,185,272**	**244,568,226**	**489,136,451**	**489,136,451**	**-**
	1.3. Technology	**Specific Sub-Objective. 1.3.1** (Technology): Adopt and Integrate Advanced Technologies	1.3.1.1 Integrate and deploy advanced technologies, including Artificial Intelligence (AI), to enhance the detection, prevention, and response capabilities against cyber attacks.	NCSA/NAIS	NCSA	5,765,009,080	3,331,672,720			-			2,433,336,360
			1.3.1.3 Develop blockchain-based policies aimed at safeguarding integrity, transparency, and trustworthiness of digital transactions.	NCSA/NAIS	NAIS	-	-	-	-	-			-
			1.3.1.4 Strengthen and upgrade cyber testing and simulation laboratories.	NCSA	NCSA	442,269,688	-			88,453,938	176,907,875	176,907,875	
			1.3.1.5 Deploy automated systems for updating and managing cybersecurity.	NCSA/NAIS	NCSA	450,000,000	-	-		90,000,000	180,000,000	180,000,000	
					Subtotal Sub-Objective	**6,657,278,768**	**3,331,672,720**	**-**	**-**	**178,453,938**	**356,907,875**	**356,907,875**	**2,433,336,360**
		1.3.2 (Technology): Cybersecurity Monitoring, Detection, and Protection through Advanced Technologies	1.3.2.1. Implementat advanced mechanisms to ensure proactive protection and resilience against Advanced Persistent Threats (APTs).	NCSA/NAIS/SIS/MOD	NCSA	895,000,000	-	-	-	179,000,000	358,000,000	358,000,000	
			1.3.2.2. Adopt cloud computing solutions for protection and defence of critical data.	NCSA/NAIS	NCSA	-	-	-	-	-			-
					Subtotal Sub-Objective	**895,000,000**	**-**	**-**	**-**	**179,000,000**	**358,000,000**	**358,000,000**	**-**
		Specific Sub-Objective. 1.3.3 (Technology): Implement "Secure by Design" Framework for Digital Infrastructures	1.3.3.1. Develop policies to ensure the systematic integration of cybersecurity measures at all stages of the digital systems lifecycle.	NCSA/NAIS	NCSA	2,660,400	886,800	886,800	886,800	-			-
			1.3.3.2 Draft guidelines for infrastructures/operators on 'security by design and by default' principles.	NCSA/NAIS	NCSA	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.3.3.3 Develop protocols/manuals to ensure cybersecurity for IoT (Internet of Things) devices and their protection from cyber attacks.	NCSA/ EPCA	NCSA/ EPCA	1,190,268	396,756	396,756	396,756	-			-
					Subtotal Sub-Objective	**8,580,996**	**2,860,332**	**2,860,332**	**2,860,332**	**-**	**-**	**-**	**-**
		Specific Sub-Objective. 1.3.4 (Technology): Effective Management of Legacy Technologies	1.3.4.1 Draft a national plan for the identification, update/isolation of outdated technologies within critical systems.	NCSA	NCSA	1,560,132	520,044	520,044	520,044	-			-
			1.3.4.2 Develop a national program on the migration towards safer andmore resilient technologies.	NCSA/ NAIS	NCSA/ NAIS	2,365,164	788,388	788,388	788,388	-			-
			1.3.4. 3 Carry out periodic checks to identify outdated or obsolete technologies.	NCSA	NCSA	6,307,104	2,102,368	2,102,368	2,102,368	-			-
					Subtotal Sub-Objective	**10,232,400**	**3,410,800**	**3,410,800**	**3,410,800**	**-**	**-**	**-**	**-**

Policy	Specific Objective	Results	Responsible Institution	Spending Institution	Total Costs	PBA			Donators			GAP
						Year 2025	Year 2026	Year 2027	Year 2025	Year 2026	Year 2027	
	Specific Sub-Objective. 1.3.5 (Technology): Use Alternative Compensating Technologies for Cybersecurity	1.3.5.1 Promotion and adopt alternative and compensatory technologies to enhance cybersecurity resilience and ensure solutions in the face of technological or financial constraints.	NCSA	NCSA	1,560,132	520,044	520,044	520,044	-			-
		1.3.5.2 Adopt alternative platforms when paid technologies are not accessible.	NCSA	NCSA	4,160,352	1,386,784	1,386,784	1,386,784	-			-
				Subtotal Sub-Objective	**5,720,484**	**1,906,828**	**1,906,828**	**1,906,828**	**-**	**-**	**-**	**-**
				Subtotal Objective	**7,576,812,648**	**3,339,850,680**	**8,177,960**	**8,177,960**	**357,453,938**	**714,907,875**	**714,907,875**	**2,433,336,360**
				Subtotal of Policy 1	**9,631,793,578**	**3,755,678,462**	**61,147,142**	**65,877,142**	**663,150,894**	**1,326,301,789**	**1,326,301,789**	**2,433,336,360**
Policy 2: Online Protection of Citizens and Promotion of a Cybersecurity Culture	**Specific Objective 2.1:** Draft and Develop the National Plan for Citizen Awareness (NPCA)	2.1.1 Analyse the current situation regarding awareness campaigns/programmes and assess the need for their revision.	NCSA/MSHMS	NCSA	2,055,000	685,000	685,000	685,000	-			-
		2.1.2 Develop a programme including continuous and segmented training tailored to stakeholder groups and their specific needs, on cyber threats and preventive measures such as phishing and data misuse.	NCSA	NCSA	793,512	264,504	264,504	264,504	-			-
		2.1.3 Prepare and disseminate clear and accessible educational materials for citizens, in user-friendly language, including children, on cyber hygiene and online safety.	NCSA/MSHMS	NCSA	6,667,275	2,222,425	2,222,425	2,222,425	-			-
		2.1.4 Create public campaigns to promote awareness and increase knowledge on cybersecurity through various media channels.	NCSA	NCSA	30,000,000	10,000,000	10,000,000	10,000,000	-			-
		2.1.5 Promote the increased use of the "RED BUTTON" for reporting illegal content.	CVE / NCSA	NCSA	-	-	-	-	-			-
				Subtotal Objective	**39,515,787**	**13,171,929**	**13,171,929**	**13,171,929**	**-**	**-**	**-**	**-**
	Specific Objective 2.2: Draft a Legal Framework for an Inclusive Citizen-Centered Approach	2.2.1 Identify the need for amendments to existing legislation to strengthen citizens' online protection.	NCSA	NCSA	1,560,132	520,044	520,044	520,044	-			-
		2.2.2 Prepare a draft law on the online protection of citizens from potential cyber threats.	NCSA	NCSA	4,160,352	1,386,784	1,386,784	1,386,784	-			-
				Subtotal Objective	**5,720,484**	**1,906,828**	**1,906,828**	**1,906,828**	**-**	**-**	**-**	**-**
	Specific Objective 2.3: Create Mechanisms for the Online Protection of Children.	2.3.1 Review pre-university curricula to assess the integration of cybersecurity and recommend necessary improvements..	NCSA/MOE	MOE	3,153,552	-	3,153,552	-	-			-
		2.3.2 Train teaching staff on cybersecurity and design a regular programme to strengthen capacities in schools.	NCSA/MOE	MOE	-	-	-	-	-			-
		2.3.3 Integrate modules on cybersecurity and online child/youth protection into curricula at all levels.	NCSA/MOE	MOE	-	-	-	-	-			-
		2.3.4 Implement awareness campaigns for parents on the use of cybersecurity applications and platforms enabling parental control.	NCSA/MOE	NCSA	3,221,532	1,073,844	1,073,844	1,073,844	-			-
				Subtotal Objective	**6,375,084**	**1,073,844**	**4,227,396**	**1,073,844**	**-**	**-**	**-**	**-**
	Specific Objective 2.4: Promote Gender Equality in the Digital Space	2.4.1 Promote education and careers for women and girls from all backgrounds in the field of technology and cybersecurity.	NCSA/NAIS/MSHMS	NCSA	30,211,293	10,070,431	10,070,431	10,070,431	-			-
		2.4.2 Organise annual dedicated traning events for women and girls in this field.	NCSA	NCSA	2,147,688	715,896	715,896	715,896	-			-
		2.4.3 Develop campaigns to promote equal opportunities for women in the digital sector.	NCSA	NCSA	2,326,662	775,554	775,554	775,554	-			-
				Subtotal Objective	**34,685,643**	**11,561,881**	**11,561,881**	**11,561,881**	**-**	**-**	**-**	**-**
	Specific Objective 2.5: Establish Adequate Mechanisms for the Online Protection of SMEs	2.5.1 Promote education for SMEs in the field of technology and cybersecurity.	NCSA	NCSA	5,470,056	1,823,352	1,823,352	1,823,352	-			-
		2.5.2 Prepare guidelines on cybesecurity measures for SMEs.	NCSA	NCSA	5,470,056	1,823,352	1,823,352	1,823,352	-			-
		2.5.3 Organise dedicated training events for SME personnel.	NCSA	NCSA	5,470,056	1,823,352	1,823,352	1,823,352	-			-
				Subtotal Objective	**16,410,168**	**5,470,056**	**5,470,056**	**5,470,056**	**-**	**-**	**-**	**-**
	Specific Objective 2.6: Develop Mechanisms for the Protection and Empowerment of Underrepresented Groups	2.6.1 Establish a national platform with educational and interactive tools to raise awareness on online safety.	NCSA	NCSA	136,000,000	136,000,000			-			-
		2.6.2 Draft and distribute educational materials tailored for underrepresented groups.	NCSA	NCSA	3,997,000	1,332,333	1,332,333	1,332,333	-			-
				Subtotal Objective	**139,997,000**	**137,332,333**	**1,332,333**	**1,332,333**	**-**	**-**	**-**	**-**
				Subtotal of Policy 2	**242,704,166**	**170,516,871**	**37,670,423**	**34,516,871**	**-**	**-**	**-**	**-**
Policy 3: Strengthening	**Specific Objective 3.1**: Harmonise Policies and Legislation	3.1.1 Establish working groups to review and recommend legislative amendments to be aligned with international directives and standards.	NCSA	NCSA	-	-	-	-	-			-
		3.1.2 Launch awareness campaigns for public authorities and private sector entities on implementation of cybersecurity policies and legislation.	NCSA	NCSA	-	-	-	-	-			-
				Subtotal Objective	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
	Specific Objective 3.2: Strengthen Regional (WB6) and International Cooperation	3.2.1 Draft a regional programme on joint training and drills on cyberattacks involving public authorities and private sector.	NCSA/ MOFA	NCSA	29,775,000	9,925,000	9,925,000	9,925,000	-			-
		3.2.2 Organise regional roundtables for sharing best practices.	NCSA/MOFA	NCSA	-	-	-	-	-			-

Policy	Specific Objective	Results	Responsible Institution	Spending Institution	Total Costs	PBA			Donators			GAP
						Year 2025	Year 2026	Year 2027	Year 2025	Year 2026	Year 2027	
International Cooperation				**Subtotal Objective**	**29,775,000**	**9,925,000**	**9,925,000**	**9,925,000**	**-**	**-**	**-**	**-**
	Specific Objective 3.3: Advance Cyber Diplomacy	3.3.1 Prepare a national plan clearly defining objectives and strategic partners for cooperation in the field of cybersecurity.	NCSA/MOFA	NCSA	1,330,200	443,400	443,400	443,400	-			-
		3.3.2 Participate in international mechanisms for cooperation in cybersecurity, with a focus on sharing practical experiences and strengthen inter-institutional dialogue on strategic challenges and solutions.	NCSA	NCSA/MOFA	-	-	-	-	-			-
		3.3.3 Establish national capacities for cyber diplomacy.	NCSA/ NAIS/ MOFA	NCSA/ NAIS/ MOFA	-	-	-	-	-			-
				Subtotal Objective	**1,330,200**	**443,400**	**443,400**	**443,400**	**-**	**-**	**-**	**-**
				Subtotal of Policy 3	**31,105,200**	**10,368,400**	**10,368,400**	**10,368,400**	**-**	**-**	**-**	**-**
Policy 4 - Fostering Innovation and Scientific Research in Cybersecurity	**Objective 4.1** Establishment of the National Cybersecurity Centre of Excellence	4.1.1 Draft and adopt regulations and guidelines for the establishment and operation of National Cybersecurity Centre of Excellence (NCCoE).	NCSA/ MOE /MOI	**NCSA**	-	-	-	-	-			-
		4.1.2 Establish mechanisms for monitoring and evaluating the performance of the NCCoE.	NCSA/ MOE /MOI	NCSA	-	-	-	-	-			-
		4.1.3 Equip the Centre with research laboratories and infrastructure for testing emerging technologies.	NCSA/ MOI	NCSA	-	-	-	-	-			-
		4.1.4 Foster Public-Private Partnerships to advance innovative research projects involving public authorities, academia, and the private sector.	NAIS/NCSA/MOI	MOI	-	-	-	-	-			-
		4.1.5 Foster and promote the exchange of knowledge and best practices on innovative cybersecurity solutions.	MOI/NCSA/NAIS	MOI	-	-	-	-	-			-
				Subtotal Objective	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
	Objective 4.2. Support Cybersecurity Startups	4.2.1 Create mechanisms to foster and facilitate the growth and operation of start-ups in information technology and cybersecurity.	MOI/NCSA	MOI	-	-	-	-	-			-
		4.2.2 Make available supportive environments for start-ups (tech hubs, incubators).	MOI/NCSA	MOI	-	-	-	-	-			-
		4.2.3 Make available the existing laboratory for the development and testing of innovative solutions and improve it.	NCSA	NCSA	-	-	-	-	-			-
		4.2.4 Involve startups in research projects for testing new technologies.	MOI/NCSA	MOI	-	-	-	-	-			-
		4.2.5 Foster strategic partnerships with large companies to enable the integration of innovative start-ups in the national cybersecurity ecosystem.	MOI/NCSA	MOI	-	-	-	-	-			-
		4.2.6 Support joint research projects between startups and higher education institutions.	NCSA/MOE/MOI/	MOI	-	-	-	-	-			-
		4.2.7 Organize hackathons, competitions, for innovative cybersecurity solutions.	MOI/NCSA	NCSA	90,000,000	30,000,000	30,000,000	30,000,000	-			-
				Subtotal Objective	**90,000,000**	**30,000,000**	**30,000,000**	**30,000,000**	**-**	**-**	**-**	**-**
	Objective 4.3. Develop Funding Programmes for Cybersecurity Research and Innovation	4.3.1 Develop national funding programmes dedicated to research and innovation in cybersecurity.	MOI/NCSA	MOI	-	-	-	-	-			-
		4.3.2 Establish a national fund to support cybersecurity research initiatives.	MOI/MOE/NCSA	NCSA	-	-	-	-	-			-
		4.3.3 Facilite access to EU grants and international donors for research and development.	MOI/NCSA	MOI/NCSA	-	-	-	-	-			-
		4.3.4 Provide fiscal incentives for businesses that invest in secure technologies and scientific research.	MOI/NCSA	MOI	-	-	-	-	-			-
				Subtotal Objective	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
				Subtotal of Policy 4	**90,000,000**	**30,000,000**	**30,000,000**	**30,000,000**	**-**	**-**	**-**	**-**
	Specific Objective 5.1 Draft the Legal Framework for the Protection Against Hybrid Cyber Threats	5.1.1 Review the national legal framework to address hybrid threats.	MOFA/AMOE/APS/MOD/SIS/MIA/MIE/CVE/NAIS/NCSA/EPCA/MOI	NCSA	3,153,552	-	3,153,552	-	-			-
		5.1.2 Update existing national strategies to match new technological developments and hybrid threat tactics.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/CVE/NAIS/NCSA/EPCA	NCSA	3,990,600	1,330,200	1,330,200	1,330,200	-			-
		5.1.3 Establish responsible structures for inter-institutional cooperation in responding to hybrid threats.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/CVE/NAIS/NCSA/EPCA	NCSA	4,730,328	1,576,776	1,576,776	1,576,776	-			-
		5.1.4 Introduce supervisory mechanisms to monitor compliance with legal framework.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/CVE/NAIS/NCSA/EPCA/MOI	NCSA	4,160,352	1,386,784	1,386,784	1,386,784	-			-
		5.1.5 Align national legislation with the international one to guarantee a unified approach in combating hybrid threats.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/CVE/NAIS/NCSA/EPCA	MOFA	-	-	-	-	-			-
		5.1.6 Establish capacities in relevant institutions based on EU acquis.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/CVE/NAIS/NCSA/EPCA	NCSA	1,995,300	665,100	665,100	665,100	-			-
				Subtotal Objective	**18,030,132**	**4,958,860**	**8,112,412**	**4,958,860**	**-**	**-**	**-**	**-**
	Specific Objective 5.2 Inter-institutional and International	5.2.1 Establish a national coordination mechanism for response to hybrid threats.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/CVE/NAIS/NCSA/EPCA	NCSA	8,205,084	2,735,028	2,735,028	2,735,028	-			-
		5.2.2 Develop mechanisms for information exchange between national and international institutions.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/CVE/NAIS/NCSA/EPCA	NCSA	-	-	-	-	-			-
		5.2.3 Organise joint training events and exercises with CIIO/IIIO for handling hybrid attacks.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/CVE/NAIS/NCSA/EPCA	NCSA	60,000,000	20,000,000	20,000,000	20,000,000	-			-
		5.2.4 Involve public–private partnerships in monitoring and responding to hybrid threats.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/CVE/NAIS/NCSA/EPCA	NCSA	-	-	-	-	-			-

Policy	Specific Objective	Results	Responsible Institution	Spending Institution	Total Costs	PBA			Donators			GAP
						Year 2025	Year 2026	Year 2027	Year 2025	Year 2026	Year 2027	
Policy 5-Protection Against Hybrid Threats	Coordination	5.2.5 Develop a dedicated and secure communication infrastructure to enable real-time exchange of sensitive information among key cybersecurity stakeholders.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/ CVE/NAIS/NCSA/EPCA	NCSA	-	-	-	-	-			-
		5.2.6 Encourage the conclusion of international cooperation agreements on protection against hybrid threats.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/ CVE/NAIS/NCSA/EPCA	NCSA	-	-	-	-	-			-
				Subtotal Objective	**68,205,084**	**22,735,028**	**22,735,028**	**22,735,028**	**-**	**-**	**-**	**-**
	Specific Objective 5.3 Establish Mechanisms for Protection Against Hybrid Threats	5.3.1 Deploy advanced tools and technologies for monitoring and early detection of hybrid threats.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/ CVE/NAIS/NCSA/EPCA	NCSA	-	-	-	-	-			-
		5.3.2 Implement dedicated platforms for information sharing on hybrid threats.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/ CVE/NAIS/NCSA/EPCA	NCSA	200,000,000	-	200,000,000	-	-			-
		5.3.3 Draft awareness-raising campaigns on the risks of disinformation and cyberattacks.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/ CVE/NAIS/NCSA/EPCA	NCSA	3,941,940	1,313,980	1,313,980	1,313,980	-			-
		5.3.4 Regularly update emergency protocols based on the latest risk assessments.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/ CVE/NAIS/NCSA/EPCA	NCSA	3,153,552	1,051,184	1,051,184	1,051,184	-			-
		5.3.5 Leverage artificial intelligence technologies for data analysis and forecasting of hybrid threats.	MOFA/AMA/APS/MOD/SIS/MIA/MIE/ CVE/NAIS/NCSA/EPCA	NCSA/NAIS	-	-	-	-	-			-
				Subtotal Objective	**207,095,492**	**2,365,164**	**202,365,164**	**2,365,164**	**-**	**-**	**-**	**-**
	Specific Objective 5. 4 Develop Mechanisms for Prevention and Investigation of Cybercrime	5.4.1 Strengthen inter-institutional cooperation in the fight against cybercrime.	MOFA/NCSA/APS	APS	-	-	-	-	-			-
		5.4.2 Improve the national legal framework to ensure harmonisation with international legislation and conventions on cybercrime.	MOFA/APS	APS	2,062,500	687,500	687,500	687,500	-			-
				Subtotal Objective	**2,062,500**	**687,500**	**687,500**	**687,500**	**-**	**-**	**-**	**-**
				Subtotal of Policy 5	**295,393,208**	**30,746,552**	**233,900,104**	**30,746,552**	**-**	**-**	**-**	**-**
				Grand Total	**10,290,996,152**	**3,997,310,285**	**373,086,069**	**171,508,965**	**663,150,894**	**1,326,301,789**	**1,326,301,789**	**2,433,336,360**

	Total Cost	Year 2025	Year 2026	Year 2027	Donators 2025	Donators 2026	Donators 2027	GAP
NAIS	-	-	-	-	-	-	-	-
NCSA	10,285,222,520	3,996,436,925	369,059,157	170,635,605	663,150,894	1,326,301,789	1,326,301,789	2,433,336,360
EPCA	-	-	-	-	-	-	-	-
MOI	-	-	-	-	-	-	-	-
MOD	-	-	-	-	-	-	-	-
CVE	557,580	185,860	185,860	185,860	-	-	-	-
MOE	3,153,552	-	3,153,552	-	-	-	-	-
MOI	-	-	-	-	-	-	-	-
MOFA	-	-	-	-	-	-	-	-
APS	2,062,500	687,500	687,500	687,500	-	-	-	-
	10,290,996,152	**3,997,310,285**	**373,086,069**	**171,508,965**	**663,150,894**	**1,326,301,789**	**1,326,301,789**	**2,433,336,360**

- - - - - -

NATIONAL CYBERSECURITY STRATEGY 2025 - 2030

Table of Contents

PART I: STRATEGIC CONTEXT

1. Introduction

In a period in which digital transformation is profoundly shaping all aspects of social, economic, and institutional life, cybersecurity has an exceptional level of importance worldwide. 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 secure and reliable digital environment for its citizens, businesses, and institutions.

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

The primary 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 guaranteeing of continuity of digital services. It also aims to enhance technical and professional capacities necessary to address the continuous challenges for the protection of the digital space, as well as to promote international cooperation in order to improve effectiveness and response to cyber incidents.

The strategy establishes a framework to enhance the preparedness and resilience of information systems and services in the country, ensuring that Albania meets the highest international standards and best practices in this field. It reflects the alignment of cybersecurity policies with those of the European Union and international partners, in order 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 stakeholders such as: public institutions, the private sector, civil society, and higher education institutions, in order to create a coordinated and inclusive cybersecurity ecosystem. This will enable the sharing of information and resources, the development of joint policies, and the awareness-raising regarding 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 all field of life, cybersecurity risks are also rapidly evolving. Global trends indicate a rise in cyberattacks, driven by state-sponsored actors, criminal organizations, and malicious groups. The Albanian state, economy, and government face continuous cyber threats that require immediate attention in order 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 substantially strengthened and improved the processes of monitoring, risk assessment, and threat management. Some of the most important achievements at the national level include the increased implementation of security measures in critical and important information infrastructures, as well as the enhancement of the experts' technical capacities through training and rigorous controls. Albania has significantly intensified its cooperation with international organizations such as NATO and the European Union, ensuring compliance with international norms. In addition, steps have been taken to inform and raise awareness among citizens and businesses regarding cybersecurity. Albania has aligned its legislation with European Union directives, thereby reinforcing cybersecurity both nationally and internationally.

The cyberattacks of recent years have emphasised the importance to improve standardized incident response procedures, build stronger network monitoring capacities, and establish centralized mechanisms for the efficient exchange of threat information.

Furthermore, in the Global Cybersecurity Index 2024, Albania has achieved remarkable progress, climbing 23 places in the global ranking, from 80th to 57th position, 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 reliable 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 trustworthy actor in the global digital era.

Despite the considerable progress that Albania has achieved in the field of cybersecurity, many tasks remain to be accomplished. Cybersecurity challenges are becoming 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, targeting not only the public sector, but also vital services such as healthcare, finance, transport, and energy.

The use of the internet for the dissemination of extremist ideologies and the recruitment of individuals for terrorist purposes represents a increasing threat, making the prevention of such activities increasingly complex. In this context, Albania’s national security is closely connected to its capacity to identify, prevent, and respond to cyber threats, including hybrid ones. A key element of this strategy is the development of dedicated intelligence structures specialized in monitoring and countering extremist and terrorist activities in cyberspace. In the framework of the fight against terrorism, a central focus is the prevention of extremist propaganda and online recruitment. This entails the use of advanced technologies to detect and shut down websites and content that promote violence and radicalization, as well as the establishment of cooperation mechanisms with international actors and online platforms.

Furthermore, social factors are increasingly influencing the cyber landscape, including online bullying, the exploitation of children and vulnerable groups, as well as attacks against organizations and individuals aimed at disinformation and financial gain through reputation damage, both at a personal and professional level.

3. Vision and Mission

3.1 Vision

The National Cybersecurity Strategy 2025-2030 envisions the establishment of a secure, resilient, 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, supercomputing, and blockchain, the strategy aims to strengthen Albania's position as a regional leader in cybersecurity and to ensure full alignment with the European Union's policies, legal framework, and regulatory standards.

Beyond technical protection, this vision reflects a broader commitment to supporting the country's political, social, and economic development, fostering cooperation between institutions, the private sector, and international partners, and creating a unified approach to addressing emerging threats and opportunities in the digital era.

Through this strategy, Albania aims not only to protect its digital space, but also to foster a culture of responsibility and awareness for cybersecurity. This inclusive commitment will enhance the country's resilience to continuous challenges, positioning Albania as 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 establish a strong and inclusive shield to protect citizens, institutions, critical and important information infrastructures in the Republic of Albania from continuous and evolving threats of cyberspace. This strategy aims to consolidate an advanced legal, technical, and organizational framework, aligned with European and international standards, in order 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 in which technology serves as a catalyst for innovation and progress. Through supporting sustainable economic and social development, the strategy not only protects national interests, but also promotes Albania's competitiveness and its capacity to play an important role in the digital transformation of the region and beyond. The mission also highlights the importance of interinstitutional and international cooperation in addressing the complex challenges of cybersecurity. It is based on a commitment to fostering a culture of cyber responsibility, including raising public awareness and strengthening technical capacities and human resources. Through this strategy, Albania aims not only to face current cyber threats, but also to build a solid foundation for the protection and secure development of the digital space of the future, thereby enhancing national cyber resilience.

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 service continuity and the stability of information systems.

The strategy aims to improve cooperation between the public and private sector, and other stakeholders to enhance defensive capacities and 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 the ability to anticipate, manage, and respond to cyberattacks, as well as to increase society's awareness and education on cybersecurity.

In this context, the strategy aims to ensure compliance with European Union norms and directives and to strengthen cooperation with international partners in addressing sophisticated and hybrid threats that may undermine 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 linked to technological, economic, and geopolitical advancements, the growth of international cooperation, as well as the emergence of sophisticated cyber threats, require a national cybersecurity strategy that is dynamic and capable of adapting to rapid changes in the digital environment.

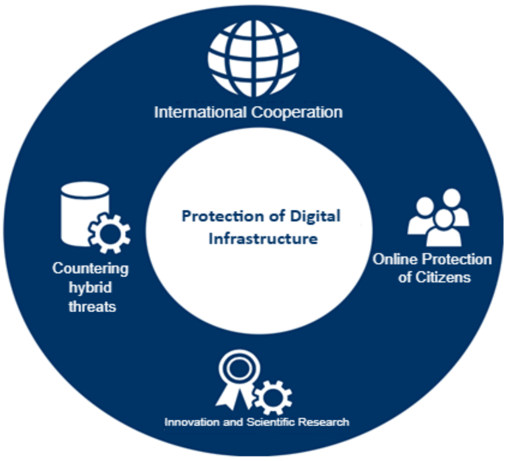
International Cooperation
Protection of Digital Infrastructure
Countering hybrid threats
Online Protection of Citizens
Innovation and Scientific Research

Figure 1. Strategy Policies

The strategy is accompanied by an action plan that defines concrete activities for its implementation, aiming at the achievement of the objectives set. This action plan specifies clear steps and timelines for each phase of the process.

- ***Purpose of policy 1: Protection of Digital Infrastructure***: The foundation of the National Cybersecurity Strategy is the protection of the country's critical and important information infrastructures, which include the networks, systems, and services that support the functioning of the state and the daily life of its citizens. This policy aims to ensure the continuity of services and the protection of information systems that sustain 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, with the objective of strengthening digital and cyber resilience.

- ***Purpose of policy 2: Online Protection 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 societal chain, reducing vulnerabilities that could be exploited by attackers. Public education and awareness-raising 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 better positioned to contribute to public debate and to advocate for improved policies. Equally important is the promotion of cyber ethics and the observance of proper online conduct, as well as to prevent online radicalizm, by fostering the use of respectful and responsible language.

  The National Cybersecurity Strategy 2025-2030 focuses on establishing 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, thereby ensuring collective and more effective protection against cyber threats. In this context, Albania is committed to actively contributing to international initiatives and agreements, particularly by diligently implementing its obligations as a NATO member state, thus reinforcing the resilience of the global digital environment.
- ***Purpose of policy 4: Advancing innovation and scientific research***: The National Cybersecurity Strategy embraces the use of advanced technologies, including artificial intelligence, *blockchain* and quantum computing, to reinforce cyber defence and to address the complex challenges of an increasingly intricate digital environment. Innovation is an fundamental pillar that contributes to enhancing advanced security protocols, enabling early detection of threats, and ensuring the resilience of the digital ecosystem. Scientific research and the adoption of new technologies strengthen Albania's strategic capability to respond effectively to cyber threats, while ensuring a trustworthy and sustainable digital environment.
- ***Purpose of policy 5: Countering hybrid threats***: To counter complex hybrid threats that exploit vulnerabilities in cyberspace, Albania is developing a proactive, resilient and adaptive defensive strategy. One of the key policies of this strategy is countering 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, enhancing 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.

Policy Objective 1: Protection of Digital Infrastructure

Protection of Digital Infrastructure is the core policy of Albania's 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 objective of protecting digital infrastructure is to establish 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 countering cyber threats will only be successful if operators of critical and important information infrastructures demonstrate the necessary cooperation and awareness regarding the importance of implementing cybersecurity measures.

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

- Processes
- Technology
- Human Resources

1. Processes

Processes play a key role in the National Cybersecurity Strategy.

They include a set of interconnected and coordinated steps aimed at protecting digital assets, information systems, and communication networks from threats and cyberattacks. Processes define how a digital infrastructure interacts with all aspects of cybersecurity, including practices that are:

- clear and well-documented in the defining roles and responsibilities;
- dynamic in responding to hybrid threats;
- continuous and adaptive in advancing 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 aligning international standards and directives in the drafting of legislation and the regulatory framework that define the management of cybersecurity at the national level. The purpose of this objective is to ensure effective protection against cyber threats and attacks, while remaining consistent with security requirements and the needs arising from the development of new technologies

Specific Objective 1.2: Enhancing Monitoring Capacities and Systems Protection

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 access for users. The purpose of this objective is to minimize risks through the implementation of proactive measures and ensuring sustainable protection against cyberattacks 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 risk mitigation at the infrastructure, sector, and national level. The purpose of this objective is to emphasizecooperation with national and international partners to address cyber risks, as well as to create communication channels for information sharing.

Specific Objective 1.4: Development of Cyber Incident Response and Management Plans

This objective covers the management and information sharing related to cyber incidents, threat intelligence, root cause analysis of incidents, reporting to improve preventive measures, and timely response. The goal is to establish clear processes for incident response and management to prevent and limit potential damage within a shorter timeframe.

Specific Objective 1.5: Securing 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 secure participation in the digital society as well as the secure use of online public and private services.

Specific Objective 1.6: Implementation of the Cybersecurity Certification Scheme

This objective aims to establish a trusted national mechanism for cybersecurity certification, aligned with the legal European Union framework. 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 Resources

The fulfilment ofthe vision and mission of the National Strategy requires the development of the appropriate skills, knowledge, and culture in the field of cybersecurity. Human resources plays an important role in strengthening the level of cybersecurity by applying their expertise in the design and implementation of security measures. This process involves all stakeholders such as policymakers, cybersecurity specialists, and users of digital systems, who must understand their roles and responsibilities in order to manage and mitigate risks and contribute to enhancing cybersecurity resilience. Education, training, and awareness programmes are essential for enhancing human resources, 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-raising 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. Moreover, the involvement of all stakeholders 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 integration of enhanced curricula in educational sector, specialized trainings, professional certifications, talent attraction and engagement, inclusiveness, and cooperation with international organizations on 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 the implementation of cybersecurity measures to prevent and manage cyber threats. The advancement on technology increases the need for a rapid response to ever more sophisticated cyberattacks. This process involves a range of major challenges to ensure a sustainable and effective protection against these complex threats.

Specific objective 3.1: The use and Integration of Advanced Technologies

The use and integration of advanced technologies, such as Artificial Intelligence (**AI**), Large Language Model programme (**LLMs**), quantum computers, quantum cryptography, and blockchain decentralized technologies, will improve cybersecurity by enabling advanced threat detection and automated responses.

Specific Objective 3.2: Monitoring, Detection, and Cyber Protection Through Advanced Technologies

Albania is committed to ensuring a level of cyber resilience proportional to 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 application of the *'secure by design'* principle integrates cybersecurity measures into all phases of the lifecycle of digital systems and services, procurement and secure deactivation. This approach ensures 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 obsolete technologies at the national level through the development and implementation of comprehensive policies aimed at their identification, updating, isolation, or replacement, contributing to strengthening cybersecurity, enhancing service resilience, and increasing reliability of critical and important information infrastructures.

Specific Objective 3.5: Adoption of Alternative Open- Source 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 (CIIs). This approach aims to ensure the continuity of cybersecurity protection and the preservation of the operational resilience of these infrastructures, especially under technological or financial constraints.

Policy Objective 2*: Online Protection* of Citizens and 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 adequacy 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- governmental organizations (NGOs), media, and civil society discuss challenges and solutions for cybersecurity. These dialogue platforms help create consensus-based policies and address the diverse community needs. Also, awareness-raising and capacity-building activities are a priority, including awareness campaigns on online risks, educational programmes for youth and underrepresented groups, as well as targeted training for professionals and wider public. Inter-institutional and cross-sectoral cooperation plays an important role in the implementation of this policy. Public institutions, private sector, NGOs, and media coordinate efforts to build a strong cybersecurity ecosystem, ensuring a comprehensive and sustainable approach to citizen protection and empowerment.

Specific Objective 1: Drafting and Development of the National Citizens' Awareness Plan (NCAP)

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 NCAP will include organized campaigns in education institutions, public institutions, and local communities, with the purpose of increasing awareness on best practices for *online* security. In this context, educational programmes will be developed to equip citizens with the necessary skills to identify and avoid cyber threats, including protection from potential cybercrimes such as fraud, identity theft, etc., creating a continuous educational chain for everyone.

Specific objective 2: Drafting of a Legal Framework for Inclusive Citizen Access

This objective aims to create and adapt an advanced legal framework that guarantees 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 online discrimination. To this end, inclusive 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: Establishing Mechanisms for the Online Protection of Children

Children represent one of the most vulnerable categories in the digital ecosystem, therefore this objective aims to create and implement specific mechanisms to guarantee their *online* safety. In this context, dedicated platforms will be developed to provide 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 caregivers in the effective supervision of children's digital activities. As part of this objective, structured awareness-raising campaigns and training programmes will also be carried out, equipping children with the necessary skills to identify and address cyber risks. This comprehensive approach seeks to create a safe and educational digital environment that promotes children's well-being and development.

Specific Objective 4: Promoting Gender Equality in the Digital Space

This objective aims to create an inclusive and secure digital environment for women and girls, focusing on their empowerment and combating all forms 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 disparities in education**, especially in science, technology, engineering and mathematics (STEM), where girls are less likely to pursue or be represented in these fields;
- **The low participation of women in the digital labour market**, including their limited representation in careers within the information and communication technologies (ICT) sector;
- **Online violence and harassment**, including cyberbullying and other forms of gender-based violence that restrict 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 lack of gender-specific administrative data**, as well as gaps in interinstitutional coordination for defining and monitoring of key gender indicators.

Through awareness-raising 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 addressing *online* harassment*,* as well as the development of support networks for professional women in the field of technology. This objective will also aim at the creation of\ policies that encourage gender equality in all aspect of the digital space and promote a supportive culture for women and girls *online.*

Specific Objective 5: Establishing Appropriate Mechanisms for the Online Protection of SMEs

Within the efforts to strengthen digital security and improve the cyber resilience of the private sector, special attention has been dedicated to promoting education in technology and cybersecurity for Small and Medium Enterprises (SMEs). This initiative aims to raise awareness and reinforce the protective capacities of SMEs, enabling them to better address the growing challenges related to cyber threats. In this regard, practical guidelines on the necessary cybersecurity measures will be developed, serving as reference resources for SMEs to improve their digital infrastructure and to implement best practices for the protection of their data and systems. Also, dedicated annual trainings will be organized for SME employees, to develop 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 create a stronger culture of security within the SME sector.

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

This objective seeks to protect and empower underrepresented groups by creating inclusive platforms that address their specific needs, ensuring equal access to digital tools and services. Through educational programmes and training, these groups will be empowered to become more active and protected in the digital space. Also, policies and mechanisms will be implemented to address online discrimination and to 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, encouraging information sharing, the development of joint capacities, and the establishment of unified standards, ensuring a collective and more effective protection against cyber threats. To this end, Albania is committed to actively contributing to international initiatives and agreements on cybersecurity, thus reinforcing the resilience of the global digital environment.

Specific objective 1: Policies and Legislation Compliance

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. Cyberattacks 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 persistent cyberattacks.

Specific Objective 2: Strengthening Regional (WB6) and International Cooperation

To build a secure and resilient digital ecosystem, no state can act alone, as cyber or hybrid attacks have demonstrated that cooperation is the most effective practice against them. 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 for addressing cyber threats and undertaking 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 information sharing and coordination of responses to cyber incidents.

Specific Objective 3: Development of Cyber Diplomacy

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

Policy Objective 4: Fostering 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, private and public sector, in increasing national capacities in the field of cybersecurity and the creation of new technological solutions. This approach not only enhances the ability to address cyber challenges, but also helps in creating an innovative and secure digital environment for Albania.

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

The establishment of the National Cybersecurity Centre of Excellence (NCCoE) as an innovative hub for research and technological development will enable close cooperation between higher education institutions, national and international research centres, as well as public and private institutions. It will promote scientific research, talents identification, 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 real-time prevention and detection of cyberattacks, with the objective of strengthening national digital security and resilience.

Specific Objective 2: Supporting Cybersecurity Start-ups

This objective aims to support the development of start-ups in the field of cybersecurity by creating an environment that fosters innovation and technological entrepreneurship. This includes facilitating access to research resources and technical expertise, providing specialized training and mentoring programmes, and promoting cooperation between the public and private sector, and higher education institutions. A particular focus will be placed on encouraging the participation of women and girls in the cybersecurity sector.

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

Funding programmes will be developed for research and innovation in cybersecurity. These programmes will include the establishment of dedicated funds, the promotion of gender equality in innovation and scientific research policies, the provision of fiscal incentives for businesses investing in secure technologies and the promotion of public-private partnerships for the co-financing of innovative projects.

Policy Objective 5: Countering Hybrid Threats

Hybrid threats involve the use of a plan or strategy in which different 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 entities.

To protect against hybrid threats, an integrated approach is required that includes strengthening the security of critical infrastructure and important information, enhancing 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 Countering Hybrid Cyber Threats

The development of an appropriate legal framework for protection against hybrid cyber threats will enable the prevention, identification and threat management. This legal framework will ensure close inter-institutional cooperation at both national and international levels, 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 information sharing and resources. Close coordination ensures a rapid and efficient response to prevent and manage the consequences of hybrid threats.

Specific Objective 3: Establishing Mechanisms for Countering Hybrid Threats

To develop an integrated and efficient structure for anticipating, identifying, and responding to hybrid threats, including cyberattacks and disinformation, the use of modern tools and technologies is required. Information-sharing platforms, along with public awareness will ensure a swift and effective response to hybrid threats, preserving national stability and security.

Specific objective 4: Establishing Mechanisms for the Prevention and Investigation of Cybercrime

Preventing cybercrime requires a proactive approach and the use of advanced technology that includes early detection and rapid response to threats. This objective aims to create a secure and resilient digital environment in the digital space, by preventing and managing the potential impacts 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, "On the organization and functioning of the National Cybersecurity Authority", as well as on the commitments and standards of the EU and other international bodies.

- The active engagement of public and private institutions provides this Strategy with the ability to remain both objective and implementable. The inter-institutional working group, together with all stakeholders involved in the consultation process, provided valuable input and repeatedly reviewed the draft in order to approve a comprehensive strategy, ensuring that every actor recognizes its role and contribute to guaranteeing the country's cybersecurity.

- This Strategy is not only a strategy for institutions, but one that promotes and supports cybersecurity protection also for individuals, citizens and, in particular, children as the future of the country. It also identifies measures aimed not only at combating cybercrime, but also at countering the use of cyberspace for terrorism and violent extremism.

The Implementing Action Plan of National Cybersecurity Strategy, 2025–2027 has been prepared on the basis of:

a) The National Cybersecurity Strategy 2025-2030 and its component Policies;

b) the budgetary plans of public institutions.

As outlined in the specific objectives and key activities proposed in this Strategy and its Implementing Action Plan, the coordinating role must be carried out by the National Cybersecurity Authority. Furthermore, this document considers the obligations arising from the European integration process and alignment with the NIS2 and EIDAS2 directives, as well as the commitments stemming from Albania's status 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 impact assessment for the implementation of this

Strategy and its Action Plan 2025–2027, with the need for periodic review based on the dynamics of developments in the field of cybersecurity.

Each responsible institution shall plan the implementation of the assigned activities by ensuring the necessary budget allocations, human resources, and technical capacities for their execution. An annual assessment will be carried out to evaluate the implementation of activities and the achievement of objectives, based on the realization of the defined indicators. Institutions responsible for the implementation of activities and the attainment of results are obliged to report according to reporting standards. The Strategy Coordinator shall prepare and publish the annual report.

Action Plan and Financial Resources for Implementation

Activity costing methodology

The necessary expenses for implementing the Action Plan have been determined by costing each of the activities of this action plan. The methodology applied for cost calculation presents a combination of approaches commonly used in cases of strategies involving multiple stakeholders. The main methodology used is activity-based costing (Activity Based Costing-ABC), where for each activity the responsible institution is identified, along with the source of cost coverage, and resources are allocated for all products and services based on the actual consumption of each activity.

The budget has been prepared based on the cost of each activity outlined in the action plan, considering its timeline, frequency of implementation, and the number of beneficiaries for certain activities. The calculation of expenditures for key activities was carried out as follows:

- The calculation of expenses for human resources is based on the estimated time required for the implementation of the activity and an average daily wage of a specific category.
- Calculation of expenses for services. For these activities, the costs of services provided by the respective institutions are considered, based on the approved standards.
- The calculation of expenses for activities related to drafting and revision of legislation, monitoring and functioning of permanent structures, etc. For these activities, the calculation considered recurrent expenses such as salaries, social insurance contributions, external expertise (when foreseen in the plan), and consumable materials.
- Calculation of expenses for activities related to studies, awareness campaigns, training programmes, external expertise, etc. The cost estimation was based on similar specific initiatives, as well as according to the nature of the activities and prevailing market costs for such services.
- For training expenses, the unit cost per participant has been considered. The unit costs applied are those used for similar trainings in the past.
- For activities where full information was not available (such as projects or studies), the method of estimation 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. To ensure its effective 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:

- Annual consolidated budget for each activity, specific objective, strategic goal, and sources of financing;
- Detailed budget by activities, sources of funding, and responsible institutions.