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 Drafting and implementation of the legal framework on Cybersecurity		1.0.1.1 Drafting of secondary legislation pursuant to Law No. 25/2024 'On Cybersecurity'.	AKSK	AKSK	2,365,164	788,388	788,388	788,388	-			-
			1.0.1.2 Harmonisation of the legal framework with the EU acquis.	AKSK	AKSK	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.0.1.3 Drafting of national and international agreements in the field of cybersecurity.	AKSK	AKSK	4,680,396	1,560,132	1,560,132	1,560,132	-			-
			1.0.1.4 Improvement and standardisation of procedures for monitoring networks and information systems, including real-time reporting and response to cybersecurity incidents.	AKSK	AKSK	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** Enhancement of Monitoring Capacities and Protection of Systems	1.1.2.1 Improvement and standardisation of procedures for monitoring networks and information systems, including real-time reporting and response to cybersecurity incidents.	AKSK/AKSHI	**AKSK**/AKSHI	12,643,452	4,214,484	4,214,484	4,214,484	-			-
			1.1.2.2 Monitoring of cyber threats in Albania's digital space through cyber threat intelligence.	AKSK/AKSHI/MM/PSH/SHISH	AKSK	11,533,860	3,844,620	3,844,620	3,844,620	-			-
			1.1.2.3 Updating of security measures and verification of their implementation by OIKI/OIRI(Operators of Critical/Important Information Infrastructure), in order to reflect changes in legislation, technology and standards.	AKSK	AKSK	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.1.2.4 Drafting of security guidelines and protocols for OIKI and OIRI (Operators of Critical/Important Information Infrastructure).	AKSK	AKSK	12,419,568	4,139,856	4,139,856	4,139,856	-			-
			1.1.2.5 Periodic review of security policies and procedures to ensure alignment with evolving threats and technological developments.	AKSK	AKSK	7,095,492	2,365,164	2,365,164	2,365,164	-			-
			1.1.2.6 Review of cybersecurity measures, including the establishment of a secure cloud environment (PaaS, SaaS, IaaS, etc.).	AKSK	AKSK	-	-	-	-	-			-
			1.1.2.7. Strengthening procedures for the assessment and testing of information technology networks and systems.	AKSK	AKSK	-	-	-	-	-			-
			1.1.2.8 Drafting of procedures for the secure use of IoT, OT, ICS, SCADA and advanced technologies.	AKSK	AKSK	-	-	-	-	-			-
					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 Implementation and periodic review of the methodology for cyber risk assessment of all systems and networks operated by OIKI and OIRI(Operators of Critical/Important Information Infrastructure).	AKSK	AKSK	3,120,264	1,040,088	1,040,088	1,040,088	-			-
			1.1.3.2 Six-monthly assessment of cyber risks through the identification of vulnerabilities, technological and geopolitical threats, as well as potential opportunities for cyber attacks.	AKSK	AKSK	6,240,528	2,080,176	2,080,176	2,080,176	-			-
			1.1.3.3 Establishment of mechanisms for cyber risk information sharing with public institutions and OIRI/OIKI (Operators of Critical/Important Information Infrastructure).	AKSK/AKSHI	AKSK	150,000,000	150,000,000	-	-	-			-
			1.1.3.4 Assessment of cybersecurity at both sectoral and national level.	AKSK	AKSK	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) Development of Cyber Incident Response and Management Plans	1.1.4.1 Periodic review and enhancement of national and sectoral cyber incident response and management plans.	AKSK	AKSK	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.1.4.2 Review and update of the national cyber incident response and management plan after each incident affecting OIRI/OIKI(Operators of Critical/Important Information Infrastructure).	AKSK	AKSK	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.1.4.3 Review and enhancement of the communication procedure for cyber incident response.	AKSK	AKSK	3,570,804	1,190,268	1,190,268	1,190,268	-			-
			1.1.4.4 Updating of the national procedure for cyber crisis management .	AKSK	AKSK	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.1.4.5 Implementation of advanced mechanisms for the detection and tracking of cyber attacks through forensic analysis and incident data correlation.	AKSK/ AKSHI/ MM	AKSK/ AKSHI/ MM	305,643,656				61,128,731	122,257,462	122,257,462	
			1.1.4.6 Preparation of a report on the in-depth investigation of cyber attacks targeting data storage systems.	AKSK/PSH	AKSK	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) Guaranteeing the integrity and security of electronic	1.1.5.1 Alignment of national 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.	AKSK	AKSK	7,095,492	2,365,164	2,365,164	2,365,164	-			-
			1.1.5.2 Preparation of secondary legislation in the field of electronic identification, trust services, and the Digital Identity Wallet.	AKSK	AKSK	9,460,656	3,153,552	3,153,552	3,153,552	-			-

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)		security of electronic transactions through Qualified Trusted Services	1.1.5.3 Conclusion of agreements with Western Balkan countries on the mutual recognition of trust services.	AKSK	AKSK	7,095,492	2,365,164	2,365,164	2,365,164	-			-
			1.1.5.4 Supervision and monitoring of qualified trust service providers to ensure full compliance with national legislation.	AKSK	AKSK	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**	**-**	**-**	**-**	**-**
		Specific Sub-Objective 1.1.6 Implementation of the Cybersecurity Certification Scheme	1.1.6.1 Drafting of the Cybersecurity Certification Scheme.	AKSK	AKSK	-	-	-	-	-			-
			1.1.6.2. Accreditation of Conformity Assessment Bodies (CABs).	DPA	DPA	-	-	-	-	-			-
			1.1.6.3.Authorization and registration of Conformity Assessment Bodies (CABs).	AKSK	AKSK	-	-	-	-	-			-
					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): Promotion and Development of Cybersecurity Culture	1.2.1.1. Drafting and implementation of national awareness-raising campaigns on cyber hygiene and security best practices, with a specific focus on employees of OIKI and OIRI(Operators of Critical/Important Information Infrastructure).	AKSK/ AKSHI	AKSK	9,460,656	3,153,552	3,153,552	3,153,552	-			-
			1.2.1.2. Development of awareness-raising campaigns aimed at promoting the use of trust services.	AKSK	AKSK	1,190,268	396,756	396,756	396,756	-			-
			1.2.1.3. Development of a dedicated training plan on cybersecurity.	AKSK	AKSK	396,756	132,252	132,252	132,252	-			-
			1.2.1.4. Cybersecurity training programmes for employees of OIKI and OIRI(Operators of Critical/Important Information Infrastructure).	AKSK	AKSK	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): Strengthening Professional Capacities	1.2.2.1 Review and integration of cybersecurity into pre-university education curricula.	MA/AKSK	AKSK	6,307,104	2,102,368	2,102,368	2,102,368	-			-
			1.2.2.2 Enhancing the technical competencies and practical expertise of cybersecurity professionals through structured participation in periodic technical trainings, international cooperation initiatives, and cyber competitions addressing real-world threats and incidents.	AKSK/AKSHI	AKSK	5,770,000	5,770,000	-	-	-			-
			1.2.2.3 Identification, recruitment and development of new cybersecurity talents through structured training programmes, mentoring schemes, and career development opportunities.	AKSK/AKSHI	AKSK	12,643,452	4,214,484	4,214,484	4,214,484	-			-
			1.2.2.4Creation of dedicated cybersecurity laboratories (cyber ranges) to enable hands-on training, practical exercises, and real-life incident simulations.	AKSK	AKSK	360,820,856	37,088,600			64,746,451	129,492,902	129,492,902	
			1.2.2.5 Capacity-building for school staff and implementation of school-based awareness campaigns "Against online radicalization and violent extremism".	CVE / MA/ ASHDMF	CVE	185,859	61,953	61,953	61,953	-			-
			1.2.2.6 Development and dissemination of counter-narratives aimed at fostering tolerance and countering online hate speech linked to radicalization and violent extremism.	CVE / MA	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): Adoption and Integration of Advanced Technologies	1.3.1.1Integration and deployment of advanced technologies, including Artificial Intelligence (AI), to enhance the detection, prevention, and response capabilities against cyber attacks.	AKSK/AKSHI	AKSK	5,765,009,080	3,331,672,720			-			2,433,336,360
			1.3.1.3 Development of blockchain-based policies aimed at safeguarding the integrity, transparency, and trustworthiness of digital transactions.	AKSK/AKSHI	AKSHI	-	-	-	-	-			-
			1.3.1.4 Strengthening and upgrading of cyber testing and simulation laboratories.	AKSK	AKSK	442,269,688	-			88,453,938	176,907,875	176,907,875	
			1.3.1.5 Deployment of automated systems to ensure continuous updating and efficient management of cybersecurity measures.	AKSK/AKSHI	AKSK	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. Implementation of advanced mechanisms to ensure proactive protection and resilience against Advanced Persistent Threats (APTs).	AKSK/AKSHI/SHISH/MM	AKSK	895,000,000	-	-	-	179,000,000	358,000,000	358,000,000	
			1.3.2.2.Adoption of cloud computing solutions to ensure secure storage, protection, and resilience of critical data.	AKSK/AKSHI	AKSK	-	-	-	-	-			-
					Subtotal Sub-Objective	**895,000,000**	**-**	**-**	**-**	**179,000,000**	**358,000,000**	**358,000,000**	**-**
		Specific Sub-Objective. 1.3.3 (Technology): Implementation of the ‘Secure by Design’ Framework for Digital Infrastructures	1.3.3.1. Development of policies to ensure the systematic integration of cybersecurity measures at all stages of the digital systems lifecycle.	AKSK/AKSHI	AKSK	2,660,400	886,800	886,800	886,800	-			-
			1.3.3.2 Drafting of guidelines for infrastructures and operators on the implementation of the 'security by design and by default' principles.	AKSK/AKSHI	AKSK	4,730,328	1,576,776	1,576,776	1,576,776	-			-
			1.3.3.3 Development of protocols and manuals to ensure the cybersecurity of IoT (Internet of Things) devices and their protection against emerging cyber threats.	AKSK/ AKEP	**AKSK**/ AKEP	1,190,268	396,756	396,756	396,756	-			-
					Subtotal Sub-Objective	**8,580,996**	**2,860,332**	**2,860,332**	**2,860,332**	**-**	**-**	**-**	**-**

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. 1.3.4 (Technology): Effective Management of Legacy Technologies	1.3.4.1 Drafting of a national plan for the identification, mitigation, and phasing out or isolation of outdated technologies within critical systems.	AKSK	AKSK	1,560,132	520,044	520,044	520,044	-			-
			1.3.4.2 Development of a national program to facilitate the migration towards secure, resilient, and sustainable technologies.	AKSK/ AKSHI	**AKSK**/ AKSHI	2,365,164	788,388	788,388	788,388	-			-
			1.3.4. 3 Carrying out periodic assessments to identify and address outdated or obsolete technologies.	AKSK	AKSK	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**	**-**	**-**	**-**	**-**
		Specific Sub-Objective. 1.3.5 (Technology): Use of Alternative Compensating Technologies for Cybersecurity	1.3.5.1 Promotion and adoption of alternative and compensatory technologies to enhance cybersecurity resilience and ensure continuity of solutions in the face of technological or financial constraints.	AKSK	AKSK	1,560,132	520,044	520,044	520,044	-			-
			1.3.5.2 Adoption of alternative platforms to ensure continuity and security of services in cases where proprietary or paid technologies are not accessible.	AKSK	AKSK	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:** Drafting and Development of the National Plan for Citizen Awareness (NPCA)		2.1.1 Analysis of the current situation regarding awareness campaigns/programmes and assessment of the need for their revision.	AKSK/MSHMS	AKSK	2,055,000	685,000	685,000	685,000	-			-
			2.1.2 Development of 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.	AKSK	AKSK	793,512	264,504	264,504	264,504	-			-
			2.1.3 Preparation and dissemination of clear and accessible educational materials for citizens, in user-friendly language, including children, on cyber hygiene and online safety.	AKSK/MSHMS	AKSK	6,667,275	2,222,425	2,222,425	2,222,425	-			-
			2.1.4 Creation of public campaigns to promote awareness and increase knowledge on cybersecurity through various media channels.	AKSK	AKSK	30,000,000	10,000,000	10,000,000	10,000,000	-			-
			2.1.5 Promotion of the increased use of the "RED BUTTON" for reporting illegal content.	CVE / AKSK	AKSK	-	-	-	-	-			-
					Subtotal Objective	**39,515,787**	**13,171,929**	**13,171,929**	**13,171,929**	**-**	**-**	**-**	**-**
	Specific Objective 2.2: Drafting of a Legal Framework for an Inclusive Citizen-Centered Approach		2.2.1 Identification of the need for amendments to existing legislation to strengthen citizens' online protection.	AKSK	AKSK	1,560,132	520,044	520,044	520,044	-			-
			2.2.2 Preparation of a draft law on the online protection of citizens from potential cyber threats.	AKSK	AKSK	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: Creation of Mechanisms for the Online Protection of Children.		2.3.1 Review of pre-university curricula to assess the integration of cybersecurity and recommend necessary improvements..	AKSK/MA	MA	3,153,552	-	3,153,552	-	-			-
			2.3.2 Training of teaching staff on cybersecurity and design of a regular programme to strengthen capacities in schools.	AKSK/MA	MA	-	-	-	-	-			-
			2.3.3 Integration of modules on cybersecurity and online child/youth protection into curricula at all levels.	AKSK/MA	MA	-	-	-	-	-			-
			2.3.4 Implementation of awareness campaigns for parents on the use of cybersecurity applications and platforms enabling parental control.	AKSK/MA	AKSK	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: Promotion of Gender Equality in the Digital Space		2.4.1 Promotion of education and careers for women and girls from all backgrounds in the field of technology and cybersecurity.	AKSK/AKSHI/MSHMS	AKSK	30,211,293	10,070,431	10,070,431	10,070,431	-			-
			2.4.2 Preparation of guidelines on cybersecurity measures for SMEs.	AKSK	AKSK	2,147,688	715,896	715,896	715,896	-			-
			2.4.3 Development of campaigns to promote equal opportunities for women in the digital sector.	AKSK	AKSK	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: Establishment of Adequate Mechanisms for the Online Protection of SMEs		2.5.1 Promotion of education for SMEs in the field of technology and cybersecurity.	AKSK	AKSK	5,470,056	1,823,352	1,823,352	1,823,352	-			-
			2.5.2 Organisation of annual training programmes dedicated to SME employees.	AKSK	AKSK	5,470,056	1,823,352	1,823,352	1,823,352	-			-
			2.5.3 Organizimi i trajnimeve vjetore të dedikuara për Punonjësit e SMEve.	AKSK	AKSK	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: Development of Mechanisms for the Protection and Empowerment of Underrepresented Groups		2.6.1 Establishment of a national platform with educational and interactive tools to raise awareness on online safety.	AKSK	AKSK	136,000,000	136,000,000			-			-
			2.6.2 Drafting and distribution of educational materials tailored for underrepresented groups.	AKSK	AKSK	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**	**-**	**-**	**-**	**-**

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	
				Subtotal of Policy 2	**242,704,166**	**170,516,871**	**37,670,423**	**34,516,871**	**-**	**-**	**-**	**-**
Policy 3: Strengthening International Cooperation	**Specific Objective 3.1**: Harmonisation of Policies and Legislation	3.1.1 Establish working groups to review and propose legislative amendments aligned with EU directives, international standards, and best practices in cybersecurity governance.	AKSK	AKSK	-	-	-	-	-			-
		3.1.2 Raise awareness among public authorities and private sector entities on the practical implementation of cybersecurity legislation, standards, and policies.	AKSK	AKSK	-	-	-	-	-			-
				Subtotal Objective	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
	Specific Objective 3.2: Strengthening Regional (WB6) and International Cooperation	3.2.1 Drafting of a regional programme to strengthen cyber resilience through joint training initiatives and cross-sector simulation exercises involving public authorities and private sector actors.	AKSK/ MEPJ	AKSK	29,775,000	9,925,000	9,925,000	9,925,000	-			-
		3.2.2 Facilitation of regional roundtables to promote the exchange of best practices and enhance cross-border cooperation in cybersecurity.	AKSK/MEPJ	AKSK	-	-	-	-	-			-
				Subtotal Objective	**29,775,000**	**9,925,000**	**9,925,000**	**9,925,000**	**-**	**-**	**-**	**-**
	Specific Objective 3.3: Advancement of Cyber Diplomacy	3.3.1 Preparation of a national plan clearly defining objectives and strategic partners for cooperation in the field of cybersecurity.	AKSK/MEPJ	AKSK	1,330,200	443,400	443,400	443,400	-			-
		3.3.2 Participation in international mechanisms for cooperation in cybersecurity, with a focus on sharing practical experiences and strengthening inter-institutional dialogue on strategic challenges and solutions.	AKSK	**AKSK**/MEPJ	-	-	-	-	-			-
		3.3.3 Enhancing national capacities for cyber diplomacy.	AKSK/ AKSHI/ MEPJ	**AKSK**/ AKSHI/ MEPJ	-	-	-	-	-			-
				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 Centre of Excellence for Cybersecurity	4.1.1 Drafting and adoption of regulations and guidelines for the establishment and operation of the National Cybersecurity Excellence Centre (QKESK).	AKSK/ MA /MEI	**AKSK**	-	-	-	-	-			-
		4.1.2 Establishment of mechanisms for monitoring and evaluating the performance of the National Cybersecurity Excellence Centre.	AKSK/ MA /MEI	AKSK	-	-	-	-	-			-
		4.1.3 Equipping the Centre with research laboratories and infrastructure for testing emerging technologies.	AKSK/ MEI	AKSK	-	-	-	-	-			-
		4.1.4 Fostering Public-Private Partnerships to advance innovative research projects involving public authorities, academia, and the private sector.	AKSHI/AKSK/MEI	MEI	-	-	-	-	-			-
		4.1.5 Fostering and promoting the exchange of knowledge and best practices on innovative cybersecurity solutions.	MEI/AKSK/AKSHI	MEI	-	-	-	-	-			-
				Subtotal Objective	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
	Objective 4.2. Support for Cybersecurity Startups	4.2.1 Creation of mechanisms to foster and facilitate the growth and operation of start-ups in information technology and cybersecurity, in line with EU digital innovation and cybersecurity initiatives.	MEI/AKSK	MEI	-	-	-	-	-			-
		4.2.2 Ensuring the availability of supportive environments for start-ups, including tech hubs and incubators.	MEI/AKSK	MEI	-	-	-	-	-			-
		4.2.3 Ensuring the availability and continuous enhancement of the existing laboratory for the development, testing, and validation of innovative cybersecurity solutions.	AKSK	AKSK	-	-	-	-	-			-
		4.2.4 Promoting the involvement of startups in research and pilot projects for the testing of new technologies.	MEI/AKSK	MEI	-	-	-	-	-			-
		4.2.5 Facilitating strategic partnerships between innovative startups and large enterprises to strengthen their integration into the national cybersecurity ecosystem.	MEI/AKSK	MEI	-	-	-	-	-			-
		4.2.6 Supporting joint research projects between startups and higher education institutions.	AKSK/MA/MEI/	MEI	-	-	-	-	-			-
		4.2.7 Organizing hackathons, competitions, and innovation-driven initiatives focused on cybersecurity solutions.	MEI/AKSK	AKSK	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. Development of Funding Programmes for Cybersecurity Research and Innovation	4.3.1 Developing national funding programmes dedicated to research and innovation in cybersecurity.	MEI/AKSK	MEI	-	-	-	-	-			-
		4.3.2 Establishing a national fund to support cybersecurity research initiatives.	MEI/MA/AKSK	AKSK	-	-	-	-	-			-
		4.3.3 Facilitating access to EU grants and international donors for research and development in cybersecurity.	MEI/AKSK	MEI/AKSK	-	-	-	-	-			-
		4.3.4 Providing fiscal incentives for businesses that invest in secure technologies and scientific research.	MEI/AKSK	MEI	-	-	-	-	-			-
				Subtotal Objective	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**
				Subtotal of Policy 4	**90,000,000**	**30,000,000**	**30,000,000**	**30,000,000**	**-**	**-**	**-**	**-**

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	**Specific Objective 5.1** Drafting of the Legal Framework for the Protection Against Hybrid Cyber Threats	5.1.1 Conducting a comprehensive review of the national legal framework to ensure its adequacy and effectiveness in addressing hybrid threats.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP/MPB	AKSK	3,153,552	-	3,153,552	-	-			-
		5.1.2 Updating and adapting national strategies to reflect technological developments and the evolving nature of hybrid threat tactics.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	3,990,600	1,330,200	1,330,200	1,330,200	-			-
		5.1.3 Establishing dedicated governance structures to ensure effective inter-institutional coordination and cooperation in responding to hybrid threats.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	4,730,328	1,576,776	1,576,776	1,576,776	-			-
		5.1.4 Introducing and reinforcing supervisory and compliance-monitoring mechanisms to ensure full implementation of the legal framework.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP/MPB	AKSK	4,160,352	1,386,784	1,386,784	1,386,784	-			-
		5.1.5 Harmonising national legislation with EU and international legal instruments to guarantee a coherent and unified approach against hybrid threats.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	MEPJ	-	-	-	-	-			-
		5.1.6 Enhancing institutional capacities through alignment with the EU acquis and the adoption of international best practices in hybrid threat management.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	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 Coordination	5.2.1 Establishing a national coordination mechanism for response to hybrid threats.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	8,205,084	2,735,028	2,735,028	2,735,028	-			-
		5.2.2 Developing structured mechanisms for information exchange between national and international institutions.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	-	-	-	-	-			-
		5.2.3 Organising joint trainings and exercises with OIKI/OIRI (Operators of Critical/Important Information Infrastructure) to strengthen preparedness and response to hybrid attacks.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	60,000,000	20,000,000	20,000,000	20,000,000	-			-
		5.2.4 Promoting public–private partnerships for the monitoring and response to hybrid threats.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	-	-	-	-	-			-
		5.2.5 Developing a dedicated and secure communication infrastructure to enable real-time exchange of sensitive information among key cybersecurity stakeholders.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	-	-	-	-	-			-
		5.2.6 Encouraging the conclusion of international cooperation agreements to enhance protection against hybrid threats.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	-	-	-	-	-			-
				Subtotal Objective	**68,205,084**	**22,735,028**	**22,735,028**	**22,735,028**	**-**	**-**	**-**	**-**
	Specific Objective 5.3 Establishment of Mechanisms for Protection Against Hybrid Threats	5.3.1 Deploying advanced tools and technologies for monitoring and early detection of hybrid threats.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	-	-	-	-	-			-
		5.3.2 Implementing dedicated platforms for information sharing on hybrid threats.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	200,000,000	-	200,000,000	-	-			-
		5.3.3 Drafting awareness-raising campaigns on the risks of disinformation and cyberattacks.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	3,941,940	1,313,980	1,313,980	1,313,980	-			-
		5.3.4 Regularly updating emergency protocols based on the latest risk assessments.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK	3,153,552	1,051,184	1,051,184	1,051,184	-			-
		5.3.5 Leveraging artificial intelligence technologies for data analysis and forecasting of hybrid threats.	MEPJ/AMA/PSH/MM/SHISH/MIA/MIE/CVE/AKSHI/AKSK/AKEP	AKSK/AKSHI	-	-	-	-	-			-
				Subtotal Objective	**207,095,492**	**2,365,164**	**202,365,164**	**2,365,164**	**-**	**-**	**-**	**-**
	Specific Objective 5. 4 Development of Mechanisms for the Prevention and Investigation of Cybercrime	5.4.1 Strengthening inter-institutional cooperation in the fight against cybercrime.	MEPJ/AKSK/PSH	PSH	-	-	-	-	-			-
		5.4.2 Improving the national legal framework to ensure harmonisation with EU legislation and international conventions on cybercrime.	MEPJ/PSH	PSH	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
AKSHI	-	-	-	-	-	-	-	-
AKSK	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
AKEP	-	-	-	-	-	-	-	-
MPB	-	-	-	-	-	-	-	-
MM	-	-	-	-	-	-	-	-
CVE	557,580	185,860	185,860	185,860	-	-	-	-
MA	3,153,552	-	3,153,552	-	-	-	-	-
MEI	-	-	-	-	-	-	-	-
MEPJ	-	-	-	-	-	-	-	-
PSH	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**

	-	-	-	-	-			-

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	