Strategic Investment Clusters for Strengthening Digital Security, Innovation, and Inclusion in Albania and the Western Balkans

Mobilizing International Support for a Secure, Resilient, and Innovative Digital Ecosystem

Contents

EXECUTIVE SUMMARY 10
POLICY 1 – Protection of Digital Infrastructure 10
POLICY 2 – Online Protection of Citizens and Cyber Culture 10
POLICY 3 – Strengthening International Cooperation 10
POLICY 4 – Promotion of Innovation and Scientific Research 11
POLICY 5 – Protection Against Hybrid Threats 11
A Regional Vision With Global Impact 11
POLICY 1 – PROTECTION OF DIGITAL INFRASTRUCTURE 12
Establishing the Extended National SOC (NSOC) 12
With Open Source Platforms & Integration with Energy + Transport + Telecom 12
Goal 12
Importance for Albania 12
Importance for the Region 12
Benefits for EU & Partners 12
Challenges & Risks 12
Cost Breakdown: €4.0M – €4.8M 12
Conclusion 12
Sectorial Healthcare SOC 13
Goal 13
Importance for Albania 13
Importance for the Region 13
Benefits for EU & Partners 13
Challenges & Risks 13
Cost Breakdown: €2.3M – €2.8M 13
Conclusion 13
Implementation of a SOC Center for Each Public and Private University in Albania 13
(Supported by the U.S. State Department via CRDF Global) 13
Goal 14
Importance for Albania 14
Importance for the Region 14
Benefits for EU & Partners 14

Challenges & Risks 14

Conclusion 14

Monitoring Operational Center for 12 Municipalities 14

Goal 14

Importance for Albania 14

Importance for the Region 14

Benefits for EU & Partners 15

Challenges & Risks 15

Cost Breakdown: €1.8M – €2.1M 15

Conclusion 15

Coordinated Cybersecurity Engagement Platform 15

(Promised by BAE Systems – UK Government).. 15

Goal 15

Importance for Albania 15

Importance for the Region 15

Benefits for EU & Partners 15

Challenges & Risks 16

Conclusion 16

Regional Governance, Risk & Compliance (GRC) Platform 16

(Supported by UK Government via BAE Systems) 16

Goal 16

Importance for Albania 16

Importance for the Region 16

Benefits for EU & Partners 16

Challenges & Risks 16

Conclusion 16

Regional Attack Surface Management (ASM) Platform 17

(Supported by UK Government via BAE Systems) 17

Goal 17

Importance for Albania 17

Importance for the Region 17

Benefits for EU & Partners 17

Challenges & Risks 17
Conclusion 17
Training 2 Experts in Security Governance for 400 Public and Private Institutions 17
(Supported by UK Government via BAE Systems) 17
Goal 17
Importance for Albania 17
Importance for the Region 18
Benefits for EU & Partners 18
Challenges & Risks 18
Conclusion 18
Counter-Ransomware Task Force (Albania + Region) 18
Goal 18
Importance for Albania 18
Importance for the Region 18
Benefits for EU & Partners 18
Challenges & Risks 18
Cost Breakdown: €2M – €2.3M 18
Conclusion 19
Regional e-Learning Platform (CNI Experts + Awareness for Employees & Citizens) 19
Goal 19
Importance for Albania 19
Importance for the Region 19
Benefits for EU & Partners 19
Challenges & Risks 19
Cost Breakdown: €1.2M – €1.5M 19
Conclusion 19
Regional Incident Attempt Categorization & Prioritization Platform 20
Goal 20
Importance for Albania 20
Importance for the Region 20
Benefits for EU & Partners 20
Challenges & Risks 20

Cost Breakdown: €750K – €950K 20

Conclusion 20

Establishing the 5G Stand-Alone Technology Testbed 20

For Telecom Providers in the Region 20

Goal 20

Importance for Albania 20

Importance for the Region 21

Benefits for EU & Partners 21

Challenges & Risks 21

Cost Breakdown: €6M – €7,3M 21

Conclusion 21

Establishing the e-ID & Trusted Services Sandbox 21

(Aligned with EU Acquis & eIDAS2) 21

Goal 21

Importance for Albania 21

Importance for the Region 21

Benefits for EU & Partners 22

Challenges & Risks 22

Cost Breakdown: €3.5M – €4.0M 22

Conclusion 22

POLICY 2 – NATIONAL PROGRAM FOR PROTECTION OF CITIZENS ONLINE 23

Regional Cyber Security Marathon (CTF) 23

For University Students, Women in Cyber, and Underrepresented Groups 23

Goal 23

Importance for Albania 23

Importance for the Region 23

Benefits for EU & Partners 23

Challenges & Risks 23

Cost Breakdown Logic 23

Conclusion 24

Encourage the Woman in Cyber (Activities and Training) 24

Goal 24

Importance for Albania 24

Importance for the Region 24

Benefits for EU & Partners 24

Challenges & Risks 24

Cost Breakdown: €1.2M – €1.8M 24

Conclusion 25

Establishing a Digital Safe Environment for Children and Teenagers 25

(With AKEP, AMA, ISPs, Ministry of Education, NGOs) 25

Goal 25

Importance for Albania 25

Importance for the Region 25

Benefits for EU & Partners 25

Challenges & Risks 25

Cost Breakdown Logic 25

Conclusion 26

Encourage the Underrepresented Groups to Participate Actively in Our Digital Society and Protect Them From Cyberbullying, Blackmail, Inappropriate Content, etc. 26

(In Coordination With Ministry of Interior, State Police, AKEP, AMA, AKSHI, Ministry of Education, Ministry of Economy, Ministry of Healthcare) 26

Goal 26

Importance for Albania 26

Importance for the Region 26

Benefits for EU & Partners 26

Challenges & Risks 26

Cost Breakdown: €2.5M – €2,9M 27

Conclusion 27

SME Monitoring Center & Regional Capacity Building 27

Goal 27

Importance for Albania 27

Importance for the Region 27

Benefits for EU & Partners 27

Challenges & Risks 27

Cost Breakdown: €1.2M – €1.6M 27
Conclusion 27
Platform for Clearly Defining and Separating Donor Activities in Albania and the Region 28
(Supported by UK Government via BAE Systems) 28
Goal 28
Importance for Albania 28
Importance for the Region 28
Benefits for EU & Partners 28
Challenges & Risks 28
Conclusion 28
Building a Resilient Regional Cyber Talent Pipeline 29
Advancing the Western Balkans Cyber Camp Alumni Network 29
Goal 29
Importance for Albania 29
Importance for the Region 29
Benefits for EU & Partners 29
Challenges & Risks 29
Cost Breakdown Logic 29
Conclusion 29
Policy 4 – INNOVATION AND SCIENTIFIC RESEARCH 30
Establishing the Center of Excellence 30
Quantum Resistance & Digital Resilience 30
+ Regional Hybrid Threat Hub 30
+ Regional Cyber Security Hub** 30
Goal 30
Importance for Albania 30
Importance for the Region 30
Benefits for EU & International Partners 30
Challenges & Risks 30
Cost Breakdown Logic 31
Conclusion 31
StartUP and Innovation Regional Hub 31

Goal 31
Importance for Albania 31
Importance for the Region 31
Benefits for EU & Partners 31
Challenges & Risks 31
Cost Breakdown Logic 32
Conclusion 32
Establishing the Talent Club in Albania 32
Goal 32
Importance for Albania 32
Importance for the Region 32
Benefits for EU and International Partners 32
Challenges & Risks 32
Estimated Cost: €400,000 – €450,000 (2–3 years) 33
Cost Breakdown Logic 33
Conclusion 33
CLUSTER 5 – COUNTERING HYBRID THREATS 34
Cyber Intelligence Group (Hybrid Threats, Geopolitics, Disinformation & Media Monitoring) 34
Goal 34
Importance for Albania 34
Importance for the Region 34
Benefits for EU & Partners 34
Challenges & Risks 34
Cost Breakdown: €1.8M – €2.1M 34
Conclusion 34
Final Conclusion 35

EXECUTIVE SUMMARY

Albania, through the National Cyber Security Authority (AKSK), is undertaking a comprehensive, future-oriented approach to strengthen national and regional cyber resilience. In a rapidly evolving digital landscape—marked by increasingly sophisticated cyberattacks, hybrid threats, and quantum-era challenges—our vision is centered on **five strategic pillars**:

1. Protection of Digital Infrastructure
2. Online Protection of Citizens and Cyber Culture
3. Strengthening International Cooperation
4. Promotion of Innovation and Scientific Research
5. Protection Against Hybrid Threats

These five pillars collectively form a **holistic regional program**, designed not only to elevate Albania's cyber capabilities, but also to contribute meaningfully to the stability, competitiveness, and digital transformation of the entire Western Balkans. All initiatives are aligned with **EU standards**, including **NIS2**, the **AI Act**, **eIDAS2**, the **EU Cyber Skills Academy**, **Digital Decade**, the **5G Security Toolbox**, and the **Strategy** for child online protection.

POLICY 1 – Protection of Digital Infrastructure

This pillar focuses on safeguarding critical and important information infrastructures, ensuring the availability, integrity, and confidentiality of data. It includes legal harmonization, continuous monitoring, risk management, incident response, and certification schemes aligned with EU standards. The goal is to build a resilient ecosystem capable of preventing and mitigating cyber threats effectively.

POLICY 2 – Online Protection of Citizens and Cyber Culture

It aims to create a secure and inclusive digital environment by raising awareness, promoting ethical online behavior, and protecting vulnerable groups such as children and underrepresented communities. Activities include national awareness plans, legal frameworks for equal access, gender equality initiatives, and mechanisms to safeguard SMEs and individuals from cybercrime and online abuse.

POLICY 3 – Strengthening International Cooperation

Recognizing cybersecurity as a global challenge, this pillar promotes harmonization of laws with international standards, regional and global partnerships, and cyber diplomacy. Albania commits to active participation in NATO and EU initiatives, sharing threat intelligence, and coordinating responses to cross-border cyber incidents for collective resilience.

POLICY 4 – Promotion of Innovation and Scientific Research

This pillar drives technological advancement through research, innovation, and collaboration between academia, private sector, and public institutions. Key actions include establishing a National Center of Excellence for Cybersecurity, supporting startups, and creating funding programs for innovative solutions like AI, blockchain, and advanced cryptography to strengthen cyber defenses.

POLICY 5 – Protection Against Hybrid Threats

It addresses complex threats combining cyberattacks with disinformation, economic pressure, and other tactics. The strategy calls for integrated legal frameworks, inter-institutional and international coordination, and advanced technological tools to predict, prevent, and respond to hybrid attacks, ensuring national security and stability.

A Regional Vision With Global Impact

Together, the five policy pilars form a coordinated, scalable, and forward-looking program that:

- Strengthens national and regional cyber resilience
- Enhances interoperability with EU and NATO cybersecurity frameworks
- Creates sustainable human capital and digital innovation ecosystems
- Supports the secure deployment of emerging technologies (5G, quantum-resistant systems, digital identity)
- Promotes social inclusion, safety, and democratic resilience

Albania stands ready to work closely with ambassadors, international organizations, and partner governments to realize this ambitious regional agenda. The projects presented offer **high-impact, scalable opportunities for donor engagement**, with the potential to transform the Western Balkans into a model of cybersecurity, digital governance, and inclusive digital development.

POLICY 1 – PROTECTION OF DIGITAL INFRASTRUCTURE

Establishing the Extended National SOC (NSOC)

With Open Source Platforms & Integration with Energy + Transport + Telecom

Goal

To expand the national SOC into a multi-sector detection and response ecosystem using scalable open-source technologies, integrating Energy, Transport, and Telecommunications into a unified monitoring fabric.

Importance for Albania

- Enhances real-time situational awareness across national critical sectors.
- Reduces cost by using open-source tools while improving capability.
- Strengthens national crisis management and response mechanisms.

Importance for the Region

- Offers a replicable model for Western Balkan countries.
- Facilitates cross-border response for infrastructure interdependencies.

Benefits for EU & Partners

- Supports protection of EU-linked energy and digital corridors (TAP, transport routes, fibre networks).
- Aligns with NIS2 obligations.

Challenges & Risks

- Complexity in sector integration.
- Need for stable human resources.

Cost Breakdown: €4.0M – €4.8M

- SOC Platform Engineering & Open-Source Adaptation: €800K – €1.0M
- Sensors & Visibility Layer for Energy/Transport/Telecom: €1.2M – €1.3M
- 24/7 SOC Operational Team (3 years): €1.2M – €1.3M
- Threat Intelligence Feeds & Automation Rules: €400K – €500K
- Hardware, Storage & Secure Connectivity: €600K – €700K

Conclusion

A foundational capability for Albania’s and the region’s cyber early-warning architecture.

Sectorial Healthcare SOC

Goal

Dedicated SOC for hospitals and national healthcare systems to detect attacks on medical networks, digital records, and medical devices.

Importance for Albania

- Healthcare disruptions directly endanger human life.
- Strengthens national health resilience and compliance with NIS2.

Importance for the Region

- Facilitates regional healthcare security cooperation and standards.

Benefits for EU & Partners

- Contributes to EU’s Health Security & Cyber Resilience initiatives.
- Protects cross-border patient referral systems.

Challenges & Risks

- Fragmented legacy systems.
- Limited cybersecurity personnel in hospitals.

Cost Breakdown: €2.3M – €2.8M

- Healthcare SOC Platform: €500K – €600K
- Medical Device & Hospital Network Sensors: €600K – €700K
- Integration With e-Health/HIS Systems: €300K – €400K
- Operations & Monitoring Team (3 years): €600K – €700K
- Training for Healthcare IT Staff: €200K – €300K

Conclusion

A critical investment preserving both public health and national security.

Implementation of a SOC Center for Each Public and Private University in Albania

(Supported by the U.S. State Department via CRDF Global)

Goal

To deploy a Security Operations Center (SOC) in every university—public and private—to create a national network of academic cybersecurity operations. This initiative boosts institutional protection while serving as a hands-on training environment for students.

Importance for Albania

- Modernizes the cybersecurity posture of educational institutions.
- Provides real-world cyber monitoring experience for students.
- Strengthens university networks, which often lack protections and are targets for ransomware.

Importance for the Region

- Builds a new ecosystem of university-based SOCs that can interconnect regionally.
- Promotes cyber education and early workforce development across the Western Balkans.

Benefits for EU & Partners

- Supports the EU Cyber Skills Academy and Digital Education initiatives.
- Prepares future cybersecurity professionals for European labor markets.
- Increases resilience of academic infrastructure, research data, and innovation ecosystems.

Challenges & Risks

- Requires ongoing technical support for universities.
- Varied IT maturity between universities may slow rollout.

Conclusion

A transformative initiative that strengthens academic cybersecurity while creating a national pipeline of skilled cybersecurity professionals.

Monitoring Operational Center for 12 Municipalities

Goal

Centralized cyber monitoring for Albania’s municipalities to protect essential local services like water, waste, local registries, and administrative services.

Importance for Albania

- Municipalities are highly vulnerable targets due to limited resources.
- Ensures continuity of citizen-facing services.

Importance for the Region

- A scalable model for protecting local governments.

Benefits for EU & Partners

- Supports EU Smart Cities secure infrastructure principles.

Challenges & Risks

- Uneven digital maturity across municipalities.

Cost Breakdown: €1.8M – €2.1M

- Monitoring Platform: €500K – €550K
- Sensors for 12 Municipalities: €600K – €650K
- Secure Network & Infrastructure: €300K – €350K
- Operational Team (3 years): €300K – €400K
- Municipal IT Training: €100K – €150K

Conclusion

A practical, high-impact initiative strengthening local governance resilience.

Coordinated Cybersecurity Engagement Platform

(Promised by BAE Systems – UK Government)

Goal

To establish a centralized national platform that coordinates all cybersecurity capacity-building efforts, donor initiatives, technical assistance projects, and institutional engagements across Albania and the Western Balkans. This platform will ensure transparency, efficiency, and alignment of donor-supported activities with Albania's national cybersecurity strategy.

Importance for Albania

- Eliminates duplication among donor projects.
- Ensures unified national priority-setting with real-time visibility.
- Allows AKSK to coordinate cyber investments, training, and engagements in a structured manner.

Importance for the Region

- Provides a model for regional coordination and shared project visibility.
- Enables cross-border collaboration for multi-country cyber initiatives.

Benefits for EU & Partners

- Ensures alignment of donor contributions with EU acquis and Western Balkans 2025 agenda.

- Improves monitoring and evaluation of donor-funded programs.
- Enhances transparency, reporting, and multi-partner coordination.

Challenges & Risks

- Requires strict governance and data-sharing rules.
- Needs strong buy-in from all stakeholders.

Conclusion

A transformative tool ensuring that all cybersecurity engagements in Albania are strategic, coordinated, and fully aligned with national and regional objectives.

Regional Governance, Risk & Compliance (GRC) Platform

(Supported by UK Government via BAE Systems)

Goal

To assess maturity and identify gaps in People, Process, and Technology across the Western Balkans, aligned with NIS2 and EU cyber governance standards.

Importance for Albania

- Enables evidence-based prioritization of cybersecurity investments.

Importance for the Region

- Supports a unified regional maturity model.

Benefits for EU & Partners

- Helps track alignment with EU acquis and accession benchmarks.

Challenges & Risks

- Requires strong governance and transparency.

Conclusion

A strategic framework enabling long-term, EU-aligned cyber governance reforms.

Regional Attack Surface Management (ASM) Platform

(Supported by UK Government via BAE Systems)

Goal

A regional shared platform to continuously identify vulnerabilities in public institutions and critical infrastructures across the Western Balkans.

Importance for Albania

- Provides proactive vulnerability identification.
- Prevents exploitation by ransomware groups and hostile actors.

Importance for the Region

- Eliminates the “weakest link” effect by harmonizing security posture.

Benefits for EU & Partners

- Supports EU-wide vulnerability management frameworks.
- Strengthens the cybersecurity perimeter of the EU Neighborhood.

Challenges & Risks

- Sensitive data-sharing agreements needed.

Conclusion

A proactive regional shield capable of detecting exposed systems before adversaries exploit them.

Training 2 Experts in Security Governance for 400 Public and Private Institutions

(Supported by UK Government via BAE Systems)

Goal

To train and certify two national-level experts who will guide and coordinate cybersecurity governance programs across more than 400 public and private institutions, ensuring full compliance with national cybersecurity law, NIS2 standards, and EU governance frameworks.

Importance for Albania

- Creates high-level domestic expertise to lead large-scale governance reform.
- Enables AKSK to operationalize cybersecurity governance across all sectors.

- Strengthens compliance, accountability, and institutional cybersecurity culture.

Importance for the Region

- Serves as a scalable training model for regional governance alignment.
- Helps standardize cybersecurity governance maturity across Western Balkans.

Benefits for EU & Partners

- Directly supports NIS2 implementation.
- Establishes governance processes consistent with EU cyber regulations.
- Enhances readiness for EU accession negotiations on digital governance.

Challenges & Risks

- Requires sustained deployment of trained experts.
- Training must be adapted to multiple sectoral needs.

Conclusion

A high-impact governance initiative that elevates Albania’s cybersecurity maturity across all institutions and aligns national capabilities with EU standards.

Counter-Ransomware Task Force (Albania + Region)

Goal

Operational task force to prevent, detect, and coordinate response to ransomware campaigns targeting Western Balkans institutions and businesses.

Importance for Albania

- Ransomware remains the top threat to government and CNIs.

Importance for the Region

- Attacks often hit multiple countries simultaneously.

Benefits for EU & Partners

- Supports the **Global Counter Ransomware Initiative (CRI).**
- Strengthens information-sharing with Europol & Interpol.

Challenges & Risks

- Requires secure environments for sharing sensitive intelligence.

Cost Breakdown: €2M – €2.3M

- Malware Analysis & Forensic Labs: €600K – €650K
- Threat Intelligence Subscriptions: €300K – €400K

- Operational Investigation Team (3 years): €600K – €650K
- Secure Communication Channels: €200K – €250K
- Training & Joint Ransomware Exercises: €300K – €350K

Conclusion

A high-impact operational capability confronting the most persistent global threat.

Regional e-Learning Platform (CNI Experts + Awareness for Employees & Citizens)

Goal

A scalable learning ecosystem offering advanced cyber training to CNI experts and awareness modules for public-sector employees and citizens.

Importance for Albania

- Helps address skill gaps at a national scale.
- Provides continuous training at low ongoing cost.

Importance for the Region

- Ensures harmonized capacity-building across the Western Balkans.

Benefits for EU & Partners

- Directly supports the **EU Cyber Skills Academy** objectives.

Challenges & Risks

- Requires continuous content updates.

Cost Breakdown: €1.2M – €1.5M

- Platform Development & Hosting: €400K – €450K
- Professional Cyber Courses: €300K – €350K
- Awareness Modules for Employees & Citizens: €200K – €250K
- Training of Trainers (ToT): €150K – €200K
- Regional Platform Management (3 years): €150K – €250K

Conclusion

A long-term investment in human capital and cyber hygiene.

Regional Incident Attempt Categorization & Prioritization Platform

Goal

A standardized incident classification system for all Western Balkan countries, enabling faster and coordinated cyber response.

Importance for Albania

- Enables unified communication and response between institutions.

Importance for the Region

- Essential for regional interoperability and joint threat response.

Benefits for EU & Partners

- Aligns region with ENISA's incident taxonomy.

Challenges & Risks

- Requires political and operational harmonization.

Cost Breakdown: €750K – €950K

- Platform Development: €300K – €350K
- Regional Integration Framework: €150K – €200K
- Training for National CSIRTs: €150K – €200K
- Governance & Harmonization Work: €150K – €200K

Conclusion

A core enabler of region-wide coordination in cybersecurity incident management.

Establishing the 5G Stand-Alone Technology Testbed

For Telecom Providers in the Region

Goal

To create a secure, controlled 5G Stand-Alone (SA) testbed where telecom operators can test security, interoperability, slicing, and zero-trust architecture aligned with European standards.

Importance for Albania

- Prepares Albania for secure 5G deployment and future 6G readiness.
- Reduces risk of critical failures in communication networks.

Importance for the Region

- Ensures harmonized 5G security implementation across Western Balkans.
- Facilitates cross-border roaming, emergency communications, and crisis management.

Benefits for EU & Partners

- Aligns with **EU Toolbox for 5G Security.**
- Supports secure integration of Western Balkan telecom providers with EU networks.

Challenges & Risks

- Requires sophisticated equipment and telecom cooperation.
- High technical expertise needed.

Cost Breakdown: €6M – €7,3M

- 5G Stand-Alone Core Infrastructure: €2M – €2.3M
- Radio Access Network (RAN) Test Components: €1.5M – €1.8M
- Security & Zero-Trust Validation Tools: €800K – €1M
- Integration With Telecom Operators: €700K – €1M
- Operational Team & Testing Programs (3 years): €1M – €1.2M

Conclusion

A forward-looking, strategic infrastructure that prepares the entire region for secure 5G deployment.

Establishing the e-ID & Trusted Services Sandbox

(Aligned with EU Acquis & eIDAS2)

Goal

A national–regional sandbox environment for testing digital identity, digital signatures, electronic seals, trust services, and digital wallets in alignment with **eIDAS2** and EU accession requirements.

Importance for Albania

- Accelerates Albania’s integration into the EU digital identity ecosystem.
- Ensures safe deployment of high-assurance identity systems.

Importance for the Region

- Harmonizes digital identity frameworks across Western Balkans.
- Facilitates cross-border digital services for citizens and businesses.

Benefits for EU & Partners

- Directly supports EU Digital Identity Framework.
- Strengthens digital trust and interoperability with EU Member States.

Challenges & Risks

- Requires close regulatory coordination.
- Needs vendor-neutral testing and certification processes.

Cost Breakdown: €3.5M – €4.0M

- Digital ID/Testbed Infrastructure: €1M – €1M
- e-Signature, e-Seal & Trust Service Validation Tools: €800K – €1M
- Digital Wallet Simulation Environment: €600K – €700K
- Regulatory & Compliance Testing Framework: €500K – €600K
- Operational Team & EU Alignment Activities (3 years): €600K – €700K

Conclusion

A high-priority EU-acquis-aligned investment enabling Western Balkan digital integration and secure digital services.

POLICY 2 – NATIONAL PROGRAM FOR PROTECTION OF CITIZENS ONLINE

Regional Cyber Security Marathon (CTF)

For University Students, Women in Cyber, and Underrepresented Groups

Goal

To establish a structured, six-month regional CTF marathon that builds hands-on practical skills in cybersecurity and promotes diversity in the field.

Importance for Albania

- Motivates students to enter cybersecurity professions.
- Helps identify top performers who can be integrated into national cyber structures.
- Strengthens the culture of ethical hacking and responsible vulnerability discovery.

Importance for the Region

- Fosters regional collaboration, competition, and networking.
- Addresses gender imbalance and supports inclusion of underrepresented groups.
- Creates a shared talent repository across Western Balkans.

Benefits for EU & Partners

- Promotes alignment with EU cyber awareness and capacity-building efforts.
- Provides an entry point for EU experts to engage with regional talent.
- Strengthens the resilience of the region through practical, skills-based training.

Challenges & Risks

- Ensuring equal representation across countries.
- Maintaining standardized difficulty levels and credible evaluation.
- Sustaining annual funding and sponsorships.

Cost Breakdown Logic

- CTF platform licensing or development: €380–400K
- Training bootcamps & expert support: €60–80K
- Prizes, student mobility, and final conference: €70–100K
- Logistics, communications, and regional coordination: €60–80K

Total: ~€570K–€660K

Conclusion

A cost-effective initiative that builds real cyber capacity, promotes inclusivity, and enhances EU–regional cooperation through continuous talent development.

Encourage the Woman in Cyber (Activities and Training)

Goal

To empower women and girls to participate actively in the cybersecurity field by providing targeted capacity-building programs, mentorship networks, awareness activities, technical training, competitions, and career-oriented opportunities.

Importance for Albania

- Women represent a significantly underrepresented segment of the cybersecurity workforce.
- Expanding female participation strengthens national cyber capabilities.
- Promotes gender equality in a strategic and high-growth sector.

Importance for the Region

- Encourages cross-border collaboration and female leadership in cybersecurity.
- Creates a Western Balkan community of skilled female cyber professionals.
- Aligns with regional objectives for inclusive digital transformation.

Benefits for EU & Partners

- Supports EU Gender Equality Strategy and Digital Decade objectives.
- Expands the pool of future experts who can participate in EU-funded cyber programs.
- Strengthens diversity within the European cybersecurity workforce.

Challenges & Risks

- Low starting participation rate of women in technical fields.
- Need for continuous engagement and mentorship to retain interest.
- Societal perceptions that discourage girls from choosing STEM careers.

Cost Breakdown: €1.2M – €1.8M

- Cybersecurity Training Programs for Women: €400K – €600K
- Regional Workshops, Hackathons & CTF for Women: €200K – €300K
- Mentorship Network & Industry Partnerships: €150K – €250K
- Awareness Campaigns in High Schools & Universities: €150K – €250K
- Scholarships, Travel Grants & Certification Support: €300K – €400K

Conclusion

A strategic investment that builds a diverse, inclusive, and future-ready cyber workforce across Albania and the Western Balkans.

Establishing a Digital Safe Environment for Children and Teenagers

(With AKEP, AMA, ISPs, Ministry of Education, NGOs)

Goal

To create a national and regional framework ensuring children's online safety through awareness campaigns, parental guidance tools, filtering solutions, and education programs integrated into schools.

Importance for Albania

- Protects children from cyberbullying, harmful content, grooming, and digital addiction.
- Builds digital literacy and resilience from early ages.
- Creates a trusted online environment that families and educators can rely on.

Importance for the Region

- Addresses a regional challenge: children increasingly exposed to harmful online behavior.
- Allows for standardization of safe-internet policies.
- Strengthens cross-border collaboration on child protection cases.

Benefits for EU & Partners

- Aligns with EU Child Protection Strategy and Digital Services Act standards.
- Enhances collaboration with Europol, INHOPE, and EU child-safety networks.
- Creates a foundation for regional safe-internet frameworks.

Challenges & Risks

- Coordination across multiple institutions.
- Balancing safety measures with children's digital rights.
- Need for continuous content monitoring and education updates.

Cost Breakdown Logic

- National digital safety curriculum for schools: €400–500K
- ISP filtering tools & reporting platforms: €1M–1.2M
- Awareness campaigns nationwide: €300–400K
- Child helpline & online reporting center expansion: €200–300K
- Teacher training programs nationwide: €400–500K

Total: ~€2.3M–2,9M

Conclusion

A socially critical initiative that protects the most vulnerable users, strengthens trust in the digital ecosystem, and supports EU-aligned safe-internet policies.

Encourage the Underrepresented Groups to Participate Actively in Our Digital Society and Protect Them From Cyberbullying, Blackmail, Inappropriate Content, etc.

(In Coordination With Ministry of Interior, State Police, AKEP, AMA, AKSHI, Ministry of Education, Ministry of Economy, Ministry of Healthcare)

Goal

To empower underrepresented groups—children, teenagers, minorities, disability persons, neural diversity persons, disadvantaged communities, and individuals with limited digital access—to participate safely and confidently in the digital environment through awareness activities, targeted training programs, safeguarding tools, and a dedicated support platform.

Importance for Albania

- Reduces digital inequality and ensures equal access to digital transformation.
- Protects youth and vulnerable individuals from online harms such as cyberbullying and blackmail.
- Strengthens public trust in national digital services and platforms.

Importance for the Region

- Promotes regional social inclusion and digital resilience.
- Harmonizes protection standards across Western Balkans societies.
- Helps reduce societal vulnerabilities that can be exploited by hybrid threat actors.

Benefits for EU & Partners

- Aligns with EU values on human rights, inclusion, and digital protection of minors.
- Supports EU's Better Internet for Kids (BIK+) strategy.
- Creates a safer digital environment aligned with the Digital Services Act (DSA).

Challenges & Risks

- Requires strong inter-institutional coordination.

- Need for continuous content moderation and platform updates.
- Diverse socio-economic conditions require adaptable training formats.

Cost Breakdown: €2.5M – €2,9M

- National Platform for Reporting and Support: €600K – €650K
- Awareness & Education Programs for Schools & Families: €500K – €600K
- Training for Teachers, Social Workers & Law Enforcement: €400K – €550K
- Content Moderation & Digital Safety Toolkits: €300K – €400K
- Regional Inclusion Campaigns & Community Outreach: €300K – €350K
- Coordination Unit Across Institutions (3 years): €400K – €450K

Conclusion

A socially meaningful initiative that promotes digital inclusion, protects vulnerable groups, and strengthens the safe and responsible use of the internet across the region.

SME Monitoring Center & Regional Capacity Building

Goal

A security monitoring and education platform for SMEs to ensure they do not become an entry point for supply-chain attacks.

Importance for Albania

- SMEs are critical in supply chains but often neglected in security investments.

Importance for the Region

- Reduces systemic risk across interconnected Balkan economies.

Benefits for EU & Partners

- Supports NIS2 supply-chain security rules.

Challenges & Risks

- Low cyber maturity in SMEs; requires ongoing coaching.

Cost Breakdown: €1.2M – €1.6M

- SME Monitoring Tools & Dashboards: €400K – €500K
- Awareness Campaigns & Trainings: €200K – €300K
- Rapid Assistance Team (3 years): €300K – €400K
- Regional Reporting Dashboard: €150K – €200K
- SME Vulnerability Scanning Tools: €150K – €200K

Conclusion

A preventive measure reinforcing the security of the entire regional economic ecosystem.

Platform for Clearly Defining and Separating Donor Activities in Albania and the Region

(Supported by UK Government via BAE Systems)

Goal

To develop a national donor coordination and transparency platform that categorizes, separates, and manages all cyber-related donor initiatives in Albania, ensuring visibility, efficiency, and alignment with national priorities.

Importance for Albania

- Prevents overlap in donor-funded activities.
- Ensures better distribution of resources to priority sectors.
- Enables AKSK to track deliverables, milestones, and donor impact.

Importance for the Region

- Can be expanded as a Western Balkan donor coordination model.
- Encourages more harmonized regional investment.

Benefits for EU & Partners

- Improves accountability and reporting for donor governments.
- Facilitates strategic planning and transparent use of funds.
- Supports results-oriented cooperation with international partners.

Challenges & Risks

- Requires continuous data updates and stakeholder engagement.
- Sensitive information must be appropriately classified and secured.

Conclusion

A vital transparency mechanism that optimizes cyber-related donor investments and reinforces national strategic coherence.

Building a Resilient Regional Cyber Talent Pipeline

Advancing the Western Balkans Cyber Camp Alumni Network

Goal

To institutionalize and expand the talent network created through regional cyber camps, transforming it into a continuous platform for learning, collaboration, and workforce placement.

Importance for Albania

- Ensures that trained youth continue to engage, grow professionally, and remain connected to national institutions.
- Creates a recruitment pipeline for public and private sectors.
- Supports NIS2 alignment by addressing critical shortages in cyber workforce.

Importance for the Region

- Strengthens long-term regional cooperation and interoperability.
- Prevents "talent isolation" by connecting top performers across borders.
- Creates a skilled workforce capable of supporting regional incident response mechanisms.

Benefits for EU & Partners

- Establishes a sustainable pool of cyber professionals aligned with EU standards.
- Supports workforce development under the EU Cyber Skills Academy and Digital Decade goals.
- Enhances stability and resilience in the Western Balkans.

Challenges & Risks

- Need for continuous engagement, not only one-time camps.
- Risk of losing alumni to migration if local ecosystems are weak.
- Requires structured governance and mentorship programs.

Cost Breakdown Logic

- Alumni platform development & maintenance: €120–150K
- Annual regional cyber camp & mobility programs: €150–170K
- Continuous training modules for alumni: €100–150K
- Coordination staff & community management: €120–150K

Total: ~€390K–620K

Conclusion

A strategic initiative to create a long-term, cross-border talent community that strengthens regional resilience and enhances cooperation with EU security and capacity-building mechanisms.

Policy 4 – INNOVATION AND SCIENTIFIC RESEARCH

Establishing the Center of Excellence

Quantum Resistance & Digital Resilience

+ Regional Hybrid Threat Hub

+ Regional Cyber Security Hub**

Goal

To create an integrated and multidisciplinary center that provides:

- Advanced training (high school → university → PhD level)
- Research on quantum-resistant technologies
- Regional hybrid threat analysis
- Cyber range exercises & cyber gym platforms
- Smart sector security (cities, transport, health, energy, agro)

Importance for Albania

- Builds Albania's capacity to defend against next-generation threats including quantum, AI-driven attacks, and hybrid operations.
- Positions Albania as a regional innovation and cyber research leader.
- Ensures long-term sustainability of national SOCs and critical infrastructures through skilled workforce and R&D.

Importance for the Region

- Serves as a **regional reference hub**, reducing fragmentation and duplicative investments.
- Supports cross-border cooperation for hybrid threat mitigation and coordinated response.
- Enhances collective resilience for all Western Balkan states.

Benefits for EU & International Partners

- Strengthens EU Neighborhood stability and contributes to NIS2 implementation.
- Creates a trusted research node for joint EU projects (Horizon Europe, Digital Europe).
- Reduces vulnerability along major European energy, transport, and communication corridors.

Challenges & Risks

- High initial investment and need for specialized equipment.
- Requirement for highly skilled trainers and researchers.
- Coordination complexity across multiple institutions and countries.

Cost Breakdown Logic

- Facility construction/renovation & labs: €5–5,5M
- Quantum-resistant & cyber research labs: €2–2,5M
- Red/Blue Team Cyber Range & Cyber Gym: €2–2,5M
- Smart Cities/Transport/Energy/Healthcare testbeds: €1–1,5M
- Staffing (researchers, trainers, technical ops): €2–3M

Total: ~€12M–15M

Conclusion

A flagship regional project that elevates Albania's strategic positioning, strengthens EU–Balkan cooperation, and creates sustainable regional cyber, hybrid-threat, and quantum-resilience capacities.

StartUP and Innovation Regional Hub

Goal

To establish a regional platform where young innovators, researchers, and entrepreneurs can collaborate, develop prototypes, receive mentorship, and access cybersecurity-specific incubation programs.

Importance for Albania

- Encourages entrepreneurship in emerging technologies.
- Stimulates the digital economy and creates new, high-value jobs.
- Connects academia, private sector, and government in one innovation ecosystem.

Importance for the Region

- Bridges technological gaps among Western Balkan countries.
- Encourages cross-border innovation partnerships.
- Reduces fragmentation and improves competitiveness in the global digital market.

Benefits for EU & Partners

- Strengthens EU's strategic objective of a competitive, secure, and innovative digital market.
- Provides a pipeline of start-ups for EU accelerators and investment instruments.
- Supports regional stability and economic development.

Challenges & Risks

- Need for strong mentorship network and industry involvement.
- Risk of low sustainability without continuous funding and business support.
- Brain drain risk if local innovation is not coupled with investment incentives.

Cost Breakdown Logic

- Incubation space, equipment, and co-working center: €800K
- Accelerator programs & mentorship networks: €400K
- Seed-funding grants for startups: €300–400K
- Staffing & operations: €300–400K

Total: ~€1.8M–2M

Conclusion

A forward-looking initiative that nurtures innovation, fosters cross-border cooperation, and aligns the region with EU digital competitiveness and cybersecurity priorities.

Establishing the Talent Club in Albania

Goal

To create a national ecosystem that identifies, mentors, and accelerates young cyber talents—starting from high schools to early professionals—through structured training, competitions, mentorship, and international exposure.

Importance for Albania

- Albania faces a significant shortage of cyber specialists across public institutions, CNIs, and the private sector.
- A Talent Club creates a long-term pipeline, reducing dependency on foreign expertise.
- It fosters a culture of innovation, digital resilience, and responsible technology use among youth.

Importance for the Region

- It becomes a model incubator for similar initiatives in the Western Balkans.
- Supports harmonization of talent development with EU frameworks and regional competitiveness.

Benefits for EU and International Partners

- Strengthens the region's stability by reducing skills gaps that adversaries exploit.
- Helps align the Western Balkans with EU standards under NIS2, Cyber Resilience Act, and Digital Decade targets.
- Creates a pool of future experts to engage in joint EU-funded research and capacity-building programs.

Challenges & Risks

- Retention of trained experts due to brain-drain risks.
- Need for sustainable funding and continuous program updates.
- Ensuring equal access for rural and underrepresented communities.

Estimated Cost: €400,000 – €450,000 (2–3 years)

Cost Breakdown Logic

- Training programs & national competitions: €120,000
- Mentorship network & expert trainers: €80,000
- Equipment & lab setup: €150,000
- National awareness/engagement campaigns: €50,000
- Coordination team (2–3 staff): €100,000–150,000

Total: ~€400K–450K

Conclusion

A strategic, low-cost, high-impact investment that strengthens Albania’s cyber workforce from the ground up and contributes to regional digital resilience.

CLUSTER 5 – COUNTERING HYBRID THREATS

Cyber Intelligence Group (Hybrid Threats, Geopolitics, Disinformation & Media Monitoring)

Goal

A national-regional intelligence cell analyzing geopolitical developments, hybrid threats, disinformation, and their impact on public institutions and private sector stability.

Importance for Albania

- Hybrid threat campaigns increasingly target society, economy, and governance.

Importance for the Region

- Hybrid operations often cross borders and require coordinated monitoring.

Benefits for EU & Partners

- Supports EU Hybrid Fusion Cell & NATO StratCom cooperation.

Challenges & Risks

- Requires specialized analysts in OSINT, geopolitical risk, and media forensics.

Cost Breakdown: €1.8M – €2.1M

- OSINT & Media Monitoring Tools: €400K – €450K
- Analyst Team (3 years): €900K – €1M
- Geopolitical Risk Data Sources: €200K – €250K
- Analytical Dashboards & Reporting Tools: €200K – €250K
- Regional Collaboration Activities: €100K – €150K

Conclusion

A strategic early-warning tool for safeguarding democratic and economic stability.

Final Conclusion

The implementation of these four clusters represents far more than a national cybersecurity agenda it constitutes a strategic investment in the stability, security, and economic resilience of the entire Western Balkans and, ultimately, Europe as a whole.

By developing regional talent, building advanced cyber defense capabilities, strengthening governance and institutional maturity, and protecting vulnerable communities, these initiatives address the full spectrum of modern digital threats. They create an interconnected ecosystem where governments, critical infrastructures, academic institutions, businesses, and citizens can operate with trust and confidence.

For Europe, the Western Balkans represent both a geographic bridge and a strategic buffer. Enhancing the region’s cyber resilience directly reinforces the European Union’s internal security, protects critical supply chains, and supports broader EU and NATO efforts to counter hybrid threats, disinformation, and geopolitical instability. A more resilient Western Balkans translates into a more resilient Europe.

These projects therefore serve a dual purpose:
they elevate Albania as a regional leader in cybersecurity, and they contribute meaningfully to the collective stability and strategic security of the European continent. Through strong partnerships with international donors, allied governments, and the private sector, Albania is committed to building a safer, more innovative, and more inclusive digital future—one that strengthens peace, fosters development, and safeguards democratic societies across the region and beyond.