Scientific and Practical Cyber Security Journal (SPCSJ) 10(1): 187 – 193 ISSN 2587-4667
Scientific Cyber Security Association (SCSA)

FROM QUANTUM LAB TO NATIONAL SECURITY: TOWARDS A NATIONAL QUANTUM SECURITY STRATEGY FOR GEORGIA

David Getsadze[1]
[1]Business and Technology University (BTU), Ministry of Defence of Georgia, Georgia

ABSTRACT: Several countries are adopting national quantum strategies, yet many states with emerging capabilities still lack a coherent quantum vision aligned with their cybersecurity and digital transformation agendas. This article proposes a step-by-step framework for developing a national quantum security strategy in such a context, using Georgia as an illustrative case. It builds on the existing ecosystem structured around the Scientific Cyber Security Association, the country's first quantum laboratory, and the Erasmus+ SECURE project, which together provide advanced infrastructure for post-quantum cryptography research, quantum random number generation and cybersecurity education. The article maps key institutions such as the Cyber Security Bureau of the Ministry of Defence, the State Security Service and the LEPL Operative-Technical Agency of Georgia as natural stakeholders in a future quantum security roadmap. It then outlines a phased roadmap over a 1–2, 3–5 and 5–10 year horizon, detailing how bottom-up initiatives can be aligned with national security, defence and critical infrastructure priorities in order to address quantum-enabled threats and exploit quantum-related opportunities. The central claim is that a national quantum security strategy for Georgia is both necessary and feasible today, provided that existing assets are leveraged strategically and coordinated across the national security community.

KEYWORDS: *Quantum security, post-quantum cryptography, national security, critical infrastructure protection, quantum-safe roadmap, quantum laboratory*

1. INTRODUCTION

Over the past decade, an increasing number of states have adopted national quantum strategies to coordinate investments in quantum technologies, research infrastructures and talent development. These strategies typically frame quantum computing, communication and sensing as long-term enablers for economic competitiveness, critical infrastructure protection and national security. However, many countries with emerging quantum capabilities still lack a dedicated quantum strategy and instead address quantum-related risks and opportunities only indirectly through broader cybersecurity or digital transformation policies.

Georgia belongs to this latter group. While the country has adopted national strategies on cybersecurity and digital transformation, quantum technologies and post-quantum security are not yet articulated as explicit pillars within its strategic planning. At the same time, a nascent ecosystem has started to form around the Scientific Cyber Security Association (SCSA), Caucasus University of Georgia and international partners, including through the Erasmus+ SECURE project, which focuses on AI, 5G and quantum-enhanced cybersecurity education and research. This creates a situation where concrete quantum-related capabilities are emerging 'from the bottom up' in the absence of a coherent 'top-down' national quantum vision.

One of the most tangible manifestations of this emerging ecosystem is the establishment of Georgia's first quantum laboratory, hosted by Caucasus University. The laboratory is equipped with devices for quantum random number generation, post-quantum cryptography research and the analysis of hardware-level and side-channel vulnerabilities, supported by high-performance computing resources. In parallel, the Erasmus+ SECURE project is developing interconnected research and educational hubs in Georgia and Ukraine, aimed at strengthening cybersecurity competence around next-generation networks

and quantum-resilient solutions. Together, these initiatives form a strategic nucleus that could underpin a future national quantum security vision.

This article uses Georgia as an illustrative case to propose a step-by-step framework for developing such a national quantum security vision in a context where bottom-up capabilities precede high-level strategic direction. It argues that leveraging existing assets—such as the quantum laboratory and the Erasmus SECURE network—can help bridge the gap between current cybersecurity and digital transformation strategies and an explicit, long-term quantum security agenda. Building on international experience while remaining grounded in Georgia's specific institutional and technological landscape, the article outlines a phased roadmap over a 5–10 year horizon, with particular attention to implications for national security and defence.

This leads to the central question guiding this article: how can an emerging quantum and post-quantum security ecosystem be translated into a coherent national quantum security vision in the absence of a formal quantum strategy? The contribution of this paper is twofold: first, it maps the current capabilities and institutional landscape in Georgia; second, it proposes a phased, bottom-up roadmap that can inform future policy discussions and strategic planning.

2. METHODOLOGY

This article adopts a conceptual and policy-oriented approach rather than an empirical or technical one. It combines a mapping of Georgia's emerging quantum and post-quantum security ecosystem—based on public information about institutions such as SCSA, the Cyber Security Bureau, the State Security Service and LEPL Operative-Technical Agency —with a review of international quantum and post-quantum strategies and roadmaps published by Allied governments, international organisations and expert bodies. The resulting framework is proposed as a strategic vision and concept note intended to inform policy discussions and guide future, more detailed technical and operational work, rather than as a definitive implementation blueprint.

3. EXISTING CAPABILITIES AND ECOSYSTEM

The transition toward a quantum-safe posture requires not only strategic foresight but also tangible technological infrastructure. While Georgia lacks a centralized quantum policy, a robust operational ecosystem has begun to take shape organically. This section provides a comprehensive mapping of the country's existing quantum and post-quantum assets. It explores how non-governmental and academic initiatives have successfully established the foundational pillars of cyber resilience—ranging from specialized research facilities to international educational networks. Ultimately, this review demonstrates that these independent, bottom-up developments possess the maturity and alignment necessary to support broader national security and defence objectives.

3.1. THE SCIENTIFIC CYBER SECURITY ASSOCIATION

The Scientific Cyber Security Association (SCSA) plays an important role in Georgia's emerging quantum and post-quantum security ecosystem. Established as a specialised organisation dedicated to advancing cybersecurity research, education and professional practice, SCSA acts as a bridge between academia, industry and governmental stakeholders. Through its projects, conferences and publications, it has gradually positioned itself as a national hub for advanced topics such as cryptography, cyber defence and secure digital transformation.

3.2. GEORGIA'S FIRST QUANTUM LABORATORY

SCSA, in cooperation with Caucasus University, has established the first quantum laboratory in Georgia, hosted at Caucasus University's premises. The laboratory is equipped with ultra-modern devices for quantum random number generation, post-quantum cryptography research and the analysis of hardware and side-channel vulnerabilities, supported by powerful servers for large-scale cryptographic and security experiments. This infrastructure is explicitly intended to support research and education in quantum

technologies and cryptographic security, and to provide a platform for future collaboration with national and international partners.

3.3. THE ERASMUS+ SECURE PROJECT AND REGIONAL HUB ROLE

The quantum laboratory forms part of a broader effort under the Erasmus+ SECURE project, which aims to build research and educational hubs in Georgia and Ukraine focusing on AI, 5G and quantum-enhanced cybersecurity. SECURE connects universities and partners from several countries in order to develop joint curricula, laboratories and a shared digital platform for experimentation and training, thereby strengthening regional capabilities in cybersecurity for next-generation networks. Within this framework, the Georgian hub centered on SCSA and Caucasus University is designed not only to serve local needs but also to contribute to a wider regional ecosystem for secure digital and quantum-resilient technologies.

3.4. LINKAGES TO NATIONAL SECURITY AND DEFENCE STAKEHOLDERS

Although Georgia does not yet have a formal national quantum strategy, the existing cybersecurity and digital transformation strategies, along with institutions such as the Cyber Security Bureau under the Ministry of Defence, provide natural interlocutors for the emerging quantum security ecosystem. The Bureau's mandate to develop defence cyber policies, secure military information systems and align with international standards creates clear avenues for cooperation with SCSA and the quantum laboratory, for example through joint testing, pilot projects and training related to post-quantum and quantum-resilient solutions. As such, the current ecosystem already contains key elements that could be integrated into a future national quantum security vision, even if this integration has not yet been formalised at the policy level.

4. TOWARDS A NATIONAL QUANTUM SECURITY VISION

A national quantum security vision for Georgia is to progressively build a secure, resilient and sovereign digital and defence ecosystem that remains trustworthy in the era of quantum technologies. This vision recognises that advances in quantum computing, communication and sensing will reshape both the offensive and defensive dimensions of cybersecurity and national security, including the potential to undermine today's cryptographic foundations and to enable new forms of secure communications and sensing. Georgia aims to anticipate these developments by leveraging its emerging quantum and post-quantum capabilities—such as the quantum laboratory, the Erasmus+ SECURE hub and existing cybersecurity institutions—to prepare for the transition to quantum-resilient cryptography, strengthen the protection of critical and defence infrastructures, and contribute to regional and international efforts for quantum-safe ecosystems.

4.1. GUIDING PRINCIPLES FOR A NATIONAL QUANTUM SECURITY VISION

First, the vision should be security-driven and mission-oriented: quantum and post-quantum technologies are not pursued as an end in themselves, but as means to ensure the confidentiality, integrity and availability of critical information systems and defence capabilities in a future quantum environment. Second, it should prioritise technological and cryptographic sovereignty, by developing domestic expertise and trusted partnerships that reduce excessive dependence on foreign solutions for quantum-resilient security, particularly in sensitive government and defence domains. Third, the vision must be interoperable and standards-aligned, actively engaging with emerging international standards and best practices for post-quantum cryptography and quantum-safe infrastructures to ensure compatibility with allies and international organisations. Finally, it should follow an incremental 'learn-by-doing' approach, starting from existing assets such as the quantum laboratory, the Erasmus+ SECURE hub and the Cyber Security Bureau of the Ministry of Defence, and gradually scaling pilot projects, training and capability development into a coherent, long-term quantum security roadmap.

4.2. SHORT-TERM PHASE (1-2 YEARS)

In the short term, the priority is to consolidate existing capabilities and establish the institutional foundations for a future quantum security roadmap. This phase should begin with a structured assessment

of quantum-related assets and vulnerabilities across government and defence networks, building on international recommendations that emphasise early discovery exercises, cryptographic inventories and stakeholder mapping as first steps towards post-quantum migration. A dedicated coordination mechanism or working group could be created, bringing together representatives from the Cyber Security Bureau of the Ministry of Defence, other relevant government agencies, SCSA, Caucasus University and Erasmus+ SECURE partners, to align expectations, share information and identify priority use cases for quantum-resilient solutions.

Concretely, this phase should also focus on awareness and capacity building: raising understanding of the quantum threat (including 'harvest now, decrypt later' risks) among policymakers and technical staff, and integrating introductory quantum and post-quantum security modules into existing cybersecurity training programmes. Pilot projects can be launched using the quantum laboratory as a testbed, for example to experiment with post-quantum algorithms, quantum random number generators and hardware vulnerability assessments in controlled environments relevant to defence and critical infrastructure. The outcome of this 1–2 year phase should be a shared situational picture, a set of initial technical and organisational pilots, and an agreed roadmap document that articulates roles, responsibilities and next-step priorities for Georgia's emerging national quantum security agenda.

In practical terms, this could include, for example, experimenting with post-quantum VPN solutions for selected inter-agency communication links, testing quantum-grade random number generators for key generation in defence and government systems, or using the quantum lab to evaluate hardware security of cryptographic modules deployed in critical infrastructure environments.

4.3. MEDIUM-TERM PHASE (3-5 YEARS)

In the medium term, the focus should shift from isolated pilots to the systematic integration of quantum-resilient measures into selected 'crown-jewel' systems in government and defence. Building on international roadmaps, this phase involves moving from planning and experimentation towards initial deployment of post-quantum cryptography and quantum-safe architectures in priority domains, while maintaining a clear risk-based approach and crypto-agile design principles. For Georgia, this could include integrating post-quantum algorithms and quantum-grade random number generation into critical communication channels, security gateways and key management systems used by central government and the defence sector, with the quantum laboratory serving as a reference environment for performance and interoperability testing.

Concurrently, the 3–5 year phase should strengthen governance, standards alignment and workforce development. This implies establishing formal governance structures for quantum and post-quantum security within existing cybersecurity and digital transformation frameworks, and ensuring that the Cyber Security Bureau and other key agencies have designated 'quantum champions' responsible for overseeing implementation. At this stage, Georgia should also deepen its engagement with international standardisation and policy processes on quantum-safe security, and expand specialised training programmes so that a core group of experts in government, academia and industry can sustain and extend the migration efforts beyond the pilot phase.

Concrete medium-term targets might include rolling out quantum-resilient remote-access solutions for defence and national security users, integrating post-quantum algorithms into secure email and document-exchange systems for high-level decision-makers, and requiring critical infrastructure operators under LEPL Operative-Technical Agency's remit to adopt crypto-agile architectures that can accommodate post-quantum migration.

4.4. LONG-TERM PHASE (5-10 YEARS)

In the long term, Georgia should aim to move from targeted quantum-resilient upgrades towards a coherent quantum-safe and quantum-enabled security posture. International timelines suggest that many national security systems are expected to complete migration to quantum-safe cryptography around the early-to-mid-2030s, with critical sectors targeted even earlier. For Georgia, the 5–10 year horizon should

therefore be used to extend post-quantum and quantum-safe architectures across a broader range of government, defence and critical infrastructure systems, while exploring selected applications of quantum communication and sensing where they offer clear operational advantages for national security.

By this stage, the goal is not only to protect against quantum-enabled threats, but also to leverage quantum technologies as enablers of defence and security capabilities, in line with emerging Allied approaches that emphasise a 'quantum-ready' posture. This includes developing or participating in secure quantum communication testbeds, advancing research collaborations on quantum-enhanced sensing and algorithms relevant to defence scenarios, and ensuring that Georgia's quantum security ecosystem—centred on institutions such as SCSA, the Cyber Security Bureau and partner universities—remains integrated into regional and international quantum initiatives. Over a 5–10 year period, sustained investment, policy alignment and international cooperation can thus transform today's bottom-up initiatives into a mature national quantum security framework that supports both resilience and technological competitiveness.

5. IMPLICATIONS FOR NATIONAL SECURITY AND DEFENCE

As quantum technologies evolve from theoretical constructs into operational capabilities, their impact on state sovereignty requires a paradigm shift in how national security is conceptualised. For Georgia, navigating this transition demands a comprehensive, 'total defence' approach where technological resilience is deeply intertwined with military and civilian readiness. This section outlines the dual-use nature of the quantum era—detailing both the existential threats to current cryptographic foundations and the unprecedented opportunities for operational advantage. Translating these technical realities into actionable policy requires a unified, inter-ministerial effort. By examining the roles of core institutions, the following analysis demonstrates why integrating bottom-up quantum initiatives into broader national security planning is an immediate strategic imperative.

5.1 QUANTUM AND POST-QUANTUM THREATS TO NATIONAL SECURITY

From a national security perspective, the primary quantum-related risk lies in the potential of cryptographically relevant quantum computers to break widely used public-key cryptosystems, such as RSA and elliptic-curve cryptography, which underpin secure government, defence and critical infrastructure communications. This threat is amplified by 'harvest now, decrypt later' strategies, whereby adversaries intercept and store encrypted traffic today with the intention of decrypting it once quantum capabilities mature, potentially exposing sensitive diplomatic, military and intelligence communications years after their initial transmission. For a country like Georgia, whose security increasingly relies on digital networks, encrypted services and interoperability with allied systems, the quantum threat thus translates directly into risks for command-and-control, situational awareness, and the long-term confidentiality of classified and other high-sensitivity data.

NATO and several national security communities have begun to frame quantum technologies as a 'double-edged' strategic factor: they can enhance sensing, navigation and secure communications, but they can also degrade an alliance's ability to deter and defend if adversaries use them to undermine existing cryptography and exploit new attack surfaces. This dual-use character means that quantum and post-quantum security can no longer be treated as a purely technical or academic matter; instead, they must be integrated into broader national security and defence planning, including capability development, interoperability requirements and ecosystem protection measures. In this context, a national quantum security strategy for Georgia is not a luxury or a branding exercise, but a necessary component of long-term defence resilience and national sovereignty in a future quantum-enabled threat environment.

5.2 OPPORTUNITIES FOR NATIONAL SECURITY AND DEFENCE

Alongside these risks, quantum and post-quantum technologies also create opportunities to strengthen national security and defence capabilities. Quantum-grade random number generation and post-quantum cryptography can improve the robustness of encryption, key management and authentication mechanisms used in government and defence systems, reducing the risk that compromised randomness or vulnerable

algorithms could undermine otherwise well-designed security architectures. Quantum-resilient solutions can thus help ensure the long-term confidentiality and integrity of sensitive communications, even in the face of future advances in quantum computing and cryptanalysis."

Beyond cryptography, defence actors and alliances increasingly view quantum sensing, navigation and communication as potential sources of operational advantage. Quantum-enhanced inertial navigation, gravimetry and magnetometry could support more precise and resilient positioning, navigation and timing in GPS-denied or contested environments, while quantum communication and key distribution promise new ways to secure data links between platforms and command centres. NATO's quantum technologies strategy explicitly highlights applications in sensing, imaging, precise positioning, navigation and secure communications, and calls on Allies to move rapidly from experiments to operational concepts and capabilities, within a broader 'quantum-ready' posture. For Georgia, participation in such developments—even initially through research collaboration, testbeds and training—offers a way to align national defence planning with emerging Allied approaches while leveraging domestic initiatives such as the SCSA quantum laboratory and Erasmus+ SECURE hub.

5.3 ROLE OF KEY NATIONAL SECURITY AND DEFENCE INSTITUTIONS

In Georgia, several institutions have mandates that make them natural stakeholders in a national quantum security strategy. The Cyber Security Bureau under the Ministry of Defence is responsible for developing and implementing defence cyber policies, securing military information systems and ensuring alignment with international cybersecurity standards, which directly positions it at the core of quantum-resilient defence planning. The State Security Service (SSG) has a broader mission to ensure the security of the state and its citizens, including counter-terrorism, protection against sabotage, and the safeguarding of critical state interests, all of which increasingly depend on trustworthy digital infrastructures and secure communications. At the national level, the Operational-Technical Agency acts as the national computer security incident response team for critical information systems, covering public administration, energy, transport, water, finance, research and digital services, and exercising regulatory authority over dozens of critical infrastructure operators.

Together, these institutions form the operational backbone of Georgia's cybersecurity and national security ecosystem, and are therefore essential partners for any quantum security roadmap. In the short term, they can participate in joint assessments, pilot projects and training activities with the quantum laboratory and Erasmus+ SECURE hub, for example by testing post-quantum cryptographic schemes, quantum-grade random number generation and hardware security evaluations on systems relevant to defence, critical infrastructure and national-level incident response. In the medium to long term, the Cyber Security Bureau, SSG and LEPL Operative-Technical Agency can help translate technical experimentation into operational doctrine, incident-response procedures, regulatory requirements and capability development plans, ensuring that quantum-resilient measures are embedded not only in government networks, but also across the wider ecosystem of critical and high-sensitivity functions that underpin Georgia's national security.

6. CONCLUSION

This article has argued that Georgia's emerging quantum and post-quantum security ecosystem, centred on the quantum laboratory, the Erasmus+ SECURE hub and key national security institutions, provides a concrete foundation for developing a national quantum security strategy even in the absence of a formal top-down policy framework. By mapping existing capabilities and proposing a phased roadmap over a 1–2, 3–5 and 5–10 year horizon, it has shown how bottom-up initiatives can be aligned with national cybersecurity, digital transformation and defence priorities to address quantum-enabled threats and exploit quantum-related opportunities. For Georgia, the central challenge is not only to protect current systems against 'harvest now, decrypt later' and future quantum attacks, but also to position itself as a proactive contributor to regional and Allied quantum-safe efforts, integrating institutions such as the Cyber Security Bureau, the State Security Service and LEPL Operative-Technical Agency into a coherent quantum-ready security posture. While the specific details of implementation will evolve with technology and policy, the core message is that a national quantum security strategy is both necessary and feasible

today, provided that existing assets are leveraged strategically and coordinated across the national security community.

REFERENCES

1. CSE (Canada). “Roadmap for the Migration to Post-Quantum Cryptography for the Government of Canada (ITSM.40.001).” 2025.
2. Erasmus+ SECURE Consortium. “Erasmus+ SECURE – Project Website.” 2024.
3. European Commission. “A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography.” 2025.
4. Europol. “Post-Quantum Cryptography: Anticipating the Quantum Threat to Law Enforcement.” Europol, 2025.
5. NATO. “Summary of NATO’s Quantum Technologies Strategy.” NATO, 2024.
6. NIST. “Post-Quantum Cryptography Project.” NIST, ongoing.
7. NSA. “Post-Quantum Cybersecurity Resources.” NSA, 2024.
8. OECD. “An Overview of National Strategies and Policies for Quantum Technologies.” OECD, 2025.
9. SCSA. “Georgia’s First Quantum Laboratory – Quantum Lab Georgia.” Scientific Cyber Security Association, 2026.