From Act to Action: Architecting a Resilient Cybersecurity Governance Framework for Sierra Leone

Joseph Nylander

Publication Date: 2025/09/19

Abstract: In an era of rapid digital transformation, the Republic of Sierra Leone stands at a critical juncture. The enactment of the Cybersecurity and Crime Act of 2021 and the establishment of the National Cybersecurity Coordination Centre (NCCC) have laid a foundational legislative and institutional groundwork. However, the transition from legal frameworks to tangible, resilient cybersecurity capabilities presents a formidable challenge. This article provides a comprehensive analysis of Sierra Leone's current cybersecurity landscape, identifying key vulnerabilities, institutional capacities, and strategic imperatives. By drawing on established international governance frameworks such as the NIST Cybersecurity Framework, ISO/IEC 27001, and the Cybersecurity Capacity Maturity Model for Nations (CMM), this article proposes a multi-layered, adaptive, and context-specific cybersecurity governance framework for Sierra Leone. The proposed framework emphasizes a whole-of-society approach, integrating public-private partnerships, fostering a vibrant cybersecurity workforce, and promoting a deeply ingrained culture of cyber awareness. It is argued that for Sierra Leone to fully harness the dividends of its digital future, it must move decisively from "Act" to "Action," architecting a governance model that is not merely compliant, but truly resilient.

How to Cite: Joseph Nylander (2025) From Act to Action: Architecting a Resilient Cybersecurity Governance Framework for Sierra Leone. *International Journal of Innovative Science and Research Technology*, 10(9), 855-858. https://doi.org/10.38124/ijisrt/25sep124

I. INTRODUCTION: THE DIGITAL DAWN AND ITS INHERENT PERILS

Sierra Leone is in the midst of a determined push towards a digital future. This ambition is encapsulated in its National Digital Development Policy and the significant investments in critical digital infrastructure, including the Africa Coast to Europe (ACE) submarine fiber-optic cable. This digital transformation is not merely a technological upgrade; it is a fundamental enabler of socio-economic development, promising to enhance financial inclusion, modernize public services, and create new avenues for economic growth. However, this burgeoning digital ecosystem brings with it a host of sophisticated and ever-evolving cyber threats. From financial fraud and data breaches to attacks on critical national infrastructure, the potential for malicious cyber activities to undermine developmental progress is immense.

The global cyber threat landscape is becoming increasingly complex, with developing nations often being disproportionately affected due to nascent cybersecurity capabilities. For Sierra Leone, the risks are amplified by a combination of factors, including a still-developing technological infrastructure, a shortage of skilled cybersecurity professionals, and a general lack of public awareness regarding cyber threats. The imperative, therefore, is to build a robust and resilient cybersecurity governance framework that can effectively mitigate these risks while enabling the country to safely navigate its digital transformation journey. This article seeks to provide a blueprint for such a framework, tailored to the unique context and challenges of Sierra Leone.

II. THE CURRENT CYBERSECURITY LANDSCAPE IN SIERRA LEONE: A SITUATIONAL ANALYSIS

Sierra Leone has made commendable strides in establishing the legal and institutional prerequisites for a national cybersecurity framework. A critical examination of the current landscape, however, reveals both significant strengths and pressing challenges.

➢ *The Legislative and Institutional Bedrock: The 2021 Act and the NCCC*

The cornerstone of Sierra Leone's cybersecurity governance is the Cybersecurity and Crime Act of 2021. This landmark piece of legislation provides a comprehensive legal framework for addressing cybercrime, protecting critical national information infrastructure, and promoting cybersecurity. Key provisions of the Act include:

- The criminalization of a wide range of cyber offenses, from illegal access and data interference to cyberstalking and online fraud.
- The establishment of the National Cybersecurity Coordination Centre (NCCC) as the central body for coordinating cybersecurity efforts in the country.
- The creation of a National Cybersecurity Advisory Council to provide strategic guidance on cybersecurity matters.
- Provisions for international cooperation in the investigation and prosecution of cybercrimes.

The NCCC, as the operational heart of the nation's cybersecurity apparatus, is mandated with a broad spectrum of responsibilities. These include incident response, the dissemination of threat intelligence, the promotion of cybersecurity awareness, and the development of cybersecurity standards and best practices. The establishment of the NCCC is a clear indication of the government's commitment to building a proactive and coordinated defense against cyber threats.

➢ *The National Strategy: A Roadmap for a Secure Digital Future*

Complementing the legal framework is Sierra Leone's National Cybersecurity Strategy (2021-2025). This strategy outlines a vision for a safe, secure, and resilient digital ecosystem and is built on several key pillars, including:

- Strengthening cybersecurity governance and coordination.
- Protecting critical information infrastructure.
- Enhancing cybersecurity incident management.
- Fortifying the legal and regulatory framework.
- Building cyber defense capabilities.
- Promoting a thriving and secure digital economy.
- Enhancing international cooperation.

This strategic document provides a crucial roadmap for the country's cybersecurity development. However, the success of this strategy hinges on its effective implementation, which in turn requires sustained political will, adequate financial resources, and the active participation of all stakeholders.

➢ *Persistent Challenges and Vulnerabilities*

Despite these positive developments, Sierra Leone faces a number of significant challenges in its quest for cyber resilience:

- The Implementation Gap: There is a considerable gap between the ambitions articulated in the 2021 Act and the National Cybersecurity Strategy and the current on-the-ground realities. The operationalization of the NCCC is still in its early stages, and the full extent of its capacity is yet to be realized.
- The Human Capital Deficit: A critical shortage of skilled cybersecurity professionals pervades both the public and private sectors. This skills gap hampers the ability to effectively manage cybersecurity risks, respond to incidents, and enforce the provisions of the 2021 Act.
- Low Levels of Public Awareness: A significant portion of the population remains unaware of common cyber threats and best practices for online safety. This makes them vulnerable to phishing scams, social engineering, and other forms of cybercrime.
- Underdeveloped Technological Infrastructure: While progress has been made, many organizations in Sierra Leone still lack basic cybersecurity measures such as firewalls, intrusion detection systems, and robust data encryption practices.
- Limited Resources: The allocation of financial and technical resources for cybersecurity remains a major constraint. This affects everything from the acquisition of modern cybersecurity technologies to the funding of training and awareness programs.

III. ARCHITECTING A RESILIENT FRAMEWORK: A MULTI-LAYERED APPROACH

To address these challenges and build a truly resilient cybersecurity posture, Sierra Leone must adopt a multi-layered and adaptive governance framework. This framework should be grounded in international best practices but tailored to the nation's specific context. The proposed framework is structured around four interconnected pillars: Strategic Governance, Operational Capabilities, Human Capital Development, and a Whole-of-Society Ecosystem.

➢ *Pillar 1: Strategic Governance* - *Setting the Tone from the Top*

Effective cybersecurity governance begins with strong leadership and a clear strategic direction. This pillar focuses on the high-level structures and processes needed to guide and oversee the nation's cybersecurity efforts.

- Empowering the National Cybersecurity Advisory Council: The council should be composed of senior representatives from key government ministries (including Defense, Finance, and Justice), the private sector (particularly telecommunications and finance), academia, and civil society. Its role should be to provide independent, expert advice to the government on cybersecurity policy and strategy, and to ensure that cybersecurity is integrated into the broader national development agenda.

- Adopting a Risk-Based Approach: Drawing on the principles of the NIST Cybersecurity Framework, Sierra Leone should adopt a risk-based approach to cybersecurity. This involves identifying the country's most critical digital assets and services, assessing the potential threats and vulnerabilities they face, and prioritizing the allocation of resources to mitigate the most significant risks. The government, through the NCCC, should lead the development of a national cybersecurity risk assessment.
- Fostering a Culture of Compliance and Continuous Improvement: Inspired by ISO/IEC 27001, the government should promote the adoption of internationally recognized cybersecurity standards and best practices across both the public and private sectors. This could be achieved through a combination of regulatory requirements for critical infrastructure operators and incentive programs for other organizations to achieve cybersecurity certifications. The framework should also emphasize the importance of continuous monitoring, regular security audits, and a commitment to ongoing improvement.
- Strengthening Legal and Regulatory Enforcement: The 2021 Act provides a strong legal foundation, but its effectiveness depends on robust enforcement. This requires specialized training for law enforcement, prosecutors, and the judiciary on the technical and legal complexities of cybercrime. A dedicated cybercrime unit within the Sierra Leone Police with advanced digital forensics capabilities is essential.

➢ *Pillar 2: Operational Capabilities - The Frontline of Cyber Defense*

This pillar focuses on the practical capabilities needed to prevent, detect, and respond to cyber threats on a day-to-day basis.

- A Fully Operational and Resourced NCCC: The NCCC must be equipped with the necessary financial, technical, and human resources to fulfill its mandate. This includes:

✓ A National Computer Security and Incident Response Team (CSIRT): The CSIRT should serve as the central point of contact for reporting and responding to cybersecurity incidents. It should have the technical expertise to conduct forensic analysis, provide technical assistance to affected organizations, and coordinate a national response to major cyberattacks.

✓ A Threat Intelligence Platform: The NCCC should develop the capacity to collect, analyze, and disseminate timely and actionable threat intelligence to all relevant stakeholders. This will enable a more proactive and predictive approach to cyber defense.

✓ A National Vulnerability Disclosure Program: The government should establish a clear and secure process for security researchers and the public to report vulnerabilities in public-facing government systems.

- Securing Critical National Infrastructure (CNI): The government must identify and classify its CNI, which includes sectors such as energy, water, transportation, finance, and telecommunications. For these designated sectors, the government should establish mandatory cybersecurity standards and conduct regular security audits to ensure compliance. Public-private partnerships will be crucial in this area, with the government and CNI operators collaborating closely on threat information sharing and incident response.
- Enhancing National Cyber Defense: The Ministry of Defence and the Republic of Sierra Leone Armed Forces must develop a dedicated cyber defense doctrine and capability to protect national security interests in cyberspace. This includes defending military networks and being prepared to respond to state-sponsored cyber threats.

➢ *Pillar 3: Human Capital Development - The Human Firewall*

Technology and policies alone are insufficient to ensure cybersecurity. A skilled and aware populace is the most critical component of a resilient cyber defense.

- Integrating Cybersecurity into the National Curriculum: Cybersecurity education should begin at the primary and secondary school levels, teaching students the fundamentals of online safety and digital citizenship.[34]
- Developing Specialized Tertiary Education Programs: Sierra Leone's universities and technical colleges should be encouraged and supported to develop undergraduate and postgraduate programs in cybersecurity. These programs should align with industry needs and provide students with both theoretical knowledge and practical, hands-on skills.
- Professional Training and Certification: The government should partner with international organizations and leading cybersecurity companies to provide professional training and certification programs for IT professionals in both the public and private sectors. This will help to upskill the existing workforce and build a cadre of certified cybersecurity experts in the country.
- National Cybersecurity Awareness Campaigns: The NCCC, in collaboration with civil society organizations and the media, should launch sustained national cybersecurity awareness campaigns. These campaigns should use a variety of channels, including radio, television, social media, and community outreach programs, to educate the public about common cyber threats and how to protect themselves online.

➢ *Pillar 4: A Whole-of-Society Ecosystem - Fostering Collaboration*

Cybersecurity is a shared responsibility. A resilient governance framework requires a vibrant and collaborative ecosystem that includes all segments of society.

- Strengthening Public-Private Partnerships (PPPs): The government should establish formal mechanisms for collaboration with the private sector. This could include a national cybersecurity information sharing and analysis center (ISAC) where the government and private companies can share threat intelligence and best practices in a trusted environment. The telecommunications and financial sectors, being primary targets for cyberattacks, are particularly important partners.

- Engaging Academia and the Research Community: Universities and research institutions can play a vital role in developing innovative cybersecurity solutions, conducting research on local and regional cyber threats, and providing policy advice to the government. The government should foster a closer relationship with the academic community to leverage their expertise.
- Empowering Civil Society: Civil society organizations are crucial for promoting digital rights, advocating for a free and open internet, and holding the government accountable for its cybersecurity policies. They can also play a key role in public awareness and education initiatives. The government should ensure that civil society has a seat at the table in all cybersecurity policy discussions.
- Proactive International Cooperation: Cyber threats are transnational by nature. Sierra Leone must actively engage in regional and international cybersecurity cooperation. This includes ratifying and domesticating international conventions such as the Malabo Convention on Cybersecurity and Personal Data Protection, participating in regional cybersecurity forums, and establishing bilateral and multilateral partnerships for information sharing and capacity building.

➢ *The Path Forward: A Phased Implementation and a Call to Action*

The architecting of a resilient cybersecurity governance framework is not a one-time event but an ongoing process of adaptation and improvement. The implementation of the proposed framework should be approached in a phased and pragmatic manner, guided by the principles of the Cybersecurity Capacity Maturity Model for Nations (CMM).

- Phase 1 (Foundational): The immediate focus should be on strengthening the operational capabilities of the NCCC, particularly its incident response function. Concurrently, a major push on national cybersecurity awareness and foundational education is needed.
- Phase 2 (Consolidation): This phase should focus on the full implementation of mandatory cybersecurity standards for critical national infrastructure and the expansion of specialized cybersecurity education and training programs. The formalization of public-private partnerships should also be a priority.
- Phase 3 (Strategic): In this phase, Sierra Leone should aim to develop a more proactive and predictive cybersecurity posture, driven by advanced threat intelligence and a mature national risk management strategy. The country should also seek to become a regional leader in cybersecurity capacity building.

IV. CONCLUSION: SECURING THE DIGITAL DIVIDEND

Sierra Leone is on the cusp of a digital revolution that holds immense promise for its future. However, to fully realize this promise, the nation must proactively address the inherent risks of the digital age. The Cybersecurity and Crime Act of 2021 has provided the legislative "Act," but the time has now come for decisive "Action."

The journey towards cyber resilience is a marathon, not a sprint. It requires sustained political commitment, strategic investment, and a collaborative, whole-of-society approach. By architecting a resilient cybersecurity governance framework that is both ambitious in its scope and pragmatic in its implementation, Sierra Leone can build a secure and prosperous digital future for all its citizens. The framework proposed in this article offers a comprehensive roadmap for this critical endeavor. The digital dividend is within reach, but it must be secured.

REFERENCES

[1]. Government of Sierra Leone. (2021). *The Cybersecurity and Crime Act, 2021*.

[2]. Government of Sierra Leone. (2021). *National Cybersecurity Policy and Strategy for Sierra Leone 2021-2025*.

[3]. Government of Sierra Leone. (2021). *National Digital Development Policy*.

[4]. International Telecommunication Union. (2018). *Guide to Developing a National Cybersecurity Strategy*.

[5]. National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*.

[6]. International Organization for Standardization. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*.

[7]. Global Cyber Security Capacity Centre, University of Oxford.[46] *Cybersecurity Capacity Maturity Model for Nations (CMM)*.

[8]. The World Bank. (2023). *Sierra Leone Digital Transformation Project*.

[9]. African Union. (2014). *African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)*.