GOVERNMENT OF SIERRA LEONE

Ministry of Information and Communications

NATIONAL CYBERSECURITY STRATEGY

(2021-2025)

Table of Content

ACRONYMS

CI	Critical Infrastructure
CII	Critical Information Infrastructure
CID	Criminal Investigation Department
CISU	Central Intelligence and Security Unit
CMM	Cybersecurity Capacity Maturity Model
CSIRT	Computer Security Incident Response Team
DDOS	Distributed Denial of Service
DOS	Denial of Service
FIRST	Forum of Incident Response and Security Teams
GDI	Government Digitalisation Initiatives
ICT	Information and Communication Technology
ISP	Internet Service Provider
ITU	International Telecommunications Union
JCU	Joint Communication Unit
M&E	Monitoring and Evaluation
MIC	Ministry of Information and Communications
MOD	Ministry of Defense
NATCOM	National Telecommunications Commission
NCAC	National Cybersecurity Advisory Council
NCS	National Cybersecurity Strategy
NCRA	National Cyber Risk Assessment
NCTWG	National Cybersecurity Technical Working Group
NGO	Non-governmental Organisation
NTT	Nippon Telegraph and Telephone
ONS	Office of National Security
PKI	Public Key Infrastructure
R&D	Research and Development

EXECUTIVE SUMMARY

In this digitally-driven revolution, Sierra Leone, like other nations, strives to create a digitally inclusive society that will transform the economy and enhance its development. In this regard, the Government of Sierra Leone formulated a ten-year digital transformation roadmap through the Ministry of Information and Communications (MIC) geared toward shaping future investment and interventions of the Government and its development partners. With such emerging dependence on cyberspace, the Government is fully aware that without a concrete and detailed cybersecurity strategy, the gains of such a strategic plan will be eroded.

Thus, with Global Partner Digital (GPD) support, MIC embarked on developing a National Cybersecurity Strategy to provide a secure and resilient cyberspace to protect national interests while preserving citizens' fundamental rights. The development process adopted a multi-stakeholder approach by engaging all relevant stakeholders from the Government, civil societies, the telecoms, academia, and the private sector in a series of consultative workshops over the last year.

Sierra Leone's Cybersecurity Capacity Maturity Model (CMM) review conducted in 2016, and the National Cybersecurity Risk Assessment (NCRA) report delivered in January 2020 formed the Strategy's foundation. While the CMM report provided a thorough insight into the country's cyber landscape with seventy-four (74) recommendations on issues ranging from Policy, Legal and Regulatory Framework, Cyberculture, Capacity Building and Standards, the NCRA report examined the existing threats and vulnerabilities within various sectors in Sierra Leone.

The Government's vision for cybersecurity is to have an enabling environment that is secured, credible, and trustworthy for using ICTs while empowering citizens with the freedom to use the Internet for the nation's socio-economic benefits safely. To achieve this vision, the National Cybersecurity Strategy identified five (5) critical strategic goals, objectives, and specific activities to be implemented within a 5-year timeframe, as indicated in the table below.

SUMMARY OF THE DRAFT NATIONAL CYBERSECURITY STRATEGY

Keyword	Strategic Goals	Strategic Objectives	Activities
CREATE	Create an Institutional, Legal & Regulatory Framework for effective governance	Establish and operationalise a national cybersecurity governance structure	• Establish a National Cybersecurity Advisory Council to perform all its functions as defined in the 2020 Cybercrime Act. • Set up a Middle-level Technical Working Group made of experts from key institutions that play a significant role in Sierra Leone's cybersecurity landscape. This Committee will be responsible for providing technical recommendations at the operational level. • Establish and operationalise a National Cyber Security Center, proposed in the Cybercrime Bill to implement the National Cybersecurity Strategy.
		Develop legal and regulatory frameworks to enhance Sierra Leone's cybersecurity posture	• Enact and popularise the 2020 National Cybercrime Bill. • Create and adopt regulations to facilitate and monitor compliance with the particularities made in the provision of the Act regarding the digital investigation, lawful interception of communication, audit requirements and the security of ICT systems and infrastructures. • Develop and enact data protection and privacy law to promote citizens' privacy and rights. • Develop and adopt a framework for adopting/implementing international cybersecurity standards as baselines in public and private institutions.
		Empower the Criminal Justice System to prevent, deter, respond to, and mitigate cybercrime	• Develop and implement specialised training programmes for judges, prosecutors, lawyers, and law enforcement officials to interpret and apply the 2021 Cybersecurity and Crime Legislation. • Develop and institutionalise cybercrime curricula across the Police and Law School to accelerate skills development required to investigate and prosecute cybercrime offences. • Capacitate the Cybersecurity Unit at the Criminal Investigation Department (CID) to enhance digital investigations and prosecution of computer-related crimes. • Establish a National Forensic Lab at the National Cybersecurity Coordination Centre to support the police in prosecuting cybercrimes. • Develop a framework for the periodic review of the cybercrime legislation, including its implementation and governance structure.
		Establish sources and mechanisms for funding the implementation of the national cybersecurity strategy	• Develop and adopt a sustainable national cybersecurity funding framework with all stakeholders. • Establish a National Cybersecurity Fund accrued from taxes levied, fines, grants-in-aid, donors' support, gifts, endowments, voluntary contributions, or any other monies as agreed in the framework. • Develop capabilities or services at the NCSIRT level that will generate revenue.

PROTECT	**Protect Critical digital Infrastructure through Response Readiness.**	Protect all Critical National Information Infrastructure (CNII) and essential services	• Develop a robust national cybersecurity risk management framework. • Develop clearly defined roles and responsibilities for all CI and CII stakeholders and establish a Critical Information Infrastructure Protection (CIIP) Unit in the National Cybersecurity Centre to coordinate and manage all critical infrastructure protection. • Develop a mechanism for regular vulnerability disclosure and information sharing between Government and CNII operators. • Establish cybersecurity assurance programs for CNII and Government Digitalisation Initiatives (GDI) with baseline standards and a quality assurance framework. • Encourage the creation of formal public-private partnerships to increase the protection of CIIs and manage risks. • Conduct regular cyber risk assessments to develop risk profiles and build a risk register to mitigate these risks.
		Establish cyber-incident response capabilities with clear roles and responsibilities	• Establish a national CSIRT to enable Sierra Leone to prevent, detect, mitigate and respond effectively to cyber incidents. • Work with sectors to set up sectoral CSIRT at the regulatory level to work in tandem with the National CSIRT to handle incidents. • Develop a robust cyber incident response framework that provides general guidelines, procedures, processes and protocols for the operation of CSIRTs. • Provide incident response capacity building to national and sectoral CSIRTs. • Establish a secure and confidential incident reporting platform for real-time sharing of incidents and threat intelligence across sectors or organisations to reduce the impact on businesses in Sierra Leone. • Affiliate the national and sectoral CSIRTs with the Forum of Incident Response and Security Teams (FIRST) and other regional CSIRTs for international cooperation in incident response.
		Develop a cyber defence strategy for deterring malicious activities in Sierra Leone's cyberspace	• Develop a communication and coordination framework for cyber defence between Joint Communication Unit (JCU) and the private/public sector. • Strengthen the JCU of the Ministry of Defense to better accomplish its objectives in both the physical and cyberspace. • Develop the cyber capabilities of the Military to detect and counter malicious cyber actors in cyberspace. • Reduce malicious cyber activities that will threaten national security. • Conduct a consistent review of the evolving threat landscape in cybersecurity to continually meet national security objectives.

		Establish a proactive national contingency plan for cybersecurity emergencies and crisis	• Develop a national cybersecurity crisis management plan with clear roles and responsibilities to be activated during a cyber-attack. • Establish policies for business continuity during a cyberattack. • Conduct various cyber-attacks scenarios, drills and simulations to test the effectiveness of the national cyber response mechanism. • Participate in international cybersecurity simulation exercises to boost response capabilities and cross-border dependencies regionally and globally.
PROMOTE	**Promote public education, awareness, online child protection, rights and privacy of Citizens**	Implement national initiatives on online child protection	• Establish policies for both adult and children's online usage in cyberspace. • Develop mechanisms that empower children and stakeholders in digital hygiene to ensure healthy and beneficial decision-making. • Develop child-friendly information platforms that appeal to children of different age brackets and, at the same time, encourage good digital citizenship. • Establish victim support mechanisms and rehabilitation.
		Promote good cybersecurity culture through public education, awareness-raising, campaigns, and capacity building for specified target groups	• Develop programmes and materials to train and improve cybersecurity practices in Sierra Leone. • Engage multiple stakeholders in the development and delivery of awareness-raising programmes. • Develop campaigns that promote the safe use of online services across the general public. • Encourage media and new media providers to disseminate information on specific cybersecurity issues and good digital citizenship. • Launch a dedicated national cybersecurity awareness month to increase public education and awareness-raising on cybersecurity issues.
		Build citizens' trust and confidence on the Internet by promoting secure and safer access	• Promote security by design across the Government and private sector for everyday use of the Internet and online services. • Encourage digital service providers to establish technical security control deployment policies as part of their services. • Establish programmes to train users in managing their privacy online and protect themselves from unwanted access. • Promote the need for security in e-services and user understanding of the importance of anti-malware software and network firewall across devices. • Develop a framework for the establishment of national PKI to enhance secure communication. • Raise public awareness of secure communication services like encrypted/signed emails.
DEVELOP	**Develop Cyber Capabilities to support**	Develop a framework for the integration of cybersecurity in the	• Develop cybersecurity curricula across primary and secondary schools and create specialised university courses and degree programmes on cybersecurity.

	national security objectives.	formal educational system	• Create cybersecurity education programmes for teachers/lecturers to ensure skilled staff is readily available to teach the newly created cybersecurity courses. • Allocate resources to cybersecurity education for public universities. • Establish incentive schemes such as scholarships to foster awareness and stimulate interest in cybersecurity career opportunities.
		Enhance workforce training and professional skills development in cybersecurity for both experts and non-experts in the public and private sector	• Identify training needs and develop appropriate training modules for targeted demographics. • Provide training for IT experts on various aspects of cybersecurity. • Create knowledge-based exchange programmes to enhance cooperation between training providers, academia and organisations. • Create a favourable environment for more private companies and organisations to offer cybersecurity Certificates in Sierra Leone.
		Foster local cybersecurity industry in Sierra Leone	• Create the enabling environment for the growth of cybersecurity start-ups and the insurance market in Sierra Leone. • Develop government incentive mechanisms to boost the private sector investment in cybersecurity.
		Promote innovation, research and development in cybersecurity	• Develop sustainable initiatives to bridge the gap between universities and the industry market. • Develop cybersecurity-focused R&D programmes in universities and other public research institutions. • Establish a framework for the effective dissemination of innovation and research findings. • Provide dedicated funding mechanisms for ongoing research.
STRENGTHEN	**Strengthen national, regional and International Cooperation**	Enhance national cooperation and collaboration in the private and public sector	• Develop sustainable public-private partnerships to enhance cybersecurity and incident response nationally. • Foster a multi-stakeholder approach to the implementation of the national cybersecurity strategy. • Strengthen formal and informal cooperation mechanisms within the police, criminal justice system, and other third parties, locally and across borders.
		Establish regional and international cooperation mechanisms to fight against cybercrime and secure the cyberspace	• Enhance Sierra Leone's diplomatic competencies in cyber-related issues to better engage in cyber-diplomacy and international cooperation. • Ratify regional and international cybersecurity treaties and obligations (including but not limited to ECOWAS directives, Malabo and Budapest Conventions). • Participate in bilateral and multilateral agreements on cybersecurity with other countries. • Participate in regional and global cyber engagements and drills to build our overall cybersecurity capabilities.

OVERVIEW OF THE CYBERSECURITY STRATEGY

2.1 Introduction

The drive toward a digital economy has created opportunities for countries in the digital south to embark on massive digitisation projects to leapfrog their socio-economic status. This trend has got many countries developing digital transformation strategies and plans that require building massive digital infrastructure to support these projects. However, with the growing cybersecurity issues, governments are developing various initiatives or techniques to protect critical assets, systems, and networks vital to the operation and stability of the nation and the livelihood of its people.

For Sierra Leone, the Government aims to transform the country by 2029 into a digitally inclusive society empowered by a digital economy. This plan, as enshrined in the National Digital Transformation Roadmap (NDTR), intends to utilise digital technologies to unleash the innate potentials of every citizen with the 'Leave No One Behind' vision of the United Nations (UN) and the 'Africa we want' principle of the African Union (AU). The digital economy offers an incredible opportunity for Sierra Leone to leapfrog and provide opportunities for its citizens to create wealth. However, the cybersecurity challenges remain a big problem and, if not adequately addressed, will erode any possible economic gain that can be made from this era.

The protection of the existing and new digital infrastructure, both public and private, is a significant segment of this Strategy. Moreover, it will also focus on citizens' cyberspace well-being by protecting their rights and promoting responsible use of the Internet via various levels of capacity building.

2.2 Purpose, Scope and Assumptions

2.2.1. Purpose of the Strategy

The National Cybersecurity Strategy (NCS) is a concrete 5-year strategic action plan geared - toward improving the country's overall cybersecurity landscape, including increasing the security and resilience of its critical infrastructure, cultivating good digital citizenry and developing appropriate legislation and regulations. Moreover, it will enable the Government and the private sector to work coherently towards implementing specific objectives, including mobilising the required resources.

2.2.2. Scope of the Strategy

The NCS is a comprehensive strategy that cuts across issues related to the government, national and international actors. It focuses on a broad scope of cyberspace activities, including infrastructure development and protection, institutional framework, legal measures, capacity building and awareness-raising, and empowering administrative justice to fight against cybercrime and cooperation at the national, regional, and international levels.

2.2.3. Assumptions

The Strategy considers the existence of some capacity scattered in different sectors for which coordination is required. More specifically, the following assumptions are taken into consideration in the development of the Strategy:

a. Existence of a Cybersecurity Policy approved by the Cabinet in 2016
b. Existence of a holistic 2020 National Cyber Risk Assessment report on the threat and vulnerabilities of critical sectors in Sierra Leone
c. Existence of a 2016 cybersecurity maturity model (CMM) assessment report that provides a comprehensive analysis of Sierra Leone's cybersecurity landscape.

2.3 The NCS within the Context of the National Development Plan

In this digital-driven age, the Government's vision, as stated in section 3.5 of Cluster 3 of the Medium-Term National Development Plan 2019 – 2023, is to leapfrog to a digital economy by leveraging on ICT as a critical enabler. This goal will bring economic diversification, stabilisation, and sustainable growth in all sectors. It will also bring efficiency and effectiveness to governance while addressing the challenges and bottlenecks of outdated practices and processes. With such projected dependence on cyberspace for service delivery across all sectors, the Government has given cybersecurity a very high priority. It has been included as part of the national security strategy, as demonstrated in Section 4.9 of Cluster 4 of the National Development Plan.

Thus, to ensure a coherent and unified approach to both security and our country's digital transformation process, the NCS will be fully harmonised and aligned with the National Security Strategy and the Digital Transformation Plan of Sierra Leone.

2.4 Vision

Our vision is to have a credible and secured cyberspace that protects national interests while empowering citizens with the freedom to safely use the Internet for the socio-economic benefit of the nation.

2.5 Mission Statement

Our mission is to ensure that Sierra Leone **c**reates institutional, legal and regulatory frameworks for effective governance, promotes public education and awareness, protects children online and the rights and privacy of citizens, develops cyber capabilities to support national security objectives, protects critical digital infrastructure through response readiness and strengthen national, regional and international cooperation.

2.6 Guiding Principles

The Sierra Leone National Cybersecurity Strategy is designed and delivered on seven (7) key guiding principles that guide the design of the vision, mission, broad strategic goals, and specific strategic objectives as listed below:

A. **Risk-based approach:** The Cybersecurity Strategy will ensure that a risk-based approach is adopted by the Government, private sector, academia and civil society in assessing and responding to cyber-related threats or issues.

   a. A **risk-based approach** means that the country, competent authorities, businesses, banks, ISPs, MNO, and Citizens will identify, assess, and understand the cyber **risk** to which they are exposed, and take the appropriate mitigation measures per the level of **risk.**

B. **Multi-stakeholder approach:** The Cybersecurity Strategy will seek to enhance all key stakeholders' effectiveness in improving the cybersecurity posture of Sierra Leone by recognising the various roles and responsibilities of different stakeholders and promoting national cooperation and coordination for cybersecurity-related activities amongst stakeholders.

C. **External Cooperation:** The Strategy will also promote bilateral, regional, and international collaboration, recognising the borderless nature of cyberspace.

D. **Respect for the rule of law and human rights:** The National Cybersecurity Strategy is aligned with the laws in force in Sierra Leone. It also aims to facilitate the promotion, protection, and enjoyment of Sierra Leone citizens' fundamental human rights and freedoms, as defined in the Sierra Leonean Constitution. All measures taken under this Cybersecurity Strategy will be consistent with Sierra Leone's international, regional, and national human rights obligations.

E. **Capacity development:** The National Cybersecurity Strategy will enable the continuous development of Sierra Leone's capacity to address fast-changing cybersecurity issues and developments.

F. **Socio-economic development:** The National Cybersecurity Strategy will ensure that Sierra Leone fully leverages cyberspace to spur broader socio-economic development and facilitate sustainable socio-economic development across the nation.

G. Addressing Cybercrime: The National Cybersecurity Strategy will promote and facilitate both individual and collective action in tackling cybercrime, recognising both the personal responsibility and collective responsibility in taking steps in combating cybercrime.

UNDERSTANDING THE CYBERSECURITY CONTEXT

3.1 Global Cybersecurity Landscape

The continuous technological evolution and innovation in all spheres of life, where security for most developers is an afterthought, has led to an explosion of cyberspace vulnerabilities. According to the 2019 NTT Security Global Cyber Intelligence report, attackers are exploiting these new loopholes to create complex Cyberattacks at an alarming rate. Moreover, these cybercriminals manipulate software and application codes for their malicious activities, and even hardware such as computer chips and patches developed to fix known application issues. Such loopholes and sophisticated tools readily available from the dark web market enable cybercriminals to exploit target organisations and hide their tracks more efficiently.

More interestingly, in 2019, the technology sector shifted to be another highly targeted sector, at par with the financial industry, followed by business and professional services. However, as stated in the Interpol 2020 Cybercrime report, the COVID 19 pandemic has caused cybercriminals to adequately adjust their attacks to target primarily government institutions or the health care sector, which promises higher financial gain. Moreover, as illustrated in Figure 1, phishing/online scams and malware (ransomware and DDOS) attacks were suggested to be the most predominant threat since the start of this pandemic.

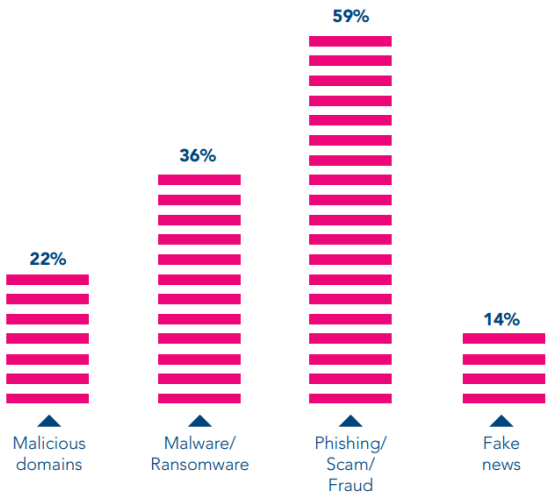

Figure 1: Distribution of the Key COVID-19 inflicted cyberthreats
Source: Interpol 2020 Cybercrime Report

Studies also revealed an increase in the average annual cost of cybercrime across all attack types from 2017 to 2018 (Figure 2), with projections that it will increase to more than $6 trillion in 2021.

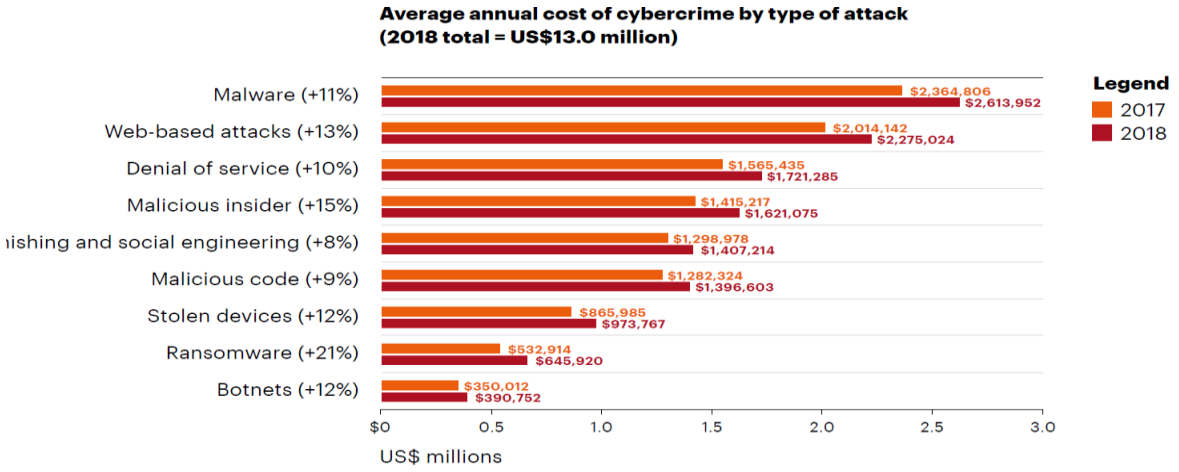

Figure 2: Average annual cost of cybercrime by type of attack
Source: Accenture Ninth Annual Cost of cybercrime Study

3.2 Regional Cybersecurity Landscape and initiatives

According to the *Cybercrime and cybersecurity – Trends in Africa report,* Africa's cyber threat intelligence landscape comprises attacks similar to the global landscape. Malware and web-based attacks appear to dominate worldwide, as indicated in Figure 3.

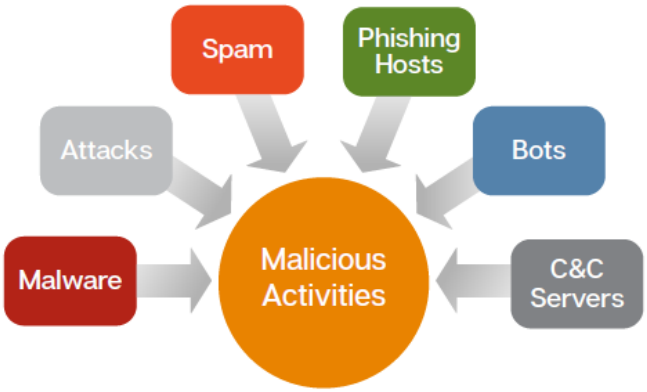

Figure 3: Africa Region Threat Landscape
Source: Cybercrime and cybersecurity – Trends in Africa

Available evidence suggests that the more the connectedness of countries, the higher the spate of cyberattacks. South Africa appears to be the most connected and leads with the highest

number of attacks, making up about 20% of all attacks in Africa. Despite the prevalence of cyberattacks in the African cybersecurity landscape, the volume of incidents in the continent represents a tiny fraction of the global attack scenarios. However, with the rate at which African nations embrace the digital age, this dynamics is expected to shift rapidly.

3.3 National Threats and Vulnerabilities Landscape

In 2016, with support from the Global Cyber Security Capacity Centre (GCSCC), Sierra Leone's Government conducted a Cybersecurity Maturity Model (CMM) assessment, revealing the country's cybersecurity maturity landscape. While in 2019, the Ministry of Information and Communications, with support from the UK Government, completed an NCRA assessment to further probe into the cybersecurity threats and vulnerabilities of critical sectors within Sierra Leone. These two reports thoroughly analyse the nation's current risks and vulnerability landscape.

3.3.1. Cyber Threat Landscape

Sierra Leone's 2020 NCRA Report shows malware and insider threats as the most significant perceived threat vectors across most sectors (Figure 4), similar to the regional and global picture. Also, accidents appear to be a predominant cyber threat actor (Figure 5), indicating a lack of awareness of crucial cybersecurity protocols by security teams at workplaces. Attacks often occur when vulnerabilities are created due to deployment of unlicensed applications, utilisation of default configuration, misconfiguration of IT systems, and not regularly deploying patches.

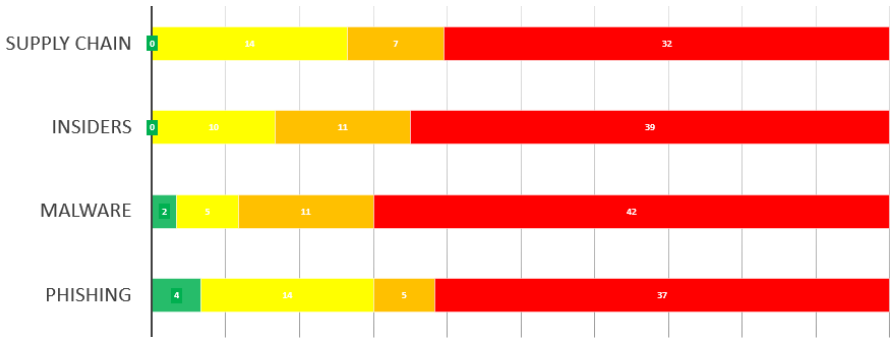

Figure 4: Threat Vector of Sierra Leone

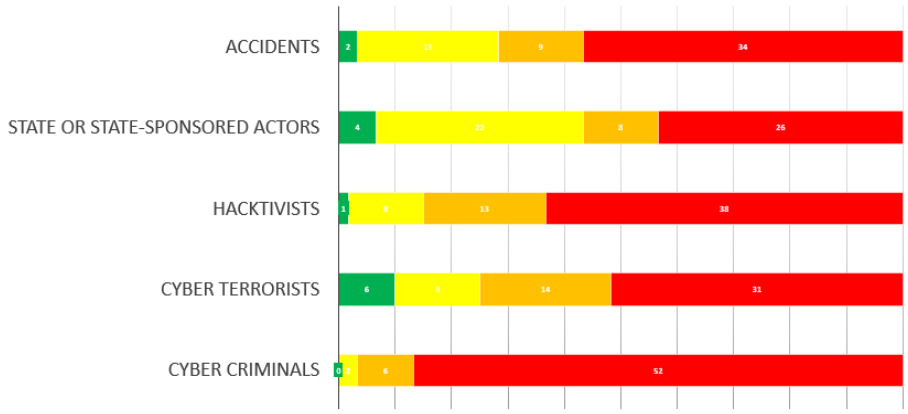

Figure 5: Threat Actors of Sierra Leone

3.3.1.1 Cyber Governance Posture

Under the cybersecurity governance posturing of Sierra Leone, the financial sector appears to have a good cybersecurity governance practice. NCRA recommends improvements should be focused at the board level and downwards to ensure that cyber training, cyber risk registers, cyber roles and responsibilities are in place and properly executed. However, as this is an important area to get right, the nation will benefit more if all the OK zone organisations receive a boost or focus.

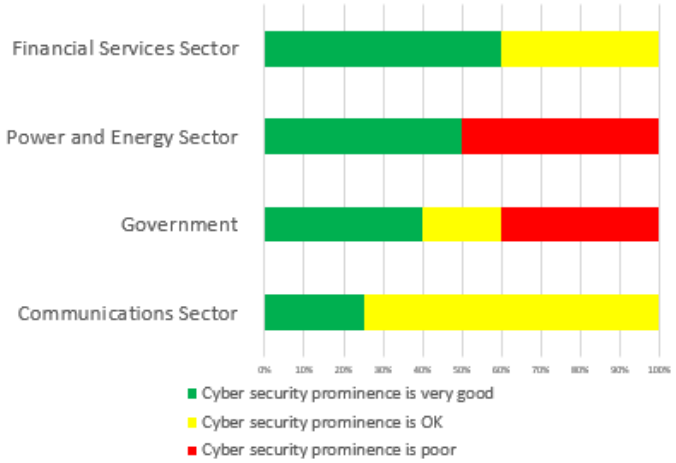

Figure 6: National SL Cybersecurity Governance Posture

3.3.1.2 Impact of Cyber Risk on Critical Services

Attack on critical services will have a financial impact on the organisation; it will also impact other essential services in other sectors. In Sierra Leone, a major cyber-attack on critical services will severely impact the telecoms, Government, and financial industry. T he education, defence, and healthcare sector will also take significant hits, as indicated in Figure 7.

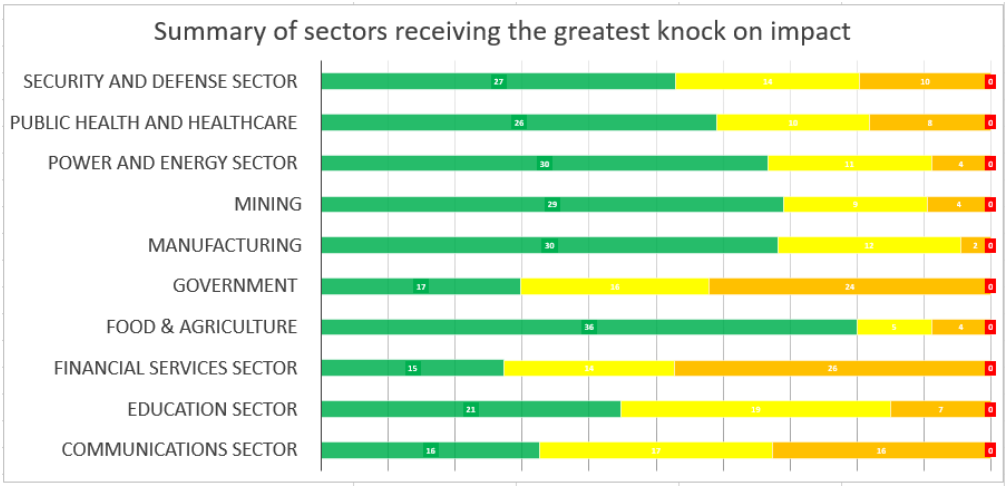

Figure 7: Impact of cyber Risk on Critical services in Sierra Leone

3.3.2. Sierra Leone Cybersecurity Maturity Level

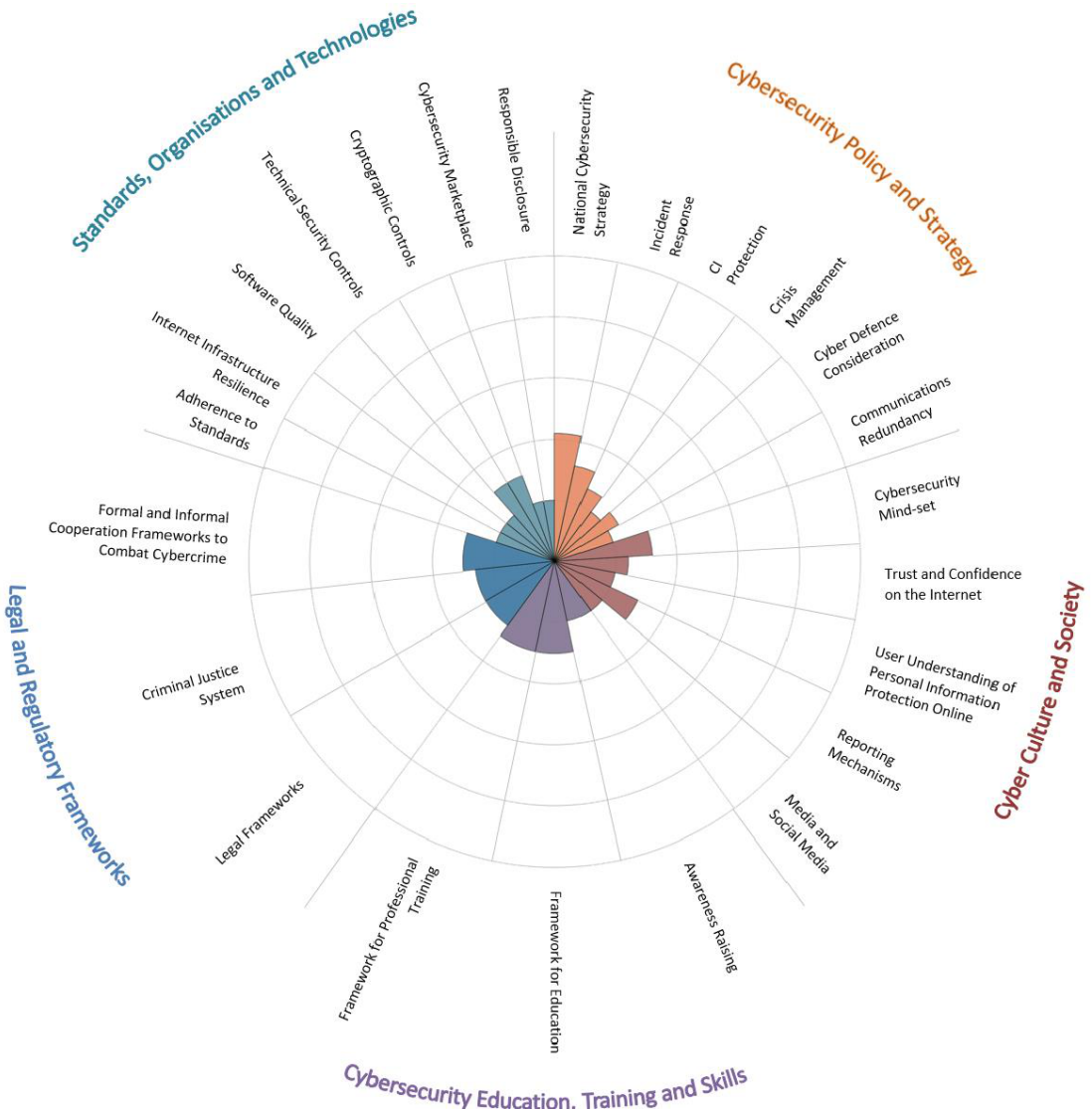

Figure 8: CMM Assessment Map for Sierra Leone

According to the 2016 CMM Assessment report, the maturity of Sierra Leone's cybersecurity capacity ranges from a start-up to a formative stage across the five various dimensions measured, as indicated in Figure 8. The report provided a thorough insight into each thematic area, highlighting gaps and providing recommendations for the nation to improve its capacity. Some of the main gaps spotted and which still exist were:

- The lack of a national Computer Security Incident Response Team (CSIRT) or command and control centre structure poses challenges to effective and coordinated incident response and management.

- Lack of a central dedicated mechanism that enables citizens to report computer-related or online incidents or crimes in Sierra Leone.
- Cybersecurity elements are not included in the national planning and evaluation of crisis management protocols and procedures.
- The country has no specific Cyber Defence Policy or Strategy.
- Though ICT infrastructure and services proliferate across the country, cybersecurity awareness-raising has not gathered momentum. Moreover, the Media and social media are not taking an active role in reporting cybersecurity threats and incidents and raising awareness.
- Cybersecurity-related courses are not yet part of the curriculum at the various levels of education, and cooperation between educational institutions is lacking.
- Cybersecurity training needs in public and private sectors are not documented, and coordination between training providers, academia and the private sector is minimal.
- Legislative gaps and inconsistent application of law have led to a lack of online protection for consumers, vulnerable groups and user data in general.
- Though law enforcement has some capacity to investigate computer-related crimes, mainly through the cybercrime unit within the Criminal Investigation Department (CID), specialised and regular training is not widely available for law enforcement officers, limiting investigative capabilities.
- Prosecutors and judges are not adequately trained to prosecute and preside over computer-related crimes.
- Domestic and international cooperation to combat cybercrime is mainly informal, particularly through INTERPOL channels. Formal mechanisms that complement these casual relationships have not yet been established.
- No coordinated effort to adopt and implement cybersecurity standards.
- Software quality is not monitored, and no secured software platforms and applications catalogue exists.
- Cryptographic techniques for protecting data at rest and in transit are not yet deployed consistently within the Government, private sector and the general public, even though leading organisations within the public and private sectors are starting to recognise the importance of cryptographic controls.
- The cybersecurity marketplace is underdeveloped, and foreign technologies are being deployed instead of producing security products domestically.

- No responsible disclosure policy or framework has been established.

Since this report's publication, the Government has taken strides to build its cybersecurity capabilities and protect citizens in cyberspace. Such interventions include:

- The development and adoption of the 2016 Cybersecurity Policy, which gives clear policy directives on cyber-related issues, including the setting up of a national cybersecurity governance structure;
- The drafting of the 2021 Cybercrime Bill, which aligns with both Malabo and Budapest conventions and is currently at a pre-legislative phase;
- Conduction of training and awareness-raising programs targeted at the private and public sector;
- Building international relations and partnerships with institutions such as the Council of Europe, Commonwealth, ITU, GFCE, ECOWAS and others in combating cybercrime and enhancing its cybersecurity;

3.3.3. Opportunities to Improve Sierra Leone's Cybersecurity Posture

The issues raised from the CMM Assessment report provide the Government with an opportunity to develop a National Cybersecurity Strategy that addresses all the identified weaknesses. The NCRA report also made some recommendations to build a robust Critical Information Infrastructure (CII) protection plan using a public-private partnership. These include:

- Develop cyber skills, awareness and training for CII managers
- Provide CII Managers access to relevant threat intelligence
- Develop enforcement of risk management thresholds through regular testing
- Investigate the dependencies between the various systems in each sector to understand how a cyber-attack would propagate and disrupt other sectors' systems
- Put in place a cybersecurity governance structure to enforce cybersecurity at CII
- Work with CII managers to develop a risk register
- Work with CII managers to reduce vulnerabilities of incident management, malware prevention, and network security.

STRATEGIC GOALS AND OBJECTIVES OF THE NATIONAL CYBERSECURITY STRATEGY

Based on the risks identified under the risk assessment report and the CMM assessment report, the Government developed several high-level strategic goals and related objectives to address these cybersecurity issues.

Figure 9: National Cybersecurity Strategic Goals for Sierra Leone (2020 -2025)- At A Glance

4.1 Strategic Goal 1: Create Institutional, Legal and Regulatory Framework for Effective Governance

Cybersecurity governance is critical to successfully implementing any cybersecurity strategy, and situating it within the right sector is a priority. Though some countries have initially located it at either the Office of the President, Office of National Security or the Ministry of

Defence, recent recommendations from international bodies have suggested the ICT Ministry as the appropriate location due to the multi-stakeholder nature of cybersecurity.

Since several legal domains touch upon various cybersecurity subject areas, nations rarely adopt a single overarching national cybersecurity law. Instead, aspects relevant to cybersecurity may be addressed in multiple legal instruments by subject area, organisational structure and authority, or other considerations. Thus, the Government is committed to implementing relevant regulations and guidelines to ensure cybersecurity is enforced across sectors. This strategic goal will also set clear leadership roles and resource allocation to ensure efficient cybersecurity governance in Sierra Leone.

Strategic Objectives

I. Establish and operationalise a national cybersecurity governance structure.
II. Develop legal and regulatory frameworks to enhance Sierra Leone's cybersecurity posture.
III. Empower the Criminal Justice System to prevent, deter, respond to, and mitigate cybercrime.
IV. Establish sources and mechanisms for funding the implementation of the national cybersecurity strategy.

4.2 Strategic Goal 2: Promote Public Education, Awareness, Child Online Protection, Rights and Privacy of Citizens

The Government of Sierra Leone will consider bringing the relevant information, understanding and competence of cybersecurity to all levels of society and its impact on everyday life. This step will require defining target groups, identifying the minimum level of awareness and competence required, and suitable measures directed at each group to achieve a satisfactory level of cybersecurity awareness and competence in society. The Government will also promote citizens' trust in the digital environment by raising awareness of the risks and applying the necessary safeguards to encourage empowerment. Creating an environment that enables freedom of Internet use with undue interruptions will empower the different stakeholders to create wealth online in peace.

Protecting children and other vulnerable groups online will require strengthening the legal regime to punish these cybercrime perpetrators. This goal will ensure that all stakeholders are given essential awareness training and standard measures to ensure minimal crimes against these stakeholders.

The Government of Sierra Leone is also committed to implementing appropriate initiatives to promote citizens' privacy and human rights, consistent with international, regional, and national human rights laws, treaties, and conventions.

Strategic Objectives:

I. Implement national initiatives on online child protection.
II. Promote good cybersecurity culture through public education, awareness-raising, campaigns, and capacity building for specified target groups.
III. Build citizens' trust and confidence on the Internet by promoting secure and safer access.

4.3 Strategic Goal 3: Protect Critical Digital Infrastructure Through Response Readiness

The NCRA report provides an excellent current state of the Critical National Information Infrastructure (CNII). Though there are pockets of effort in the different sectors to protect these infrastructures, the Government plans to centralise the protection of these CIs and create the necessary risk management framework using a multi-stakeholder approach. The Government will provide additional support to the public and private sector actors in fulfilling their responsibilities, including sharing information on joint risk analysis, models for risk assessment and accreditation of risk management methods, harmonisation of training measures, and technology assessment analyses.

Moreover, the Government aims to develop national and sectorial Computer Security Incident Response Teams (CSIRT) as specialised teams to react to cyberattacks on networks and critical infrastructures. The sector team will work with the national team to secure systems in the

sectors and support private sector operators in responding to cyber incidents. The CSIRT will be trained in incident response capabilities to ensure an efficient response to cyber-attacks.

The Government of Sierra Leone will also develop a national crisis management plan to respond to attacks that may affect several sectors and threaten national security.

Strategic Objectives:

I. Protect all Critical National Information Infrastructure (CNII) and essential services.
II. Establish cyber-incident response capabilities with clear roles and responsibilities.
III. Develop a cyber defence strategy for deterring malicious activities in Sierra Leone cyberspace.
IV. Establish a proactive national contingency plan for cybersecurity emergencies and crises.

4.4 Strategic Goal 4: Develop Cyber Capabilities to Support the National Security Objectives

Cybersecurity skills in most African countries are non-existent. In many countries, there are pockets of certification courses and training offered by private organisations. As new cybersecurity and digital infrastructures are rolled out, there will be demands for a skilled workforce to manage the security of the infrastructures in the private and Government sectors.

The Government of Sierra Leone will take a holistic approach to train the cybersecurity workforce. It will assess the force needed in the unfolding cybersecurity landscape and develop a National Framework by adopting the NICE (National Initiative for Cybersecurity Education) Cybersecurity Workforce Framework. This framework will provide an educational curriculum and required professional training for different cybersecurity capacities.

Under this goal, the Government will also nurture the cybersecurity industry in Sierra Leone by promoting entrepreneurship for young innovators to develop skills in cybersecurity products in the long term.

Strategic Objectives:

I. Develop a framework for the integration of cybersecurity in the formal educational system.
II. Enhance workforce training and professional skills development in cybersecurity for experts and non-experts in the public and private sectors.
III. Foster local cybersecurity industry in Sierra Leone.
IV. Promote innovation, research and development in cybersecurity.

4.5 Strategic Goal 5: Strengthen National, Regional and International Cooperation

Cybersecurity is borderless and requires both local and international cooperation. In-country, there is a need to establish a public-private partnership for handling cybersecurity incidents which can be done by ensuring cybersecurity activities are done jointly between the Government and private sectors. Such an initiative will foster cooperation at the local level and promote efficiency in handling cyber incidents.

Law enforcement will improve mutual assistance by working closely with Interpol to establish a 24/7 contact centre for rapid response to requests for retaining evidence and extradition of cyber criminals. The Government will also take the necessary steps to ascend to the Budapest Convention and ratify the Malabo Convention to ascertain it meets regional and international standards in the fight against cybercrime, securing its cyberspace and protecting its citizens' data. Furthermore, the nation will foster international partnerships by joining international forums such as FIRST to strengthen its cyber capabilities and effective coordination of cyber-related issues.

Strategic Objectives:

I. Enhance national cooperation and collaboration in the private and public sector
II. Establish regional and international cooperation mechanisms to fight against cybercrime and secure the cyberspace

5 STRATEGIC OBJECTIVES AND IMPLEMENTATION PLAN

For the purpose of setting up timelines for implementation, the following timelines will be used.

Term	***Period***	***Remarks***
Short Term	*Up to 2 years*	
Medium-term	*2 – 4 Years*	
Long Term	*5years +*	

Strategic Goal 1: Create institutional, legal and regulatory framework for effective governance				
No.	**Strategic Objectives**	**Specific Activities**	**Time frame**	**Responsible Agency / Stakeholder**
1.1	Establish and operationalise a national cybersecurity governance structure	1.1.1 Establish a National Cybersecurity Advisory Council with authority to perform all its functions as defined in the 2021 Cybercrime Act. 1.1.2 Set up a Middle-level Technical Working Group made of experts from key institutions that play a significant role in Sierra Leone's cybersecurity landscape. This Committee will be responsible for providing technical recommendations at the operational level. 1.1.3 Establish and operationalise a National Cyber Security Center, proposed in the Cybercrime Bill to implement the National Cybersecurity Strategy.	Short Term	Ministry of Information and Communications

1.2	Develop legal and regulatory frameworks to enhance Sierra Leone's cybersecurity posture	1.2.1 Enact and popularise the 2021 National Cybersecurity and Crime Act. 1.2.2 Create and adopt regulations to facilitate and monitor compliance with the particularities made in the provision of the Act regarding the digital investigation, lawful interception of communication, audit requirements and the security of ICT systems and infrastructures. 1.2.3 Develop and enact data protection and privacy law to promote citizens' privacy and rights. 1.2.4 Develop a framework for adopting/implementing international cybersecurity standards to be utilised as baselines in public and private institutions.	Medium Term	Ministry of Information and Communications/ Attorney Generals department/NCRA
1.3	Empower the Criminal Justice System to prevent, deter, respond to, and mitigate cybercrime	1.3.1 Develop and implement specialised training programmes for judges, prosecutors, lawyers, and law enforcement officials to interpret and apply the 2021 Cybersecurity and Crime legislation. 1.3.2 Develop and institutionalise cybercrime curricula across the Police and Law School to accelerate skills development required to investigate and prosecute cybercrime offences. 1.3.3 Capacitate the Cybersecurity Unit at the Criminal Investigation Department (CID) to enhance digital investigations and prosecution of computer-related crimes. 1.3.4 Establish a National Forensic Lab at the National Cybersecurity Coordination Centre to	Medium-term	MIC/ Attorney Generals Dept/ Sierra Leone Police/ Sierra Leone Judiciary/ Regulatory Authorities/ Responsible agencies

		support the police in prosecuting cybercrimes 1.3.5 Develop a framework for the periodic review of the cybercrime legislation, including its implementation and governance structure.		
1.4	Establish sources and mechanisms for funding the implementation of a national cybersecurity strategy	1.4.1 Develop and adopt a sustainable national cybersecurity funding framework with all stakeholders. 1.4.2 Establish a National Cybersecurity Fund accrued from taxes levied, fines, grants-in-aid, donors' support, gifts, endowments, voluntary contributions, or any other monies as agreed in the framework. 1.4.3 Develop capabilities or services at the NCSIRT level that will generate revenue.	Short to Medium-term	MIC/ Ministry of Finance

Strategic Goal 2: Promote public education and awareness, child online protection, and rights and privacy of Citizens				
No.	**Strategic Objectives**	**Specific Activities**	**Time frame**	**Responsible Agency / Stakeholder**
2.1	Implement national initiatives on child online protection	2.1.1 Establish policies for both adult and children's online usage. 2.1.2 Develop mechanisms that empower children and stakeholders in digital hygiene to ensure healthy and beneficial decision-making. 2.1.3 Develop child-friendly information platforms that appeal to children of different age brackets and, at the same time, encourage good digital citizenship. 2.1.4 Establish victim support mechanisms and rehabilitation.	Short term	MIC, Ministry of Education, Ministry of Gender and Children's Affairs, Civil Societies

2.2	Promote good cybersecurity culture through public education, awareness-raising, campaigns, and capacity building for specified target groups	2.2.1 Develop programmes and materials to train and improve cybersecurity practices in Sierra Leone. 2.2.2 Engage multiple stakeholders in the development and delivery of awareness-raising programmes. 2.2.3 Develop campaigns that promote the safe use of online services across the general public. 2.2.4 Encourage media and new media providers to disseminate information on specific cybersecurity issues and good digital citizenship. 2.2.5 Launch a dedicated national cybersecurity awareness month to increase public education and awareness-raising on cybersecurity issues.	Short to Medium-term	MIC/Public & Private Sectors/Civil Societies/ International Partners
2.3	Build citizens' trust and confidence on the Internet by promoting secure and safer access	2.3.1 Promote security by design across the Government and private sector for everyday use of the Internet and online services. 2.3.2 Encourage digital service providers to establish policies for technical security control deployment as part of their services. 2.3.3 Establish programmes to train users in managing their privacy online and protect themselves from unwanted access. 2.3.4 Promote the need for security in e-services and user understanding of the importance of anti-malware software and network firewall across devices. 2.3.5 Develop a framework for the establishment of national PKI to enhance secure communication. 2.3.6 Raise public awareness of secure communication services like encrypted/signed emails.	Short to Medium-term	MIC/Private Sector/Civil Society/ International Partners/ GDI Owners

Strategic Goal 3: Protect Critical digital Infrastructure through Response Readiness.				
No.	**Strategic Objectives**	**Specific Activities**	**Time frame**	**Responsible Agency / Stakeholder**
3.1	Protect all Critical National Information Infrastructure (CNII) and essential services	3.1.1 Develop a robust national cybersecurity risk management framework. 3.1.2 Develop clearly defined roles and responsibilities for all CI and CII stakeholders and establish a Critical Information Infrastructure Protection (CIIP) Unit under the National Cybersecurity Department to coordinate and manage all critical infrastructure protection. 3.1.3 Develop a mechanism for regular vulnerability disclosure and information sharing between Government and CNII operators. 3.1.4 Establish cybersecurity assurance programs for CNII and Government Digitalisation Initiatives (GDI) with baseline standards and a quality assurance framework. 3.1.5 Encourage the creation of formal public-private partnerships to increase the protection of CIIs and managing of risks. 3.1.6 Conduct regular cyber risk assessments to develop risk profiles and build a risk register to mitigate these risks.		MIC /Public & Private Sector/ CI Operators
3.2	Establish cyber-incident response capabilities with clear roles and responsibilities	3.2.1 Establish a national CSIRT to enable Sierra Leone to prevent, detect, mitigate and respond effectively to cyber incidents. 3.2.2 Work with sectors to set up sectoral CSIRT at the	Short Term	MIC/Attorney General/ Police service/ Judicial service/Regulators

		regulatory level to work with the National CSIRT to handle incidents. 3.2.3 Develop a robust cyber incident response framework that provides general guidelines, procedures, processes and protocols for the operation of CSIRTs. 3.2.4 Provide incident response capacity building to national and sectoral CSIRTs. 3.2.5 Establish a secure and confidential incident reporting platform for sharing incidents and threat intelligence across sectors or organisations in real-time, to reduce the impact on businesses in Sierra Leone. 3.2.6 Affiliate the national and sectoral CSIRTs with the Forum of Incident Response and Security Teams (FIRST) and other regional CSIRTs for international incident response cooperation.		
3.3	Develop a cyber defence strategy for deterring malicious activities in Sierra Leone's cyberspace	3.3.1 Develop a communication and coordination framework for cyber defence between Joint Communication Unit (JCU) and the private/public sector. 3.3.2 Strengthen the JCU of the Ministry of Defence to better accomplish its objectives in both the physical and cyberspace. 3.3.3 Develop the cyber capabilities of the Military to detect and counter malicious cyber actors in cyberspace. Reduce malicious cyber activities that will threaten national security.	Medium to Long term	MIC/ Sierra Leone Police Service & Academy/ RSLAF

		3.3.4 Conduct a consistent review of the evolving threat landscape in cybersecurity to continually meet national security objectives.		
3.4	Establish a proactive national contingency plan for cybersecurity emergencies and crisis	3.4.1 Develop a national cybersecurity crisis management plan with clear roles and responsibilities to be activated during a cyber-attack. 3.4.2 Establish policies for business continuity during a cyberattack. 3.4.3 Conduct various cyber-attacks scenarios, drills and simulations to test the effectiveness of the national cyber response mechanism. 3.4.4 Participate in international cybersecurity simulation exercises to boost response capabilities and cross-border dependencies regionally and globally.	Short to medium term	MIC/Judicial service/ Attorney General's Department / Police /CID Sierra Leone Bar Association/ Law school/ ONS/ CNII Operators

Strategic Goal 4: Develop Cyber Capabilities to support the national security objectives				
No.	**Strategic Initiative**	**Specific Activities**	**Time frame**	**Responsible Agency / Stakeholder**
4.1	Develop a framework for the integration of cybersecurity in the formal educational system	4.1.1 Develop cybersecurity curricula across primary and secondary schools and create specialised university courses and degree programmes on cybersecurity. 4.1.2 Create cybersecurity education programmes for teachers/lecturers to ensure	Short to medium term	MIC/ Ministry of Education/ GDI Owners/ Academia

		skilled staff is readily available to teach the newly created cybersecurity courses. 4.1.3 Allocate resources to cybersecurity education for public universities. 4.1.4 Establish incentive schemes such as scholarships to foster awareness and stimulate interest in cybersecurity career opportunities.		
4.2	Enhance workforce training and professional skills development in cybersecurity for both experts and non-experts in the public and private sector	4.2.1 Identify training needs and develop appropriate training modules for targeted demographics. 4.2.2 Provide training for IT experts on various aspects of cybersecurity. 4.2.3 Create knowledge-based exchange programmes to enhance cooperation between training providers, academia and organisations. 4.2.4 Create a favourable environment for more private companies and organisations to offer cybersecurity Certificates in Sierra Leone.	Short to medium term	MIC/ Private and Public Sector
4.3	Foster local cybersecurity industry in Sierra Leone	4.3.1 Create the enabling environment for the growth of cybersecurity start-ups and the insurance market in Sierra Leone. 4.3.2 Develop government incentive mechanisms to boost the private sector investment in the cybersecurity industry	Short to medium	MIC/ CNII operators & GDI owners
4.4	Promote innovation, research and development in cybersecurity	4.4.1 Develop sustainable initiatives to bridge the gap between universities and the industry market. 4.4.2 Develop cybersecurity-focused R&D programmes in universities and other public research institutions. 4.4.3 Establish a framework for the effective dissemination of innovation and research findings. Provide dedicated funding mechanisms for ongoing research.	Short Term	MIC/National CSIRT/ NATCOM/ sector CSIRTs/ Private Sector

Strategic Goal 5: Strengthen National, Regional and International Cooperation				
No.	**Strategic Objectives**	**Specific Activities**	**Time frame**	**Responsible Agency / Stakeholder**
5.1	Enhance national cooperation and collaboration in the private and public sector	5.1.1 Develop sustainable public-private partnerships to enhance cybersecurity and incident response nationally. 5.1.2 Foster a multi-stakeholder approach to the implementation of the national cybersecurity strategy. 5.1.3 Strengthen formal and informal cooperation mechanisms within the police, criminal justice system, and other third parties locally and across borders.	Medium Term	MIC/ Ministry of Education/ Universities/Research Institutions
5.2	Establish regional and international cooperation mechanisms to fight against cybercrime and secure the cyberspace	5.2.1 Enhance Sierra Leone's diplomatic competencies in cyber-related issues to better engage in cyber-diplomacy and international cooperation. 5.2.2 Ratify regional and international cybersecurity treaties and obligations (including but not limited to ECOWAS directives, Malabo and Budapest Conventions). 5.2.3 Participate in bilateral and multilateral agreements on cybersecurity with other countries. 5.2.4 Participate in regional and global cyber engagements and drills as a means of building our overall cybersecurity capabilities	Short to Medium-term	MIC/ Private Sector / Ministry of Foreign Affairs

6 KEY STAKEHOLDERS

6.1 Roles and Responsibilities

Cybersecurity is a collective effort, and the responsibility for implementing the identified lines of action is divided among multiple stakeholders. In Sierra Leone, the Ministry of Information and Communication (MIC), through the National Cybersecurity Centre, is responsible for implementing the Strategy. This established Centre will work under the Ministry's supervision with the National Cybersecurity Technical Working Group under the policy and strategic direction of the Cybersecurity Advisory Council.

The strategy's ultimate aim is to set up an operational body that will effectively coordinate cybersecurity in Sierra Leone that reports through MIC to the Presidency. MIC will assign national agencies roles to implement different aspects of the Action Plan based on their competencies and areas of interest that affect them.

Key Stakeholders for the implementation will include the following Government agencies:

Name of Agency	**Area of Implementation Support**
National Cybersecurity Centre	Coordination, Awareness-Raising, Critical Infrastructure Protection, Incidents Response and Reporting at national level
Police CID Cybercrime Unit	Cybercrime investigation
Ministry of Foreign Affairs and International Cooperation	International cooperation
Ministry of Justice	Cybercrime jurisprudence
Attorney General's Department	Review of Law, Cybercrime prosecution
Ministry of Defense	Cyber defence
Ministry of Internal Affairs	Cybercrime Issues and Enforcement of the Law
National Telecommunications (NATCOM)	Regulation of the Telecom Sector, Incidents Response and Reporting at Sectoral level

Bank of Sierra Leone	Regulation of the Financial Sector, Incidents Response and Reporting at Sectoral level
National Security	Regulation of the Security Sector, Incidents Response and Reporting at Sectoral level, National Security issues
Ministry of Gender and Children's Affairs	Online Child Protection
Ministry of Education (Basic and Tertiary)	Develop cyber capabilities in the Educational System

A multi-stakeholder approach will be used in the implementation of the strategy. This approach will require bringing on board other stakeholders like the private sector and civil society from time to time to participate in discussions on implementing certain aspects of the strategy that relates to them.

7 FUNDING & RESOURCE NEEDS

The Government of Sierra Leone shall set up a dedicated cybersecurity fund to finance cybersecurity. Funds will come from but are not limited to the following sources:

a. Annual Budget Allocation
b. Taxes
c. Grants

The funds will be sustainable and support other cybersecurity projects, including research and development and the growth of the local cybersecurity industry.

8 MONITORING & EVALUATION

The Government of Sierra Leone shall adopt a cybersecurity monitoring and evaluation framework to monitor the progress of the implementation of the strategy. Sierra Leone will develop benchmarks for measuring progress. Each objective will have performance indicators to measure success. Ultimately the Government of Sierra Leone will procure risk management software to measure the implementation progress.

9 STRATEGY REVIEW PROGRESS

Due to the evolving nature of cyber threats and the resulting need to continuously develop up-to-date responses, subject areas in cybersecurity requires that an NCS be periodically evaluated, and if necessary, reviewed. The evaluation will be made to gain insight into the *existing initiatives' status quo* and measure the strategy's implementation and overall efficiency in meeting its stated objectives. Thus, the Government will reassess the NCS objectives and corresponding Action Plan items periodically. The review process includes having a clear overview of the implementation of an NCS and ensuring coherence with other national strategies, initiatives and legal instruments**.** Appropriate performance measurement mechanisms will be considered to facilitate rational and well-directed use of resources.

APPENDIX A: GLOSSARY OF TERMS

For this Strategy Document, the following terms are defined:

Cyberspace – The global domain created by the interconnection of communication and information systems.

Cybersecurity – The Protection of information systems forming cyberspace from attacks, assuring confidentiality, integrity and availability of information/data processed in this environment, detection of attacks and cyber incidents, activation of counter-response mechanisms and recovering systems to conditions before the cybersecurity incident.

Cyber Defense – The operationalisation of security to deter, prevent, detect, withstand and recover from a cyberattack; The set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers being critical.

Cyberattack – A security incident initiated in cyberspace to cause harm by compromising communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems.

Cybercrime – Crimes committed through the use of digitally enabled devices, where the devices are either used as a tool to commit a crime, the target of the crime or as a storage device in the commission of an offence.

Cyber-attack – A deliberate attempt to damage, disrupt, or gain unauthorised access to a computer, computer system or electronic communication network.

Cyberwarfare –the use of digital attacks like computer viruses and hacking --by one country to disrupt the vital computer systems of another, to create damage, death and destruction.

Hacktivist – uses computer-based techniques such as hacking as a form of civil disobedience to promote a political agenda or social change.

Human Rights - are the fundamental rights and freedoms to which everyone is entitled based on their common humanity.

Information Systems - Systems included in providing any service, transaction and information/data through information and communication technologies.

Information Security – a set of practices designed to keep personal data secure from unauthorised access and alteration during storing or transmitting from one place to another.

Internet Security - comprises various **security** measures exercised to ensure the **security** of online transactions. In the process, **internet security** prevents attacks targeted at browsers, network, operating systems, and other applications.

Malware – is any software intentionally designed to cause damage to a computer, server, client, or computer network.

National Cybersecurity – Cybersecurity provided at a national scale for any hardware and software systems associated with all services, transactions, information/data provided through the information and communication technologies that constitute national cyberspace.

National Cybersecurity Strategy – A tool by which policymakers identify strategic objectives (ideally consistent with national values and interests) pinpoint the resources available and guide how such resources are to be applied to reach strategic goals.

Threat - The potential cause of an incident that may cause damage to an institution or system.

Ransomware – Malicious software that denies the user access to their files, computer or device and in some cases threatens to publish user's private data unless a ransom is paid.

Risk - The potential risk of causing damage by using vulnerabilities in one or more information entities.

Safeguard – A risk-reducing measure that acts to detect, prevent, or minimise loss associated with the occurrence of a specific threat or category of threats.

Social Engineering – The psychological manipulation of people into performing actions or divulging confidential information.

Vulnerability – Bugs in a software program that can be exploited by attackers to perform unauthorised actions within a computer system.

APPENDIX B: National Cybersecurity Advisory Council

The National Cybersecurity Advisory Council comprising of the Vice President as Chairman and the following other members:

a. Minister of Finance
b. Attorney-General and Minister of Justice
c. Minister of Internal Affairs
d. Minister of Foreign Affairs and International Cooperation
e. National Security Coordinator of the Office of National Security
f. Director-General of Central Intelligence and Security Unit
g. Chief of Defence Staff of the Republic of Sierra Leone Armed Forces
h. Inspector-General of Sierra Leone Police
i. Director-General of National Telecommunication Commission
j. Governor of the Bank of Sierra Leone
k. National Cyber Security Coordinator (Secretary)
l. Director of Communications of the Ministry of Information and Communications
m. Minister of Information and Communications
n. Barrister appointed by H.E. the President with 15 years of experience

APPENDIX C: National Cybersecurity Technical Working Group

a. One Member from Bank of Sierra Leone, the Financial Regulator
b. One Member from the Financial Intelligence Unit
c. One Member from Office of the National Security
d. One Member from the Ministry of Defence /RSLAF
e. One Member from Sierra Leone Police
f. One Member from Sierra Leone ISPs Association
g. One Member from NATCOM
h. Two Participants from the Academia (University of Sierra Leone, Njala)
i. One Participant from the Civil Society Organisations

Printed by
Government Printing Department