

2020 Cyber Crimes Bill

Sierra Leoneans in Technology

Response



Scan to download a copy



Download a copy at <http://bit.ly/slnt-response>

Outline

- Letter
- Executive Summary
- High-Level Findings and Recommendations
- Review Committee Team Members
- Contact Details
- Detail Findings and Recommendations
 - Part I – Preliminary
 - Part II – Critical National Information Infrastructure
 - Part III – Powers And Procedures
 - Part IV – International Cooperation
 - Part V – Offences
 - Part VI - Administration And Enforcement
 - Part VII - Miscellaneous Provisions
- References

About SLinT

SLinT is a network of more than 100 Sierra Leonean technology professionals located around the world

Date: Wednesday 31st, March 2021

From: Sierra Leoneans in Technology (SLinT)

To: The Government of Sierra Leone (GoSL) and interested parties

Re: Concerns Regarding the Cyber Crimes 2020 Bill

SLinT (Sierra Leoneans in Technology), a concentrated, progressive and apolitical group of Sierra Leonean technology professionals worldwide, commend the Ministry of Information and Communication's decision and hard work towards the 2020 Cyber Crimes Acts currently in review in Parliament. We strongly believe that we need these types of legislations, when done right, to help the country develop and use technology effectively while protecting the public in the suggested standards and instruments by way of the tabled legislation.

While the Ministry and its partners have done an excellent job putting the bill forward, we know the passing of such legislation is a massive uptake in a problematic domain to find professionals globally, knowing those limits within Sierra Leone for Cyber Security professionals. Cyber Crime is a global phenomenon that is at the top of every government's legal system across the world at the moment. It requires urgent attention via legislation on the possible crimes that can be committed and the potential violations of our fundamental human rights and privacy, irrespective of which government is in power.

Hence, the approach should beg us to look at this with absolute neutrality and scrutiny to safeguard our nascent democracy. SLinT has asked a community with over 100 members listed from all walks of Technology professions ranging from (Law, Cybersecurity, Network Security, Software engineers, Management Consultants, Technology Architects, Blockchain, Cryptocurrency, Professors, Technology entrepreneurs, and many more). These members come from some of the most coveted Technology and consulting global giants to work for, such as (Microsoft, Amazon, Facebook, Apple, Oracle, Google, IBM, Accenture, Northrop Grumman, and many more).

Our candidates' pool, ranges from professors, senior management consultants, and advisers to governments worldwide, to entrepreneurs doing business in Sierra Leone and abroad. We host the most extensive set of qualified Sierra Leonean technology professionals worldwide. We strongly believe that it is time to put these Sierra Leonean conglomerates of brains to work for Sierra Leone. We hope that you would heed our unbiased advice and know that this is intended to be a constructive engagement for this bill and possible future assistance in utilizing Sierra Leonean talents overseas as means of addressing the brain drain.

While we have benefited from the host of technology professionals who were able to provide feedback, we have also incorporated the layperson's viewpoints in this document. And although this is our preliminary assessment in a short period to respond, we may provide several iterations to the government. We can serve as a resource for rectifications and general advice.

We once again congratulate the Ministry for the attempt to pioneer a much needed remedy in the fight against Cybercrimes in the country. We look forward to working with them in getting this right, to avoid a mistake that can send the judiciary into a tailspin of civil right violations obscuring the core focus on crimes that may have been committed.

Sincerely,



Tamba Sheku Lamin
President and Executive Board Member
Sierra Leoneans in Technology (SLinT)





EXECUTIVE SUMMARY

Executive Summary

SLinT believes that the Cyber Crimes Act in its current state has some reasonable provisions that are needed to decrease cybercrimes in Sierra Leone. After our preliminary, professional and neutral review of the bill, we found that the **legislation has significant loopholes, cannot be effectively implemented, and represents a threat to data protection, citizens' privacy, human rights, and freedom of expression.**

The current bill will make it very easy for police officers, the Minister, Judges, and Authorized persons to misuse their office powers to violate data protection laws, privacy, and Sierra Leonean citizens' human rights. The bill extends the offence of criminal responsibility to numerous acts that may have been committed through a computer system without providing the safeguards to guarantee civil liberties and fair adjudication of matters. It concentrates investigative and enforcement powers with undefined fines and penalties to the Minister and a few others, undermining this bill's intent as a new risk to the outcomes of the Sierra Leone Truth and Reconciliation Commission (TRC) report.

Computer Security or security in cyberspace is not as simple as catching the cybercriminal. It is about preventing the cybercriminal from committing cybercrimes such as stealing or changing valuable national security data. If the cybercriminal is allowed to break into a secured system, existing standards, guidelines, principles, tools, and processes are used to investigate the crime. This Cyber Crimes bill is the perfect legislation to investigate and convict the cybercriminal. Governments and companies typically spend large sums of money on preventing cybercrimes from happening by developing and enacting standards, policies, and guidelines and training employees and citizens on secure computer systems.

SLinT is **recommending that this bill is put on hold for further inclusive review with all relevant stakeholders.** While at the same time, we implement the **data protection and privacy legislation as a precursor to enacting this bill,** to guarantee due process for all citizens irrespective of background, government, or favours as a matter of urgency. The view of amending the bill after passing it now on its current fast-paced trajectory to enactment seems wrong in plain sight of these concerns.

Executive Summary Part I – Preliminary & Part II – Critical National Information Infrastructure

Findings

- **Part I – Preliminary**
 - Definitions for some key terms and phrases used in the bill are missing, leaving them up for interpretation by the police officers, judges, authorized persons, and the Minister. Examples; Privacy, Authorized Persons, Terms and Conditions, Such Conditions, reasonable grounds, reasonably required
- **Part II – Critical National Information Infrastructure**
 - Existing documentation, standards, policies, and guidelines to professionally classify computer systems as **Critical National Information System** are missing in the bill. The President and the Minister should not be the people deciding what constitutes a **Critical National Information System**.
 - It will be impossible to implement the “Audit” and inspection of critical national information infrastructure if standards, guidelines, and policies are not available to require each system to log every user and system activity. Computer systems cannot be adequately audited if they are not designed and implemented to log every user and system activity.



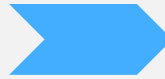
Recommendations

- **Part I, Section I – Preliminary**
 - Define each key term or phrase used in the bill. Example; Privacy, Authorized Persons, Terms, and Conditions, Such Conditions, reasonable grounds, reasonably required
- **Part II, Section 2, subsection (1) - Designation of Critical National Information Infrastructure**
 - Use an independent expert body to develop, and establish standards, policies and guidelines for what constitutes a “**Critical National Information Infrastructure**.”
- **Part II, Section 3 - Audit and inspection of Critical National Information Infrastructure**
 - Develop standards, policies, and guidelines that are followed by all vendors, suppliers, MDAs, organizations, businesses, Etc. that are in the business of implementing critical information systems to ensure all systems are secured by default and all system and user activities are logged to facilitate accurate and efficient information systems audits.

Executive Summary - Part III – Powers And Procedures

Findings

- **Part III – Powers And Procedures**
 - There are no existing data protection and privacy laws to guide police officers and other authorized persons to protect data collected during investigations. The privacy of the accused persons' may be arbitrarily violated
 - The bill will allow any police officer or authorized person without adequate training or qualification in cybercrimes to apply to the High Court judge for a warrant.
 - Digital evidence will be accessed on-site by police officers who are not trained and qualified digital forensic experts without following an established chain of custody procedure
 - Evidence may not be assigned to a digital forensics expert to analyze and report findings.
 - The judges' standards to validate that the police officer is qualified to investigate a cybercrime are missing.
 - Electronic evidence collected during investigations may not be handled professionally due to a lack of existing standards and training.
 - Data protection and privacy may not be respected when a search is extended to related systems.



Recommendations

- **Part III – Powers And Procedures**
 - Develop and enact **strong data protection and privacy laws** to ensure standards are followed when data is collected during investigations.
 - Create standards, policies, and guidelines that are followed by all investigating officers involved in evidence collection, processing, and storage
 - Change the phrase “**police officer**” to “**enforcement officers trained and experienced in investigating cybercrimes**” with **renewable cyber crimes related credentials** to investigate and prosecute cybercrimes
 - Add provisions in the bill to ensure digital evidence are assigned to a digital forensics expert to analyze and report findings and make provision for dismissal of tampered evidence
 - Stipulate in data privacy and protection regulations, a Data Minimization requirement for service providers who collect and store user data, as in the EU’s GDPR.
 - If data privacy and protection regulations cannot be enacted before the Cybercrime bill is passed, ensure there is a separate section or clause that stipulates the data minimization requirement and make it apply to all entities that will collect and/or store user data.

Executive Summary - Part III – Powers And Procedures

Preliminary Findings

- **Part III – Powers And Procedures**
 - Forcing an accused person to render any information to aid an investigation without his/her lawyer's presence may violate their rights.
 - Data intended for evidence may not be securely accessed or copied to preserve the data integrity due to the lack of standards, policies, procedures, and training
 - Not all information described in the bill may be relevant to investigating cybercrimes. MDAs, businesses, and organizations will be allowed to violate their consumers' privacy to comply with some of the bill's provisions



Recommendations

- **Part III – Powers And Procedures**
 - Add provisions in the bill to require the following before it's implemented.
 - Develop and enact policies, procedures, and guidelines for:
 - The warrant request process
 - The process to collect and handle evidence
 - Chain of custody
 - Device collection
 - Email collection
 - Storage and inventory
 - Evidence examination process
 - Evidence analysis, and
 - Evidence reporting
 - Establish a Forensics Lab to include
 - Restricted access
 - Tools including hardware and software
 - Personnel Qualifications

Executive Summary - Part IV – International Cooperation

Findings

- **Part IV – International Cooperation**
 - The Attorney-General will be allowed to mutually assist and disclose Sierra Leone's data to foreign states and international agencies without regard for international treaties and relationships, human rights records, data protection, and privacy laws?
 - Sierra Leone will be allowed to provide information to foreign states and agencies without a mutual assistance treaty or arrangement in place.
 - Sierra Leone or a foreign state or agency may request the expeditious preservation of data stored for mutual assistance, search, access, seizure, and security or disclosure of the data without following due process. As a result, the GoSL or foreign states may gain access to protected data that will violate citizens' privacy.
 - An exception is made for political offences or offences related to political offences



Recommendations

- **Part IV, Section 13, subsection (1) - Spontaneous information**
 - **Change the text to the following;**
 - “ *The Attorney-General may, subject to this Act, the data protection and privacy laws, and with a prior request, forward to a foreign state, information obtained under this Act, where he considers that the disclosure of such information may-*”
- **Part IV, Section 13, subsection (1) - Spontaneous information**
 - **Change the text to the following;**
 - “The Attorney-General may only cooperate with a foreign state or international agency that Sierra Leone has a mutual assistance treaty or arrangement in force for the purpose of –”
- **Part IV, Section 19, subsection (2)(a) - Expedited disclosure of preserved traffic data**
 - Remove Part IV, Section 19, subsection (2)(a).
 - It is unfair to make exceptions for political offence or an offence related to a political offence

Executive Summary - Part IV – International Cooperation

Findings

- **Part IV – International Cooperation**
 - Foreign states can request Sierra Leone to keep confidential the facts of any requests for mutual assistance. However, there is no joint statement for Sierra Leone to ask the foreign state to keep secret the facts of any requests for mutual assistance from Sierra Leone.
 - “all appropriate measures” and “preserve the specified data in accordance with the procedures” may be misinterpreted very easily.
 - A foreign state may request the search, access, security or disclosure of data stored by means of a computer system located within Sierra Leone, including data that has been preserved under section 18 with first obtaining a valid warrant to extend its investigations overseas. This will open the door for rogue state actors to misuse the system.



Recommendations

- **Part IV – International Cooperation**
 - Add a provision to ensure that Sierra Leone can request foreign states and international agencies to keep confidential the facts of any requests for mutual assistance from Sierra Leone.
 - Clearly define the meaning of “**all appropriate measures**” and “**preserve the specified data in accordance with the procedures**” in the bill to ensure it cannot be misinterpreted.
- **Part IV, section 20, subsection (2) – Mutual assistance regarding accessing of stored computer data**
 - Add a provision to require the foreign state or international agency to prove that a warrant has already been obtained to extend the investigations overseas.
 - Add procedures and standards to validate the authenticity of request from foreign states and international agencies.

Executive Summary - Part V – Offences

Findings

- **Part V – Offences**

- The fines and term of imprisonment for accused persons or organizations convicted would be dictated by the Minister of Information and Communications - a political appointee of the Executive Branch. It is essential to ensure that the law's application is not arbitrary but on the specifics predetermined without bias.
- Exceptions are not provided for so-called “ethical” hackers trained to detect vulnerabilities in computer systems and networks.
- Standards, policies, and guidelines to mark and display a message on critical information infrastructure are missing.
- Identity theft, cyberstalking and cyberbullying, and impersonation content is vague and open to multiple interpretations.
- Cybersquatting offence is extended to international domain names for which no MDA or corporate entity in Sierra Leone has control. This will open the door for foreign governments and corporations to sue individuals and corporations in Sierra Leone on no basis.



Recommendations

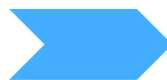
- **Part V – Offences**

- For all offences, please specify the **imprisonment period** and/or **fine amount** in the sections to ensure the Minister and Judge cannot arbitrarily change it favouring anyone. For all fines in Part V, change all appearances of the following text.
 - “*commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe*” to “**commits an offence and is liable upon conviction to imprisonment for a period not exceeding [PERIOD], or a fine not exceeding [AMOUNT], or both.**”
- In Part III – Offences and Penalties of the Nigeria “[Cybercrimes \(Prohibition, prevention, ECT\) Act, 2015](#)” you will see an excellent example of how it is done to avoid favoritism.
- You can also see examples in [PART II - Offences , Section 4, subsection \(1\) of the HIPCAR Model Policy Guidelines and Legislative Text](#)
- Make conditional exceptions for so-called “ethical” hackers who are trained to detect vulnerabilities in computer systems and networks.
- Add “for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent,” to subparagraph (a) of Section 35, subsection (2),

Executive Summary - Part V – Offences

Findings

- **Part V – Offences**
 - There are provisions in the online child sexual abuse offences that will allow child pornography to be used for bona fide scientific or medical research or law enforcement without consent and regard for privacy.
 - The bill adds a second layer of registration for internet cafes. This requirement will reduce the number of internet cafes in the country and, therefore, access to the internet. Also, it will add extra cost for café owners because the majority of our internet cafes today are not registered as companies, and the National Telecommunications Commission may not be adequately equipped to register these cafes quickly.
 - It may be impossible to implement and enforce a “breach of confidence by service providers” due to the lack of existing service level agreements (SLA) between the service providers and consumers and adequate enforcement of current consumer rights laws.
 - A corporation may be required to close its business and forfeit all of its assets if found guilty. Politicians and competitors can misuse these provisions.



Recommendations

- **Part V, section 38, subsection (3) – Online child sexual abuse**
 - Change to
 - *“Notwithstanding subsection (1) a person shall not be deemed to have committed an offence if he does an act intended for a bona fide scientific or medical research or law enforcement and followed the data protection and privacy laws of Sierra Leone”*
- Remove part V, section 40, subsection (1)b or add provisions to allow sole proprietor, enterprises and partnership businesses to register and operate a cybercafe.
- Require the Ministry of Information and NATCOM to develop standards that will require service providers to issue service level agreements (SLA) to consumers that can be honored
- **Part V, section 44, subsection (3) – Reporting cyber threats**
 - Change to
 - *“Notwithstanding subsection (1), where a body corporate is convicted of an offence under this Act, the Court may order that the body corporate shall pay a fine not exceeding [AMOUNT], or imprisonment for a period not exceeding [PERIOD], or both ”*

Executive Summary - Part VI - Administration And Enforcement

Findings

• Part VI - Administration And Enforcement

- The Minister will nominate the National Cyber Security Coordinator, who will head the National Cyber Security Incidence Response Coordination Center. The Minister is a political appointee with no cybersecurity experience; hiring incompetent individuals to lead that team could affect the citizens and the country's national security.
- The standards to determine the qualifications for the Computer security incident response team (CSIRT) are not stated in the bill.
- Concerns have been publicly raised by the Minister of Information and communications that Sierra Leone does not have Cybercrime legal practitioners at the moment. Having someone else leading this effort with little or no experience in Cybersecurity (threat and incident response) will be detrimental to the success of this bill's implementation. It might negatively impact citizens if poor decisions are made due to the lack of expertise.
- The fees levied on the service provided may lead to price hikes and, as a result, stifle technology innovation, access to financial services, affordable communications, and internet services.
- The head of the Financial Intelligence Unit (FIU) is not included in the National Cybersecurity Advisory Council. FIU is a critical player in fighting money laundering and terrorism, and the internet is used in committing these crimes
- The companies or institutions managing the national gateway into and out of sierra leone are not included in the National Cybersecurity Advisory Council.



Recommendations

• Part VI - Administration And Enforcement

- Add provisions to make The National Cyber Security Coordinator tenured like that of the Auditor-General or similar agencies upon parliament's approval.
- Make the National Cyber Security Coordinator public position to all and be strict on years of experience, excluding educational experience. The individual should have worked as a Cybersecurity expert for at least ten years and have worked in incident response threat and computer forensic. They have to understand compliance and must have a strong policy background in Cybersecurity.
- Consult other countries with reputable CSIRT institutions (other African countries, like Nigeria, South Africa, Rwanda, Etc.).
- Ensure that the CSIRT institution is unique and has the right individuals for each role. Remember, there will be lives of innocent citizens involved, and every wrong decision made will impact an individual wrongfully found guilty.
- Principles of scientific interpretation increase the reliability and defensibility of decisions throughout an investigation, not only in the final expert testimony phase. Such formalization of decision making is particularly valuable when dealing with digital evidence due to the potential for information overload, inaccuracy, error, and bias. To confront these challenges consistently and to reduce the risk of mistakes, it is vital to have qualified experts investigating these cases.
- Add the head of FIU and those of the companies or institutions managing our national internet/communications gateway. They have the tools to see the threats coming into Sierra Leone and going out of Sierra Leone.

Executive Summary - Part VII – Miscellaneous Provisions

Our Preliminary Findings

- **Part VII - Miscellaneous Provisions**
 - There are no related cybersecurity bills or laws referenced in the bill.
 - A standalone Cyber Crime bill without related laws for Data Protection and Privacy can leave loopholes for violating human rights, privacy, and data integrity.



Our Preliminary recommendations

- **Part VII - Miscellaneous Provisions**
 - Provide a reasonable and timely timeline for a Data Protection and Privacy bill.
 - Develop a "Search and Seizure of Digital Evidence" plan, law, or policy and guidelines.



HIGH-LEVEL FINDINGS AND RECOMMENDATIONS

High Level Findings and recommendations – Part II

Finding and Sections

Part II, Section 2, subsection (1) - Designation of Critical National Information Infrastructure

- No prior documentation, standards, policies or guidelines identifying or defining “**Critical National Information System**”
- It is best practice to define Critical Systems prior to enacting a Cyber Crime Act to ensure the right systems are included.

Part II, Section 3 - Audit and inspection of Critical National Information Infrastructure

- Computer systems cannot be audited properly if they are not designed and implemented using standards that require them to log every user and system activity.



Why it's important

- Potential abuse of power; it should not be arbitrary.

- This is important because computer systems need to be secured. The goal is to prevent the cybercriminal from gaining unauthorized access. If they manage to gain access, the activity logs will provide insights to investigate the crime.



Recommendation

- Clearly define “Critical National Information Infrastructure”.
- Use an independent expert body to develop and establish standards for what constitutes a “Critical National Information Infrastructure”.
- Need renewable credential system. We recommend three years.

- Create standards, policies, and guidelines that are followed by all vendors implementing critical information systems to ensure all system activities are logged to facilitate audits.

High Level Findings and recommendations – Part III (1/9)

Finding and Sections

Part III, Section 5, subsection (3) (a) & (b) - Search and seizure of stored computer data

- No legal procedures for search and seizure
- Digital evidence should not be accessed on site. After the search and seizure process, a chain of custody should be established until the evidence is assigned to a digital forensics expert to analyze and report his/her findings

Part III, Section 7, subsection (2) (b) & (c) – Production order

- Violation of consumers privacy. No data protection in place. Not all information described in this section may be relevant to a case.
- Electronic evidence should be relevant to the case, which cannot be defined until there is a case. During the warrant request, an investigator can request what is needed and the relevancy to the case.



Why it's important

- Without a clear definition of current best practices and defining practical evidence processing steps, targeted solutions to problems and weaknesses are impossible.

- It violates the rights of individuals to be free from unwarranted searches and seizures in their private spaces.



Recommendation

- Create standards, policies, and guidelines followed by all vendors implementing critical information systems to ensure all system activities are logged to facilitate audits.

- Identify key challenges to privacy and outline the legal and technical protections available to the public.
- Create and enact strong data protection and privacy laws and reference them in this section
- Mandate security awareness training for all companies dealing with electronic devices connected to critical system

High Level Findings and recommendations – Part III (2/9)

Finding and Sections

Part III, Section 5, subsection (1) - Search and seizure of stored computer data

- Any police officer or authorized person without adequate training or qualification in cybercrimes can apply to a judge of the High Court.
- The qualifications of the "authorized person" is not defined
- Reasonable grounds is not defined
- No clear description or qualification and authority
- 'reasonably required' is not defined
- The standards to be used by the judge to validate that the police officer is qualified to investigate such crime

Part III, Sections (4) Scope of powers and procedures, (5) Search and seizure of stored computer data, (6) Record of and access to seized data and (7) Production order

- No assurance is given to the public that electronic evidence will be handled with due process and by a professional.
- Data protection and privacy may not be respected when a search is extended to related systems

Why it's important

- A loophole for abuse of authority
- An unqualified police officer can mishandle evidence and violate citizens human rights and privacy and any person or organizations associated with the person being investigated.
- The "authorized person" can be anyone who may or may not qualify and, if not qualified, can mishandle evidence
- Cybercrimes are investigated by specialized law enforcement officers that are qualified in investigating cybercrimes, and they undergo regular training and certification

- Sierra Leone does not have data protection and privacy laws in place today. As a result, investigators and service providers can easily use this bill to violate the privacy of citizens

Recommendation

- Develop supporting standards, policies, procedures, and guidelines for recruiting and training law enforcement officers responsible for investigating cybercrimes.
- Develop supporting standards, policies, procedures, and guidelines for digital evidence processes based on industry standards and best practices.
- Change the phrase "police officer" to "trained and qualified law enforcement officer" with renewable credentials to investigate and prosecute cybercrimes.

- Define protocols for digital evidence
- Address data data protection and privacy concerns and follow established standards for ensuring privacy during investigation
- Make provision for dismissal of tampered evidence
- Define Chain of Custody

High Level Findings and recommendations – Part III (3/9)

Finding and Sections

Part III, Section 5, subsection (1) - Search and seizure of stored computer data.

- The term “Police Officer” is used. A police officer may not be qualified to handle electronic evidence.
- In most cases, professionalism is not being used when there is an investigation. Sometimes, it ends up worse than pre-investigation of the said Cyber Crime. There should be special task force to investigate and make an arrest for such crimes. These officers should be familiar with Cyber and the policies, standards and guidelines involved in this area. Not every police officer should handle such cases.

Part III, Section 8, subsection (5).c – Expedited preservation and partial disclosure of traffic data.

- Forcing an accused to render any information to aid an investigation without his/her lawyer's presence is a violation of their rights.

Why it's important

- The usage of "Police Officer" may lead to improper handling of evidence during a search and seizure.

Recommendation

- Change “police officer” to “law enforcement officer” with credentials to investigate cybercrimes
- Replace “Police Officer” with “Investigating Officer” An Investigating Officer must be qualified.

High Level Findings and recommendations – Part III (4/9)

Finding and Sections

Part III, Section 5, subsection (4) - Search and seizure of stored computer data.

- How does this authorized personnel extend search across borders? Assume the other computer system is in the USA or other EU countries with different computer or cyber policy specific to that nation.

Part III, Section 6, subsection (4) - Record of and access to seized data.

- Data intended to be used as evidence must be securely accessed or copied to preserve the integrity of the data.

Part III, Section 7, subsection (1) - Record of and access to seized data.

- From a data or Cyber-related point of view, whoever is requesting a service provider outside of Sierra Leone to provide service to an institution in Sierra Leone must be knowledgeable on the other country's data governance laws. Not sure if a Sierra Leone Judge can order a request like that.

Why it's important

Deliberately left blank
Referenced in other slides

Recommendation

Deliberately left blank
Referenced in other slides

High Level Findings and recommendations – Part III (5/9)

Finding and Sections

Part III, Section 5, subsection (7) - Search and seizure of stored computer data.

- 'Misuse of powers' is not defined

Part III, Section 5, subsection (8) - Search and seizure of stored computer data.

- Vague and arbitrary
- Why is it the Minister that should prescribe punishment?

Part III, Section 7, subsection (2) – Production order

- No data protection policy or legislation in place to protect the privacy and rights of individuals.
- For example, billing and payment information may not need to be disclosed for certain investigations.
- See also subsection 6, subparagraph (f); section 5, subsection (5); and section 6, subsection (2), subparagraph (b).

Why it's important

- If service providers are forced to hand over subscriber data, they may release more data to investigators than necessary for the case in question if they have collected and stored the information in such a way that does not allow them to reveal only the required data items selectively. This would infringe on individuals' privacy, putting potentially confidential information at risk of disclosure to unauthorised parties.

Recommendation

- The process and requirement to obtain and use data as evidence should be defined in the context of data privacy and rights of the individual.
- Stipulate in data privacy and protection regulations a Data Minimization requirement for service providers who collect and store user data, as in the EU's GDPR.
- If data privacy and protection regulations cannot be enacted before the Cybercrime bill is passed, ensure there is a separate section or clause that stipulates the data minimization requirement and make it apply to all entities that will collect and/or store user data.

High Level Findings and recommendations – Part III (6/9)

Finding and Sections

Part III, Section 8, subsection (2) - Expedited preservation and partial disclosure of traffic data.

Part III, Section 10, subsection (1) - Interception of content data.

- Too broad, therefore potential for abuse of powers, especially as smartphones are classed as computer systems and data privacy laws do not exist - To “collect or record content data of ... transmission,” could easily be repressively abused



Why it's important

- This effectively allows service providers and the government to snoop on users' communications. It could easily be repressively abused.



Recommendation

Deliberately left blank
Referenced in other slides

High Level Findings and recommendations – Part III (7/9)

Finding and Sections

Part III, Section 8, subsection (1) – Expedited preservation and partial disclosure of traffic data.

- You cannot acquire evidence for criminal investigation and stated such risk on the data. In digital evidence processing, the most critical effort is to ensure that the evidence is not tampered with, modified, lost or rendered inaccessible in any form.

Part III, Section 8, subsection (5) – Expedited preservation and partial disclosure of traffic data.

- We found this to be vague. We assumed this section refers to "an authorised" person attempting to collect evidence or who can request police assistance?
- The word "mutual" is also vague and without clear definitions of who or what "mutual assistance" refers to leaves room for discretion, improper evidence process and a violation of privacy and human rights.

Why it's important

- If they ignore proper forensics practice to process electronic evidence and continue as described, they risk destroying vital evidence or having evidence inadmissible in a court of law.
- The lack of laws to mandate regulatory compliance and liability if specific data are not adequately protected could cause severe legal ramifications.
- Adding the aptitude to practice sound digital forensics will ensure the overall integrity of evidence presented in court.
- A good understanding of the legal and technical aspects will help capture vital information to prosecute a case if the intruder is caught.

Recommendation

- Develop Data Protection and Privacy Acts.
- Create policies, procedures and guidelines for:
 - Investigation request process
 - Collecting and handling evidence
 - Chain of custody
 - Device collection
 - Email collection
 - Storage and inventory
 - Evidence examination process
 - Evidence analysis, and
 - Evidence reporting
- Establish a Forensics Lab to include
 - Restricted access
 - Tools including hardware and software
 - Personnel Qualifications

High Level Findings and recommendations – Part III (8/9)

Finding and Sections

Part III, Section 9, subsection (3) - Real-time collection of traffic data

- No directives or laws to maintain privacy while collecting data in real-time during transmission.
- No mechanisms in place to be able to decrypt and encrypted data being transmitted?

Part III, Section 10, subsection (1) - Interception of content data

- The government or anyone should not be snooping on any citizen's data without their consent. This is a violation of one's privacy. Also, no clear definition of "serious offence" in this case?



Why it's important

Deliberately left blank
Referenced in other slides



Recommendation

Deliberately left blank
Referenced in other slides

High Level Findings and recommendations – Part III (9/9)

Finding and Sections

Part III, Section 10, subsection (3) (a) (b) - Interception of content data

- It is possible that the owner of the computer system is not the one committing the crime (or know nothing about a crime being committed with his/her computer system)—no clear guide on how the privacy of the owner of the computer system will be protected.



Why it's important

Deliberately left blank
Referenced in other slides



Recommendation

Deliberately left blank
Referenced in other slides

Findings and recommendations – Part IV (1/4)

Finding and Sections

Part IV, Section 13, subsection (1) - Spontaneous information

- This section is very open and has the potential for misuse. The Attorney-General will have too much power to disclose information to foreign states
- In the absence of standalone data protection and privacy law and clear definition of “Such condition”, the Attorney-General may be using their judgement to determine what is confidential and that is an area of concern for the misuse of power

Part IV, Section 14, subsection (1) - Powers of the Attorney-General

- Any foreign state or international agency may not be an appropriate language. What about foreign states and international agencies with which Sierra Leone has no international relationships and does not follow appropriate international human rights, data protection, and privacy laws?

Why it's important

- The information may have been obtained illegally without consent. The Attorney-General is not a cybercrime expert and may not have the required skills, tools and ability to prove that (1) the foreign state requesting the information had followed the laws of its state and international laws (2) That prescribed standards and processes were followed when the information was obtained in Sierra Leone.

Recommendation

- Recommendation for Part IV, Section 13, subsection 1

Findings and recommendations – Part IV (2/4)

Finding and Sections

Part IV, Section 15, subsection (2)a & b - Authority to make and act on mutual assistance requests

- “terms and conditions” and “such conditions” are not clearly defined anywhere. What are these terms and conditions? What existing standards, policies or guidelines will be followed to guide what is included or excluded in the terms and conditions stated here.

Part IV, Section 15, subsection (6) - Authority to make and act on mutual assistance requests

- Foreign states can request Sierra Leone to keep confidential the facts of any requests for mutual assistance. However, there is no reciprocal statement for Sierra Leone to ask the foreign state to be confidential

Why it's important

Deliberately left blank
Referenced in other slides

Recommendation

Deliberately left blank
Referenced in other slides

Findings and recommendations – Part IV (3/4)

Finding and Sections

Part IV, Section 17 - Confidentiality and limitation of use

1. Sierra Leone will be allowed to provide information that may include PII to foreign states and agencies without a mutual assistance treaty or arrangement.

Part IV, Section 18, subsection (1) - Expedited preservation of stored computer data

1. Sierra Leone or a foreign state or agency may request the expeditious preservation of data stored for mutual assistance, search, access, seizure and security or disclosure of the data without following due process. This will make it possible for the GoSL or foreign states to access data that is private and open it to misuse.

Part IV, Section 18, subsection (3) - Expedited preservation of stored computer data

1. “all appropriate measures” and “preserve the specified data in accordance with the procedures” may be misinterpreted very easily. What is considered appropriate measures according to this bill? The procedures to properly preserve data is not specified or referenced in this bill.

Why it's important

Deliberately left blank
Referenced in other slides

Recommendation

Deliberately left blank
Referenced in other slides

Findings and recommendations – Part IV (4/4)

Finding and Sections

Part IV, Section 19, subsection (2)a - Expedited disclosure of preserved traffic data

- An exception is made for political offence or offences related to a political offence

Part IV, Section 20, subsection (1) - Mutual assistance regarding accessing of stored computer data

- We were unable to find statements related to data protection and privacy laws to be followed

Part IV, Section 21, subsection (1) - Trans-border access to stored computer data

Part IV, Section 22, subsection (1) - Mutual assistance in real time collection of traffic data

Part IV, Section 23, subsection (1) - Mutual assistance regarding interception of content data

Why it's important

Deliberately left blank
Referenced in other slides

Recommendation

Deliberately left blank
Referenced in other slides

High Level Findings and recommendations – Part V (1/6)

Finding and Sections

Part V, Section 25, subsection (1)

Unauthorised access.

- Vague and concentrated power given to the Minister and Judges.
- Too arbitrary to leave sentencing decisions to the Minister and Judges.



Why it's important

- A Minister is a member of the Executive Branch and a Cabinet Member that can be replaced at any time by the President. They may not be a disinterested party for want of favor
- This will open a wide door for unfair adjudication of matters



Recommendation

- Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "[Cybercrimes \(Prohibition, prevention, ECT\) Act, 2015](#)", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at [PART II - Offences , Section 4, subsection \(1\) of the HIPCAR Model Policy Guidelines and Legislative Text](#)
- Change the text in Part V, Section 25, subsection (1) Unauthorised access to the following; "A person, including a corporation, partnership, or association, who intentionally and without authorisation causes a computer system to perform a function with intent to secure access to the whole or a part of a computer system or to enable such access to be secured, commits an offence and is liable upon conviction to imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both."

High Level Findings and recommendations – Part V (2/6)

Finding and Sections

Part V, Section 26, subsection (1)
Unauthorised access to protected system.

Part V, Section 27, subsection (1) -
Unauthorised data interception.

Part V, Section 28, subsection (a) -
Unauthorised data interference.

Part V, Section 29 subsection - Unauthorised
system interference.

Part V, Section 30 subsection 1 - Misuse of
device.

Why it's important

- It is important to make sure that application of the law is not arbitrary but on the specifics predetermined without bias.
- It does not take into account trained security professionals who may have to conduct security audits on systems (so-called “ethical hackers.” This may make it difficult for them to carry out their duties.

Recommendation

- Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "[Cybercrimes \(Prohibition, prevention, ECT\) Act, 2015](#)", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at [PART II - Offences , Section 4, subsection \(1\) of the HIPCAR Model Policy Guidelines and Legislative Text](#)
- Make exceptions for so-called “ethical” hackers who are trained to detect vulnerabilities in computer systems and networks. For example, see Section 30, subsection (2).

High Level Findings and recommendations – Part V (3/6)

Finding and Sections

Part V, Section 31 subsection – Unauthorised disclosure of password.

Part V, Section 32 subsection (1) – Computer-related forgery.

Part V, Section 32 subsection – Computer fraud.



Why it's important

- It is important to make sure that application of the law is not arbitrary, but on the specifics predetermined without bias.
- The reference of data in context needs some clarification.



Recommendation

- Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "[Cybercrimes \(Prohibition, prevention, ECT\) Act, 2015](#)", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at [PART II - Offences , Section 4, subsection \(1\) of the HIPCAR Model Policy Guidelines and Legislative Text](#)
- Basic Computer Awareness training is needed
- This goes back to the responsibilities of the institutions. Do they have Security Awareness Trainings in place to educate their users on computer usage, etc.?
- If such happens, who will be responsible for the alteration of the data in question? What is the institution doing to prevent the occurrences of data alteration?

High Level Findings and recommendations – Part V (4/6)

Finding and Sections

Part V, Section 33 subsection (1)– Identity theft and impersonation.

Part V, Section 34 subsection (1) – Electronic signature.

Part V, Section 35 subsection (1)– Cyber stalking and cyber bullying.

Part V, Section 36 subsection – Cyber Squatting.

Part V, Section 37 subsection – Infringements of copyright and related rights.

Part V, Section 38 subsection – Online child sexual abuse.

Why it's important

- It is important to make sure that application of the law is not arbitrary but on the specifics predetermined without bias.
- Could easily be abused
- “Ought to know” too ambiguous

Recommendation

- Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "[Cybercrimes \(Prohibition, prevention, ECT\) Act, 2015](#)", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at [PART II - Offences , Section 4, subsection \(1\) of the HIPCAR Model Policy Guidelines and Legislative Text](#)
- Add “for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent,” to subparagraph (a) of Section 35, subsection (2),
- Clear definition of “ought to know” needs to be noted

High Level Findings and recommendations – Part V (5/6)

Finding and Sections

Part V, Section 39 subsection (1) – Attempting and aiding or abetting.

Part V, Section 40 subsection (1), B – Registration of Cybercafes.

Part V, Section 41 subsection – Cyber terrorism.

Part V, Section 42 subsection – Racist and xenophobic offences.

Part V, Section 43 subsection – Reporting cyber threats.

Part V, Section 44 subsection – Breach of confidence by service providers.

1.



Why it's important

- It is important to make sure that application of the law is not arbitrary, but on the specifics predetermined without bias.



Recommendation

- Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria ["Cybercrimes \(Prohibition, prevention, ECT\) Act, 2015"](#), you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at [PART II - Offences , Section 4, subsection \(1\) of the HIPCAR Model Policy Guidelines and Legislative Text](#)
- A fine must be defined.
- Share the burden with purchaser

High Level Findings and recommendations – Part V (6/6)

Finding and Sections

Part V, Section 41 subsection – Cyber terrorism.

Part V, Section 42 subsection – Racist and xenophobic offences.

Part V, Section 43 subsection – Reporting cyber threats.

Part V, Section 44 subsection – Breach of confidence by service providers.

Part V, Section 45 subsection – Employees responsibility.

Part V, Section 46 subsection (2) – Corporate liability.



Why it's important

- It is important to make sure that application of the law is not arbitrary but on the specifics, predetermined without bias.



Recommendation

- Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "[Cybercrimes \(Prohibition, prevention, ECT\) Act, 2015](#)", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at [PART II - Offences , Section 4, subsection \(1\) of the HIPCAR Model Policy Guidelines and Legislative Text](#)

High Level Findings and recommendations – Part VI (1/3)

Finding and Sections

Part VI, Section 47 subsection (1) & (2) – Corporate liability.

- There is a concern that the head of this position is based on an appointment by the Minister.
- There is already concern that SL does not have Cybercrime legal practitioners. Having someone else leading this effort with little or no experience in Cybersecurity (threat and incident response) will be detrimental to this bill's implementation and might negatively impact citizens if poor decisions are made due to the lack of expertise.
- The CSIRT head is unlike being a head of IT. This individual should have some good years of cybersecurity experience, no criminal record (corruption included). Otherwise, there could be bias in investigating and solving sensitive issues that pertain to specific people or persons in question of an incident. The motivation will be different if the person in charge is acting independently, based on their expertise and integrity. Rather than through connection.



Why it's important

- If for any reason, an incompetent individual is serving as the head in this position, that individual could make poor decisions. And those decisions could affect innocent citizens



Recommendation

- Make the position public to all and be strict on years of experience, excluding educational experience. The individual should have worked as a Cybersecurity expert for at least ten years and have worked in incident response and threat, computer forensic, Etc. They have to understand compliance and have a strong policy background in Cybersecurity

High Level Findings and recommendations – Part VI (2/3)

Finding and Sections

Part VI, Section 47, subsection (2) a to f – Corporate liability.

- Does the government have a cybercrime team?
- What are the minimum experience requirement for a SL CSIRT personnel?



Why it's important

- Principles of scientific interpretation increase the reliability and defensibility of decisions throughout an investigation, not only in the final expert testimony phase. Such formalization of decision making is particularly valuable when dealing with digital evidence due to the potential for information overload, inaccuracy, error and bias. To confront these challenges consistently and to reduce the risk of mistakes, it is important to have qualified experts investigating these cases.



Recommendation

- Consult other countries with reputable CSIRT institutions (other African countries, like Nigeria, South Africa, Rwanda, Etc.)
- Ensure that this institution is unique and have the right individuals for each area. Remember, there will be lives of innocent citizens involved, and every wrong decision made will impact an individual found guilty wrongfully.

High Level Findings and recommendations – Part VI (3/3)

Finding and Sections

Part VI, Section 49, subsection (1) d – Functions and powers of Council

- I don't see any area on the bill that states how often the bill will be reviewed or revisited; including periodic amendment by the National Cybersecurity Advisory Council Committee.
- This is not much of a finding, but rather a question. Will the promotion of the educational program, research, etc. be in collaboration with other institutions in the country.



Why it's important

- Anything computer and cyber related, changes everyday and it is best practice to revisit the bill periodically and make amendment where necessary
- Will there be a cybersecurity awareness month. Are there any established curriculum already for schools and institutions?



Recommendation

- Make room to update the bill periodically and establish version control on the bill.
- The bill should include teachings of computer and cybercrime, including data privacy, in early education to university level, and within businesses and government institutions.

High Level Findings and recommendations – Part VII

Finding and Sections

Part VII, Section 51– as it considers necessary or expedient for giving effect to Regulation.

- There are no related cybersecurity bills or laws referenced in the bill.



Why it's important

- A standalone Cyber Crime bill, without related laws for Data Protection and Privacy, can leave loopholes for violation of human rights, privacy and data integrity.



Recommendation

- Provide a reasonable and timely timeline for a Data Protection and Privacy bill.
- Develop a "Search and Seizure of Digital Evidence" plan, law, or policy and guidelines.



Review Committee Team Members

Review Committee Team Members



Tamba Lamin

DPS. M.Sc., Tech. Mgmt.
Certified Tech. Architect
President, SLinT.



Evelyn Lewis

BA. Info. System.
Techpreneur & Executive
Board Member, SLinT



**Aminata Kondeh
(SSCP)**

M.Sc., Digital Forensics & Cyber
Investigations
Executive Board Member, SLinT



**Alie Bangura
(CISSP, PMP)**

Executive Board Member,
SLinT



Akindele Decker

Poet, Writer and
Digital Heritage
Professional



Mohamed K. Musa

M.Sc., Software Engineering
Adjunct Professor,
Cybersecurity



Daniel Chaytor

M.Sc., Software Engineering
Lecturer and Head of
Department, IPAM



Desmond Macfoy

MBA, BEng
Chief Operating Officer at
KNS



Mohamed Lebbie

Malware Analyst
Researcher

Review Committee Team



Sahr Lebbie

Vice-President,
Executive Board
Member, SLinT



Salieu Mansaray

M.Sc., IT, MCP
ISOC Chairperson



Abdulai Swarray

M.Sc., Cybersecurity,
Executive Board
Member, SLinT



Thomas Songu

Ph.D. MIS
Head of ICT, Njala



**Confidential
Name, CISM**

M.Sc., MBA, CISM,
Certified Ethical Hacker



**Bintu Fatmata
Jonah, CISA, CISSP**

M.Sc., IT



**SLINT General
Members**

Sierra Leonean



**Emmanuel Saffa-
Abdulai**

Solicitor, Barrister-at-law



Elvis T. Enoch

Solicitor, Barrister-at-law

Contact Details

Sierra Leoneans in Technology (SLinT) 

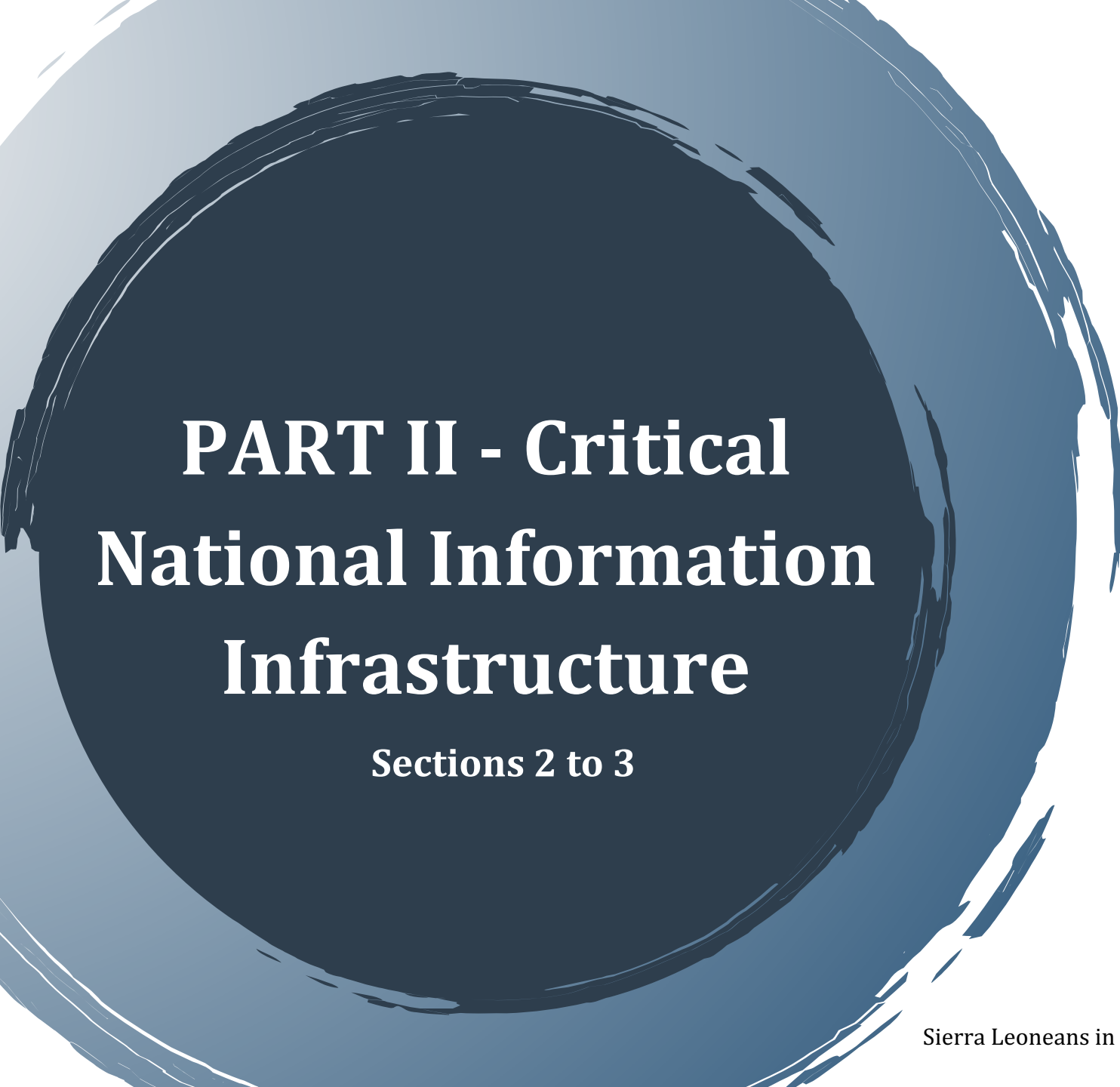
+1 (240) 812-9133 

info@slint.org 

<https://members.slint.org> | <https://slint.org> 



DETAIL FINDINGS AND RECOMMENDATIONS



PART II - Critical National Information Infrastructure

Sections 2 to 3

Part II-Critical National Information Infrastructure

2. Designation of certain computer systems as Critical National Information Infrastructure.
3. Audit and inspection of Critical National Information Infrastructure

Part II-Critical National Information Infrastructure

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

6	No.	The Cyber Crime Act	2020
PART II-CRITICAL NATIONAL INFORMATION INFRASTRUCTURE			
Designation of Critical National Information Infrastructure.	2	(1) The President may, on the recommendation of the Minister by Order published in the Gazette, designate certain computer systems, computer data or traffic data vital to Sierra Leone or any combination of those matters, as constituting Critical National Information Infrastructure.	
	(2)	A Presidential Order made under subsection (1), may prescribe minimum standards, guidelines, rules or procedures in respect of -	
	(a)	the protection or preservation of Critical National Information Infrastructure;	
	(b)	the general management of Critical National Information Infrastructure;	
	(c)	access to, transfer and control of data in Critical National Information Infrastructure;	
	(d)	infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any designated Critical National Information Infrastructure;	
	(e)	the storage or archiving of data or information designated as Critical National Information Infrastructure;	
	(f)	recovery plans in the event of disaster, breach or loss of the Critical National Information Infrastructure or any part of it; and	
	(g)	any other matter required for the adequate protection, management and control of data and other resources in any Critical National Information Infrastructure.	

No.	The Cyber Crime Act	2020	7
3	A Presidential Order made under subsection (1) of section 2 may require the National Computer Security Incident Response Team established by the coordinating body under paragraph (c) of subsection (1) of section 47 to audit and inspect any Critical National Information Infrastructure at any time to ensure compliance with this Act.	Audit and inspection of Critical National Information Infrastructure	
PART III - POWERS AND PROCEDURES			
4	(1) Powers and procedures under this Act shall be applicable to and may be exercised with respect to -	Scope of powers and procedures	
	(a)	criminal offences under this Act;	
	(b)	criminal offences committed by means of a computer system, including mobile phones and other electronic equipment, under any other law; and	
	(c)	the collection of evidence in electronic form of a criminal offence under this Act or any other law.	
	(2)	In a trial of an offence under any law, the fact that evidence has been generated, transmitted or seized from or identified in a search of a computer system, shall not of itself prevent that evidence from being presented, relied upon or admitted.	
5	(1) Upon an application by a police officer or other authorised person to a Judge of the High Court that there is reasonable grounds to believe that there may be in a specified computer system, program, data, computer data storage medium material which -	Search and seizure of stored computer data.	
	(a)	may be reasonably required as evidence in proving a specifically identified offence in a criminal investigation or criminal proceedings;	

Part II, Section 2, subsection (1) - Designation of Critical National Information Infrastructure

- No prior documentation, standards, policies or guidelines identifying or defining “Critical National Information System”

- Potential for abuse of power; it should not be arbitrary.

- What constitutes a “Critical National Information Infrastructure” should be predefined.
- Use an independent expert body to develop and establish standards and policies for what constitutes a “Critical National Information Infrastructure.”
- Need renewable personnel cybersecurity and clearance credentialing system.

Part II, Section 3 - Audit and inspection of Critical National Information Infrastructure

- Computer systems cannot be audited properly if they are not designed and implemented using standards that require them to log every user and systems activity.

- This is important because computer systems need to be secured. The goal is to prevent the cybercriminal from gaining unauthorized access. If they manage to gain access, the activity logs will provide insights to investigate the crime

- Create standards, policies, and guidelines to be followed by all vendors implementing critical information systems to ensure all system activities are logged to facilitate audits.

PART III - Powers and Procedures

Sections 4 to 12

Part III: Powers and Procedures

- 4.Scope of powers and procedures.
- 5.Search and seizure of stored computer data.
- 6.Record of and access to seized data.
- 7.Production order.
- 8.Expedited preservation and partial disclosure of traffic data.
- 9.Real-time collection of traffic data.
- 10.Interception of content data.
- 11.Confidentiality and limitation of liability.
- 12.Territorial jurisdiction.

Part III: Powers and Procedures – slide 1 of 7

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

8	No.	The Cyber Crime Act	2020
(b) has been acquired by a person as a result of the commission of an offence]			
the Judge may issue a warrant which shall authorise the police officer or other authorised person, with such assistance as may be necessary, to access, seize or secure a specified computer system, program, data or computer data storage medium.			
(2) A warrant issued under subsection (1) shall authorise a police officer or other authorised person to -			
(a) seize or secure a computer system or part of it or a computer-data storage medium;			
(b) make and retain a copy of computer data;			
(c) maintain the integrity of stored computer data;			
(d) render inaccessible or remove computer data in the accessed computer system;			
(e) have access to, inspect and check the operation of a computer system to which the warrant applies;			
(f) have access to any information, code or technology which has the capability of unscrambling encrypted data contained or available to a computer system into an intelligible format for the purpose of the warrant;			
(g) require a person possessing knowledge about the functioning of a computer system or measures applied to protect a computer data thereon, to provide the necessary computer data or information, to enable a police officer or other authorised person in conducting an activity authorised under this section.			

12	No.	The Cyber Crime Act	2020
(2) For the purposes of this section, "subscriber information" means any information contained in the form of data or any form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, by which can be established -			
(a) the type of communication service used, the technical provisions taken thereto and the period of service;			
(b) the subscriber's identity, postal, geographic, electronic mail address, telephone and other access number, billing and payment information available on the basis of the service agreement or arrangement; or			
(c) any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.			
(3) A Judge of the High Court may, by order, require a person -			
(a) to whom an order is made under subsection (1), or			
(b) in control of a computer system, to whom a warrant issued under subsection (1) of section 5;			
to keep such order or warrant confidential.			
(4) A person who fails to comply with an order under subsection (1) commits an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.			
(5) A police officer or other authorised person who uses the powers granted under subsection (1) for a purpose other than that stated in subsection (6) commits an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.			

No.	The Cyber Crime Act	2020	9
(b) have access to such reasonable technical and other assistance as he may require for the purposes of the warrant.			
(3) An application under subsection (1) shall provide reasons explaining why it is believed that -			
(a) the material sought will be found on the premises to be searched; or			
(b) the purpose of a search may be frustrated or seriously prejudiced unless an investigating officer arriving at the premises can secure immediate entry to them.			
(4) Where a police officer or other authorised person authorised to search or access a specific computer system or part of it, under subsection (2), has grounds to believe that the data sought is stored in another computer system and such data is accessible from or available to the initial system, the police officer or other authorised person may extend the search or accessing to such other system or systems.			
(5) Computer data seized under subsection (2) shall only be lawfully used for the purpose for which it was originally obtained.			
(6) A police officer or other authorised person shall -			
(a) only seize a computer system under subsection (2) when it is -			
(i) not practical to seize or secure the computer data; or			
(ii) necessary to ensure that data will not be destroyed, altered or otherwise interfered with;			

No.	The Cyber Crime Act	2020	13
(6) An application under subsection (1) shall state the reasons explaining why it is believed that -			
(a) a specified computer data sought is likely to be available with a person mentioned in subparagraph (a) or (b) of subsection (1);			
(b) an investigation may be frustrated or seriously prejudiced unless the specified computer data or the subscriber information, as the case may be, is produced;			
(c) the type of evidence suspected is likely to be produced by a person mentioned in subparagraph (a) or (b) of subsection (1);			
(d) subscribers, users or unique identifiers who are the subject of an investigation or prosecution, may be disclosed as a result of the production of the specified computer data;			
(e) an identified offence is an offence in respect of which the order is sought;			
(f) measures taken shall prepare and ensure that the specified computer data will be produced -			
(i) whilst maintaining the privacy of other users, customers and third parties; and			
(ii) without the disclosure of data of any party who is not part of the investigation; and			
(g) measures taken shall prepare and ensure that the production of the specified computer data is carried out through technical means such			

Part III, Section 5, subsection (3) (a) & (b) - Search and seizure of stored computer data

- There are subjective legal issues on procedures for search and seizure.
- Digital evidence should not be accessed on-site. After the search and seizure process, a chain of custody should be established until the evidence is assigned to a digital forensics expert to analyze and report his/her findings.

Part III, Section 7, subsection (2) (b) & (c) – Production order

- Violation of consumers privacy. No data protection in place. Not all information described in this section may be relevant to a case.
- Electronic evidence should be relevant to the case, which cannot be defined until there is a case. During the warrant request, an investigator can request what is needed and the relevance to the case.

- Without a clear definition of current best practices outlining effective evidence processing, targeted solutions to problems and weaknesses are impossible.
- Create standards, policies, and guidelines that are followed by all investigating processes involved in evidence collection.
- Identify key challenges to privacy and outline the legal and technical protections available to the public.
- Create and enact strong data protection and privacy laws and reference them in this section.
- Mandate security awareness training for all companies dealing with electronic devices connected to critical systems.
- It violates the rights of individuals to be free from unwarranted searches and seizures in their private spaces.

Part III: Powers and Procedures cont. ...

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

8	No.	The Cyber Crime Act	2020
	(b)	has been acquired by a person as a result of the commission of an offence,	
		the judge may issue a warrant which shall authorise the police officer or other authorised person, with such assistance as may be necessary, to access, seize or secure a specified computer system, program, data or computer data storage medium.	
	(2)	A warrant issued under subsection (1) shall authorise a police officer or other authorised person to -	
	(a)	seize or secure a computer system or part of it or a computer-data storage medium;	
	(b)	make and retain a copy of computer data;	
	(c)	maintain the integrity of stored computer data;	
	(d)	render inaccessible or remove computer data in the accessed computer system;	
	(e)	have access to, inspect and check the operation of a computer system to which the warrant applies;	
	(f)	have access to any information, code or technology which has the capability of unscrambling encrypted data contained or available to a computer system into an intelligible format for the purpose of the warrant;	
	(g)	require a person possessing knowledge about the functioning of a computer system or measures applied to protect a computer data therein, to provide the necessary computer data or information, to enable a police officer or other authorised person in conducting an activity authorised under this section;	

30	No.	The Cyber Crime Act	2020
	(b)	exercise reasonable care while the computer system or computer data storage medium is retained.	
	(7)	A police officer or other authorised person who causes the powers granted under this section to be exercised in an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.	
	(8)	A person who obstructs a police officer or other authorised person in the lawful exercise of the powers under this section commits an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.	
	6.	(1) Where a computer system or data has been removed or rendered inaccessible, following a search or seizure, the person who made the search or seizure shall, at the time of the search or seizure or as soon as practicable after the search -	
	(a)	make a list of what has been seized or rendered inaccessible, with the date and time of seizure, and	
	(b)	give a copy of that list to -	
	(i)	the occupier of the premises; or	
	(ii)	the person in control of the computer system.	
	(7)	Subject to subsection (1), a police officer or other authorised person shall, on request, present a person -	
	(a)	who has custody or control of a computer system;	
	(b)	who has right to data or information seized under subsection (2) of section 5; or	
	(c)	acting on behalf of a person under subparagraph (a) or (b).	

No.	The Cyber Crime Act	2020	9
(b)	have access to such reasonable technical and other assistance as he may require for the purposes of the warrant.		
(3)	An application under subsection (1) shall provide reasons explaining why it is believed that -		
(a)	the material sought will be found on the premises to be searched; or		
(b)	the purpose of a search may be frustrated or seriously prejudiced unless an investigating officer arriving at the premises can secure immediate entry to them.		
(4)	Where a police officer or other authorised person authorised to search or access a specific computer system or part of it, under subsection (2), has grounds to believe that the data sought is stored in another computer system and such data is accessible from or available to the initial system, the police officer or other authorised person may extend the search or accessing to such other system or systems.		
(5)	Computer data seized under subsection (2) shall only be lawfully used for the purpose for which it was originally obtained.		
(6)	A police officer or other authorised person shall -		
(a)	only seize a computer system under subsection (2) when it is -		
(i)	not practical to seize or secure the computer data; or		
(ii)	necessary to ensure that data will not be destroyed, altered or otherwise interfered with;		

No.	The Cyber Crime Act	2020	31
	to access and copy computer data on the system or give such person a copy of the computer data.		
(7)	A police officer or other authorised person may refuse to give access to or provide copies seized under subsection (2) if he has reasonable grounds to believe that giving access to or providing copies would -		
(a)	constitute a criminal offence; or		
(b)	prejudice -		
(i)	an investigation; or		
(ii)	any prosecution.		
(8)	Notwithstanding subsection (3), a Judge of the High Court may, upon sufficient and reasonable grounds, allow a person under subparagraph (a) or (b) of subsection (2) to access or copy computer data.		
7.	(1) Where it is necessary or desirable for the purposes of an investigation, a Judge of the High Court may upon an application, order -		
(a)	a person in possession or control of specified data stored in a computer system or a computer data storage medium; or		
(b)	a service provider in possession or control of specified subscriber information relating to services offered -		
(i)	in Sierra Leone; or		
(ii)	based outside Sierra Leone but, offering its services in Sierra Leone.		
	to submit information in his possession or control.		

Part III, Section 5, subsection (1) - Search and seizure of stored computer data

- Any police officer or authorized person without adequate training or qualification in cybercrimes cannot apply for warrants.
- No clear description, qualification, and authority are defined for “Authorized person.”
- ‘Reasonable grounds’ is not defined.
- A judge must validate police officers requesting warrants through outlined standards and procedures.

Part III, Sections (4) Scope of powers and procedures, (5) Search and seizure of stored computer data, (6) Record of and access to seized data and (7) Production order

- No assurance is given to the public that electronic evidence will be handled with due process and by professionals.
- In the absence of data protection and privacy laws, search and seizure may be extended to systems that are not specified in the warrant.

- A loophole for abuse of authority
- An unqualified police officer can mishandle evidence and violate the privacy and human rights of the person being investigated and all other people or organizations connected to that person.
- An authorized person can be anyone who may or may not qualify, and if not qualified, can mishandle evidence.
- Cybercrimes are investigated by specialized law enforcement officers who are qualified to investigate cybercrimes and undergo regular training and certifications.

- Sierra Leone does not have data protection and privacy laws in place today. As a result, investigators and service providers can easily use this bill to violate the privacy of citizens

- Develop supporting standards, policies, procedures, and guidelines for recruiting and training law enforcement officers responsible for investigating cybercrimes.
- Develop supporting standards, policies, procedures, and guidelines for digital evidence processes based on industry standards and best practices.
- Change the phrase “police officer” to “trained and qualified law enforcement officer” with renewable credentials to investigate and prosecute cybercrimes.
- Define protocols for digital evidence collection and storage.
- Address data protection and privacy concerns and follow established standards for ensuring privacy during an investigation.
- Make provision for dismissal of tampered evidence.
- Define Chain of Custody.

Part III: Powers and Procedures cont. ...

Text from the Bill		Findings	Why is it important	Recommendations
8	No. The Cyber Crime Act 2020	No. The Cyber Crime Act 2020 9	Part III, Section 5, subsection (1) - Search and seizure of stored computer data. <ul style="list-style-type: none">Unqualified "Police Officer" may lead to improper handling of evidence during a search and seizure.Change “police officer” to “law enforcement officer” with credentials to investigate cybercrimes.	
<p>(b) has been acquired by a person as a result of the commission of an offence.</p> <p>the Judge may issue a warrant which shall authorise the police officer or other authorised person, with such assistance as may be necessary, to access, seize or secure a specified computer system, program, data or computer data storage medium.</p> <p>(2) A warrant issued under subsection (1) shall authorise a police officer or other authorised person to -</p> <p>(a) seize or secure a computer system or part of it or a computer-data storage medium;</p> <p>(b) make and retain a copy of computer data;</p> <p>(c) maintain the integrity of stored computer data;</p> <p>(d) render inaccessible or remove computer data in the accessed computer system;</p> <p>(e) have access to, inspect and check the operation of a computer system to which the warrant applies;</p> <p>(f) have access to any information, code or technology which has the capability of unscrambling encrypted data contained or available to a computer system into an intelligible format for the purpose of the warrant;</p> <p>(g) require a person possessing knowledge about the functioning of a computer system or measures applied to protect a computer data therein, to provide the necessary computer data or information, to enable a police officer or other authorised person in conducting an activity authorised under this section;</p>		<p>(b) have access to such reasonable technical and other assistance as he may require for the purposes of the warrant.</p> <p>(3) An application under subsection (1) shall provide reasons explaining why it is believed that -</p> <p>(a) the material sought will be found on the premises to be searched; or</p> <p>(b) the purpose of a search may be frustrated or seriously prejudiced unless an investigating officer arriving at the premises can secure immediate entry to them.</p> <p>(4) Where a police officer or other authorised person authorised to search or access a specific computer system or part of it, under subsection (2), has grounds to believe that the data sought is stored in another computer system and such data is accessible from or available to the initial system, the police officer or other authorised person may extend the search or accessing to such other system or systems.</p> <p>(5) Computer data seized under subsection (2) shall only be lawfully used for the purpose for which it was originally obtained.</p> <p>(6) A police officer or other authorised person shall -</p> <p>(a) only seize a computer system under subsection (2) when it is -</p> <p>(i) not practical to seize or secure the computer data; or</p> <p>(ii) necessary to ensure that data will not be destroyed, altered or otherwise interfered with;</p>		<p>● The term “Police Officer” is used; a police officer may not be qualified to handle electronic evidence.</p> <p>● There should be special task forces to investigate and make an arrest for cyber-related crimes.</p>
34	No. The Cyber Crime Act 2020	No. The Cyber Crime Act 2020 35	Part III, Section 8, subsection (5),c – Expedited preservation and partial disclosure of traffic data. <ul style="list-style-type: none">Forcing an accused to render any information to aid an investigation without the presence of his/her lawyer is a violation of their rights.	
<p>Expedited preservation and partial disclosure of traffic data</p> <p>as mirroring or copying of relevant data and not through physical custody of computer systems or devices.</p> <p>8 (1) A police officer or other authorised person may, where he is satisfied that -</p> <p>(a) a specified computer data stored in a computer system or computer data storage medium is reasonably required for the purposes of a criminal investigation; and</p> <p>(b) there is a risk or vulnerability that the computer data may be modified, lost, destroyed or rendered inaccessible,</p> <p>by written notice given to a person in possession or control of the computer system or computer data storage medium, require that person to undertake expedited preservation of the computer data.</p> <p>(2) A notice under subsection (1) may require a person in possession or control of the computer system or computer data storage medium to disclose sufficient traffic data about the communication to identify-</p> <p>(a) the service providers; and</p> <p>(b) the path through which the communication was transmitted.</p> <p>(3) The period of preservation of data required under subsection (1) shall not exceed 90 days.</p> <p>(4) The period of preservation of data under subsection (3) may be extended by a Judge of the High Court for a further specified period of time, on an application by a police officer or other authorised person, where such extension is reasonably required for the purposes of -</p>		<p>(a) an investigation or prosecution;</p> <p>(b) avoiding a risk or vulnerability that the computer data may be modified, lost, destroyed or rendered inaccessible; or</p> <p>(c) averting overly burdensome cost of such preservation on the person in control of the computer system.</p> <p>(7) A person to whom a notice under subsection (1) is given shall-</p> <p>(a) be responsible to preserve the data for -</p> <p>(i) a period not exceeding 90 days as specified in subsection (3); or</p> <p>(ii) any extended period permitted by a Judge of the High Court under subsection (4).</p> <p>(b) respond expeditiously to requests for assistance, whether to facilitate requests for police assistance or mutual assistance requests; and</p> <p>(c) disclose as soon as practicable, a sufficient amount of the raw content data to enable a police officer or other authorised person to identify any other telecommunications providers involved in the transmission of the communication.</p> <p>9 (1) Where there are reasonable grounds to believe that traffic data associated with specified communications is reasonably required for the purposes of a specific criminal investigation, a Judge of the High Court may, on an application by a police officer or other authorised person, order a service provider to-</p> <p>Real-time collection of traffic data.</p>		

Part III: Powers and Procedures cont. ...

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

30	No.	The Cyber Crime Act	2020
	(b)	exercise reasonable care while the computer system or computer data storage medium is retained.	
	(7)	A police officer or other authorised person who misuses the powers granted under this section commits an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.	
	(8)	A person who obstructs a police officer or other authorised person in the lawful exercise of the powers under this section commits an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.	
Record of and access to seized data.	6.	(1) Where a computer system or data has been removed or rendered inaccessible, following a search or seizure, the person who made the search or seizure shall, at the time of the search or seizure or as soon as practicable after the search -	
	(a)	make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and	
	(b)	give a copy of that list to -	
	(i)	the occupier of the premises; or	
	(ii)	the person in control of the computer system.	
	(2)	Subject to subsection (1), a police officer or other authorised person shall, on request, permit a person -	
	(a)	who has custody or control of a computer system;	
	(b)	who has right to data or information seized under subsection (2) of section 5; or	
	(c)	acting on behalf of a person under subparagraph (a) or (b).	

No.	The Cyber Crime Act	2020	11
		to access and copy computer data on the system or give such person a copy of the computer data.	
	(3)	A police officer or other authorised person may refuse to give access to or provide copies seized under subsection (2) if he has reasonable grounds to believe that giving access to or providing copies would -	
	(a)	constitute a criminal offence; or	
	(b)	prejudice -	
	(i)	an investigation; or	
	(ii)	any prosecution.	
	(4)	Notwithstanding subsection (3), a Judge of the High Court may, upon sufficient and reasonable grounds, allow a person under subparagraph (a) or (b) of subsection (2) to access or copy computer data.	
	7.	(1) Where it is necessary or desirable for the purposes of an investigation, a Judge of the High Court may upon an application by a police officer or other authorised person, order -	
	(a)	a person in possession or control of specified data stored in a computer system or a computer data storage medium; or	
	(b)	a service provider in possession or control of specified subscriber information relating to services offered -	
	(i)	in Sierra Leone; or	
	(ii)	based outside Sierra Leone but, offering its services in Sierra Leone;	
		to submit information in his possession or control.	

Part III, Section 6, subsection (4) - Record of and access to seized data.

- Data intended to be used as evidence must be securely accessed or copied to preserve the integrity of the data.

Part III, Section 7, subsection (1) - Record of and access to seized data.

- To collect evidence from a service provider whose data resides in another country, the investigating officer must understand the governance laws where the data is stored.

See recommendations on Data Protection and Privacy laws.

Part III: Powers and Procedures cont. ...

Text from the Bill

Findings

Why is it important

Recommendations

10 No. The Cyber Crime Act 2020

(b) exercise reasonable care while the computer system or computer data storage medium is retained.

(7) A police officer or other authorised person who manages the powers granted under this section commits an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.

(8) A person who obstructs a police officer or other authorised person in the lawful exercise of the powers under this section commits an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.

(9) Where a computer system or data has been damaged or rendered inaccessible, following a search or seizure, the person who made the search or seizure shall, at the time of the search or seizure or as soon as practicable after the search -

(a) make a list of what has been seized or rendered inaccessible, with the date and time of seizure; and

(b) give a copy of that list to -

(i) the occupier of the premises; or

(ii) the person in control of the computer system.

(7) Subject to subsection (3), a police officer or other authorised person shall, on request, permit a person -

(a) who has custody or control of a computer system;

(b) who has right to data or information seized under subsection (2) of section 5; or

(c) acting on behalf of a person under subparagraph (a) or (b).

11 No. The Cyber Crime Act 2020

(2) For the purposes of this section, "subscriber information" means any information contained in the form of data or any form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, by which can be established -

(a) the type of communication service used, the technical provisions taken thereto and the period of service;

(b) the subscriber's identity, postal, geographic, electronic mail address, telephone and other access number, billing and payment information available on the basis of the service agreement or arrangement; or

(c) any other information on the site of the installation of communication equipment available on the basis of the service agreement or arrangement.

(3) A Judge of the High Court may, by order, require a person -

(a) to whom an order is made under subsection (1); or

(b) in control of a computer system, to whom a warrant issued under subsection (1) of section 5.

to keep such order or warrant confidential.

(4) A person who fails to comply with an order under subsection (3) commits an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.

(5) A police officer or other authorised person who uses the powers granted under subsection (1) for a purpose other than that stated in subsection (4) commits an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.

No. The Cyber Crime Act 2020 11

to access and copy computer data on the system or give such person a copy of the computer data.

(3) A police officer or other authorised person may refuse to give access to or provide copies under subsection (2) if he has reasonable grounds to believe that giving access to or providing copies would -

(a) constitute a criminal offence; or

(b) prejudice -

(i) an investigation; or

(ii) any prosecution.

(4) Notwithstanding subsection (3), a Judge of the High Court may, upon sufficient and reasonable grounds, allow a person under subparagraph (a) or (b) of subsection (2) to access or copy computer data.

7 (1) Where it is necessary or desirable for the purposes of Production an investigation, a Judge of the High Court may upon an application made by a police officer or other authorised person, order -

(a) a person in possession or control of specified data stored in a computer system or a computer data storage medium; or

(b) a service provider in possession or control of specified subscriber information relating to services offered -

(i) in Sierra Leone; or

(ii) based outside Sierra Leone but, offering its services in Sierra Leone;

to submit information in his possession or control.

No. The Cyber Crime Act 2020 11

(5) An application under subsection (1) shall state the reasons explaining why it is believed that -

(a) a specified computer data sought is likely to be available with a person mentioned in subparagraph (a) or (b) of subsection (1);

(b) an investigation may be frustrated or seriously prejudiced unless the specified computer data or the subscriber information, as the case may be, is produced;

(c) the type of evidence suspected is likely to be produced by a person mentioned in subparagraph (a) or (b) of subsection (1);

(d) subscribers, users or unique identifiers who are the subject of an investigation or prosecution, may be disclosed as a result of the production of the specified computer data;

(e) an identified offence is an offence in respect of which the order is sought;

(f) measures taken shall prepare and ensure that the specified computer data will be produced -

(i) whilst maintaining the privacy of other users, customers and third parties; and

(ii) without the disclosure of data of any party who is not part of the investigation; and

(g) measures taken shall prepare and ensure that the production of the specified computer data is carried out through technical means such

Part III, Section 5, subsection (7) - Search and seizure of stored computer data.

- Misuse of powers is not defined

Part III, Section 5, subsection (8) - Search and seizure of stored computer data.

- Vague and arbitrary
- Why is it the Minister that should prescribe punishment?

Part III, Section 7, subsection (2) – Production order

- No data protection policy or legislation in place to protect the privacy and rights of individuals.
- For example, billing and payment information may not need to be disclosed for certain investigations.
- See also subsection 6, subparagraph (f); section 5, subsection (5); and section 6, subsection (2), subparagraph (b).

Part III: Powers and Procedures cont. ...

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

14	No.	The Cyber Crime Act	2020
		as mirroring or copying of relevant data and not through physical custody of computer systems or devices.	
Expedited preservation and partial disclosure of traffic data.	8	(1) A police officer or other authorised person may, where he is satisfied that - (a) a specified computer data stored in a computer system or computer data storage medium is reasonably required for the purposes of a criminal investigation; and (b) there is a risk or vulnerability that the computer data may be modified, lost, destroyed or rendered inaccessible, by written notice given to a person in possession or control of the computer system or computer data storage medium, require that person to undertake expeditious preservation of the computer data. (2) A notice under subsection (1) may require a person in possession or control of the computer system or computer data storage medium to disclose sufficient traffic data about the communication to identify - (a) the service providers; and (b) the path through which the communication was transmitted. (3) The period of preservation of data required under subsection (1) shall not exceed 90 days. (4) The period of preservation of data under subsection (3) may be extended by a Judge of the High Court for a further specified period of time, on an application by a police officer or other authorised person, where such extension is reasonably required for the purposes of -	

Part III, Section 8, subsection (2) - Expedited preservation and partial disclosure of traffic data.

- Could easily be repressively abused.

Part III, Section 10, subsection (1) - Interception of content data.

- Too broad; therefore, the potential for abuse of powers, especially as smartphones are classed as computer systems and data privacy laws do not exist - To “collect or record content data of ... transmission” could easily be repressively abused.

Deliberately left blank
Referenced in other slides

16	No.	The Cyber Crime Act	2020
		(a) collect or record traffic data in real-time; and (b) provide specified traffic data to the police officer or other authorised person. (2) An Order for the real-time collection or recording of traffic data under sub-section (1) shall not be for a period beyond what is absolutely necessary and in any event not for more than 90 days. (3) A period of real-time collection or recording of traffic data under subsection (2) may be extended by a Judge of the High Court for a further specified period of time, on an application by a police officer or other authorised person, where the extension is reasonably required for the purposes of - (a) an investigation or prosecution; (b) further real-time collection or recording of traffic data necessary to achieve the purpose for which the Order under sub-section (1) was made; (c) ensuring that the real-time collection or recording of traffic data is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation; (d) preventing the investigation of being frustrated or seriously prejudiced; and (e) averting overly burdensome cost of such extension on the person in control of the computer system. (4) An application under subsection (1) shall state reasons explaining why it is believed that -	

No.	The Cyber Crime Act	2020	17
	(a) a traffic data sought will be available with the person in control of the computer system; (b) a type of traffic data suspected will be found on that computer system; (c) the subject of an investigation or prosecution may be found on that computer system; (d) an identified offence is an offence in respect of which the order is sought; (e) measures shall be taken to maintain the privacy of other users, customers and third parties; and (f) there will be no disclosure of data of any party not part of the investigation. (3) A Judge of the High Court may also require a service provider to keep confidential, an Order under subsection (1) and a warrant issued under subsection (1) of section 5. (4) A service provider who fails to comply with an Order under subsection (1) commits an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by regulation made under this Act, prescribe. (5) (1) Where there are reasonable grounds to believe that the content of a specifically identified electronic communication is reasonably required for the purposes of a specific investigation in respect of a serious offence, a Judge of the High Court may, on an application by a police officer or other authorised person, order a service provider to - (a) collect or record; or (b) co-operate and assist a competent authority in the collection or recording of,	Real-time collection of traffic data. Interception of content data.	

Part III: Powers and Procedures cont. ...

Text from the Bill

34 No. The Cyber Crime Act 2020

as monitoring or copying of relevant data and not through physical custody of computer systems or devices.

Expedited preservation and partial disclosure of traffic data.

8. (1) A police officer or other authorised person may, where he is satisfied that -

(a) a specified computer data stored in a computer system or computer data storage medium is reasonably required for the purposes of a criminal investigation; and

(b) there is a risk or vulnerability that the computer data may be modified, lost, destroyed or rendered inaccessible,

by written notice given to a person in possession or control of the computer system or computer data storage medium, require that person to undertake expeditious preservation of the computer data.

(2) A notice under subsection (1) may require a person in possession or control of the computer system or computer data storage medium to disclose sufficient traffic data about the communication to identify -

(a) the service provider; and

(b) the path through which the communication was transmitted.

(3) The period of preservation of data required under subsection (1) shall not exceed 90 days.

(4) The period of preservation of data under subsection (3) may be extended by a Judge of the High Court for a further specified period of time, on an application by a police officer or other authorised person, where such extension is reasonably required for the purposes of -

No. The Cyber Crime Act 2020 35

(a) an investigation or prosecution;

(b) avoiding a risk or vulnerability that the computer data may be modified, lost, destroyed or rendered inaccessible; or

(c) averting overly burdensome cost of such preservation on the person in control of the computer system.

(5) A person to whom a notice under subsection (1) is given shall -

(a) be responsible to preserve the data for -

(i) a period not exceeding 90 days as specified in subsection (3); or

(ii) any extended period permitted by a Judge of the High Court under subsection (4);

(b) respond expeditiously to requests for assistance, whether to facilitate requests for police assistance or mutual assistance requests; and

(c) disclose as soon as practicable, a sufficient amount of the non-content data to enable a police officer or other authorised person to identify any other telecommunications providers involved in the transmission of the communication.

9. (1) Where there are reasonable grounds to believe that traffic data associated with specified communications is reasonably required for the purposes of a specific criminal investigation, a Judge of the High Court may, on an application by a police officer or other authorised person, order a service provider to -

Real-time collection of traffic data.

Findings

Part III, Section 8, subsection (1) – Expedited preservation and partial disclosure of traffic data.

- You cannot acquire evidence for criminal investigation and stated such risk on the data. In digital evidence processing, the most critical effort is to ensure that the evidence is not tampered with, modified, lost or rendered inaccessible in any form.

Part III, Section 8, subsection (5) – Expedited preservation and partial disclosure of traffic data.

- I find this vague. I assumed this section refers to "an authorised" person attempting to collect an evidence; or who can request police assistance?
- The word "mutual" is also vague and without clear definitions of who or what "mutual assistance" refers to leaves room for discretion, improper evidence process and a violation of privacy and human rights.

Why is it important

- If the forensics practice to properly process electronic evidence is ignored and continue as described, there is a risk of destroying vital evidence or having evidence inadmissible in a court of law.
- The lack of laws to mandate regulatory compliance and liability if specific data are not adequately protected could cause severe legal ramifications.
- Adding the aptitude to practice sound digital forensics will ensure the overall integrity of evidence presented in court.
- A good understanding of the legal and technical aspects will help capture vital information to prosecute a case if the intruder is caught.

Recommendations

- Develop Data Protection and Privacy Acts.
- Create policies, procedures and guidelines for:
 - Investigation request process
 - Collecting and handling evidence
 - Chain of custody
 - Device collection
 - Email collection
 - Storage and inventory
 - Evidence examination process
 - Evidence Analysis, and
 - Evidence reporting
- Establish a Forensics Lab to include
 - Restricted access
 - Tools including hardware and software
 - Personnel Qualifications

Part III: Powers and Procedures cont. ...

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

16	No.	The Cyber Crime Act	2020
	(a)	collect or record traffic data in real-time, and	
	(b)	provide specified traffic data to the police officer or other authorised person.	
	(2)	An Order for the real-time collection or recording of traffic data under sub-section (1) shall not be for a period beyond what is absolutely necessary and in any event not for more than 90 days.	
	(3)	A period of real-time collection or recording of traffic data under subsection (2) may be extended by a Judge of the High Court for a further specified period of time, on an application by a police officer or other authorised person, where the extension is reasonably required for the purposes of -	
	(a)	an investigation or prosecution;	
	(b)	further real-time collection or recording of traffic data necessary to achieve the purpose for which the Order under sub-section (1) was made;	
	(c)	ensuring that the real-time collection or recording of traffic data is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation;	
	(d)	preventing the investigation of being frustrated or seriously prejudiced; and	
	(e)	averting overly burdensome cost of such extension on the person in control of the computer system.	
	(4)	An application under subsection (1) shall state reasons explaining why it is believed that -	
	No.	The Cyber Crime Act	2020
	(a)	a traffic data sought will be available with the person in control of the computer system;	
	(b)	a type of traffic data suspected will be found on that computer system;	
	(c)	the subject of an investigation or prosecution may be found on that computer system;	
	(d)	an identified offence is an offence in respect of which the order is sought;	
	(e)	measures shall be taken to maintain the privacy of other users, customers and third parties; and	
	(f)	there will be no disclosure of data of any party not part of the investigation.	
	(3)	A Judge of the High Court may also require a service provider to keep confidential, an Order under subsection (1) and a warrant issued under subsection (1) of section 5.	
	(6)	A service provider who fails to comply with an Order under subsection (1) commits an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by Resolution made under this Act, prescribe.	
	10	(1) Where there are reasonable grounds to believe that interception of the content of a specifically identified electronic communication is reasonably required for the purposes of a specific investigation in respect of a serious offence, a Judge of the High Court may, on an application by a police officer or other authorised person, order a service provider to-	
	(a)	collect or record; or	
	(b)	co-operate and assist a competent authority in the collection or recording of.	

Part III, Section 9, subsection (3) - Real-time collection of traffic data

- No directives or laws to maintain privacy while collecting data in real-time during transmission.
- No mechanisms in place to be able to decrypt and encrypted data being transmitted?

Part III, Section 10, subsection (1) - Interception of content data

- The government or anyone should not be snooping on any citizen's data without their consent. This is a violation of one's privacy. Also, what is defined as a serious offence in this case?

Part III: Powers and Procedures cont. ...

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

18	No. The Cyber Crime Act 2020	19
content data of specified communication within the jurisdiction transmitted by means of a computer system, in real-time.	(4) A period of real-time collection or recording of content data under subsection (3) may be extended by a Judge of the High Court for a further specified period of time, on an application by a police officer or other authorised person, where the extension is reasonably required for the purposes of -	
(2) An Order for the real-time collection or recording of content data under sub-section (1) shall not be for a period beyond 90 days.	(a) an investigation or prosecution;	
(3) An application under subsection (1) shall state reasons explaining why it is believed that -	(b) achieving the objective for which the warrant is to be issued;	
(a) the content data sought will be available with the person in control of the computer system;	(c) ensuring that the real-time collection or recording of content data is carried out whilst maintaining the privacy of other users, customers and third parties and without the disclosure of information and data of any party not part of the investigation;	
(b) the type of content data suspected will be found on a computer system;	(d) preventing an investigation from being frustrated or seriously prejudiced; and	
(c) an identified offence is the offence for which the warrant is sought;	(e) averting overly burdensome cost of such real-time recording and collection on the person in control of the computer system.	
(d) further disclosures are needed to achieve the purpose for which the warrant is to be issued, where authority to seek real-time collection or recording on more than one occasion is needed.	(5) A Judge of the High Court may also require a service provider to keep confidential, an order made under subsection (1) and a warrant issued under subsection (1) of section 5.	
(e) measures taken shall ensure that the real-time collection or recording is carried out whilst maintaining the privacy of other users, customers and third parties without the disclosure of information and data of any party not part of the investigation;	(6) A service provider who fails to comply with an order under subsection (1) commits an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.	
(f) the investigation may be frustrated or seriously prejudiced unless the real time collection or recording is permitted; and	11. (1) A service provider shall not be subject to civil or criminal liability, unless it is established that the service provider	Confidentiality and limitation of liability.
(g) to achieve the purpose for which the warrant is being applied, real time collection or recording by a person in control of a computer system is necessary.	(a) had actual notice, actual knowledge or willful and malicious intent and not merely through omission or failure to act; or	

Part III, Section 10, subsection (3)
(a) (b) - Interception of content data

- It is possible that the owner of the computer system is not the one committing the crime (or know anything about a crime being committed using his/her computer system)—no clear guide on how the privacy of the owner of the computer system will be protected.



PART IV

International Cooperation

Sections 13 to 24

Part IV: International Cooperation

- 13. Spontaneous information
- 14. Powers of the Attorney-General
- 15. Authority to make and act on mutual assistance requests
- 16. Extradition
- 17. Confidentiality and limitation of use
- 18. Expedited preservation of stored computer data
- 19. Expedited disclosure of preserved traffic data
- 20. Mutual assistance regarding accessing of stored computer data
- 21. Trans-border access to stored computer data
- 22. Mutual assistance in real time collection of traffic data
- 23. Mutual assistance regarding interception of content data
- 24. Point of contact

Part IV: International Cooperation

Text from the Bill		Findings	Why is it important	Recommendations
<div><div><div>No.20The Cyber Crime Act2020</div><div>(b) had facilitated, aided or abetted the use by any person of a computer system controlled or managed by the service provider in contravention of this Act or any other law.</div><div>(2) A service provider shall not be liable under this Act or any other law for -</div><div>(a) maintaining and making his services available; or</div><div>(b) the disclosure of any data or other information to the extent required or in compliance with the exercise of powers under this Act.</div><div>Territorial jurisdiction.12. (1) The High Court shall have jurisdiction over any violation of this Act, including any violation committed by a Sierra Leone national regardless of the place of commission.</div><div>(2) The Jurisdiction of the High Court under subsection (1), shall lie</div><div>(a) within Sierra Leone;</div><div>(b) with the use of a computer system wholly or partly situated in Sierra Leone; or</div><div>(c) when by such commission, damage is caused to a natural or juridical person who, at the time the offence was committed, was in Sierra Leone.</div><div>PART IV - INTERNATIONAL COOPERATION</div><div>Spontaneous information.13. (1) The Attorney-General may, subject to this Act and without prior request, forward to a foreign state, information obtained under this Act, where he considers that the disclosure of such information may-</div></div></div> <div><div><div>No.21The Cyber Crime Act202021</div><div>(a) assist the foreign state in initiating or carrying out an investigation or prosecution; or</div><div>(b) lead to a request for co-operation by a foreign state.</div><div>(2) Information provided under subsection (1), may be subject to such conditions including confidentiality, as the Attorney-General may require.</div><div>(3) Where a foreign state cannot comply with conditions required under subsection (2), it shall notify the Attorney-General, who shall determine whether the information should nevertheless be provided and where the foreign state accepts the information subject to the conditions, it shall be bound by them.</div><div>14. (1) The Attorney-General may cooperate with any foreign state or international agency for the purpose of -</div><div>(a) investigating or prosecuting offences under this Act; or</div><div>(b) collecting electronic evidence related to an offence punishable under the laws of Sierra Leone.</div><div>(2) The Attorney-General shall communicate directly with the appropriate authority of a foreign state responsible for sending, answering, executing or transmitting requests for mutual assistance or extradition.</div><div>(3) Notwithstanding subsection (2), in case of urgency, requests may be sent directly from judicial authority to judicial authority, provided that the appropriate authority of the requested state is notified by the appropriate authority of the requesting state.</div><div>(4) For urgent request or communication, the International Police Organisation network may be used.</div><div>Powers of the Attorney-General.</div></div></div>		<p>Part IV, Section 13, subsection (1) - Spontaneous information</p> <ul style="list-style-type: none">This section is very open and has the potential for misuse. The Attorney-General will have too much power to disclose information to foreign statesIn the absence of standalone data protection and privacy law and clear definition of “Such condition”, the Attorney-General may be using their judgement to determine what is confidential and that is an area of concern for the misuse of power <p>Part IV, Section 14, subsection (1) - Powers of the Attorney-General</p> <ul style="list-style-type: none">Any foreign state or international agency may not be an appropriate language. What about foreign states and international agencies with which Sierra Leone has no international relationships and does not follow appropriate international human rights, data protection, and privacy laws?	<ul style="list-style-type: none">The information may have been obtained illegally without consent. The Attorney-General is not a cybercrime expert and may not have the required skills, tools and the ability to prove that (1) the foreign state requesting the information must follow the laws of the state and international laws (2) Ensure that prescribed standards and processes were followed when the information was obtained in Sierra Leone.	<ul style="list-style-type: none">Recommendation for Part IV, Section 13, subsection 1

Part IV: International Cooperation

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

22 No. The Cyber Crime Act 2020

Authority to make and act on mutual assistance requests.

15. (1) The Attorney-General may make requests on behalf of Sierra Leone to a foreign state for mutual assistance in an investigation commenced or prosecution instituted in Sierra Leone, relating to a computer related offence or collection of electronic evidence.

(2) The Attorney-General may, in respect of a request from a foreign state for mutual assistance in an investigation commenced or prosecution instituted in that state -

(a) grant the request, in whole or in part, on such terms and conditions as may be deemed necessary;

(b) refuse the request on such conditions as he deems necessary; or

(c) postpone a request, in whole or in part, after consulting with the appropriate authority of the foreign state, on the ground that granting the request would be likely to prejudice the conduct of an investigation or prosecution in Sierra Leone.

(3) Mutual assistance requests under this section shall be effectuated-

(a) in accordance with the procedures specified by a foreign state, except where it is incompatible with the laws of Sierra Leone; or

(b) where the conduct alleged does not constitute a crime in both the foreign state and in Sierra Leone.

(4) The Attorney-General shall, where appropriate, before refusing or postponing assistance, after having consulted with the foreign state, consider whether the request may be granted partially or subject to such conditions, as he deems necessary.

No. The Cyber Crime Act 2020 23

(5) The Attorney-General shall promptly inform a foreign state of -

(a) the outcome of the execution of a request for mutual assistance;

(b) any reason that renders impossible, the execution of a request for mutual assistance or is likely to delay it significantly; or

(c) any reason for refusal or postponement of a request for mutual assistance.

(6) A foreign state may request that Sierra Leone keeps confidential the fact of any request for mutual assistance, except to the extent necessary for its execution and if Sierra Leone cannot comply with the request for confidentiality, it shall promptly inform the foreign state, which shall then determine whether the request should nevertheless be executed.

16. (1) This Act complements the Extradition Act, 1974 (Act No. 11 of 1974) which makes provision for the extradition of persons accused or convicted of an offence in another country.

(2) Extradition shall not be requested for an offence unless it is an offence in both the foreign state and in Sierra Leone.

(3) An offence under this Act shall be extraditable if the penalty imposed is imprisonment for a term of not less than one year or a fine equivalent to the penalty of one year imprisonment.

(4) Extradition will be subject to the conditions provided for by the law of the foreign state or applicable extradition treaties, including the grounds on which the foreign state may refuse extradition.

(5) In line with the extradite or prosecute principle, where extradition is refused on the sole basis of-

Part IV, Section 15, subsection (2)a & b - Authority to make and act on mutual assistance requests

- “terms and conditions” and “such conditions” are not clearly defined anywhere. What are these terms and conditions? What existing standards, policies or guidelines will be followed to guide what is included or excluded in the terms and conditions stated here.

Deliberately left blank
Referenced in other slides

Part IV, Section 15, subsection (6) - Authority to make and act on mutual assistance requests

- Foreign states can request Sierra Leone to keep confidential the facts of any requests for mutual assistance. However, there is no joint statement for Sierra Leone to ask the foreign state to be confidential.

Deliberately left blank
Referenced in other slides

Part IV: International Cooperation

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

24	No.	The Cyber Crime Act	2020
	(a)	the nationality of the person sought to be extradited; or	
	(b)	Sierra Leone having jurisdiction over the offence,	
		the investigation or prosecution shall be conducted and the matter reported to the foreign state.	
Confidentiality and limitation of use.	17.	Where there is no mutual assistance treaty or arrangement in force between a foreign state and Sierra Leone, Sierra Leone shall make the supply of information in response to a request on condition that it is-	
	(a)	kept confidential; or	
	(b)	used only for investigations or prosecutions stated in the request.	
Expedited preservation of stored computer data.	18.	(1) A foreign state may request or obtain the expeditious preservation of data stored by means of a computer system, located within Sierra Leone, in respect of which it intends to submit a request for mutual assistance, for the search, access, seizure, security or disclosure of the data.	
	(2)	A request for preservation of data submitted under subsection (1) shall specify the-	
	(a)	authority seeking the preservation of data;	
	(b)	offence that is the subject of an investigation or prosecution, including a brief summary of the related facts;	
	(c)	stored computer data to be preserved and its relationship to the offence;	
	(d)	available information identifying the custodian of the stored computer data or the location of the computer system;	
	(e)	necessity of the preservation of data; and	

No.	The Cyber Crime Act	2020	25
(f)	intention to submit a request for mutual assistance for the search, access, seizure, security, or disclosure of the stored computer data.		
(3)	Upon receiving a request under subsection (1), the Attorney-General shall take all appropriate measures to expeditiously preserve the specified data in accordance with the procedures and powers under this Act.		
(4)	A request under subsection (1) shall be effected where the conduct alleged does not constitute a crime in both the foreign state and in Sierra Leone.		
(5)	A preservation of data effected in response to a request under subsection (1) shall be for a period not less than 90 days, in order to enable the foreign state, to submit a request for the search, access, seizure, security or disclosure of the data and following the receipt of such a request, the data shall continue to be preserved until a final decision is taken on that pending request.		
Expedited disclosure of preserved traffic data.	19.	(1) Where during the course of executing a request under section 18, with respect to a specified communication, it is discovered that a service provider in another state was involved in the transmission of the communication, the Attorney-General shall expeditiously disclose to the foreign state, sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.	
	(2)	Expedited disclosure of preserved traffic data under subsection (1) may only be withheld where the -	
	(a)	request concerns a political offence or an offence related to a political offence; or	
	(b)	Attorney-General considers that the execution of the request is likely to prejudice the sovereignty of Sierra Leone, security or public interest.	

Part IV, Section 17 - Confidentiality and limitation of use

- Sierra Leone will be allowed to provide information that may include Personally Identifiable Information (PII) to foreign states and agencies without a mutual assistance treaty or arrangement.

Part IV, Section 18, subsection (1) - Expedited preservation of stored computer data

- Sierra Leone or a foreign state or agency may request the expeditious preservation of data stored for mutual assistance, search, access, seizure and security or disclosure of the data without following due process. This will make it possible for the GoSL or foreign states to access private data and open it to misuse.

Part IV, Section 18, subsection (3) - Expedited preservation of stored computer data

- “all appropriate measures” and “preserve the specified data following the procedures” may be misinterpreted very easy. What is considered appropriate measures according to this bill? The procedures to properly preserve data is not specified or referenced in this bill.

Part IV, Section 19, subsection (2)a - Expedited disclosure of preserved traffic data

- An exception is made for political offence or offences related to a political offence.

Page 24 and 25

- Confidentiality and limitation of use.
- Expedited preservation of stored computer data.
- Expedited disclosure of preserved traffic data.

Deliberately left blank
Referenced in other slides

Part IV: International Cooperation

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

26	No.	The Cyber Crime Act	2020
Mutual assistance regarding accessing of stored computer data.	20.	(1) A foreign state may request the search, access, security or disclosure of data stored by means of a computer system located within Sierra Leone, including data that has been preserved under section 15.	
		(2) When making a request under subsection (1), the foreign state shall provide adequate information on the following- (a) the name of the authority conducting the investigation or prosecution to which the request relates; (b) a description of the nature of the criminal offence and a statement setting out a summary of the relevant facts and laws; (c) a description of the purpose of the request and of the nature of the assistance being sought; (d) in the case of a request to restrain or confiscate assets believed on reasonable grounds to be located in Sierra Leone, details of the offence in question, particulars of any investigation or prosecution commenced in respect of the offence, including a copy of any relevant restraining or confiscation order; (e) details of any procedure that the foreign state wishes to be followed by Sierra Leone in giving effect to the request, particularly in the case of a request to take evidence; (f) a statement setting out any wishes of the foreign state concerning confidentiality relating to the request and the reasons for those wishes;	

No.	The Cyber Crime Act	2020	27
(g)	details of the period within which the foreign state wishes the request to be complied with;		
(h)	where applicable, details of the property, computer, computer system or device to be traced, restrained, seized or confiscated and of the grounds for believing that the property is believed to be in Sierra Leone;		
(i)	details of the stored computer data, data or program to be seized and its relationship to the offence;		
(j)	information identifying the custodian of the stored computer data or the location of the computer, computer system or device;		
(k)	an agreement on the question of the payment of the damages or costs of fulfilling the request; and		
(l)	any other information that may assist in giving effect to the request.		
(3)	Upon receiving a request under subsection (1), the Attorney-General shall take all appropriate measures to obtain necessary authorisation including a warrant to execute in accordance with the procedures and powers under this Act or any other law.		
(4)	Upon obtaining necessary authorisation under subsection (3), including a warrant to execute, the Attorney-General may seek the support and cooperation of the foreign state during such search and seizure.		
(5)	Upon conducting the search and seizure under subsection (4), the Attorney-General shall provide the results of such search and seizure, as well as the evidence seized, to the foreign state.		

Part IV, Section 20, subsection (1) - Mutual assistance regarding accessing of stored computer data

- We were unable to find statements related to data protection and privacy laws to be followed

Deliberately left blank
Referenced in other slides

Deliberately left blank
Referenced in other slides

Part IV: International Cooperation

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

28	No.	<i>The Cyber Crime Act</i>	2020
Trans-border access to stored computer data.	21	Subject to this Act, a police officer or other authorised person may, without authorisation-	
	(a)	access publicly available (open source) stored computer data, regardless of where the data is located geographically; or	
Mutual assistance in real time collection of traffic data.	(b)	access or receive through a computer system in Sierra Leone, stored computer data located in a foreign state, if such police officer or other authorised person obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system.	
	22	(1) A foreign state may request the Attorney-General to provide assistance in real time collection of traffic data associated with specified communications in Sierra Leone transmitted by means of a computer system.	
	(2)	A request for assistance under subsection (1) shall specify-	
	(a)	the authority making the request;	
	(b)	the offence that is the subject of a criminal investigation or prosecution and a brief summary of the related facts;	
	(c)	the name of the authority with access to the relevant traffic data;	
	(d)	the location at which the traffic data may be held;	
	(e)	the intended purpose for the required traffic data;	
	(f)	sufficient information to identify the traffic data;	

No.	<i>The Cyber Crime Act</i>	2020	29
(g)	further details of relevant traffic data;		
(h)	the necessity for use of powers under this section; and		
(i)	the terms for the use and disclosure of the traffic data to third parties.		
(3)	Upon receiving a request under subsection (1), the Attorney-General shall take all appropriate measures to obtain necessary authorisation including a warrant to execute upon the request in accordance with the procedures and powers under this Act or any other law.		
(4)	Upon obtaining necessary authorisation including a warrant to execute a request under subsection (1), the Attorney-General may seek the support and cooperation of the foreign state during the search and seizure.		
(5)	Upon conducting the measures under this section, the Attorney-General shall provide the results of such measures as well as real-time collection of traffic data associated with specified communication to the foreign state.		
23	(1) A foreign state may, in relation to a serious offence in that state, request or provide assistance in the real time collection or recording of content data of specified communication transmitted by means of a computer system in Sierra Leone.		
(2)	A request for assistance under subsection (1) shall specify-		
(a)	the authority making the request;		
(b)	the offence that is the subject of a criminal investigation or prosecution and a brief summary of the facts;		
(c)	the name of the authority with access to the relevant communication;		
(d)	the location at which or nature of the communication;		

Part IV, Section 21, subsection (1)
- Trans-border access to stored computer data

Part IV, Section 22, subsection (1)
- Mutual assistance in real time collection of traffic data

Part IV, Section 23, subsection (1)
- Mutual assistance regarding interception of content data

Deliberately left blank

Referenced in other slides

Deliberately left blank

Referenced in other slides

Part V - Offences

Sections 25 to 46

Part V: Offences

- 25. Unauthorised access.
- 26. Unauthorised access to protected system.
- 27. Unauthorised data interception.
- 28. Unauthorised data interference.
- 29. Unauthorised system interference.
- 30. Misuse of device.
- 31. Computer-related forgery.
- 32. Computer fraud.
- 33. Identity theft and impersonation.
- 34. Electronic signature.
- 35. Cyber stalking and cyber bullying.
- 36. Cyber Squatting.
- 37. Infringements of copyright and related rights.
- 38. Online child sexual abuse.
- 39. Attempting and aiding or abetting.
- 40. Registration of cybercafé.
- 41. Cyber terrorism.
- 42. Racist and xenophobic offences.
- 43. Reporting of cyber threats.
- 44. Breach of confidence by service providers.
- 45. Employees responsibility.
- 46. Corporate liability.

Part V: Offences

Text from the Bill		Findings	Why is it important	Recommendations
<div><div>30</div><div>No.</div><div>The Cyber Crime Act</div><div>2020</div></div> <div><div>(e)</div><div>the intended purpose for the required communication;</div></div> <div><div>(f)</div><div>sufficient information to identify the communication;</div></div> <div><div>(g)</div><div>details of the data of the relevant interception;</div></div> <div><div>(h)</div><div>the recipient of the communication;</div></div> <div><div>(i)</div><div>the intended duration for the use of the communication;</div></div> <div><div>(j)</div><div>the necessity for use of powers under this section; and</div></div> <div><div>(k)</div><div>the terms for the use and disclosure of the communication to third parties.</div></div> <div><div>(3)</div><div>Upon receiving a request under subsection (1), the Attorney-General shall take appropriate action to execute the request in accordance with the procedures and powers under this Act.</div></div> <div><div>(4)</div><div>The Attorney-General shall, on executing the request under subsection (3), provide the results of such action as well as real time collection or recording of content data of specified communication to the foreign state.</div></div> <div><div>Point of contact.</div><div>24</div><div>(1)</div><div>A police officer or other authorised person investigating or prosecuting cybercrime shall designate a point of contact available on a 24-hour, 7-days-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigation or prosecution of offences related to computer systems and data, or for the collection of evidence in electronic form.</div></div> <div><div>(2)</div><div>Immediate assistance to be provided under subsection (1) shall include -</div></div> <div><div>(a)</div><div>the provision of technical advice;</div></div>	<div><div>No.</div><div>The Cyber Crime Act</div><div>2020</div><div>31</div></div> <div><div>(b)</div><div>the preservation of data pursuant to expedited preservation of stored computer data and expedited disclosure of preserved traffic data; and</div></div> <div><div>(c)</div><div>the collection of evidence, the provision of legal information, and locating of suspects.</div></div> <div><div>(3)</div><div>A point of contact under subsection (1), shall -</div></div> <div><div>(a)</div><div>be resourced with and possess the requisite capacity to securely and efficiently carry out communication with other points of contact in other states, on an expedited basis;</div></div> <div><div>(b)</div><div>have the authority and be empowered to coordinate and enable access to international mutual assistance under this Act or if applicable extradition procedures, upon an expedited basis.</div></div> <div><div>PART IV - OFFENCES</div></div> <div><div>25.</div><div>(1)</div><div>A person, including a corporation, partnership, or association, who intentionally and without authorisation causes a computer system to perform a function with intent to secure access to the whole or a part of a computer system or to enable such access to be secured, commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div></div> <div><div>(2)</div><div>For the purposes of this section, a person secures access to computer data stored in a computer system if by causing a computer system to perform a function he -</div></div> <div><div>(a)</div><div>alters or erases computer data; or</div></div> <div><div>(b)</div><div>copies, transfers or moves computer data to</div></div>	<p>Part V, Section 25, subsection (1) Unauthorised access.</p> <ul style="list-style-type: none">• Vague and concentrated power given to the Minister and Judges• Too arbitrary to leave sentencing decisions to the Minister and Judges	<ul style="list-style-type: none">• A Minister is a member of the Executive Branch and a Cabinet Member that can be replaced anytime by the President. We cannot control how fair they will be• This will open a wide door for favoritism	<ul style="list-style-type: none">• Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "<u>Cybercrimes (Prohibition, prevention, ECT) Act, 2015</u>", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at <u>PART II - Offences , Section 4, subsection (1) of the HIPCAR Model Policy Guidelines and Legislative Text</u>• Change the text in Part V, Section 25, subsection (1) Unauthorised access to the following; “A person, including a corporation, partnership, or association, who intentionally and without authorisation causes a computer system to perform a function with intent to secure access to the whole or a part of a computer system or to enable such access to be secured, commits an offence and is liable upon conviction to imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.”

Sierra Leoneans in Technology (SLinT) | <https://slint.org> | <https://members.slint.org>

No.

The Cyber Crime Act

2020

31

(b)

the preservation of data pursuant to expedited preservation of stored computer data and expedited disclosure of preserved traffic data; and

(c)

the collection of evidence, the provision of legal information, and locating of suspects.

(3)

A point of contact under subsection (1), shall -

(a)

be resourced with and possess the requisite capacity to securely and efficiently carry out communication with other points of contact in other states, on an expedited basis;

(b)

have the authority and be empowered to coordinate and enable access to international mutual assistance under this Act or if applicable extradition procedures, upon an expedited basis.

PART V - OFFENCES

25

(1)

A person, including a corporation, partnership, or association, who intentionally and without authorisation causes a computer system to perform a function with intent to secure access to the whole or a part of a computer system or to enable such access to be secured, commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.

Unauthorised access.

(2)

For the purposes of this section, a person secures access to computer data stored in a computer system if by causing a computer system to perform a function he -

(a)

alters or erases computer data, or

(b)

copies, transfers or moves computer data to -

Part V, Section 25, subsection (1) Unauthorised access.

- Vague and concentrated power given to the Minister and Judges
- Too arbitrary to leave sentencing decisions to the Minister and Judges

- A Minister is a member of the Executive Branch and a Cabinet Member that can be replaced anytime by the President. We cannot control how fair they will be
- This will open a wide door for favoritism

- Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "Cybercrimes (Prohibition, prevention, ECT) Act, 2015", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at PART II - Offences , Section 4, subsection (1) of the HIPCAR Model Policy Guidelines and Legislative Text
- Change the text in Part V, Section 25, subsection (1) Unauthorised access to the following; "A person, including a corporation, partnership, or association, who intentionally and without authorisation causes a computer system to perform a function with intent to secure access to the whole or a part of a computer system or to enable such access to be secured, commits an offence and is liable upon conviction to imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both."

Part V: Offences

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

32	No	The Cyber Crime Act	2020
		(i) a computer system or computer data storage medium other than that in which it is stored; or	
		(ii) a different location in the same computer system or computer data storage medium in which it is stored;	
		(c) has the computer data output from the computer system in which it is held, whether by having it displayed or in any other manner;	
		(d) uses the computer data.	
		(3) For the purposes of this section, "unauthorised" means access of any kind, to a computer system, program or data, by a person who has been authorised to access a specific data in a computer system and without lawful excuse, whether temporary or not, cause a computer system to perform a function other than those authorised, with intent to secure access to the whole or a part of a computer system or to enable such access to be secured.	
		(4) The absence of authority to secure access to the whole or any part of a computer system under subsection (1) includes instances where there may exist general authority to access a computer system but a specific type, nature or method of access may not be authorised.	
		(5) For the purposes of this section intention or recklessness need not relate to-	
		(a) a particular computer system;	
		(b) a particular program or data; or	
		(c) a program or data of any particular kind.	
		(6) A person shall be deemed to have contravened subsection (1)-	

No.	The Cyber Crime Act	2020	33
	(a) in the absence of proof that the accused has the requisite knowledge to access the computer, program or data;		
	(b) notwithstanding the fact that committing the offence is impossible;		
	(c) in the absence of a program or data of any particular kind.		
	26. (1) A person, including a corporation, partnership, or association, who intentionally or without authorisation causes a computer system to perform a function with intent to secure access to a computer or program or data used directly in connection with or necessary for a Critical National Information Infrastructure commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.	Unauthorised access to protected system.	
	(2) A person, including a corporation, partnership, or association, who has been authorised to access a specific data in a computer system and without lawful excuse, whether temporary or not, causes a computer system to perform a function other than that authorised, or intentionally permits tampering of such computer systems with intent to secure access to the whole or a part of a computer system or to enable such access to be secured, commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.		
	(3) The absence of authority to secure access to the whole or any part of any computer system under subsection (1) includes instances where there may exist general authority to access a computer system but a specific type, nature or method of access may not be authorised.		
	(4) For the purposes of this section intention or recklessness need not relate to-		
	(a) a particular computer system;		
	(b) a particular program or data; or		
	(c) a program or data of any particular kind.		

Part V, Section 26, subsection (1)
Unauthorised access to protected system.

- Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "[Cybercrimes \(Prohibition, prevention, ECT\) Act, 2015](#)", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at [PART II - Offences , Section 4, subsection \(1\) of the HIPCAR Model Policy Guidelines and Legislative Text](#)

Part V: Offences

Text from the Bill	Findings	Why is it important	Recommendations
<div>34</div> <div>No.</div> <div>The Cyber Crime Act</div> <div>2020</div> <div>Unauthorized data interception.</div> <div>27. (1) A person, including a corporation, partnership, or association, who intentionally and without authorisation intercepts or causes to be intercepted non-public transmissions of data to or from a computer system, whether directly or indirectly, the transmission of which -</div> <div>(a) results in a significant financial loss;</div> <div>(b) threatens national security;</div> <div>(c) causes physical injury or death to any person; or</div> <div>(d) threatens public health or public safety;</div> <div>commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe:</div> <div>(2) Where a person, including a corporation, partnership, or association, intentionally and without authorisation, intercepts or causes to be intercepted, the transmission of data to or from a computer system over a telecommunication under subsection (1), it is immaterial whether -</div> <div>(a) the unauthorised interception is not directed at -</div> <div>(i) a telecommunications system;</div> <div>(ii) a particular computer system;</div> <div>(iii) a program or data of any kind; or</div> <div>(iv) a program or data held in any particular computer system;</div> <div>(b) an unauthorised interception or an intended effect of it is permanent or temporary.</div> <div>Unauthorized data interference.</div> <div>28. A person, including a corporation, partnership, or association, who intentionally or without authorisation does an act in relation to a computer system which -</div>	<div>No.</div> <div>The Cyber Crime Act</div> <div>2020</div> <div>35</div> <div>(a) causes destruction, damage, deletion, erasure, deterioration, generation, modification or alteration of a program or data or any aspect or attribute related to the program or data;</div> <div>(b) renders a program or data meaningless, useless or ineffective;</div> <div>(c) obstructs, interrupts or interferes with the use of any program or data or any aspect or attribute related to the program or data;</div> <div>(d) causes denial, prevention, suppression or hindrance of access to a program or data or any aspect or attribute related to the program or data or to any person entitled to it;</div> <div>(e) causes impairment to the operation of a program;</div> <div>(f) causes impairment to the reliability of any data, aspect or attribute related to a program or data;</div> <div>(g) causes impairment to the security of a program or data or any aspect, attribute related to a program or data; or</div> <div>(h) enables any of the acts mentioned in paragraphs (a) to (g) to be done.</div> <div>commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div> <div>29. A person, including a corporation, partnership, or association, who intentionally or without authorisation does an unauthorised act in relation to a computer system which -</div>	<p><u>Part V, Section 27, subsection (1) - Unauthorised data interception.</u></p> <p><u>Part V, Section 28, subsection (a) - Unauthorised data interference.</u></p> <p><u>Part V, Section 29 subsection - Unauthorised system interference.</u></p>	<ul style="list-style-type: none">Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "Cybercrimes (Prohibition, prevention, ECT) Act, 2015", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at PART II - Offences , Section 4, subsection (1) of the HIPCAR Model Policy Guidelines and Legislative Text

Part V: Offences

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

36	No.	<i>The Cyber Crime Act</i>	2020
	(a)	interferes with, hinders, damages, prevents, suppresses, deteriorates, impairs or obstructs the functioning of a computer system;	
	(b)	interferes with, hinders, damages, prevents, suppresses, deteriorates, impairs or obstructs the communication between or with a computer system;	
	(c)	interferes with or hinders access to a computer system;	
	(d)	impairs the operation of a computer system;	
	(e)	impairs the reliability of a computer system;	
	(f)	impairs the security of a computer system; or	
	(g)	enables any of the acts mentioned in paragraphs (a) to (f) to be done,	
		commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe:	
		Provided that it shall not be an offence if interference with a computer system is undertaken in compliance and in accordance with the terms of a warrant issued under this Act or any law:	
Misuse of device.	30	(1) A person, including a corporation, partnership, or association, who intentionally or without authorisation manufactures, adapts, sells, procures for use, receives, possesses, imports, offers to supply, distributes or otherwise makes available -	
	(a)	a device designed or adapted primarily for the purpose of committing an offence under this Act; or	

No.	<i>The Cyber Crime Act</i>	2020	37
(b)	a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed, designed or adapted primarily for the purposes of a computer system,		
	commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.		
(2)	Notwithstanding subsection (1) a person shall not be deemed to have committed an offence if he does an act under subsection (1), -		
(a)	for the purpose of training, testing or protection of a computer system; or		
(b)	in compliance of and in accordance with the terms of a judicial order issued or in exercise of a power under this Act or any law.		
(3)	For the purpose of subsection (1), possession of a program or a computer password, access code, or similar data includes having -		
(a)	possession of a computer system which contains the program or a computer password, access code, or similar data,		
(b)	possession of a data storage device in which the program or a computer password, access code, or similar data is recorded; or		
(c)	control of a program or a computer password, access code, or similar data that is in the possession of another person.		

Deliberately left blank
Referenced in other slides

- Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "[Cybercrimes \(Prohibition, prevention, ECT\) Act, 2015](#)", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at [PART II - Offences , Section 4, subsection \(1\) of the HIPCAR Model Policy Guidelines and Legislative Text](#)

Part V: Offences

Text from the Bill

38	No.	<i>The Cyber Crime Act</i>	2020
Unauthorised disclosure of password.	31.	A person, including a corporation, partnership, or association, who intentionally or without authorisation discloses to another person a password, access code or other means of gaining access to any program or data held in a computer system -	
	(a)	for any wrongful gain;	
	(b)	for any unlawful purpose; or	
	(c)	to occasion any loss,	
		commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.	
Computer-related forgery.	32.	(1) A person, including a corporation, partnership, or association, who intentionally or without authorisation inputs, alters, deletes or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable or intelligible, commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.	
	(2)	A person, including a corporation, partnership, or association, who dishonestly or with similar intent -	
	(a)	for wrongful gain;	
	(b)	for wrongful loss to another person; or	
	(c)	for any economic benefit for oneself or for another person,	
		intentionally or without authorisation inputs, alters, deletes or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable	

No.	<i>The Cyber Crime Act</i>	2020	39
<p>or intelligible commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</p>			

32. A person, including a corporation, partnership, or association, who intentionally causes loss of property, valuable security or consideration to another person by - Computer fraud.

- (a) inputting, alteration, modification, deletion, suppression or generation of a program or data;
- (b) interference, hindrance, impairment or obstruction with the functioning of that computer system; or
- (c) copying, transferring or moving data or program to another computer system, device or storage medium other than that in which it is held or to a different location in any other computer system, device or storage medium in which it is held;
- (d) using any data or program; or
- (e) having any data or program output from the computer system in which it is held, whether by having it displayed or in any other manner.

with fraudulent or dishonest intent of procuring, without right, an economic benefit for himself or for another person commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.

Findings

**Part V, Section 31 subsection –
Unauthorised disclosure of
password.**

**Part V, Section 32 subsection (1) –
Computer-related forgery.**

**Part V, Section 32 subsection –
Computer fraud.**

Why is it important

- Credential shared during a social engineering expedition can lead to wrongful prosecution
- In the event the Minister is incapacitate who assumes the sentencing role

Recommendations

- Specify the imprisonment period and/or fine amount in the section to ensure the Minister and Judge cannot arbitrarily change it in favor of their friends and family. In Part III – Offences and Penalties of the Nigeria “Cybercrimes (Prohibition, prevention, ECT) Act, 2015” you will see a good example of how its done to avoid favoritism and misuse of power. You can also see examples at PART II - Offences , Section 4, subsection (1) of the HIPCAR Model Policy Guidelines and Legislative Text
- The clause must clearly include intent as a prelude to committing the crime a remedy for mistake should be considered.
- •The court of law should handle sentencing and fines, and both must be clearly mentioned as defined in the Nigerian version noted above.
- •Security awareness training must be made available computer and electronic device users working in sensitive sectors

Part V: Offences

Text from the Bill	Findings	Why is it important	Recommendations
<div><div>40</div><div>No. The Cyber Crime Act 2020</div><div>Identity theft and impersonation. 33. (1) A person, including a corporation, partnership, or association, who is engaged in the services of any financial institution, and as a result of his special knowledge commits identity theft of its employer, staff, service providers and consultants with the intent to defraud commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div><div>(2) A person, including a corporation, partnership, or association, who fraudulently -</div><div>(a) or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, or</div><div>(b) impersonates another entity or person, living or dead, with intent to -</div><div>(i) gain advantage for himself or another person;</div><div>(ii) obtain any property or an interest in any property;</div><div>(iii) cause disadvantage to the person or entity being impersonated or another person; or</div><div>(iv) avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice, commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div></div> <div><div>No. The Cyber Crime Act 2020 41</div><div>(3) A person, including a corporation, partnership, or association, who makes or causes to be made, either directly or indirectly, any false statement as a material fact in writing, knowing it to be false and with the intent that it be relied upon respecting his identity or that of any other person or his financial condition or that of any other person for the purpose of procuring the issuance of a card or other instrument to himself or another person commits an offence and shall be liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div><div>34. A person, including a corporation, partnership, or association, who with the intent to defraud and or misrepresent, forges through electronic devices another person's signature or company mandate commits an offence and shall be liable on conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div><div>35. (1) A person, including a corporation, partnership, or association, who individually or with another person, willfully and repeatedly communicates, either directly or indirectly, with another person, if he knows or ought to have known that his conduct -</div><div>(a) is likely to cause that person apprehension or fear of violence to him or damage or loss on his property; or</div><div>(b) detrimentally affects that person,</div><div>commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div><div>(2) A person, including a corporation, partnership, or association, who knowingly or intentionally sends a message or other matter by means of a computer system or network that-</div></div>	<p><u>Part V, Section 33 subsection (1)– Identity theft and impersonation.</u></p> <p><u>Part V, Section 34 subsection (1) – Electronic signature.</u></p> <p><u>Part V, Section 35 subsection (1)– Cyber stalking and cyber bullying.</u></p>	<ul style="list-style-type: none">• A single-gender is mentioned here.• In the event the Minister is incapacitated, who assumes the role of sentencing?	<ul style="list-style-type: none">• Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "<u>Cybercrimes (Prohibition, prevention, ECT) Act, 2015</u>", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at <u>PART II - Offences , Section 4, subsection (1) of the HIPCAR Model Policy Guidelines and Legislative Text</u>• This clause has a loophole, and open to misinterpretation needs to include the opposite gender. Pronoun for the other gender to be inserted• The court of law should handle sentencing and fines, and both must be clearly mentioned as defined in the Nigerian version noted above.

Part V: Offences

Text from the Bill		Findings	Why is it important	Recommendations
<div><div>42</div><div>No. The Cyber Crime Act 2020</div><div><div>(a) is grossly offensive, pornographic or of an indecent, obscene or menacing character or causes any such message or matter to be so sent, or</div><div>(b) he knows to be false, for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent,</div></div><div>commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div><div>(3) Notwithstanding subsection (1) a person shall not be deemed to have committed an offence if he does an act -</div><div><div>(a) for the purpose of preventing or detecting crime;</div><div>(b) in compliance of and in accordance with the terms of a judicial order issued or in exercise of any power under this Act or any law; or</div><div>(c) which is in the interest of the public.</div></div><div>Cyber Squatting</div><div>36. (1) A person, including a corporation, partnership, or association, who intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by an individual, body corporate or belonging to a government institution in Sierra Leone, on the internet or any other computer network, without authority or right and for the purpose of interfering with the use by the owner, registrant or legitimate prior user, commits an offence and is liable on conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div></div>		<div><div>No. The Cyber Crime Act 2020 43</div><div>(2) In awarding penalty against an offender under this section, a court shall have regard to the following -</div><div><div>(a) refusal by the offender to relinquish, upon formal request by the rightful owner of a name, business name, trademark, domain name, or other word or phrase registered, owned or in use by any individual, body corporate or belonging to the Government of Sierra Leone; or</div><div>(b) any attempt by the offender to obtain compensation in any form for the release to the rightful owner for use of the name, business name, trademark, domain name or other word or phrase registered, owned or in use by the individual, body corporate or belonging to the Government of Sierra Leone.</div></div><div>(3) In addition to the penalty specified in this section, the court may make an order directing an offender to relinquish such registered name, mark, trademark, domain name or other word or phrase to the rightful owner.</div><div>37. A person, including a corporation, partnership, or association, who, through input, alteration, modification, deletion, suppression or generation of a program or data or through use of a computer, computer system or electronic device willfully infringes any rights protected under the Copyright Act, 2011 (Act No. 8 of 2011) or any law in force for protection of copyrights and related rights, commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div><div>Infringement of copyright and related rights.</div><div>38. (1) A person, including a corporation, partnership, or association, who, intentionally -</div><div>Online child sexual abuse.</div></div>	<p>Part V, Section 36 subsection – Cyber Squatting.</p> <p>Part V, Section 37 subsection – Infringements of copyright and related rights.</p> <p>Part V, Section 38 subsection – Online child sexual abuse.</p>	<ul style="list-style-type: none">Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "Cybercrimes (Prohibition, prevention, ECT) Act, 2015", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at PART II - Offences , Section 4, subsection (1) of the HIPCAR Model Policy Guidelines and Legislative Text

Part V: Offences

Text from the Bill	Findings	Why is it important	Recommendations
<div><div>44</div><div>No. The Cyber Crime Act 2020</div><div><p>(a) possesses, distributes, produces, views,downloads, transmits, disseminates, circulates, delivers, exhibits, lends for gain, exchanges, barter, sells or offers for sale, lets on hire or offers to let on hire, prints, photographs, copies, provides location, requests for, offers in any other way, or makes available in any way child pornography through a computer system or storage data medium; or</p><p>(b) acquiesces a child's participation in pornography;</p><p>commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</p><p>(7) A person, including a corporation, partnership, or association, who intentionally poses, groom or solicits, through any computer system or network, to meet a child for the purpose of-</p><p>(a) engaging in sexual activity with the child;</p><p>(b) engaging in sexual activity with the child where-</p><p>(i) coercion, inducement, force or threat is used;</p><p>(ii) a recognised position of trust, authority or influence over the child, including within the family is abused; or</p><p>(iii) a child's mental or physical disability or situation of dependence is abused;</p><p>commits an offence and shall be liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</p></div><div>45</div></div>	<div><div>No. The Cyber Crime Act 2020</div><div><p>(3) Notwithstanding subsection (1) a person shall not be deemed to have committed an offence if he does an act intended for a bona fide scientific or medical research or law enforcement.</p><p>(4) For purposes of this section -</p><p>"child" means a person under the age of 18 years;</p><p>"child pornography" includes data which, whether visual or audio, depicts -</p><p>(a) a child engaged in sexually explicit conduct;</p><p>(b) a person who appears to be a child engaged in sexually explicit conduct; or</p><p>(c) realistic images representing a child engaged in sexually explicit conduct.</p></div><div><p>Part V, Section 39 subsection (1) – Attempting and aiding or abetting.</p><p>Part V, Section 40 subsection (1), B – Registration of Cybercafes.</p></div></div>	<div><ul style="list-style-type: none">How does the law handle current cyber café operator (Compliant timeline)</div>	<div><ul style="list-style-type: none">Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "Cybercrimes (Prohibition, prevention, ECT) Act, 2015", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at PART II - Offences , Section 4, subsection (1) of the HIPCAR Model Policy Guidelines and Legislative TextCurrent cyber café operators and some small businesses must be given a compliant timeline should not be subjected to immediate punitive actions.</div>

Part V: Offences

Text from the Bill		Findings	Why is it important	Recommendations
<div>46</div> <div>No.</div> <div>The Cyber Crime Act</div> <div>2020</div> <div>(b) registered with National Telecommunications Commission established under the Telecommunications Act, 2006 (Act No. 9 of 2006) as a business concerned with providing computer access to the internet.</div> <div>(2) A person, including a corporation, partnership, or association, who perpetrates electronic fraud or online fraud under this Act using a cyberspace, commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div> <div>Cyber terrorism.</div> <div>41. (1) A person who accesses or cause to be accessed a computer or computer system or network for purposes of a terrorist act, commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div> <div>(2) For purposes of this section, "terrorist act" shall have the same meaning as provided under the Anti-Money Laundering and Combating of Financing of Terrorism Act, 2012 (act No. 2 of 2012).</div> <div>Racist and xenophobic offences.</div> <div>42. (1) A person, including a corporation, partnership, or association, who with intent-</div> <div>(a) distributes or otherwise makes available, racist or xenophobic material to the public through a computer system or network;</div> <div>(b) threatens through a computer system or network any other person or group of persons for the reason of belonging to a group distinguished by race, colour, descent, national or ethnic origin, as well as, religion,</div>	<div>No.</div> <div>The Cyber Crime Act</div> <div>2020</div> <div>47</div> <div>(c) insults publicly through a computer system or network any other person or group of persons distinguished by race, colour, descent or national or ethnic origin, as well as religion, or</div> <div>(d) distributes or otherwise makes available, to the public, material which denies or approves or justifies acts constituting genocide or crimes against humanity,</div> <div>commits an offence and is liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div> <div>(2) For the purpose of subsection (1), "crime against humanity" includes any of the following acts committed as part of a widespread or systematic attack directed against any civilian population, with knowledge of the attack: murders, extermination, enslavement, deportation or forcible transfer of population, imprisonment, torture rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilisation or any other form of sexual violence of comparable gravity, persecution against an identifiable group on political, racial, national, ethnic, cultural, religious or gender grounds, enforced disappearance of persons, the crime of apartheid, other inhumane acts of similar character intentionally causing great suffering or serious bodily or mental injury;</div> <div>"genocide" means any of the following acts committed with intent to destroy in whole or in part, a national, ethnic, racial or religious group as such: killing members of the group, deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part, imposing measures intended to prevent births within the group, forcibly transferring children of the group to another group.</div>	<p><u>Part V, Section 41 subsection – Cyber terrorism.</u></p> <p><u>Part V, Section 42 subsection – Racist and xenophobic offences.</u></p>	<ul style="list-style-type: none">• The use of Terrorist Act is vague in this context	<ul style="list-style-type: none">• Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "Cybercrimes (Prohibition, prevention, ECT) Act, 2015", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at PART II - Offences , Section 4, subsection (1) of the HIPCAR Model Policy Guidelines and Legislative Text• A terrorist act is broad and needs to be clearly defined to avoid misuse of the word and wrongful impressment of innocent citizens• Define the crime and outline the various punishments one is exposed to as a violator.

Part V: Offences

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

48	No.	The Cyber Crime Act	2020
		"racist or xenophobic material" means any written or printed material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.	
Reporting cyber threats.	43.	(1) A person or institution that operates a computer system or network, whether public or private, shall immediately inform the National Computer Security Incidence Response Team of an attack, intrusion and other disruption liable to hinder the functioning of another computer system or network, and the National Computer Security Incidence Response Team shall take necessary and appropriate measures to protect computer systems and networks.	
	(2).	In order to protect a computer system or network under subsection (1), the National Computer Security Incidence Response Team may propose the isolation of an affected computer system or network pending the resolution of the issues.	
	(3).	A person or institution who fails to report an incident of an attack, intrusion or other disruption liable to hinder the functioning of another computer system or network to the National Computer Security Incidence Response Team, within 7 days of its occurrence, commits an offence and is liable to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.	
	No.	The Cyber Crime Act	2020
	44.	(1) A person or institution which, being a computer based service provider and or vendor does an act with intent to defraud and by virtue of his position as a service provider, forges, illegally used security codes of the consumer with the intent to gain a financial and or material advantage or with intent to provide less value for money in his or its services to a consumer commits an offence and upon conviction is liable to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.	Breach of confidence by service providers.
	(2).	Where an offence under this Act committed by a body corporate is proved to have been committed on the instigation or with the connivance of or attributable to any neglect on the part of a director, manager, secretary or other like officer of the body corporate or any officer purporting to act in any such capacity, he, as well as the body corporate, where practicable, shall be deemed to have committed the offence.	
	(3).	Notwithstanding subsection (1), where a body corporate is convicted of an offence under this Act, the Court may order that the body corporate shall be wound up and all its assets and properties forfeited to the state.	
	(4).	Nothing contained in this section shall render a person liable to punishment, where he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of the offence.	
	45.	(1) Without prejudice to any contractual agreement between an employer and employee, an employee shall relinquish or surrender all codes and access rights to his employer immediately upon disengagement from employment.	Employees responsibility

Part V, Section 43 subsection – Reporting cyber threats.

Part V, Section 44 subsection – Breach of confidence by service providers.

Part V, Section 45 subsection – Employees responsibility.

- Specify the imprisonment period and/or the penalty amount in the section to ensure the Minister and Judge cannot arbitrarily change it favouring their friends and family. In Part III – Offences and Penalties of the Nigeria "[Cybercrimes \(Prohibition, prevention, ECT\) Act, 2015](#)", you will see an excellent example of how it's done to avoid favouritism or misuse of power. You can also see examples at [PART II - Offences , Section 4, subsection \(1\) of the HIPCAR Model Policy Guidelines and Legislative Text](#)

Part V: Offences

Text from the Bill	Findings	Why is it important	Recommendations
--------------------	----------	---------------------	-----------------

<div>30</div> <div>No.</div> <div>The Cyber Crime Act</div> <div>2020</div> <div>(2) An employee who, without any lawful reason, continues to hold onto the code or access right of his employer after disengagement without any lawful reason commits an offence and shall be liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div> <div>Corporate liability</div> <div>46. (1) A natural person, who exercises management or supervisory authority, based on - (a) power of representation of a legal person; (a) authority to take decisions on behalf of a legal person; (c) authority to exercise control within a legal person, acting either individually or as part of an organ of the legal person, commits an offence under this Act, for the benefit of the legal person, the legal person shall be liable for the offence under this Act. (2) Where a natural person commits a criminal offence under this Act, for the benefit of a legal person, due to the lack of supervision or control by a natural person, the legal person shall be liable for the offence under this Act.</div> <div>PART VI - ADMINISTRATION AND ENFORCEMENT</div> <div>47. (1) There shall be a National Cyber Security Incident Response Coordination Center responsible for managing cyber security incidents in Sierra Leone headed by the National Cyber Security Coordinator, nominated by the Minister. (2) The National Cyber Security Coordinator shall be responsible for cyber security issues under this Act including -</div> <div>Co-ordination and enforcement</div>	<div>No.</div> <div>The Cyber Crime Act</div> <div>2020</div> <div>51</div> <div>(a) provision of support to computer systems and networks in preventing and combating cybercrime in Sierra Leone;</div> <div>(b) formulation and implementation of national cyber security policy and cyber security strategy;</div> <div>(c) overseeing of the management of computer forensic laboratories;</div> <div>(d) provision of support to the Judiciary and other law enforcement agencies in the discharge of their functions in relation to cybercrime in Sierra Leone;</div> <div>(e) promotion of Sierra Leone's involvement in international cyber security cooperation; and</div> <div>(f) doing such other acts or things that are necessary for the effective performance of the functions of the relevant security and enforcement agencies under this Act.</div> <div>48. (1) There is established, a National Cybersecurity Advisory Council comprising the President as Chairman and the following other members - (a) the Minister, Ministry of Finance; (b) the Attorney-General and Minister of Justice; (c) the Minister of Internal Affairs;</div> <div>Establishment of the National Cybersecurity Advisory Council</div>	<div>Part V, Section 46 subsection (2) – Corporate liability.</div>	<ul style="list-style-type: none">Specify the imprisonment period and/or fine amount in the section to ensure the Minister and Judge cannot arbitrary change it in favor of their friends and family. In Part III – Offences and Penalties of the Nigeria “<u>Cybercrimes (Prohibition, prevention, ECT) Act, 2015</u>” you will see a good example of how its done to avoid favoritism and misuse of power. You can also see examples at <u>PART II - Offences , Section 4, subsection (1) of the HIPCAR Model Policy Guidelines and Legislative Text</u>
--	--	---	--



Part VI

Administration and Enforcement

Sections 47 to 50

Part VI: Administration and Enforcement

- 47. Co-ordination and enforcement.
- 48. Establishment of the National Cybersecurity Advisory Council.
- 49. Functions and powers of the Council.
- 50. Establishment of National Cybersecurity Fund.

Part VI: Administration and Enforcement

Text from the Bill		Findings	Why is it important	Recommendations
<div>50</div> <div>No.</div> <div>The Cyber Crime Act</div> <div>2020</div> <div>Corporate liability.</div> <div>(2) An employee who, without any lawful reason, continues to hold unto the code or access right of his employer after disengagement without any lawful reason commits an offence and shall be liable upon conviction to such fine or term of imprisonment as the Minister may, by Regulation made under this Act, prescribe.</div> <div>46. (1) A natural person, who exercises management or supervisory authority, based on -</div> <div>(a) power of representation of a legal person;</div> <div>(a) authority to take decisions on behalf of a legal person;</div> <div>(c) authority to exercise control within a legal person, acting either individually or as part of an organ of the legal person,</div> <div>commits an offence under this Act, for the benefit of the legal person, the legal person shall be liable for the offence under this Act.</div> <div>(2) Where a natural person commits a criminal offence under this Act, for the benefit of a legal person, due to the lack of supervision or control by a natural person, the legal person shall be liable for the offence under this Act.</div> <div>PART VI - ADMINISTRATION AND ENFORCEMENT</div> <div>47. (1) There shall be a National Cyber Security Incidence Response Coordination Center responsible for managing cyber security incidents in Sierra Leone headed by the National Cyber Security Coordinator, nominated by the Minister.</div> <div>(2) The National Cyber Security Coordinator shall be responsible for cyber security issues under this Act including -</div>		<div>No.</div> <div>The Cyber Crime Act</div> <div>2020</div> <div>51</div> <div>(a) provision of support to computer systems and networks in preventing and combating cybercrime in Sierra Leone;</div> <div>(b) formulation and implementation of national cyber security policy and cyber security strategy;</div> <div>(c) overseeing of the management of computer forensic laboratories;</div> <div>(d) provision of support to the Judiciary and other law enforcement agencies in the discharge of their functions in relation to cybercrime in Sierra Leone;</div> <div>(e) promotion of Sierra Leone's involvement in international cyber security cooperation; and</div> <div>(f) doing such other acts or things that are necessary for the effective performance of the functions of the relevant security and enforcement agencies under this Act.</div> <div>48. (1) There is established, a National Cybersecurity Advisory Council comprising the President as Chairman and the following other members -</div> <div>(a) the Minister, Ministry of Finance;</div> <div>(b) the Attorney-General and Minister of Justice;</div> <div>(c) the Minister of Internal Affairs;</div> <div>Establishment of the National Cybersecurity Advisory Council.</div>	<div>Part VI, Section 47 subsection (1) & (2) – Corporate liability.</div> <div>There is a concern that the head of this position is based on an appointment by the Minister.</div> <div>There is already a concern that SL does not have Cybercrime legal practitioners. Having someone else leading this effort with little or no experience in Cybersecurity (threat and incident response) will be detrimental to the success of this bill's implementation and might negatively impact citizens if poor decisions are made due to the lack of expertise.</div> <div>The CSIRT head is not the same as being ahead of IT. This individual should have several years of experience in Cybersecurity, no criminal record (corruption included). Otherwise, there could be bias in investigating and solving sensitive issues that pertain to specific people or person in question of an incident. The motivation will be different if the person in charge is acting independently, based on their expertise and integrity. Rather than through connection.</div>	<div>If for any reason an incompetent individual is serving as the head in this position, that individual could make poor decisions. And those decisions could affect innocent citizens.</div> <div>Make the position public to all and be strict on years of experience excluding educational experience. The individual should have worked as a Cybersecurity expert for at least 10 years and have worked in incident response and threat, computer forensic, etc. They have to understand compliance and have a strong policy background in Cybersecurity.</div>

Part VI: Administration and Enforcement

Text from the Bill		Findings	Why is it important	Recommendations
50	No. The Cyber Crime Act 2020	No. The Cyber Crime Act 2020 51	Part VI, Section 47, subsection (2) a to f – Corporate liability. <ul style="list-style-type: none">Does the government have a cybercrime team?What is the minimum experience requirement as an SL CSIRT personnel?	<ul style="list-style-type: none">Principles of scientific interpretation increase the reliability and defensibility of decisions throughout an investigation, not only in the final expert testimony phase. Such formalization of decision-making is particularly valuable when dealing with digital evidence due to the potential for information overload, inaccuracy, error and bias. To confront these challenges consistently and to reduce the risk of mistakes, it is important to have qualified experts investigating these cases.Consult other countries with reputable CSIRT institutions (other African countries, like Nigeria, South Africa, Rwanda, Etc.)Ensure that this institution is unique and have the right individuals for each area. Remember, there will be lives of innocent citizens involved, and every wrong decision made will impact an individual found guilty wrongfully.
<p>Corporate liability.</p> <p>46. (1) A natural person, who exercises management or supervisory authority, based on -</p> <ul style="list-style-type: none">(a) power of representation of a legal person;(a) authority to take decisions on behalf of a legal person;(c) authority to exercise control within a legal person, acting either individually or as part of an organ of the legal person, <p>commits an offence under this Act, for the benefit of the legal person, the legal person shall be liable for the offence under this Act.</p> <p>(2) Where a natural person commits a criminal offence under this Act, for the benefit of a legal person, due to the lack of supervision or control by a natural person, the legal person shall be liable for the offence under this Act.</p> <p>PART VI - ADMINISTRATION AND ENFORCEMENT</p> <p>47. (1) There shall be a National Cyber Security Incident Response Coordination Center responsible for managing cyber security incidents in Sierra Leone headed by the National Cyber Security Coordinator, nominated by the Minister.</p> <p>(2) The National Cyber Security Coordinator shall be responsible for cyber security issues under this Act including -</p>		<p>(a) provision of support to computer systems and networks in preventing and combating cybercrime in Sierra Leone;</p> <p>(b) formulation and implementation of national cyber security policy and cyber security strategy;</p> <p>(c) overseeing of the management of computer forensic laboratories;</p> <p>(d) provision of support to the Judiciary and other law enforcement agencies in the discharge of their functions in relation to cybercrime in Sierra Leone;</p> <p>(e) promotion of Sierra Leone's involvement in international cyber security cooperation; and</p> <p>(f) doing such other acts or things that are necessary for the effective performance of the functions of the relevant security and enforcement agencies under this Act.</p> <p>48. (1) There is established, a National Cybersecurity Advisory Council comprising the President as Chairman and the following other members -</p> <p>Establishment of the National Cybersecurity Advisory Council.</p> <ul style="list-style-type: none">(a) the Minister, Ministry of Finance;(b) the Attorney-General and Minister of Justice;(c) the Minister of Internal Affairs;		

Part VI: Administration and Enforcement

Text from the Bill	Findings	Why is it important	Recommendations	
<div><div>54</div><div>No.</div><div>The Cyber Crime Act</div><div>2020</div></div> <div><div>(d) promote the development of educational programs and research in cyber security defences, techniques and processes.</div></div> <div><div>(2) The Council shall have power to regulate its proceedings and make standing orders with respect to the holding of its meetings, notices to be given, the keeping of minutes of its proceedings and such other matters as Council may, from time to time determine.</div></div> <div><div>Establishment of National Cybersecurity Fund.</div><div>50. (1) There is established a fund which shall be known as the National Cyber Security Fund.</div><div>(2) There shall be paid and credited into the Fund established under subsection (1) and domiciled in the Central Bank of Sierra Leone -</div><div>(a) a levy of 0.005 of all electronic transactions by the businesses specified in the Schedule;</div><div>(b) grants-in-aid and assistance from donor, bilateral and multilateral agencies;</div><div>(c) all other sums accruing to the Fund by way of gifts, endowments, bequests or other voluntary contributions by persons and organisations;</div><div>Provided that the terms and conditions attached to such gifts, endowments, bequests or contributions will not jeopardize the functions of the Agency; and</div><div>(d) all other monies or assets that may, from time to time accrue to the Fund.</div></div>	<div><div>No.</div><div>The Cyber Crime Act</div><div>2020</div><div>55</div></div> <div><div>(3) All monies accruing to the Fund shall be exempted from income tax and all contributions to the Fund shall be tax deductible.</div></div> <div><div>(4) The levy imposed under paragraph (a) of subsection (2) shall be remitted directly by the affected businesses or organizations into the Fund domiciled in the Central Bank within a period of 30 days.</div></div> <div><div>(5) An amount not exceeding 30 percent of the Fund may be allocated for programs relating to public education and awareness raising on cyber security issues.</div></div> <div><div>(6) The office of the National Computer Security Incidence Response Team Coordination Centre shall keep proper records of the accounts which shall be audited in accordance with guidelines provided by the Auditor-General of Sierra Leone.</div></div> <div><div>PART VII - MISCELLANEOUS PROVISIONS</div></div> <div><div>51. as it considers necessary or expedient for giving effect to Regulations this Act.</div></div>	<p><u>Part VI, Section 49, subsection (1) d – Functions and powers of Council</u></p> <ul style="list-style-type: none">I don't see any area on the bill that states how often the bill will be reviewed or revisited, including a periodic amendment by the National Cybersecurity Advisory Council Committee.This comment is not a finding but rather a question. Will the promotion of the educational program, research, Etc., be in collaboration with other institutions in the country.	<ul style="list-style-type: none">Anything computer and cyber-related changes every day, and it is best practice to revisit the bill periodically and make amendment where necessaryWill there be an enforcement of a cybersecurity awareness month. Is there any established curriculum already for schools and institutions?	<ul style="list-style-type: none">Make room to update the bill periodically and establish version control on the bill.The bill should include computer and cybercrime teachings, including data privacy, in early education and up to the university level. Of course, all businesses and government institutions.



PART VII - MISCELLANEOUS PROVISIONS

Section 51

Part VII: MISCELLANEOUS PROVISIONS

51. Regulations

Part VII: MISCELLANEOUS PROVISIONS

Text from the Bill	Findings	Why is it important	Recommendations
<p>PART VII - MISCELLANEOUS PROVISIONS</p> <p>51. as it considers necessary or expedient for giving effect to Regulations. this Act.</p>	<ul style="list-style-type: none">There are no related cybersecurity bills or laws referenced in the bill.	<ul style="list-style-type: none">A standalone Cyber Crime bill, without related laws for Data Protection and Privacy can leave loopholes for violation of human rights, privacy and data integrity.	<ul style="list-style-type: none">Provide a reasonable and timely timeline for a Data Protection and Privacy bill.Develop a "Search and Seizure of Digital Evidence" plan, law, or policy and guidelines.



References

References

1. Okoiti v. Communications Authority of Kenya. <https://globalfreedomofexpression.columbia.edu/cases/okoiti-v-communications-authority-kenya/>
2. Kenya Human Rights Commission v. Communications Authority of Kenya. <https://globalfreedomofexpression.columbia.edu/cases/kenya-human-rights-commission-v-communications-authority-kenya/>
3. Kenya 2018 Human rights issues included: arbitrary infringement of citizens' privacy rights; censorship; The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa. <http://www.scielo.org.za/pdf/pelj/v22n1/15.pdf>
4. An overview of the digital forensic investigation infrastructure of Ghana. <https://www.sciencedirect.com/science/article/pii/S2589871X20300619>
5. Ensuring the Legality of the Digital Forensics Process in South Africa. <https://research.ijcaonline.org/volume68/number23/pxc3887432.pdf>
6. Digital Forensic Standards for Digital Forensic Practitioners in South Africa. <https://www.acfesa.co.za/resources/Documents/Digital%20Forensic%20Standards%20for%20Digital%20Forensic%20Practitioners%20in%20South%20Africa%20-%20July%202020.pdf>
7. Comparison of Budapest Convention Articles on International Cooperation and clauses included in the Trinidad & Tobago Cybercrime Legislations) - February 2021. <https://rm.coe.int/0900001680a1a06a>
8. South Africa Introduces Revised Cybercrime Legislation, Acknowledging Criticism. <https://www.cfr.org/blog/south-africa-introduces-revised-cybercrime-legislation-acknowledging-criticism>
9. Webinar with US Department of Justice and Council of Europe – 2020. <https://www.coe.int/en/web/cybercrime/-/cybercrime-in-africa-and-the-challenges-of-international-cooperation>
10. Capacity-building on cybercrime and e-evidence. The experience of EU/Council of Europe joint projects 2013-2017. <https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-April-2017/V1702143.pdf>
11. The Search and Seizure of Digital Evidence by Forensic Investigators in South Africa. <http://www.scielo.org.za/pdf/pelj/v22n1/15.pdf>
12. An overview of the digital forensic investigation infrastructure of Ghana. <https://www.sciencedirect.com/science/article/pii/S2589871X20300619>
13. Ensuring the Legality of the Digital Forensics Process in South Africa. <https://research.ijcaonline.org/volume68/number23/pxc3887432.pdf>
14. EMERGING MARKETS TELECOMMUNICATION SERVICES LTD v. ENEYE - <http://lawpavilionpersonal.com/ipad/books/46193.pdf>
15. RAPHAEL CUBAGEE VRS MICHAEL YEBOAH ASARE & 2ORS.pdf - <https://ghalii.org/gh/judgment/Supreme%20Court/2018/184/RAPHAEL%20CUBAGEE%20VRS%20MICHAEL%20YEBOAH%20ASARE%20%26%202ORS.pdf>
16. M W K v another v Attorney General & 3 others [2017] - <https://globalfreedomofexpression.columbia.edu/cases/eg-v-attorney-general/>
17. Samson Mumo Mutinda v Inspector General National Police Service & 4 others [2014] - https://repository.up.ac.za/bitstream/handle/2263/60070/Morusoi_Right_2017.pdf?sequence=1&isAllowed=y