LIRNEasia
Pro-poor. Pro-market.

Evaluating policy influence

LIRNEasia inputs for Cyber Security Bill

LIRNEasia
August 2023

Background and objective of this report:

- On May 23rd 2019, the Government of Sri Lanka posted the Draft Cyber Security Bill on the SL CERT website and invited public comments/input.
- LIRNEasia submitted written comments in response to the SL CERT's request.
- Our comments submitted on 5th June 2019 are available at https://lirneasia.net/2019/06/comments-on-the-cyber-security-bill-sri-lanka-2019/

- Subsequently in August 2023, the Government of Sri Lanka posted an updated version of the Cyber Security Bill and invited public comments
- LIRNEasia once again submitted written comments on 18th August 2023, which can be accessed here https://lirneasia.net/2023/08/comments-on-the-cyber-security-bill-sri-lanka-2023/

- **The purpose of this report is to analyze the extent to which our 2019 input has been taken into account in the the updated (August 2023) version of the proposed bill**

The most significant impacts of the LIRNEasia comments are:

Institutional arrangements clarified:

- June 2019 Bill
- This refers to three separate institutions: the Cyber Security Agency of Sri Lanka (CSASL), the National Cyber Security Operations Center (NCSOC), and the existing Sri Lanka Computer Emergency Readiness Team (SLCERT).
- Commenting on this, LIRNEasia pointed out that it was not clear why three separate institutions were necessary. The comments also pointed out that the separation of powers, roles and responsibilities across the three organisations were unclear and gave a detailed explanation of how this was problematic

- August 2023 Bill
-

  In the Bill issued in 2023 the institutional arrangements have been simplified to resolve the issues pointed out above. The Bill provides for establishment of one authority: Cyber Security Regulatory Authority of Sri Lanka (the 'Authority'), which will be the apex executive body for the implementation of all matters relating to civilian aspects of cyber security (Section 3). SLCERT is to be wound up when the Bill becomes an Act of Parliament and the powers and functions exercised by the SLCERT will be exercised by the Authority. (Section 18)

The most significant impacts of the LIRNEasia comments are:

‘Cyber Security Incident’ defined

- June 2019 Bill
- As noted in the LIRNEasia comments, the June 2019 Bill referred repeatedly to “cyber security incident[s]”. For example: Part VII 21(3) “Every person who being the owner of a CII who fails, without reasonable cause, to fulfill the obligations imposed under this Act or fails to report cyber security incidents to the Agency and CERT... ‘ The LIRNEasia comments pointed out that in spite of this, the Bill did not define what entails a “cyber security incident’.

- August 2023 Bill
- The term cyber security incident has been defined as follows: ‘…means any act or activity carried out without lawful authority on a computer, computer system or related devices that may affect the cyber security of that computer, computer program, computer system or device’

The most significant impacts of the LIRNEasia comments are:

Recommendations regarding imposition of penalties partially adopted:

- June 2019 Bill
- LIRNEasia comments pointed out that by mandating a fixed penalty (financial and jail time), the Bill violates the important principle that the punishment should be proportional to the crime. Attacks on a CII that causes billions of rupees of damage and one that causes hundreds of rupees of damage could be treated equally when assigning such penalties. The comments proposed that other methods of calculating fines should be considered - for example, a penalty that increases by a prescribed amount each day an identified security violation is left unaddressed.

- August 2023 Bill
- In the 2023 Bill prior amendments have been made to accommodate some the recommendations. With regard to penalties, a warning in writing is to be issued by the Board, and time period may be specified in the warning to conform to the requirements, or to show cause as to why such requirements are not being complied with.
- The Agency should also take into consideration the ‘nature and the gravity of such non – compliance.’ If the warning is not complied with the Agency shall, ‘…taking into consideration the nature and gravity of such non-compliance, by notice require such person to pay a penalty not exceeding rupees one million’. -Sec 25(2)
- Furthermore if the person commits a second offence, such person shall also ‘…be liable to the payment of an additional penalty of twice the amount’ - Section 25 (3)

The most significant impacts of the LIRNEasia comments are:

Qualifications of Board of Directors amended:

- In the 2019 version the regulatory authority is the Cyber Security Agency of Sri Lanka (CSASL). Section 5 gives the constitution of the Board of directors of the Agency: four ex officio members and “three members appointed by the Minister, each of whom have over 25 years’ experience and have demonstrated professional excellence in the fields of Information and Communication Technology, Public or Private sector Management, Law or Finance.” (Section 5(1)(b))

- LIRNEasia commented that the requirement of “over 25 years’ experience” for a Board member was unnecessarily prescriptive as Cybersecurity and the complexity of threats evolve exponentially with each year. LIRNEasia also recommended that the composition of the Board should allow for the appointment of personnel from at least two key sectors, i.e. Financial Services (banking), and Internet Service Providers (ISPs) or Telecommunications Network Operators or Information Communications Technology (ICT) Service Providers

- <u>August 2023 Bill</u>
- In the 2023 version the regulatory authority is the Cyber Security Regulatory Authority, and the years of experience for an appointed Board member has been reduced to 15 years.

- As per section 6, the Board will have five ex officio members and ‘…four persons appointed by the President, (hereinafter referred to as the “appointed members”) each of whom shall have over fifteen years of experience and demonstrated professional excellence in the fields of cyber security, information and communication technology, public or corporate sector administration, management, law or finance.’

Impact of comments

Assessment of impact of comments - 1

Section in June 2019 Bill	Comments	Level of impact
Section 3. (1) There shall be established an agency which shall be called the Cyber Security Agency of Sri Lanka (hereinafter referred to as ‘‘the Agency’’) for the purposes of this Act . (3) The Agency shall be the Apex and Executive body for all matters relating to cyber security policy in Sri Lanka and shall be responsible for the implementation of the National Cyber Security Strategy of Sri Lanka. (2) In the discharge of its powers and functions, the Agency shall at all times consult Sri Lanka Computer Emergency Readiness Team and ensure the said powers are carried out through the institutions established under Part IV of this Act 15.(1) The Sri Lanka Computer Emergency Readiness Team, incorporated as a Company under the Companies Act No. 7 of 2007 (herein after referred to as “the CERT”) shall be the national point of contact for cyber security incidents in Sri Lanka. (2) The CERT shall at all times assist the Agency in the exercise, performance and discharge of its powers and functions under this Act 16.(1) There shall be a National Cyber Security Operations Centre (hereinafter referred to as “NCSOC”) designated by the Minister for the purpose of this Act.	The proposed bill refers to three separate institutions: The Cyber Security Agency of Sri Lanka (CSASL), the National Cyber Security Operations Center (NCSOC), and the existing Sri Lanka Computer Emergency Readiness Team (SLCERT). Of these, CSASL is meant to be the “apex and executive body for all matters relating to cyber security policy in Sri Lanka and shall be responsible for the implementation of the National Cyber Security Strategy of Sri Lanka” (Part II 3(3)). This implies that SLCERT and NCSOC will be subordinate to CSASL. However it is not immediately obvious why three separate institutions are necessary. Siloes and delays in communication across institutions are not conducive to the cybersecurity area, where working fast and staying ahead of emergent threats is imperative. Increased budgets and bloated institutional structures are also unaffordable in budget- and skills-constrained countries like Sri Lanka.have the personnel to actively compel registration and compliance. The separation of powers, roles and responsibilities across the three organisations are unclear. For example, NCSOC and SLCERT both appear to have responsibility for proactive and reactive handling of cybersecurity (Part IV 15(3)(b)). It also appears that both organizations are a first point of contact for cybersecurity matters in Sri Lanka - for example, SLCERT will “act as the National Point of Contact for handling cyber security incidents”, but NCSOC shall “gather cyber threat intelligence from local and international sources” which appears to make NCSOC also a natural point of contact. Furthermore, Part IV 15(3)(h) states that SLCERT will share cyber threat intelligence with government institutions, other sectors, and members of the public in a timely manner. Part IV 16(5)(d) states that NCSOC will provide cyber threat intelligence information to law enforcement authorities, SLCERT and to the Agency to prevent cyber security incidents. Another confusion is about the seemingly relative imbalance of power between CSASL and SLCERT. Part II 4(2) states that “in the discharge of its powers and functions, the Agency [CSASL] shall at all times consult Sri Lanka Computer Emergency Readiness Team [SLCERT] and ensure the said powers are carried out through the institutions established under Part IV of this Act.” While it is natural that consultation shall occur with an agency that is likely to have a high level of expertise, it is unclear why CSASL has to consult SLCERT at all times.	Accepted

Assessment of impact of comments: 2

Section in June 2019 Bill	Comments	Level of impact
Section 12 (5) The term of the office of the Director General appointed under subsection (1) hold office for a period of three years from the date of appointment and shall be eligible for reappointment. (9) The Director General may be removed from office by the Agency in the event that he – (a) becomes permanently incapable of performing his duties; (b) has done any act which is of a fraudulent or illegal character or is prejudicial to the interest of the Agency; or (c) has failed to comply with any directions issued by the Agency.	Re-appointment should be subject to the Director General meeting agreed performance criteria (key performance indicators, KPIs). It is important that the CSASL remains a nimble, efficient and effective organisation if the objectives of the Strategy are to be achieved. Removal of the Director General: Should also include consistently fails to perform in accordance with agreed performance criteria (KPIs). Major breaches (once defined) should count as a blow to performance in such KPIs.	Not accepted

Assessment of impact of comments: 3

Section in June 2019 Bill	Comments	Level of impact
4. (1) The powers, duties and functions of the Agency shall be to :- (c) identify and designate Critical Information Infrastructure (hereinafter referred to as "the CII") both in government and other relevant sectors, in consultation with relevant stakeholders; (d) develop strategies and plans for the protection of CII in consultation with the owners of CII;	The bill gives CSASL the power to identify and designate CIIs. Designating a computer system as a CII could even be used as a method of control (e.g. to extend government control over private institutions and systems), a way to extending criminality to actions that are otherwise acceptable but politically inconvenient. This would have a chilling effect on freedom of expression, privacy as well as investment incentives. It is proposed therefore that the CSASL should follow a transparent, consultative and a multistakeholder process to classify (and de-classify) CIIs prior to Gazetting. Such procedures should be adopted especially when designating non-governmental infrastructure as a CII. There should be opportunity for the impacted parties to make submissions and be heard before such decisions are finalised. It is also possible to err on the side of being overly cautious when it comes to classifying CIIs, and feel that including any and everything as CII is the solution. Yet each designation imposes costs on the owners of the CII, and reactive measures cost more than proactive measures to ensure security. Where possible, the economic costs and benefits of designating a system as a CII should be addressed prior to its designation. Where quantification is not possible, a qualitative discussion should be done.	Partially accepted The 2023 Bill provides for for 'the identification of a computer, computer program, computer system or related device as a "Critical National Information Infrastructure" (CNNI).' There is no multi stakeholder process and no clear and transparent criteria given on how CNNIs will be identified. However the Authority must inform the owner regarding the classification. Furthermore Section 20 (3) specifies that the Authority may '..if it considers appropriate, obtain the views of the owner of such Critical National Information Infrastructure relating to such a Critical National Information Infrastructure and publish such Critical National Information Infrastructure in the Gazette."

Assessment of impact of comments - 4

Section in June 2019 Bill	Comments	Level of impact
21. (1) Every person who being the owner of a CII who fails, without reasonable cause, to fulfill the obligations imposed under this Act or fails to report cyber security incidents to the Agency and CERT, in accordance with section 19(1) (c) to (f), commit an offence under this Act and shall on conviction be liable to a fine not exceeding two hundred thousand rupees or to imprisonment for a term not exceeding two years or to both such fine and imprisonment.	The proposed act also refers repeatedly to "cyber security incident[s]". For example: Part VII 21(3) *"Every person who being the owner of a CII who fails, without reasonable cause, to fulfill the obligations imposed under this Act or fails to report cyber security incidents to the Agency and CERT,... etc.* Yet nowhere does it define what entails a "cyber security incident", and could result in operations being inundated with everything from lost passwords upwards, or the reverse - only being notified when billion shave gone missing. a. It is however possible that a "cyber security incident" be defined so broadly that it criminalizes behaviour that should not be, or it takes away other fundamental freedoms such as the freedom of expression, or the right to privacy. As such, the definition of what entails a "cyber security incident" should be done in a consultative, transparent and multi-stakeholder process. There should be a process to update this definition at a regular intervals.	Partially accepted. The term 'Cyber security incident' has been defined in the 2023 Bill. However there is no provision for updating the definition or mention that the definition was arrived at through a consultative process.

Assessment of impact of comments - 5

Section in June 2019 Bill	Comments	Level of impact
21. (1) Every person who being the owner of a CII who fails, without reasonable cause, to fulfill the obligations imposed under this Act or fails to report cyber security incidents to the Agency and CERT, in accordance with section 19(1) (c) to (f), commit an offence under this Act and shall on conviction be liable to a fine not exceeding two hundred thousand rupees or to imprisonment for a term not exceeding two years or to both such fine and imprisonment.	By mandating a fixed penalty (financial and jail time), the Bill violates the important principle that the punishment should be proportional to the crime. Attacks on a CII that causes billions of rupees of damage and one that causes hundreds of rupees of damage could be treated equally when assigning such penalties. We propose other methods of calculating fines be considered - for example, a penalty that increases by a prescribed amount each day an identified security violation is left unaddressed. Here, the number of days acts as a proxy for the damage caused. Another question to be asked is if there a need to introduce punitive actions on parties deemed to have failed in their responsibilities to contain any fallout from "cybersecurity incidents"? Will this be an effective approach to address the problem?	Partially accepted. In the 2023 Bill, prior to imposition of penalties a warning in writing is to be issued by the Board, and time period may be specified in the warning to conform to the requirements, or to show cause as to why such requirements are not being complied with. If the warning is not complied with the Agency shall, '…taking into consideration the nature and gravity of such non-compliance, by notice require such person to pay a penalty not exceeding rupees one million'. - Sec 25(2) Furthermore if the person commits a second offence, such person shall also '…be liable to the payment of an additional penalty of twice the amount' - Section 25 (3)

Assessment of impact of comments - 6

Section in June 2019 Bill	Comments	Level of impact
24. The Agency or any other officer authorized in writing in that behalf by the Agency, for the purpose of ascertaining whether the provisions of this Act or any regulation made thereunder are being complied with may, on reasonable ground - (a) enter, inspect and search premises of the designated CIIs; (b) examine and take copies of any document , record or part thereof pertaining to such CIIs; (c) examine any person whom he has reasonable cause to believe that such person is an owner or employee of such CII.	Power to enter a CII premises should only be afforded to CSASL if they are in possession of a warrant issued by a court. CSASL should first be required to apply for such a warrant and the courts have to be satisfied that there is enough reason to permit such entry and investigation to issue such a warrant. The warrant preferably should authorise a named investigation officer, and any other officer whom CSASL has authorised, in writing to accompany the investigation officer. The warrant should specify the document or record that can be examined and copies to be taken. The copies taken should only be limited to what has been listed in the warrant. The warrant should be valid for a specified period and not be issued for an indefinite period of time.	Partially accepted Section 28 of 2023 Bill (2) For the purpose of carrying out any function under subsection (1), written consent to enter such premises shall be obtained from the owner, occupier or the person in charge of such premises. (3) Where the consent required to be obtained under subsection (2) is unfairly refused, any officer of the Authority specifically authorized by the Director General under subsection (1) may obtain from a Magistrate's Court, a search warrant for the purpose of entering such premises and exercising all or any of the powers conferred upon such officer by such search warrant.