5 June 2019

Mr. Lal Dias
CEO
Sri Lanka CERT|CC
Room 4-112, BMICH
Bauddhaloka Mawatha
Colombo 07

Dear Mr. Dias:

LIRNE*asia*'s Response to Ministry of Digital Infrastructure and Information Technology (MDIIT) and Sri Lanka CERT|CC's Invitation for Comments on the Cyber Security Bill

LIRNE*asia* welcomes the opportunity to submit our views and comments on the proposed Cyber Security Bill.

LIRNE*asia* is a pro-poor, pro-market think tank whose mission is catalyzing policy change through research to improve people's lives in the emerging Asia Pacific. LIRNE*asia* has been active in Sri Lanka and the rest of the Asia-Pacific region since 2005, conducting research and advocating for policy changes in the ICT sector.

Our response is attached for your kind consideration.

For questions regarding this submission, please contact Yudhanjaya WIjeratne, Senior Researcher, LIRNE*asia* at yudhanjaya@lirneasia.net or +94-11-2671160.

Thank you.
Sincerely,

<Signed>

Helani Galpaya
Chief Executive Officer
helani@lirneasia.net

CC: (1) Mr. D. C. Dissanayake, Secretary, MDIIT
(2) Mr. Jayantha Fernando, Director & Legal Advisor, ICTA
(3) Mr. Gamini Wanasekera, Advisor to the Hon. Minister, MDIIT

Attachment: LIRNEasia's comments on proposed Cyber Security Bill

Attachment 1: LIRNEasia's comments on proposed Cyber Security Bill

This submission is in response to SLCERT's invitation to comment on the Cyber Security Bill uploaded on its website on 23rd May 2019.

Our submission addresses specific concerns related to the institutional arrangements, powers and functions and the governance and administration of the Cyber Security Agency of Sri Lanka.

Because we believe the framing of the Cyber Security environment in the country should be done well, we also provide a separate thesis on a different, and more effective approach to cybersecurity, by using elements of public health policy (see point 15).

Comments on Institutional Arrangements: CSASL, SLCERT, NCSOC

1. 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.
    a. **If subordinate organizations to CSASL must be created, one possibility is that the functions of the SLCERT and NCSOC be joined together under a single institution.**
    b. **We may take lessons from Singapore which has a well-defined structure with the National Cybersecurity Agency of Singapore as the "national agency overseeing cybersecurity strategy, operation, education, outreach, and ecosystem development"[1] and the Singapore Computer Emergency Response Team (SingCERT) a unit within the Agency responsible for facilitating the detection, resolution and**

[1] https://www.csa.gov.sg/

prevention of cyber security related incidents on the Internet relevant to Singapore.[2]

2. 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.
    a. **If two separate organizations (SLCERT and NCSOC) that are subordinate to CSASL must be maintained, one possible solution is to designate clearly that one institution handles proactive measures (broadly defined), while the other, SLCERT, handles reactive measures.**
    b. **If two separate organizations (SLCERT and NCSOC) that are subordinate to CSASL must be maintained, it should be clearly defined who will deal with outside institutions - within and outside of Sri Lanka.**

3. 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.
    a. **Propose removing the need to consult "at all times", and specify subjects and topics on which SLCERT shall be consulted.**

[2] https://www.csa.gov.sg/singcert

b. **Propose defining clearly the process of consultation, the course of action when CSASL disagrees with SLCERT's recommendations.**

4. Further contributing to the confusion of hierarchies is Part II 5(1)(a)(iv), which states that a member nominated by the Board of Sri Lanka Computer Emergency Readiness Team is to be an ex-officio member of the CSASL Board. It is unclear why a member of a subordinate institution (SLCERT) should have a seat in the CSASL Board. The reverse makes sense, thinking through normal governance hierarchies.
    a. **Propose at a minimum to allow a Board Member from CSASL to sit on the SLCERT Board.**
    b. **Propose removal of the mandate to have an SLCERT Board member sit on the CSASL Board.**

Comments on CSASL's powers and functions

5. **Classification of CIIs:** The bill gives CSASL the power to identify and designate CIIs. This is of course a necessary step in ensuring that the identified CIIs are adequately protected. It is clear that the CSASL may designate not just government information infrastructure, but also designate whole or parts of privately owned and operated information infrastructure as a CII. Again, this too is necessary, since various sectors (e.g. banking or power/energy information infrastructure) can be seen as vital to the functioning of the nation and its economy. However, it is also possible under conditions of poor oversight to engage in regulatory overreach and designate CIIs too broadly. 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.
    a. **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.

6. 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.
    a. **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.**

7. **Pro-active classification of CIIs and related measures:** The power to classify CIIs as stated in the bill could be interpreted as applying to existing information infrastructure. However, more effective is including classification procedure at infrastructure conceptualization and design stage. This would enable *"security by design"* and similar principles to be incorporated into the infrastructure, and force procurement of infrastructure developers to relevant performance standards. As such, the power to designate CIIs should be interpreted and applied to all stages of infrastructure design and operation.

8. 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.

9. **Offences and Penalties:** 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, 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.
    a. **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.**
    b. **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?**

10. **Due process in the Power of entry, inspection and search:** Part IX 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."*
    a. **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. See Part 6(39) in Singapore's CSA Act for wording on this as a best practice approach: https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312#pr39-.

Comments about governance and administration of CSASL

11. **Qualifications of Board members:** Part II 5(1)(a)(iv) states *"three members appointed by the Minister, (hereinafter referred to as "appointed members") 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."*
    a. **The requirement of "over 25 years' experience" for a Board member is unnecessarily prescriptive. Why 25 years and ambiguity on what specific experience a potential candidate might have? Cybersecurity and the complexity of threats evolve exponentially with each year, from tech-empowered mob action (Anonymous), to code that attacks nuclear reactors (StuxNet) to sophisticated state-affiliated attack/defense groups such as Dragonfly, the Equation Group, APT-3 and APT-10: what is the relevance of experience from unrelated fields?**
    b. **It would be better suited to have someone younger and well versed in recent cybersecurity developments and mitigations to be given a seat on the CSASL Board.**

12. **Board Composition:** Part II 5(1)(a) makes allowances for seven (7) Board members: Secretary from the Ministry of Defence, Secretary from the Ministry of Public Administration, Secretary from the Ministry of Digital Infrastructure and Information Technology (MDIIT), an SLCERT member, and three members appointed by the Minister of MDIIT.

a. **Instead of three Board members appointed by the MDIIT Minister, the composition of the Board must allow for the appointment of 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, to be represented on the Board. It is likely that they will also be able to command more domain knowledge in their respective areas.**

b. **Provisions should be made to ensure that a Civil Society representative is a member of the Board to ensure that privacy and human rights aspects of cyber security are considered in CSASL's activities.**

c. **Provisions should be made so that representatives from the Police and Armed Forces respectively can be part of this Board, as sufficiently large breaches have implications for national security and, in some cases, the use of physical violence may be required to apprehend suspects. Furthermore, interplay between investigations undertaken by branches of the Police or Military may lead to previously unknowable insights.**

13. **Appointment of the Director General:** Part III 12(5) states *"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."*

    a. **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.**

14. **Removal of the Director General:** Part III 12(9) states that *"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."*

a. **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.**

Overarching comments on cybersecurity at a national level

15. **Reframing the thinking on cybersecurity:** In the age of modern cybersecurity and highly connected systems, the classical approach of designating "infrastructure" may not be secure enough (or technically feasible) to maintain effective proactive cyberdefense. We propose examining critical systems and the network of computer connections that they inhabit, and using public-health approaches such as herd immunity and quarantine to effectively isolate and protect systems and implement regulations for critical information paths. For the full thesis, please refer to https://lirneasia.net/2019/06/cybersecurity-graph-theory-and-public-health/.

16. **Beyond government CII:** The Bill is an excellent first step in ensuring the critical infrastructure needed for ensuring the security and proper functioning of the country by focusing on critical elements such as defense, immigration, financial sectors. However, "cybersecurity" needs to be much more broadly conceptualized, and it must apply to what individuals can and should do to stay safe, and what recourse they have to seek damages when their security is violated at individual level. This is beyond the scope of a cybersecurity Bill, and must be looked at as a whole - by considering this, the Computer Crime Bill, the Electronic Transaction Bill, the existing laws of the country (including the criminal code), and international treaties (such as those related to human rights) that Sri Lanka has ratified. Scenario testing would help understand what private citizens need in terms of legal frameworks, and help understand the gaps in cyber security that are still not addressed under any existing law in the country.