Abstract No: SI-07

A qualitative analysis on strengths and weaknesses of Cyber Security Bill 2019 in Sri Lanka

L. G. C. Vithakshana*

Department of Statistics & Computer Science, Faculty of Science, University of Kelaniya, Sri Lanka
chathura_2019@kln.ac.lk*

The Internet as we know it today, is a stark contrast to what it was in its formative years in terms of accessibility, usage, security, user interface and cost to the user. With the development of the Internet and its wide use by businesses for commercial reasons, cybercrimes are also increasing. It is becoming more difficult to protect the computer systems against these crimes. In recent years, an increasing number of cyber-attacks on government domains and private infrastructure within Sri Lanka, raised the need for a robust Cyber Security Strategy to regulate and protect against cyber-attacks. The objective of this research is to qualitatively analyse the strategies and weaknesses of the Cyber Security Bill, 2019 (Bill). The study is carried out as a library-based qualitative analysis based on the Bill as the primary data source while conference papers, journal articles, and online news resources were used as secondary sources. The data collection method was via the Internet. The analysis was carried out by comparing the Bill with reliable sources, including, National Institute of Standards and Technology (NIST) and Computer Emergency Readiness Team (CERT). Throughout the Bill, a lack of interpretation of the extract definitions of terms has been identified. According to the proposed Bill, there are three principal government bodies responsible for identifying and mitigating cyber threats: Cyber Security Agency of Sri Lanka (the Agency), National Cyber Security Operations Centre, and CERT. The newly established government entities must work alongside with well-established private organisations, which may cause conflicts when critical decisions have to be made. Furthermore, the Bill has not mentioned any proactive or reactive mechanism for surveillance, monitoring, and response to social media abuses. Even though the Bill has introduced penalties and imprisonment for violation of the Act, there were no clear limitations defined in the context of cybersecurity and cybercrimes; at what minimum level, an action became a cybersecurity law violation and became a cybercrime. The mechanism to appoint the Director-General of the Agency is not at an acceptable standard, while only two primary qualifications have been required. Well-defined and comprehensive interpretations of cybersecurity-related terms are necessary for this bill to avoid conflicts, while identifying, and regulating the cybercrimes and associated activities. From the perspective of the organisational structure, it might be more efficient to have a centralized structure to ensure timely, quick and critical action to mitigate cybercrimes. A Centralised responsible organisation to act for all cybersecurity-related issues, would be advisable. A suitable criterion for the appointment of the Director-General of the Agency should be established and should not be primarily driven by the seniority and experience, but also assess the suitability with background checks on the person with extensive qualifications. The Board of Directors are also appointed by the Minister himself, which might be driven by political biases. Instead, they can be selected by a panel of experts in the cybersecurity field, national security officials, and law enforcement authorities. Furthermore, a wide range of areas should be covered by the Bill, including power plant protection, banking sector, telecommunication, and healthcare. Proposing the Bill is an exceptional jump towards the brighter future of protection of Sri Lanka's Cyberspace. However, it should go through significant discussions and necessary revisions incorporated for it to become truly effective in combatting cybercrimes in the country.

Keywords: Cybercrime, Cyber Security Bill, Cyberwarfare, Information security, Sri Lanka