A Critical Examination of Whether The National Security of Sri Lanka is Adequately Protected in Cyberspace

DU Jayasinghe[1#] and GD De Silva[1]

[#]dulmi.jayasinghe@gmail.com

Abstract: *The 21st Century is the century of Hi-tech and is no stranger to cyberattacks. Even Sri Lanka has undergone many cyberattacks in the past which have also raised national security concerns. Whilst Sri Lanka has enacted legislation to deal with computer crimes such as the Computer Crime Act No. 24 of 2007, Evidence (special provisions) Act No 1995, Electronic Transactions Act No. 19 of 2006, Payment Devices Frauds Act No 30 of 2006, and the Intellectual Property Rights Act No. 36 of 2003, there are no enacted cybersecurity laws. In fact, the two Bills, namely the Cyber Security Bill and the Defence Cyber Commands Act have still not been passed even though it was proposed in 2018. Consequently, only Section 06 of the Computer Crime Act No. 24 of 2007 mentions computer crime offences committed against national security. Thereby, the research problem of this article is to examine whether the current cyber laws in Sri Lanka are sufficient to adequately protect the country's national security in cyberspace. The research objectives of this research are to examine whether the current cyber laws protect the national security in Sri Lanka (1), to evaluate the implementation process in the criminal justice system in terms of cyber laws (2) and to gain some perspectives on how other countries such as the United Kingdom and the United States of America have formulated legislation to protect their country's national security in the cyberspace. This research is an internet-based desk-based research and concludes that the existing legislation is insufficient to adequately protect the national security in Sri Lanka and that it is imperative to enact the two draft cybersecurity Bills at the earliest.*

Keywords: *Cyber-attacks, National Security, Cyber Security Laws*

1. Introduction

Cybercrimes is a rampant issue in Sri Lanka. The following examples illustrate that hacking websites containing sensitive data can be exploited politically, economically and socially, which would lead to a national security concern. For instance when the hacktivist collective Anonymous hacked the websites of the Ceylon Electricity Board, the Sri Lanka Police, and the Department of Immigration and Emigration through distributed denial-of-service (DDoS) attacks (Attanayake, 2022). Another instance was when a group of hackers hacked on five different occasions, five websites belonging to state institutions such as Sri Lanka Police, Health Ministry, the Ceylon Electricity Board, the Hector Kobbekaduwa Agrarian Research and Training Institute and the Southern Provincial Council (Fernando, 2021). Next, when the Bangladeshi Grey Hat Hackers hacked 22 government websites that were sub domains of the North Central province (Anon, n.d.) and when hacker 'Davy Jones' hacked into the site of Sri Lanka Foreign Employment Bureau and the Ports Authority website (Anon, n.d.) as well as when the State television channel Rupavahini was also hacked (Anon, n.d.).

National Security is defined by Mario Nobilo as *"an interaction between Political, Economic, Military, Legal, Social and other internal and*

external social factors through that individual states attempt to ensure their state sovereignty, integrity and political independence for rapid social development" (Mendis, 1992). Sri Lanka has the following legislation to combat cybercrimes, namely, the Computer Crime Act No. 24 of 2007, Evidence (Special Provisions) Act No 1995, Electronic Transactions Act No. 19 of 2006, Payment Devices Frauds Act No 30 of 2006, and the Intellectual Property Rights Act No. 36 of 2003, of which Section 06 of the Computer Crime Act No. 24 of 2007 mentions offences committed against national security. Nevertheless, there are no legislation in Sri Lanka currently which prevents, mitigates, or responds to cyber security threats. Therefore, there are no impediments to the country's national security. Despite the many cyberattacks that Sri Lanka has faced, it was only in 2018 that two bills on cybersecurity were proposed to be passed (EconomyNext, 2021). However, to date, the two Bills, namely the Cyber Security Bill and the Defence Cyber Commands Act have not been passed. Jeff Kosseff has defined cybersecurity law as *"a legal framework that promotes the confidentiality, integrity, and availability of public and private information, systems, and networks, through the use of forward-looking regulations and incentives, with the goal of protecting individual rights and privacy, economics and national security"* (Kosseff, 2018).

Accordingly, the research problem of this article examines whether the current cyber laws in Sri Lanka are sufficient to adequately protect the country's national security in cyberspace. The research objectives of this research are to examine the current cyber laws protecting national security in Sri Lanka (1), to evaluate the implementation process in the criminal justice system in terms of cyber laws (2) and to gain some perspectives of how other countries such as the United Kingdom and the United States of America have formulated legislation to protect their country's national security in the cyberspace.

2. Methodology

This is a library-based, qualitative research. Special reference is made to secondary sources such as Sri Lankan legislation, Bills, as well as scholarly articles, reports, electronic sources, academic writings, books and newspapers relevant to national security and cyber security in Sri Lanka, the United Kingdom and the United States of America.

3. Results and Discussion

WHETHER THE CURRENT CYBER LAWS PROTECT THE NATIONAL SECURITY IN SRI LANKA

As aforementioned, there are several legislations which have been introduced to deal with the criminal justice system in the development of the Information and Communication Technology (ICT) Industry. Among these, the Computer Crime Act No 24 of 2007 is the main legislation which discusses about the protection of national security in Sri Lanka in the context of cyberattacks.

Section 6 of the Computer Crime Act No. 24 of 2007 provides that any person who intentionally performs any malfunction from a computer, which is going to be an imminent threat or danger to the national security, national economy or public order shall be guilty of an offence. However, it is noteworthy that the interpretation clause of the Computer Crime Act No. 24 of 2007 does not attempt to define the terms 'public order' or 'types of imminent threats to national security'. Due to the lack of a standard interpretation, discrepancies are created during the legal implementation process. For instance, on 08th June 2021, fake news was circulated on social

media platforms by stating that *"the Presidential Secretariat, Foreign Ministry, Medical Research Institute, Survey Department, and several other websites had been hacked"* (NewsWire, 2021). Consequently, the Police arrested a 28-year-old boy without a warrant, under the Prevention of Terrorism Act and Computer Crime Act No. 24 of 2007 (Kothalawala, 2021). However, the legal professionals argued that the Computer Crime Act No. 24 of 2007 has not recognized 'online fake news' as an imminent threat to national security. Therefore, this incident highlights that there is no consensus between the legal practitioners and the Police regarding the execution of the Computer Crime Act No. 24 of 2007 and that even though the Computer Crime Act No. 24 of 2007 enforces penal sanctions on any person who commits an offence which is an imminent threat or danger to national security, this legislation is insufficient in terms of monitoring, detecting, preventing and/or managing incidents in the cyberspace. Thereby, it is imperative to note that not only does Sri Lanka need cybercrime laws which take care of the criminal justice aspect of the breaches of cyber security but also cyber security laws which deal with the prevention of cybercrime (Anon, 2018).

IMPLEMENTATION PROCESS OF CYBER LAWS IN THE ICT CRIMINAL JUSTICE SYSTEM OF SRI LANKA

In the process of approving the Cyber Security Bill, it is stated that *"Electronic communication across cyberspace has been recognized as a crucial factor that can directly affect national security"* (Gamini Gunaratna, 2022). This statement indicates the importance of strengthening the cyber security laws in Sri Lanka.

Accordingly, Sri Lankan Criminal Justice System is functioning with the collaboration of several authorities to safeguard the country from cyberattacks. Firstly, there is a Cyber Crime Unit in the Sri Lanka Police within the scope of the Criminal Investigation Department (CID). In the Cyber Crime Unit, there is a number of experienced and well-qualified officers to proceed with criminal investigations. The second significant step is the establishment of the Computer Emergency Readiness Team -Coordination Centre (CERT-CC) in 2006. Furthermore, CERT-CC initiated the establishment of the E-Government Policy in 2009. Following the civil war in Sri Lanka, the E-Government strategy had a positive impact on both the social and economic development of the country. However, the lack of an institutional framework for the further standardization of national infrastructure can be recognized as the main disadvantage of this E-Government strategy (Rainford, n.d.).

Even though there are institutions, which monitor, detect, prevent, mitigate, and manage incidents in cyberspace, the draft Cyber Security Bill establishes the Digital Infrastructure Protection Agency of Sri Lanka and empowers the Sri Lanka Computer Emergency Readiness Team (CERT). This means that once the Cyber Security Bill is passed in Parliament, the Digital Infrastructure Protection Agency of Sri Lanka will be able to recommend cyber security policies and standards for the Government of Sri Lanka and facilitate the implementation of these policies and standards in government institutions and other sectors as well as act as the central point of contact for cyber security in Sri Lanka, and act as the interface for the multi-directional and cross-sector sharing of information related to cyber threat indicators, defensive measures, cyber security risks, incidents, analysis, and warnings in relation to cyber security for government institutions and other sectors, among other powers, duties and functions of the Digital Infrastructure

Protection Agency (Cybersecurity Bill, 2019). Similarly, according to Section 15 of the draft Cyber Security Bill, the Sri Lanka Computer Emergency Readiness Team shall be the national coordination point of contact for cyber security incidents and threats in Sri Lanka. Further, some of the powers and functions mandated by Section 15 (4) of the draft Bill are to conduct and manage cyber security services for government institutions and other sectors when requested, and to provide national-level cyber threat information to the Digital Infrastructure Protection Agency, to establish and maintain membership, to collaborate with international computer emergency readiness teams to ensure effective coordination and response to cybersecurity-related incidents in Sri Lanka and to monitor the designated Critical Infrastructure Information owned by the government and other sectors in order to detect, investigate and respond to potential cyber threat. Therefore, there is a timely need for the two draft Cyber security Bills to be enacted in the country because at present Sri Lanka is vulnerable to managing cyberattacks as apparent from the many cyberattacks that have taken place recently.

It is in this light that this research recommends the importance of hastening the process of passing the Cybersecurity Bill. As a result, Sri Lanka should prioritize bringing all stakeholders together and strengthening the cybersecurity-related criminal justice system. This is extremely important to prevent any incidents which may breach national security in the future.

EXAMINING HOW OTHER COUNTRIES HAVE ENACTED CYBER SECURITY LAWS TO PROTECT THE COUNTRY'S NATIONAL SECURITY

The United Kingdom and the United States of America have enacted thorough cyber security laws to protect their country's national security in cyberspace. Both these countries have a common law legal system.

UNITED KINGDOM

An important piece of cybersecurity legislation in the United Kingdom is the Network and Information Systems Regulations 2018 (NIS Regulations), which implemented the EU Cybersecurity Directive 2016 prior to Brexit (Technology Law Dispatch, 2022). Per this legislation, operators of essential services and relevant digital service providers are mandated to register with the relevant competent authorities, meet a baseline level of cybersecurity requirements, and report any incident which has a significant impact on the continuity of the essential services (Technology Law Dispatch, 2022).

A series of cyberattacks occurred in the United States of America in the recent past. One such incident was the colonial pipeline ransomware attack which infected some of the pipeline's digital systems and subsequently shut it down for several days (Kerner, 2022). Another incident was the cyberattack on SolarWinds, a major US information technology firm, where foreign hackers used the hack to spy on private companies such as the FireEye, a cyber security firm and the Department of Homeland Security and Treasury Department and this had gone undetected for months (Jibilian and Canales, 2020). Another cyberattack which occurred recently was a massive hack on the Microsoft Exchange email server software. It is noteworthy that the United Kingdom by observing the situation in the United States of America decided to enact new legislation as part of its new National Cyber Strategy as well as update the NIS Regulations and widen its list of companies to include Managed Service

Providers (MSPs) which provide specialized online and digital services (GOV.UK, n.d.).

As ascertained, Sri Lanka is no stranger to cyberattacks. However, unlike the United Kingdom which strives to enact strong cybersecurity laws by observing other countries, even when Sri Lanka itself has undergone cyberattacks, the Legislature is imperceptive in passing cyber security laws to mitigate and/or prevent any further attacks. This is why, similar to the United Kingdom, Sri Lanka must establish relevant authorities where operators of essential services and digital service providers are mandated to register with the relevant authority and meet the desired cyber security requirements.

UNITED STATES OF AMERICA

Cyber security regulation in the United States America comprises directives from the Executive branch and legislation from Congress that safeguards information technology and computer systems (Hardeep Singh, 2015). Some of the federal laws in the United States of America dealing with cyber security are as follows. 1996 Health Insurance Portability and Accountability Act (HIPAA), 1999 Gramm-Leach-Bliley Act, and 2002 Homeland Security Act, which included the Federal Information Security Management Act (FISMA) (Hardeep Singh, 2015). Per these regulations, it is mandated that healthcare, financial and government entities have to ensure the security of their systems and data (EES, 2021). Further, according to the Federal Information Security Management Act (FISMA), all federal agencies have to implement information security policies, concepts and standards (EES, 2021). This is in stark contrast to the situation in Sri Lanka, where the individual institutions and organisations are responsible for their own cyber security and have to ensure that they are adequately protected in the face of any cyberattacks.

Next, in terms of state laws, in the United States of America, most states have passed legislation imposing security requirements. For example, the SHIELD Act of New York requires reasonable security for personal information and specific measures that may satisfy that standard (ICLG, 2019). In California, the California Consumer Privacy Act (CCPA) sets statutory penalties if it can be proved that the impacted business failed to implement a reasonable security procedure to protect personal information (EES,2021). Massachusetts regulations impose specific security requirements regarding personal information which also include the implementation of a written security programme and encryption of certain data (EES,2021). When comparing this situation to Sri Lanka, as aforementioned, it is apparent that currently there are no cyber security laws for the monitoring, detection, prevention, mitigation and management of incidents. As such, it is imperative that the two draft Bills, be passed as soon as possible by the Legislature, especially since the draft Cyber Security Bill establishes the Digital Infrastructure Protection Agency and the Sri Lanka Computer Emergency Readiness Team (to assist the Digital Infrastructure Protection Agency).

4. Conclusion

In conclusion, it is clear that Sri Lankan cyber laws are still insufficient to adequately protect the country's national security in cyberspace. As a result, this study emphasizes the significance of enacting the Cyber Security Bill and the Defence Cyber Commands Act by 2022. It is ascertained that Section 6 of the Computer Crime Act No. 24 of 2007 is the one and only provision available to protect the national security of the country in cyberspace. Thus, the absence of cyber security laws cannot be

fulfilled through the existing legal provisions. Further, after evaluating the criminal justice system in Sri Lanka in terms of cyberspace it can be determined that as a first step the two Bills relating to Cyber Security should be prioritized by bringing all stakeholders together and passing comprehensive cyber security laws. The discussion revealed that policymakers must accelerate the passing of the draft Cybersecurity Bill and the Defence Cyber Commands Act in order to monitor, detect, prevent, mitigate and manage incidents in cyberspace. Finally, similar to the United Kingdom and the United States of America, Sri Lanka should also have sector specific cyber security laws and take proactive measures to identify potential cyber threats that may arise in Sri Lanka, by observing the vulnerabilities that other countries face, so that specific legislation which deals with that particular matter can also be enacted. In this manner, the national security of Sri Lanka will be protected in cyberspace.

References

Anon, (2018). AG stresses on importance of cyber security for socio-economic growth | ශ්‍රී ලංකා තොරතුරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනය - ICTA. [online] Available at: https://www.icta.lk/news/ag-stresses-on-importance-of-cyber-security-for-socio-economic-growth/ [Accessed 3 Jul. 2022].

CSIS (2021). *Significant Cyber Incidents | Center for Strategic and International Studies*. [online] www.csis.org. Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Cyber Security Bill.[online] Available at: https://cert.gov.lk/documents/Cyber%20Security%20Bill.pdf.

EconomyNext. (2021). Poorly worded legal provisions can be construed to cover 'fake news': Sri Lanka lawyer. [online] Available at: https://economynext.com/poorly-worded-legal-provisions-can-be-construed-to-cover-fake-news-sri-lanka-lawyer-82815/. [Accessed 3 Jul. 2022].

EconomyNext. (2021). *Sri Lanka to draft new cyber security legislation; two separate bills proposed*. [online] Available at: https://economynext.com/sri-lanka-to-draft-new-cyber-security-legislation-two-separate-bills-proposed-86936/ [Accessed 8 Jul. 2022].

EES (2021). *Cybersecurity laws and regulations in US 2022*. [online] EES Corporation. Available at: https://www.eescorporation.com/cybersecurity-laws-and-regulations-in-us/#:~:text=HIPAA%2C%20Gramm%2DLeach%2DBliley [Accessed 5 Jul. 2022].

Euronews. (2022). *Oil terminals disrupted after European ports hit by cyberattack*. [online] Available at: https://www.euronews.com/2022/02/03/oil-terminals-disrupted-after-european-ports-hit-by-cyberattack [Accessed 7 Jul. 2022].

Fernando, L. (n.d.). *Cyber attacks on five state websites*. [online] Daily News. Available at: https://www.dailynews.lk/2021/05/24/local/250031/cyber-attacks-five-state-websites.

GOV.UK. (n.d.). *New laws proposed to strengthen the UK's resilience from cyber attack*. [online] Available at: https://www.gov.uk/government/news/new-laws-proposed-to-strengthen-the-uks-resilience-from-cyber-attack.

Hardeep Singh (2015). *A Glance At The United States Cyber Security Laws*. [online] Appknox.com. Available at: https://www.appknox.com/blog/united-states-cyber-security-laws.

ICLG (2019). Gambling Singapore Chapter. *Gambling 2019 | Laws and Regulations | Singapore | ICLG*. [online] doi:https://iclg.com.

International Comparative Legal Guides International Business Reports. (n.d.). International Comparative Legal Guides. [online] Available at: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/germany.

Jibilian, I. and Canales, K. (2020). *Here's a simple explanation of how the massive SolarWinds hack happened and why it's such a big deal*. [online] Business Insider. Available at: https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

Katharina.kiener-manu (2019). *Cybercrime Module 3 Key Issues: The Role of Cybercrime Law*. [online] Unodc.org. Available at: https://www.unodc.org/e4j/en/cybercrime/module-3/key-issues/the-role-of-cybercrime-law.html.

Kosseff, J. (2018). *Defining Cybersecurity Law*. [online] papers.ssrn.com. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3225691 [Accessed 30 Jun. 2022].

Mendis, V. (1992). *National Security Concepts of States Sri Lanka*. [online] Available at: https://unidir.org/sites/default/files/publication/pdfs//national-security-concepts-of-states-sri-lanka-en-441.pdf [Accessed 3 Jul. 2022].

NewsWire. (2021). *ITSSL Chairman arrested over fake news on cyber attack on state-owned websites*. [online] Available at: https://www.newswire.lk/2021/06/08/itssl-chairman-arrested-over-fake-news-on-cyber-attack-on-state-owned-websites/ [Accessed 8 Jul. 2022].

Rainford, S. (n.d.). *SRI LANKA e-Sri Lanka: An Integrated Approach to e- Government Case Study*. [online] Available at: https://www.unapcict.org/sites/default/files/2019-01/e-Sri%20Lanka%20-%20An%20Integrated%20Approach%20to%20e-Government%20Case%20Study.pdf.

Rest of World. (2022). *Anonymous wanted to help Sri Lankans. Their hacks put many in grave danger*. [online] Available at: https://restofworld.org/2022/anonymous-sri-lankans-hacks-danger/ [Accessed 1 Jul. 2022].

Technology Law Dispatch. (2022). *Cybersecurity 2.0: the UK follows suit with the EU in launching cybersecurity law reform*. [online] Available at: https://www.technologylawdispatch.com/2022/03/data-cyber-security/cybersecurity-2-0-the-uk-follows-suit-with-the-eu-in-launching-cybersecurity-law-reform/#:~:text=One%20of%20the%20key%20pieces.

Technology Law Dispatch. (2022). *Cybersecurity 2.0: the UK follows suit with the EU in launching cybersecurity law reform*. [online] Available at: https://www.technologylawdispatch.com/2022/03/data-cyber-security/cybersecurity-2-0-the-uk-follows-suit-with-the-eu-in-launching-cybersecurity-law-reform/#:~:text=One%20of%20the%20key%20pieces.

Welle (www.dw.com), D. (n.d.). *Chinese APT 27 hackers targeting companies, says Germany | DW | 26.01.2022*. [online] DW.COM. Available at: https://www.dw.com/en/chinese-apt-27-hackers-targeting-companies-says-germany/a-60564091

Author Biography

Ms. Dulmi Jayasinghe is a temporary lecturer at the Department of Law, Faculty of Arts, University of Peradeniya. She obtained her LL. B (Hons) from the Department of Law, Faculty of Arts, University of Peradeniya and a Professional Qualification in Human Resource Management from CIPM. Her research interests are Labour Law, ICT Law, International Humanitarian Law, and Constitutional Law.

Ms. Gayanthi Dilmini De Silva is currently following her apprenticeship under a President's Counsel working in the Appellate Courts. She read for her Bachelor of Laws at the Department of Law, Faculty of Arts, University of Peradeniya, and also has a Diploma in Diplomacy & World Affairs conducted by the Bandaranaike Institute of Diplomatic Relations (BIDTI). Her research interests include Constitutional Law, International Law, Property Law, Alternate Dispute