Randeniya, M., Palliyaguru, R. and Amaratunga, D., 2023. Legal and policy provisions for protecting energy and telecommunication infrastructure against hazards: Comparison between Sri Lanka and other countries. In: Sandanayake, Y.G., Waidyasekara, K.G.A.S., Ramachandra, T. and Ranadewa, K.A.T.O. (eds). *Proceedings of the 11th World Construction Symposium*, 21-22 July 2023, Sri Lanka. [Online]. pp. 700-711. DOI: https://doi.org/10.31705/WCS.2023.57. Available from: https://ciobwcs.com/papers/

LEGAL AND POLICY PROVISIONS FOR PROTECTING ENERGY AND TELECOMMUNICATION INFRASTRUCTURE AGAINST HAZARDS: COMPARISON BETWEEN SRI LANKA AND OTHER COUNTRIES

Maheshi Randeniya[1], Roshani Palliyaguru[2] and Dilanthi Amaratunga[3]

ABSTRACT

In the recent years, Sri Lanka's focus on its infrastructure has grown due to its significance to the country's economy, security, and quality of life. A resilient critical infrastructure system is crucial in reducing the impact of natural and human induced risks and weaknesses. In this context, comprehensive knowledge of a nation's legal and policy framework would be of great assistance in building pathways towards strengthening the resilience of critical infrastructure systems. Concerning the need, this study aims to assess the ability of the existing legal and policy framework for complex, interdependent infrastructure systems in Sri Lanka to protect its energy and telecommunication infrastructure against natural and human-induced hazards. The objectives of the study include: (1) determining the existing legal and policy framework for energy, telecommunication infrastructure in Sri Lanka; and (2) comparing the legal and policy provisions for protecting these infrastructures against hazards in Sri Lanka with the international context. The study involved a comprehensive literature synthesis to understand the scope of critical infrastructure in the global context. Further, preliminary interviews were conducted to obtain the direction for the identification of the existing legal and policy framework related to the infrastructure sectors in Sri Lanka. Finally, the study examined the available provisions in the framework, alongside a desk study, to assess their effectiveness in safeguarding critical infrastructure. A comparison between Sri Lanka and the international context highlighted significant gaps in the legal and policy framework, particularly in terms of protecting the nation's infrastructure.

Keywords: *Critical Infrastructure; Law and policy; Resilience; Protection of Infrastructure.*

[1] MSc Candidate, University of Peradeniya, Kandy, Sri Lanka, maheshirandeniya1@gmail.com
[2] Senior Lecturer, University of Vocational Technology, Ratmalana, Sri Lanka, rpalliyaguru@uovt.ac.lk
[3] Professor, University of Huddersfield, UK, d.amaratunga.hud.aclk

1. INTRODUCTION

Critical infrastructure is comprised of systems and assets. They can be either virtual or physical. These infrastructures are essential and any disruption to them can have a serious impact on a nation's economic stability, public health and safety, national security, and quality of life. According to Randeniya et al. (2022, p.11) critical infrastructure can be identified as "system of identifiable sectors whose destruction or incapacity would have an enervative impact on the economic sustainability, public health and safety, quality of life, and national security of a country". The identified infrastructure sectors are energy, water, telecommunication, finance, transportation, and essential services. Only two infrastructure sectors were considered for this study due to the overwhelming amount of information relating to all six sectors and the difficulty of presenting all six in one study. The critical infrastructures that are being analysed in this study are:

- Energy, and
- Telecommunication.

The current infrastructure, which has been standing for the past twenty years, has started to deteriorate in quality. The manner in which the government and the inhabitants renew and protect the infrastructure will determine the quality of life for future generations as well as national security and disaster resilience (Adams, 2017). Even though the local laws and policies have been implemented concerning the infrastructure and the gaps have been identified for the protection of the infrastructure, some of the infrastructure's legal and policy frameworks have failed to stipulate the criminal and civil penalties clearly. Having a proper legal and policy framework would support the legitimacy of the organizations in charge of the infrastructure and therefore sustain their longevity. Due to the global character of the information and knowledge on the economy, minimum common international standards have long been acknowledged as crucial. Government policies and how they are reflected in the law influences how infrastructures and services developed are used. The development of the country and the interconnect ability of national legal systems are facilitated by such shared standards. (Pournader et al., 2020). Currently there are no studies conducted under legal and policy frameworks in Sri Lanka considering the infrastructure sector. This study aims to assess the ability of the existing legal and policy framework for complex, interdependent infrastructure systems in Sri Lanka to protect its energy and telecommunication infrastructure against natural and human-induced hazards.

The quantity and variety of infrastructures have become more threat-resistant over the last few decades, and they have begun to secure their ongoing operation and development at the national level. Natural disasters, mechanical malfunctions, inadequate design, or human action ranging from theft/arson to terrorist attacks can all cause disruption or the destruction of its operation.

2. LITERATURE REVIEW

Most of the countries have legal elements relating to the protection of infrastructure. These elements address issues such as infrastructure protection, civil and criminal penalties against improper use of the infrastructure and protects any intellectual property pertaining to the infrastructure. Some countries have specific legal means when addressing critical infrastructure protection but most of the other countries have

no specific legal provisions regarding critical infrastructure protection. Even where countries do have specific provisions on dealing with the critical infrastructure, differences exist between the countries on how to protect the infrastructure. Most frequently the critical infrastructure protection is done through applying industry norms and standards.

In the study, laws and policies are being discussed at both the national and international scale. Countries such as Australia, Canada and United States of America were taken into consideration for the study to compare with the Sri Lankan context due to them being developed countries and having the strongest infrastructure systems. As well as, being the countries, which are known for taking best care of its' citizens therefore the best care towards the overall infrastructure system from both physical and social point of view.

3. METHODOLOGY

3.1 DATA COLLECTION

For this study, six preliminary interviews were done to collect the empirical data on the acts which are most important when it comes to the infrastructure sectors and secondly, a desk study-literature review was conducted to examine the gaps and protective measures taken in the Sri Lankan regulatory framework. The preliminary interviews were conducted among professionals attached to energy and telecommunication infrastructures with an experience of over twenty years to analyse the findings derived from the desk study and to finally determine whether Sri Lanka has addressed the issues regarding the protection of critical infrastructures. During the preliminary interviews, the interviewees were asked whether there were any specific policy or legal framework implemented towards protecting the infrastructure sector and if so, to elaborate on how the protection measures are taken towards the infrastructure. Furthermore, the interviewees were asked whether there were any legal and policy frameworks towards building resilience of the particular infrastructure sector. According to the information given in the interviews, the next section presents the legislations that were taken into consideration.

4. DATA ANALYSIS

4.1 INTERNATIONAL CONTEXT

4.1.1 Telecommunications Infrastructure

Telecommunication is at the heart of the transition towards a digital society. Cybersecurity is the primary foundation that guarantees the safety of the digital economy, inspires confidence in all users, and promotes economic growth. The importance of digital technology for sustaining the economy is demonstrated by the swift adoption of it by homes and businesses after the COVID-19 outbreak. To enhance the benefits of the digital world, the controlling of the threats which comes along must be done.

Australia

One of the biggest hazards to Australians is malicious online activity. The epidemic brought attention to how everchanging cyber threats are. Opportunistic cybercriminals

have modified their techniques to profit on Australians connecting, working, and learning online (Burchaers et al.,2022)

The Australian government has "the Security of Critical Infrastructure Act 2018" as the main governing body. Civil penalty provisions of this Act can be enforced using civil penalty orders, injunctions, and enforceable undertakings may be accepted in relation to compliance with civil penalty provisions. Additionally, in order for this Act to apply to a specific asset, the Minister can privately proclaim it to be a vital infrastructure asset. A private declaration would be made only if there was an imminent risk to national security.

The Australian Government has acted in strengthening the protection of Australian citizens, their data and critical infrastructure from the most complex threats. Through spending a sizable sum of money, the Australian Government has improved the AFP's (Australian Federal Police) capacity to look into and to prosecute cybercriminals. The AFP has been able to create target development teams to strengthen technical cyber capabilities, and improve operational capacity (Critical Infrastructure Centre, 2020).

National Critical Infrastructure Resilience Framework (NCIRF)

This is a governmental policy that aims to protect energy and telecommunication infrastructure from potential disruption. It seeks to strengthen the resilience of critical infrastructure to physical, cyber, and human threats, and to ensure that it can remain operational in the face of any potential disruption. The framework is designed to ensure that Australia's critical infrastructure is secure, resilient and able to provide services when needed. It sets out a range of measures that energy and telecommunication infrastructure operators, owners and users can take to protect their assets, as well as strategies for responding to and recovering from any disruption. By strengthening the resilience of critical infrastructure, the NCIRF helps to ensure that Australia's energy and telecommunication networks remain reliable, secure, and available to users.

United States of America

Attacks on government computer systems, bank computer systems, and systems utilized in interstate and international commerce are prohibited by the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984.

In this they have stipulated criminal penalties, including asset forfeiture, for unauthorised access and improper use of federal government or financial institution computers and networks, or in interstate or international commerce or communication, and improper use of protected information, causing damage to or threatening to cause damage to a computer, using the computer to commit fraud, trafficking in stolen computer passwords. It has also provided a statutory exemption for intelligence and law enforcement activities and criminalised electronic trespassing on and using federal government systems outside the scope of allowed access. (Fischer, 2014).

Homeland Security Act of 2002

According to Guermazi and Satola (2005) the Department of Homeland Security undertakes several responsibilities for the safety of the information infrastructure that were previously handled by other authorities (Department of Homeland Security). It mandates that DHS offer information on threats and vulnerabilities, support for crisis management, and technical assistance with regard to

recovery plans for critical information systems to state, local, and private entities. Additionally, this enhanced some of the criminal penalties for cybercrime and permitted the Secretary of Homeland Security to designate eligible technologies as being subject to specific safeguards from liability in claims connected to their use in response to an act of terrorism. Furthermore, the DHS demanded collaboration between the sector-specific agencies and the DHS Office for Infrastructure Protection (Fischer, 2014; Roche,1998).

Communications Act of 1934

The Federal Communications Commission (FCC) was created and granted control over domestic and foreign wired and wireless commercial communications. That provides the president with control over communications equipment and stations during emergencies. (Fischer, 2014).

4.1.2 Energy Infrastructure

Canada

To improve the safety and security of the operation of a regulated facility, the Canadian government passed the "Canadian Energy Regulator Act (S.C. 2019, c. 28, s. 10)". Under this law, the Commission may, by order, direct the holder to repair, reconstruct, or alter part of the regulated facility and may also order that, until the work is completed, that part of the regulated facility will not be utilised or be utilised in accordance with any conditions specified by the Commission. Anybody that violates a rule imposed under section 96, is guilty of an offense and liable (Canadian Energy Regulator Act, 2019).

- If found guilty on indictment, a fine of no more than $1,000,000, a period of no more than five years in prison, or both; or
- Upon summary conviction, a fine of no more than $100,000, a period of no more than one year's imprisonment, or both.

Energy policy acts as a proxy for the function and value of many other interrelated sectors from telecommunication, agriculture, defence, manufacturing, finance and transportation.

The Canadian energy regulator Act acknowledges that the owners and operators bear the primary duty for enhancing the resilience of critical infrastructure. The perfect combination of security measures which addresses intentional and unintentional incidents, business continuity procedures which handles disruptions and guarantee the continuation of essential services, and emergency management planning which ensures that adequate response protocols are in place to address unforeseen disruptions and natural disasters can increase the resilience of critical infrastructure.

Nuclear Liability and Compensation Act (S.C. 2015, c. 4, s. 120)

This act states that if damage are caused by a preventive measure taken under subsection 20(1) in relation to an operator's nuclear installation or in relation to any transportation for which the operator is responsible, then only that operator and no one else is liable for damage that occurs within Canada or its exclusive economic zone.

The continued criminal actions of robbery, vandalism, public order extremism, and extreme weather conditions all pose threats to the energy system, but terrorism and

cyberattacks also carry significant hazards. The primary terrorist hazard emanates from international Islamist extremism as epitomised by way of al-Qaida. Digital assaults may be perpetrated through broadly one-of-a-kind groups or individuals with diverse motives. Much of Canada's national crucial infrastructure is now both constructed upon or monitored and controlled with the aid of cyber data and communications technologies (ICT) which makes it prone to electronic attacks and the cascading consequences of disruptions in different important infrastructures. Vital energy infrastructure structures include many one-of-a-kind agencies and groups which can be connected to every other electronically in the area and to different infrastructure sectors via records structures. Reliance on SCADA technology in addition will increase vulnerability to network disasters and digital attacks making the energy quarter as a whole very inclined. Cyber-attacks may be launched to obtain or corrupt facts, disrupt offerings or plan similarly assaults on infrastructure. The supply and integrity of those structures and the records transmitted is incredibly dependent on top physical, non-public and technical shielding protection procedures (Energy Policy, 2015).

Extreme climate events cause significant strain on power distribution systems. In general, the consequences of environmental hazards entail incident responses, emergency management and adaptation to such environmental occurrences. Numerous regions in Canada have experienced severe natural disasters resulting in loss of life and extensive property damage. Generally, Natural failures encompass an expansion of meteorological and geological hazards of which floods are the maximum frequent and the main motive of assets harm and death. Hurricanes, earthquakes, and wildfires also are a part of the natural chance panorama and might result in the discontinuity of power substances which in turn are probably to have an effect on recuperation efforts (Energy Policy, 2005).

The Public Safety Act (2002)

A number of legislative amendments had been enacted to offer Regulators with a clear statutory basis for regulating the safety as well as the safety factors of interprovincial and worldwide energy belonging an exchange necessitated with the aid of a growing realisation that the oil, gas and nuclear/electric power centres have been appealing, high price/high impact goals for terrorists (Public Safety Act, 2002).

Critical Infrastructure Resilience Strategy (CIRS)

This was established to safeguard Canada's electricity and telecommunications infrastructure against terrorism, malicious cyberattacks, and natural catastrophes. The three key areas of the plan are risk management, collaboration, and awareness and education. It promotes public-private collaboration to create efficient critical infrastructure protection plans. Enhancing the security and resilience of Canada's energy and telecommunications networks is another goal of the CIRS. In order to maintain the security and dependability of the nation's energy and telecommunications networks, this entails stepping up cybersecurity precautions and strengthening coordination between the federal, provincial, and territorial governments. The CIRS contributes to the defense of Canada's energy and communications infrastructure against foreign threats by performing these actions (Department of Home Affairs, 2018).

United States of America

Federal Power Act

This established the Federal Energy Regulatory Commission (FERC) and granted it control over the transmission and sale of electricity across state lines. Over the past several years, worries regarding the electric grid's susceptibility to cyberattack have grown significantly. Even though the Power Coverage Act of 2005 (P.L. 109-58) gave FERC responsibility for creating reliability standards for power structures, challenges to that authority and to the usefulness of the standards-improvement process to effectively respond to unexpectedly emerging cybersecurity threats have raised questions about the need to strengthen FERC's authority to address those threats, especially given the advancement of the intelligent-grid era. After deliberations it was decided that FERC would not be given jurisdiction over electric powered infrastructure and with response to the cybersecurity concerns, in the 112th Congress, S. 1342, FERC was given expanded cybersecurity authority (Department of Energy, 2018).

National Infrastructure Protection Plan (NIPP)

It is an extensive collection of plans, methods, and initiatives created to safeguard the vital infrastructure of the country against criminal activity. The National Infrastructure Protection Program (NIPP) offers a framework for public and commercial institutions to coordinate their efforts to safeguard the country's energy and telecommunication facilities from conventional and emerging security risks. The NIPP also specifies risk management procedures that businesses should use to safeguard their vital infrastructure. The NIPP aims to ensure that energy and telecommunication infrastructures are secured from dangers like terrorism, natural disasters, and cyber-attacks by coordinating efforts among government, business, and other stakeholders (Department of Homeland Security, 2013).

4.2 SRI LANKAN CONTEXT

4.2.1 Telecommunication Infrastructure

Sri Lanka Telecommunications Act (No. 25 of 1991) - Sect 47

According to the act, anyone who intentionally destroys, removes, tampers with, or interferes with any telecommunication set up line, post, or other items that are a part of or used in any telecommunication system or inside the service of any carrier will be found guilty of an offense and subject to a fine of no more than 20,000 rupees, a term of imprisonment of either description of no more than six months, or both such punishments, upon conviction (Telecommunications Act 27, 1996 & Singh, 2019).

State of Cybercrime Legislation

According to Singh (2020); Oxford Business Group (n.d.) these Acts deal with the main statutes that address offenses including unauthorised access to a computer, data, or network, unauthorised use of malware, launching denial-of-service attacks, unauthorised interceptions, and unauthorised data use.

- Computer Crimes Act No. 24 of 2007
- Payment Devices Frauds Act No. 30 of 2006
- Intellectual Property Act No. 36 of 2003

According to United Nations (2007) there are other statutes that support the implementation of the Budapest Convention for Cybercrime. These include:

- Mutual Assistance in Criminal Matters Act No. 25 of 2002 (Amended in 2018)
- Financial Transactions Reporting Act No. 6 of 2006

The Mutual Assistance in Criminal Cases (Amendment) Act, which outlines the conditions under which certain nations, including Sri Lanka, may give aid in criminal cases. It's also important to note that Sri Lanka works to complete its data protection and cyber security laws in 2019 (Lawnet Ministry of Justice, 2019).

The Cybersecurity Bill passed all the preliminary procedural stages, and it is waiting for cabinet approval and enactment. The Act's goals are to protect the Critical Information Infrastructure, ensure that Sri Lanka's National Cyber Security Strategy is implemented effectively, prevent, mitigate, and respond to cyber security threats and incidents effectively and efficiently, establish the Sri Lanka Cyber Security Agency, and empower the institutional framework to provide a safe and secure cyber security environment (Ministry of Technology, 2019).

Cyber Security Act, No. of 2019

To protect the critical information infrastructure and effectively and efficiently prevent, mitigate, and respond to cyber security threats and occurrences.

4.2.2 Energy Infrastructure

Ceylon Electricity Board Act (1987)

The electricity board act has not taken any major precautions towards the infrastructure protection, but it has stipulated the parties responsible for the construction, maintenance and operation of the generation stations and sub stations also the penalties for the ones who cause harm to the structures (CEB Act, 1987).

Electricity Act No. 20 of 2009

In this the electricity board has taken protective measures by Strengthening of Centralised Monitoring System (CMS) which monitors and records the quality of electricity supply and helps to detect power outages, power theft and other irregularities. This improved network security, and a system maintenance was also implemented to provide for the installation of security devices in electricity networks to prevent power theft and other illegal activities and to require electricity operators to ensure that all electricity infrastructure is maintained in an efficient and safe manner. Also, the regulatory framework was improved to ensure the efficient and reliable supply of electricity and to protect the public from dangerous and hazardous situations that can arise due to the electricity infrastructure.

In this a separate security unit was established within the Ministry of Power and Renewable Energy to coordinate energy security policies and to monitor the energy supply chain. An energy security policy was developed to ensure the continuity of energy supply (National Energy Policy, 2015).

An independent security council was also established to monitor and review energy security policies of the government. This can be considered as an important milestone due to the establishment of an energy security information exchange system to share critical information among stakeholders which has not been done before in the energy

sector prior to this policy. Also strengthening cyber security measures to protect the critical energy infrastructure were taken with this policy

5. RESEARCH FINDINGS AND DISCUSSION

According to an interviewee, the national energy policy covered the Sri Lankan energy sector and the protection of the infrastructure, but it has not referred to the protection of the structural or physical buildings of the infrastructure sector, rather it has talked about the protection of the people who work there and any personnel who can be affected by the infrastructure sector. Energy sector in Sri Lanka does not have many protective measures in the legal area but they have stipulated the penalties which follow those who damage the properties and structures. Furthermore, when considering the telecommunication sector, interviewees have stated that the TRCSL (Telecommunication Regulatory Commission Sri Lanka) protect consumers as well as operators, and are feeding information updating operators, consumers. CERT-cybercrimes, which investigates and provides reports regarding issues, but they do not pursue structural protection of the infrastructure.

It was found that the Canadian government has measure taken against damages by human personnel which goes from $1,000,000 to $100,000. The USA has stated about the penalties which would be given for any acts relating to disruption of power due to the sensitivity of the infrastructures and by considering the national security, economic stability, and the quality of life of the citizens in the country. Moreover, USA has measures taken against the cyber threat due to most of the functions being automated and digitised. Starting from manufacturing sector to the healthcare sector, the telecommunication sector has penetrated within the other sectors and due to the complexity and diversity of the systems, the possibility of getting a cyber-attack is high. Therefore, necessary precautions were taken in the cybercrimes Act in relation to the penalties that accompany the crimes, whereas in Australia they have enforced using civil penalty orders or injunctions, and enforceable undertakings are accepted in relation to compliance with civil penalty provisions for noncompliance with the law.

All three countries, Canada, Australia, and USA have their own penalty systems to enforce once a person would inflict damage on the structures but in Sri Lanka the judicial system does not talk about the penalties which would come with the cyber vulnerability. Neither Australia nor USA have provided specific laws on the protection of the telecommunication structures, but they do have protection measures taken pertaining the information concerning the telecommunication infrastructure. In Sri Lanka, the judicial system does not have many polices to protect the infrastructures, but it does cover the information regarding telecommunication. The energy infrastructure in USA, Canada has taken the protection of the energy infrastructure from both, physical and cyber harm. Such attacks lead to disruption of power which would eventually build up towards economic chaos due to the high dependency on the energy sector. These countries have become heavily dependent on top physical, non-public, and technical shielding protection procedures for safeguarding the energy sector due to the high digitalisation of the sector. Furthermore, these countries have imposed heavy penalties anyone who causes harm to the structures. The individuals would get both civil and criminal penalties including imprisonment, probation, fines or a combination of these. However, the severity of the penalties would be determined by the nature and extent of the damages caused.

According to the study it was clear that while USA has the National Infrastructure Protection Plan (NIPP) which provides a comprehensive framework for enhancing the protection of the nation's critical infrastructure. This plan includes guidance on how to reduce risks associated with natural disasters, cyber threats, and other hazards. Additionally, the USA has a number of laws, regulations, and policies related to disaster management, infrastructure security, and resilience. Canada has the Critical Infrastructure Resilience Strategy (CIRS) provides guidance on how to protect critical infrastructure against natural disasters, cyber threats, and other hazards. Additionally, the Canadian government has several laws, regulations, and policies related to disaster management, infrastructure security, and resilience. Australia has the National Critical Infrastructure Resilience Framework (NCIRF) provides guidance on how to protect critical infrastructure against natural disasters, cyber threats, and other hazards. Additionally, the Australian government has several laws, regulations, and policies related to disaster management, infrastructure security, and resilience. Sri Lanka does not have specific legal and policy provisions for protecting infrastructure against hazards. The country does, however, have a number of laws and regulations related to disaster management and resilience under particular acts and policies that provide guidance for infrastructure protection.

6. CONCLUSIONS

The primary aim of this study was to identify the existing legal and policy framework for energy, telecommunication infrastructure in Sri Lanka and to compare the legal and policy provisions for protecting these infrastructures against hazards in Sri Lanka with the international context.

The legal and policy framework for energy, telecommunication infrastructure in Sri Lanka is set out in the Ceylon Electricity Board Act (1987), Electricity Act No. 20 of 2009, Telecommunications Act No. 25 of 1991 and the National Energy Policy (2015). Also, these were identified as the existing legal and policy framework for energy, telecommunication infrastructure in Sri Lanka. The Electricity Act provides for the regulation of the generation, transmission, distribution, and supply of electricity, as well as the establishment of the Sri Lanka Electricity Regulatory Commission (SLERC). The Telecommunications Act governs the regulation of the telecommunication industry in Sri Lanka, including the licensing of telecommunications service providers. The National Policy on Energy and Telecommunications sets out the overall policy framework for the energy and telecommunications sectors in Sri Lanka, while the National Energy Policy provides a roadmap for the development of the energy sector in Sri Lanka.

Despite the steps taken by the Sri Lankan government, there is still room for improvement in the protection of infrastructure from natural and human-induced hazards in Sri Lanka, for instance, there is a need to better integrate existing the laws and regulations into a unified framework that covers all aspects of infrastructure protection, and to strengthen the implementation of these laws and regulations. In addition, there is a need to develop more effective policies and strategies to address the specific needs of each type of infrastructure, such as water and energy. Finally, there is a need to increase public awareness and education about natural and human-induced hazards and their impacts on infrastructure.

Thus, the study findings can be used as a reference when conducting further studies on energy and telecommunications infrastructure.

7. REFERENCES

Adams, K. T. (2017). *Circular economy in construction: current awareness, challenges and enablers*. ice publishing. https://www.icevirtuallibrary.com/doi/epdf/10.1680/jwarm.16.00011

United States Department of Energy (2005). *Key federal legislation*. https://www.govinfo.gov/content/pkg/PLAW-109publ58/pdf/PLAW-109publ58.pdf.

Government of Canada Justice Laws. (2019). *Canadian energy regulator act*. https://laws-lois.justice.gc.ca/eng/acts/C-15.1/page-5.html#h-1162174.

Lawnet Ministry of Justice (1987). *Ceylon electricity act*. https://www.lawnet.gov.lk/ceylon-electricity-board-3/

Ceylon Electricity Board (2009). *Ceylon electricity act*, No 20.https://ceb.lk/front_img/img_reports/1532497620Act_No._20_(E)_of_2009.

Critical Infrastructure Centre (2020). Protecting *critical infrastructure and systems of national significance*. Australian department of home affairs. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/critical-infrastructure-resilience.

Department of Homeland Security (2018). *National critical infrastructure resilience framework (NCIRF)*. https://www.dhs.gov/sites/default/files/publications/dhs_resilience_framework_july_2018_508.

Department of Home Affairs (2018). *Critical infrastructure resilience strategy (CIRS)*. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/critical-infrastructure-resilience#:~:text=The%20Critical%20Infrastructure%20Resilience%20Strategy,the%20face%20of%20all%20hazards.

Department of Homeland Security (2013). *National infrastructure protection plan (NIPP)*. https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.

Department of Energy (2018). *The Federal Power Act*. https://www.energy.gov/oe/articles/federal-power-act.

Government of Canada (2015).*Energy policy*.https://www.nrcan.gc.ca/our-natural-resources/domestic-and-international-markets/transportation-fuel-prices/energy-policy/15903.

Fischer, E. A. (2014), *Federal laws relating to cybersecurity: overview of major issues, current laws, and proposed legislation*, congressional research service. https://sgp.fas.org/crs/natsec/R42114.pdf

Guermazi, B. and Satola, D. (2005) *Creating the right enabling environment for ICT, E-Development: From Excitement to Effectiveness*. The world bank publishers. https://books.google.lk/books?hl=en&lr=&id=Ot15bvCzLx8C&oi=fnd&pg=PA23&dq=Guermazi,+B.+and+Satola,+D.+(2005)+Creating+the+right+enabling+environment+for+ICT,+E-Development:+From+Excitement+to+Effectiveness.+The+world+bank+publishers.&ots=R21p2e2v4R&sig=2_Im_eQtMOuPkhRdyg3ZGoxHyPg&redir_esc=y#v=onepage&q&f=false

Singh, V. (2019, August 19). *Introduction to digital security laws in Nepal, Sri Lanka, and Bangladesh*. Ikigai Law. Retrieved July 11, 2023 from https://www.ikigailaw.com/introduction-to-digital-security-laws-in-nepal-sri-lanka-and-bangladesh/

Singh, V. (2020, January 06). *Introduction to digital security laws in Sri Lanka*. Ikigai Law. Retrieved July 11, 2023 from https://www.mondaq.com/security/879840/introduction-to-digital-security-laws-in-sri-lanka.

Lawnet Ministry of Justice (2019). *Legal reforms for information and communication technologies.* https://www.lawnet.gov.lk/legal-reforms-for-information-and-communication-technologies/

Ministry of Technology (2019) Cyber *security act.* *https://www.cert.gov.lk/documents/Cyber%20Security%20Bill.pdf*

Pournader, M., Shi, Y., Seuring, S., & Koh, S. L. (2020). Blockchain applications in supply chains, transport and logistics: a systematic review of the literature. *International Journal of Production Research*, 58(7), pp.2063-2081.

Public Safety Act, (2002). *Public Safety Act*, https://laws.justice.gc.ca/eng/acts/P-31.5/index.html

Randeniya, M., Palliyaguru, R. and Amaratunga, D., 2022. Defining critical infrastructure for Sri Lanka. In: Sandanayake, Y.G., Gunatilake, S. and Waidyasekara, K.G.A.S. (eds). *Proceedings of the 10th World Construction Symposium, Sri Lanka,* 24-26 June 2022, pp.313-325.

Roche, E. M. (1998). Critical foundations: protecting America's infrastructures, *Journal of Global Information Technology Management, 1(1), pp.49-50.*

Oxford Business Group (n.d.*). Sri Lanka moves to expand ICT infrastructure and improve the population's digital literacy.* Retrieved June 9, 2023, from https://oxfordbusinessgroup.com/overview/targeted-approach-efforts-expand-infrastructure-and-improve-digital-literacy-are-laying-groundwork.

Sri Lanka Telecommunications (1996). *Telecommunications Act.* https://www.lawnet.gov.lk/sri-lanka-telecommunications-2/.

S., Burchaers, K.Brown, B.Virtue. (2022, October 27). *The privacy, data protection and cybersecurity law review: Australia.* The Law Reviews. Retrieved July 11, 2023 from https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/australia

United Nations. Economic Commission for Europe (2007). *Information and communication technology policy and legal issues for Central Asia: guide for ICT policymakers.* United Nations Publications. https://unece.org/fileadmin/DAM/ceci/publications/ict.pdf