Equilibrium of Cybersecurity and Data Privacy: Analysing Cyber Terrorism in International Context

SCTS Fernando[1#], WMRK Wijesundara[1], and DNY Welaratne[1]

[1] *Faculty of Law, General Sir John Kotelawala Defence University, Ratmalana, Sri Lanka*
[#] fernandoclare7@gmail.com

Abstract— *Since the dawn of information technology, terrorists have used cyberspace as a weapon to carry out their intentions. At the moment, cyber technology provides cyber terrorists with a comprehensive and complicated set of information and instruments with which to continue their attacks on governments. The usage of tools and the motivations of cyber terrorism have an impact on cyber security and data protection both directly and indirectly. This study identifies the effect of cyber terrorism on cyber security and data protection and focuses on the relevant cases that have arisen out of cyber terrorism and legal frameworks that have established in addressing cyber terrorism, cyber security, and data protection. The study analyses the new trends of cyber security risks arising through cyber terrorism and examine how data breaches affect privacy and leads to cyber-terrorism. This primary research is evident almost at every stage of cyber-attack it affects cyber security and data protection as a subsidiary result. This study has identified the insufficiency of the laws addressing cyber terrorism. This qualitative research is primarily supported by case laws, journal articles and statues. Primarily it evident the necessity of separated direct laws as well as penal code recognition for cyber terrorism and the amendments should be taken place to address cyber terrorism, cyber security, and data protection from time to time depending on the innovations of cyber technology, for the perception of minimizing the terrorist attacks and negative impacts on it.*

Keywords— **Information technology, cyber terrorism, cyber security, data protection, cyber space**

I.INTRODUCTION

Cyberattacks, which are even known as cybercrimes, are vital regarding security threats. A modern cybercrime can occur as Hacking, BOTS and BOTNETS, key loggers, Website Defacement, Malware – Viruses, Distributed Denial of Service (DDOS) Attacks, Phishing, Vishing, Phreaking, and Identity Theft.

According to defense analyst Dorothy Denning a cyber-terrorism can be defined as "Unlawful attacks and threats of attack against computer, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives."

Cyber terrorism literally equals to a cyber-attack, and it only get the structure of the terrorist activity when the terrorist has used cyber space for the use of attacking a government and for the perception of interfering their data and system interference. Thus, an act to be a terrorist act, it must involve the political motivation.

Therein it is clear the terrorists use cyber techolonolgy for the fulfillment of the purposes such as to aid their terrorist actions and for the use of cyber technology as a weapon in attacking as terrorist activities. Cyber-attacks by terrorist might effect on physical cause of damage, destruction of infrastructure, effect on unity and sovereignty and destruction of economy and threatening the government of a certain country. The terrorist possibly focuses on control system and data on cyber space to succeed their motives.

The cyber terrorist often includes the objectives such as:

- Causing air traffic including for military networks, financial system, and telecommunication.
- Disruption of economic and industrial with the intention of causing damage to the safeguarded data and theft confidential data.
- Causing damage to the civilians including loss of life, physical injuries, air clashes, and theft of information.
- Causing disruption for essential part of the government with the intention of develop a fear within the government.

With the development of the information technology, the established data of a certain owner is in a certain kind of a risk with regarding its security. Thus, the need of address the protection of data and its privacy is essential body to be focused parallel to the development through several sectors of the information technology.

There have been several legal frameworks as well as technology tools that have been developed for safeguarding and ensuring the protection of the data. However, it is a question whether the existing legal framework as well as measures are mostly sufficient for the upcoming cyber

threats with the development of the technology through eras.

Cyber-terrorism might effect on the protection of confidential data of a certain authority as often cyber terrorism involves unauthorized access to protected data either for the intent of theft or disruption of data. Critically due to compound of reasons, a cyber-terrorism and cyber security and data protection interrelates with each other. Therefore, through the development of the cyber technology addressing a cyber-terrorism and its effect on cyber security and data protection yet remains as a necessity.

II. METHODOLOGY

Both primary and secondary materials are used in this qualitative study, including relevant case laws, books, journal articles, statutes, and online sources. In this research, the Sri Lankan context as well as the Indian context and the American legal standards has been comparatively examined. This study is primarily focused on cyber terrorism, which has had a significant negative impact on the sector information technology. It also analyzes how cyber terrorism interacts with data privacy and cyber security issues, as well as how it has evolved into a variety of different formats while exploiting legal loopholes. Furthermore, the main goal of this study is to investigate the Equilibrium of cybersecurity and data privacy by analyzing cyber terrorism in an international context.

III. FACTS AND FINDINGS

A. Cases related to cyber terrorism

There are significant cases that illustrates the cyber terrorism through cyber space, and each cases demonstrate the use of technology and variation of cyber-attacks by terrorist.

The cyber-attack on Kudankulam Nuclear power plant which was caused through Malware by North Korean hacker group called “group B” as associates with “group C’’ on the NPCIL system and was identified the infected PC have belonged by who was connected on the internet connected network which was used for administrative purposes. In addition, the networks are being continuously monitored. (Mallick, 2019)

During a two-week period in 1998, ethnic Tamil guemllas bombarded Sri Lankan embassies with 800 emails every day. “We are the Internet Black Tigers, and we're sending these messages to obstruct your communications”, it said in the messages. It was described as the first known terrorist strike on a nation's computer networks by intelligence officials. (Bulathgama, n.d.)

During the 1999 conflict in Kosovo, hacktivists opposing NATO bombings targeted NATO systems with denial-of-service assaults and bombarded them with e-mail bombs. Additionally, sources state that a variety of Eastern European nations sent highly politicized, virus-filled emails to corporations, government agencies, and academic institutions. Also frequent were web defacements.

The Electronic Disturbance Theater (EDT) has been staging Web sit-ins against several websites in support of the Mexican Zapatistas since December 1997. At a predetermined moment, thousands of protesters use software to direct their browsers to a target site, flooding it with frequent, erratic download requests. Animal rights organizations have also utilized EDT's software to target organizations that are alleged to harm animals. When they gathered in Seattle in late 1999, the electro hippies another group of hacktivists conducted Web sit-ins against the WTO.

One of the deadliest instances of cyber terrorists at work occurred when crackers in Romania obtained unauthorized access to the computers in charge of an Antarctic research station's life support systems, putting the 58 scientists working there in risk. More recently, in May 2007, Estonia was the target of a massive cyberattack by Russian hackers that some evidence implies was orchestrated by the Russian government, even though Russian officials deny any involvement. It appears that the relocation of a Russian World War II memorial from central Estonia sparked this incident.

According to Hitachi payment services Pvt. Ltd, 2016 breach of debit card database was the one of largest data breach amongst Indian history as a Cyber-attack caused by Malware that was injected into its system. It has affected 3.2 million debit cards in 2016. The major Indian banks such as SBI, HDFC Bank, ICICI, YES Bank and Axis Bank, have been worst affected through this incident. Further, it mentioned that it had no idea how much data had been exposed. (Gopakumar, 2017)

The terrorist attack on Mumbai on 2006 was also done with cyber space where the terrorist has able to use most advanced technologies such as Global Positioning System, Blackbeerys, and CDs with high-resolution satellite images, cell phones with switchable SIM cards and satellite phones. Meanwhile the cyber-attack by Pakistan on the following year was occurred with hacked into the websites of the India institutions of remote sensing. (Viswanathan, 2012)

When a major U.S. bank's computerized systems were breached two decades ago, a crew of resourceful thieves from many continents led by a young computer programmer in St. Petersburg, Russia began secretly taking money. This was a bank robbery for the modern era no disguise, no letter, no gun in 1994. In addition, The Melissa virus, which was still a relatively new concept to many Americans, first took control of the victims' Microsoft Word application in 1999 are some of the major cases relates US context. (Anon., n.d.)

B. Legal framework

The India has identified the cyber terrorism through their significant legal framework with the common intention of mitigating future cyber terrorists' attacks. According to the amendment that was made in 2009 for the Information Act, 2000 addresses cyber terrorism as well. Section 66f of the amended Act states the punishment for cyber terrorism. Further the Section 66 which refers about the computer related offences, Section 65 that refers about tampering with computer sources documents, Section 66C that refers to punishment for identity theft and Section 66E which relates to punishment of violation of privacy also indirectly address the cyber terrorism as cyber terrorist activities interconnected with use of cyber space.

The legal framework address also the Cyber security and data privacy with the same Information Act 2000, through the amendment made on it in 2009. Section 43A of the Act refers to the compensation for the failure to protect data. Section 72A refers to the punishment for disclosure of information in breach of lawful contract.

The Sri Lanka has also set up prominent legal frameworks for the perception of addressing cyber terrorism. The Prevention of Terrorism Act No. 48 of 1979, which refers about the means of terrorism, the Computer Crimes Act No. 24 of 2007 which has criminalized computer related offences including cyber terrorism consist with the reference of the essential areas such as unauthorized access to computer system, disclosure of information, and offences related computer data. Telecommunication Act No. 25 of 1991 has also made addressing of regards to telecommunication networks to prevent and investigate cyber related offences. In addition, it should be needed to establish that neither of Act have not directly address the point of cyber terrorism. However, those Acts are associated with cyber terrorism indirectly.

The legal framework that has established to address the cyber security and data privacy under Sri Lankan context often refers the same acts of Computer Crimes Act No. 24 of 2007 and the Telecommunication Act No. 25 of 1991. Instead, Personal Data Protection Act No. 4 of 2020 that covers the guidelines of the protection of personal data, Electronic Transactions Act No. 19 of 2006, which address on ensures the security and integrity of electronic communications, and Computer Crimes Act No. 24 of 2007 refers on cyber security and data protection.

US as a country of being faced to cyber terrorist attacks often have addressed the legal framework for the cyber terrorism by U.S. Patriot Act 18 U.S.C, and the Computer Fraud and Abuse Act 18 U.S.C. However, these laws also do not address in a direct way, instead it associates with surrounded rules, that co-related with cyber terrorism.

Cyber security and data protection have been addressed by several legal frameworks under the U.S context. Computer system abuse is prohibited by the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030. It relates to cyber security. Federal computers, bank computers, and Internet-connected computers are all protected by it. Further, the Cybersecurity Enhancement Act of 2014, Federal Exchange Data Breach Notification Act of 2015, National Cybersecurity Protection Advancement Act of 2015, and Cybersecurity Information Sharing Act are the significant legal frameworks that upheld for the cyber security and data protection that address through different parameters under US context.

C. New trends of cyber security through cyber terrorism

Cyber terrorists are increasingly using advanced persistent threats (APTs), which are persistent, targeted attacks meant to compromise the network of a particular company. These attacks have several stages and frequently include very technical evasion strategies.

Attacks using ransomware have grown to be a major threat in recent years, and cyberterrorists have been known to use this strategy. They break into systems, encrypt data, and then demand ransom payments to unlock the data. To maximize their damage, cyberterrorists may target important infrastructure, governmental institutions, or commercial enterprises.

Attacks on the Software Supply Chain: Cyber terrorists are aware of the potential weaknesses in the software supply chain and seek to take advantage of them. They can introduce malware or backdoors into widely used software by hacking a reliable vendor or provider, leading to widespread compromise when the software is used.

Internet of Things (IoT) Exploitation: As IoT devices proliferate, cyberterrorists now have a larger attack area to exploit. To take control of them and use them as part of botnets for carrying out significant DDoS attacks or for other nefarious purposes, they may target weak IoT devices.

Phishing emails and bogus websites are only two examples of the social engineering and phishing tactics that cyber terrorists use to mislead people into disclosing personal information or downloading dangerous malware. This method is employed to transmit malware or gain unauthorized access to computer systems.

Cyberattacks by nation-states: Some cyberterrorism operations are supported by nation-states looking to obstruct or gain an advantage over other nations. Political, economic, or social instability can result from state-sponsored cyberattacks that seriously damage military systems, essential infrastructure, or government institutions.

Information weaponization: Through the weaponization of information, cyberterrorists hope to sway public opinion, stir up social unrest, or disseminate false information. They use internet forums, false news websites, and social media channels to spread their message, sway public opinion, and inspire violence.

Cyber terrorists keep a close eye on and take use of evolving technologies. For instance, they might utilize

machine learning (ML) and artificial intelligence (AI) to develop more sophisticated terrorist attack vectors or improve their capacity to elude detection.

IV. DISCUSSION

Cyber terrorism and cyber security and data protection are not contiguous from its literal meaning. However, it can be understood that there is an interconnection between these two distinctive elements. Cyber terrorism literally means the use of cyber space as a weapon for their terrorist purpose and what they do might depend on their motive. Cyber security and data protection are the essential elements that have been developed for the protection of data on a secured storage portem. Thus, there are technologies and relevant laws addressing cyber security and data protection, through that it able to protect the data. The linkage between cyber terrorism arises in where the terrorist has accessed to the protected data of government and either have theft or disrupted of data. Therein, this leads to a breach of the security of cyber and protected data.

When considering the major impacts on cyber security and data protection by cyber terrorism, often it is clear that the cyber terrorism may involve in steal of sensitive data including government data, industrial data, financial records, and intellectual property data. Data breaches jeopardize data privacy and put people at risk of identity theft. 2014 cyber-attack on Sony Pictures Entertainment resulted by the North Korean hackers, which resulted in the loss and public disclosure of sensitive communications, employee data, and unreleased movies. The hack demonstrated the possible impact of cyber terrorism on data security.

Cyber terrorism usually involves the use of sophisticated cyber-attacks or heightened cyber-attacks for targeting governmental systems, Critical infrastructure, and Organizations. These attacks frequently involve innovative strategies and technologies that can outperform standard security measures, providing substantial problems for cyber security experts. The 2015 cyber-attack on Ukraine's power grid, attributed to a Russian cyber espionage group, resulted in widespread power outages affecting hundreds of thousands of people. The attack targeted the operational technology (OT) systems controlling the grid, demonstrating the potential impact of cyber terrorism on critical infrastructure.

Data breaches have the potential to compromise systems and networks. If these hacked systems are connected to key infrastructure or sensitive government networks, cyber terrorists might use them to obtain unlawful access, disrupt operations, or inflict significant harm. The stolen data from breaches may give the required information to properly exploit these hacked systems.

In certain circumstances, compromised data may contain usernames, email addresses, and passwords. Cyberterrorists can use this information to conduct credential stuffing attacks, in which they attempt to acquire illegal access to users' other internet accounts by using the same login credentials. If successful, these account takeovers can lead to further privacy infractions or serve as a springboard for more serious cyber-attacks.

Cyber terrorists may create and spread malware such as viruses, worms, ransomware, or spyware to infiltrate networks and collect data. Individuals and businesses may suffer data breaches, financial losses, and privacy violations because of this. Thus, it reveals the overall impact of cyber terrorism on cyber security and data protection in several dimensions.

1. Indian Context

When considering the Cyber terrorism through Indian context, in the case of Kudankulam Nuclear Power Plant cyber-attack, the North Korean hackers' group have used malware link and sent to the official and personal mail accounts. Once the link clicked, the malware spread over the IT Networks. It has been identified that the hackers have already known the IP address and they have not disrupted the system but have extracted confidential data. This demonstrated that cyber terrorism affected on cyber security and data protection as hackers have gathered confidential data, which have protected. (Mallick, 2019)

The legal framework on cyber terrorism through Section 66f of 2009 amendment to the Information Technology Act provides that whoever cause accesses to computer resources without authorization with the intention of causing damage for sovereignty, unity and extract and disruption of confidential data might be punishable with imprisonment. When it comes to the cyber security and data protection related laws, Section 43 refers to the fact that where relevant party has failed to protect the data will be compensated for the negligence of could not be able to protect data with taking necessary measurements. In addition, Section 72 A is quite significant as it refers to the fact that the party who has disclosed the confidential data will be compensated. This illustrates that both sections are useful even in addressing cyber terrorism in instances such as the relevant authority have not maintained a strong passwords and key loggings and disclosure of confidential data on a certain consideration. Thus, this demonstrated that even the Laws address on two specific segments can used for the perspective of both areas.

2. Sri Lankan Context

In 1998, the LTTE terrorist group have sent 800 e-mails for the Sri Lankan embassies and in recent few years ago on 3rd of June 2021, they have hacked the former Prime Minister Mahinda Rajapaksha's website as well. This provides the capability of use of technology for their motives and due to all these hackings; it influenced threat to security of governmental data. (Bulathgama, n.d.)

When considering the legal framework on cyber terrorism, the government use Prevention of Terrorism Act No. 48 of 1979 where from Section 2 refers that this act may use for the "unlawful activities" related to the terrorist and Section 16 of the same Act addresses the offences through use of any means of communication. Thus, as the cyber terrorism involves terrorist activity and used cyber space for their activities, these Sections hold for addressing cyber terrorism. Further Computer Crimes Act No. 24 of 2007 also plays a pivotal role in addressing cyber terrorism. Sections 3 to Section 10 address the unauthorized access and obstruction to access to computer, unauthorized disclosure of passwords and unauthorized interception of data.

The legal framework for the cyber security and data protection address through the same Act of Computer Crimes Act No. 24 of 2007 where it has criminalized, prohibited and penalized unauthorized access to a computer, unauthorized obstruction of access to a computer, destruction of computer data through Section 3, 5, 8, 9, 10, and 15. Also through Section 16 of the Personal Data Protection Act No. 4 of 2020 provide the set of obligation for data controllers regarding data security and safeguards. In this forum, it is thus clear that the same Act can be used to address Cyber terrorism, Cyber security, and Data Protection.

3. US Context

The Melissa virus, which has a significant role in cyber-attack history of US, has caused through hijacked of the Microsoft outlook email system and have sent messages with a virus-laden attachment as "sexy.jpg" or "naked wife" and once the document started downloading the virus has quickly spread over the system. The attack has influenced on cyber security and their functions have been destroyed by the virus. The use of viruses for the intention of causing network blocks, system destruction for a moment and threaten the civilians, cause effect to the cyber security and protected data. Through these viruses they could have easily able to cause what they have intended to do though they have not accessed for the data. (Anon., n.d.)

When considering the legal forum of addressing cyber terrorism under US legal background USA PATRIOT Act (2001) which has expanded laws addressing cyber terrorism and which has laws such as The Computer Fraud and Abuse Act (CFAA) (1986) that indirectly address cyber terrorism through Section 1030 where refers about fraud and computer related activities. In addition, the legal framework on cyber security and data protection is addressed through the same Section of 1030 of The Computer Fraud and Abuse Act (CFAA) (1986). Further through Section 8 of Cybersecurity Information Sharing Act (CISA) (2015) refers about Privacy and Civil Liberties Protections, also majorly impacted on cyber security and data protection as a legal framework.

As a whole from the Indian, Sri Lankan and US context, the cases that have arisen through different attacks by different technologies have linked with leading towards effect on cyber security and data protection. Even direct and indirect legal frameworks on cyber terrorism interconnected with cyber security and data protection as a same effort of establishing a margin for address the terrorist activities and parties who are trying to go beyond the authorized use of computer technology. However, it is demonstrated that no country has been able to address cyber terrorism through a separate legal portem. Also, the Acts have not updated with the time for the perception of addressing new upcoming technologies and strategies of cyber space. Through these kinds of loopholes, a cyber terrorist can easily succeed their motives even causing damage for the cyber security and data protection at the end.

When drifting apart the cases up to 2021 and have look on some recent significant cases of cyber terrorism, in May 2023, the spearfishing attack on a well-known politician was connected to Chinese-sponsored hackers by Belgium's cyber security agency. In January 2023 several cyberattacks were launched by hackers against the national defense networks of Malaysia. According to Malaysian officials, the hacking efforts were discovered in time to prevent any network compromise. In March 2023, using a DDoS attack, Russian hackers briefly took down the website of the French National Assembly. Hackers claimed that the attack was carried out because of France's backing for Ukraine and it was stated in a Telegram post. In December 2022, Hackers with ties to China targeted people in the Asia Pacific region working in the government, education, and research sectors through phishing attacks. These attacks contained espionage malware software. In April 2022, a gang targeted several Ukrainian media organizations to permanently access their networks and gather private data. The organization is inked to the GRU in Russia. In February 2023, Between August and November 2022, an espionage operation was carried out by a North Korean hacker outfit. Targeting industries like chemical engineering, medical research, healthcare, defense, energy, and a research institution, hackers stole over 100MB of data from each victim while going unnoticed. The organization has ties to the North Korean leadership. When it comes to the month of March 2023, a new exploit from a Chinese espionage cell targeting political organizations in Taiwan and Ukraine was found by Slovakian cybersecurity researchers (Anon., 2023). These cases raised in between 2022 to 2023 demonstrate though there are legal frameworks that have established for addressing cyber terrorism, cyber security and data protection, the use of cyber space for the fulfillment of motives of terrorist have not ended. Thus, it will raise a question on guarantee of security of the data as cyber terrorism directly and indirectly affects cyber security and data protection.

Data breaches can have a substantial impact on privacy and can lead to cyber terrorism indirectly. Personal information, such as names, addresses, social security numbers, or financial information, is frequently exposed because of data breaches. Cybercriminals can use this stolen information for a variety of nefarious objectives, such as identity theft, financial fraud, or blackmail. In certain circumstances, data breaches give vital information to cyber terrorists, allowing them to target persons, businesses, or important infrastructure. The stolen data might contain information on vulnerabilities, system configurations, or access credentials that can be used to execute more complex and targeted cyber assaults, such as those linked with cyber terrorism. Data breaches have the potential to compromise systems and networks. If these hacked systems are connected to key infrastructure or sensitive government networks, cyber terrorists might use them to obtain unlawful access, disrupt operations, or inflict significant harm. The stolen data from breaches may give the required information to properly exploit these hacked systems. Further Large-scale data breaches diminish public faith in organizations' capacity to safeguard sensitive information. This lack of trust can create an atmosphere in which individuals and organizations are more vulnerable to manipulation and disinformation, thus boosting the spread of cyber terrorist propaganda or recruiting activities. The United States Office of Personnel Management (OPM) suffered a huge data breach in 2015, exposing the personal information of millions of present and former federal employees. Security clearance information and background investigation documents were among the material obtained. While the breach was not an act of cyber terrorism in and of itself, the stolen information might be used by cyber terrorists to target persons in sensitive government posts or gain access to important government networks.

V. CONCLUSION

Since the 1990s with the development of technology, cyber terrorism uses different techniques depending on their motives and it has affected directly and indirectly on cyber security and data protection. The legal framework that has been established in addressing Cyber terrorism, Cyber security and data protection interrelated with each area. However, though several frameworks contribute to addressing cyber terrorism, most legal frameworks do not address cyber terrorism. Especially when considering through Indian, Sri Lankan and US context the absence of direct framework on cyber terrorism can be identified. The significant cyber-attacks between the year 2022 and 2023 proves the insufficiency of the current legal frameworks. In addition, the anonymity contributes terrorist in hiding their identity leads towards the impact of impossibility in tracking cyber terrorist who was behind in related cyber-attacks. Avoiding the laws by cyber terrorist as well as with the acknowledgement of current laws they might create or seek a path to avoid being liable under the laws. Thus, this might critically effect on Cyber security and data protection. Therefore, to address the issues related to cyber terrorism, cyber security and data protection, the relevant measures must be taken.

Considering to Indian, Sri Lankan, and US context as the laws and regulation have taken to prevent cyber terrorism is in low level, the laws should be developed from time to time depend on development of technology and even cyber security and data protection. There must be direct Acts in addressing cyber terrorism. Most cyber terrorism has been taken often due to the lack of acknowledgement on relevant laws and there must be awareness programmes for civilians to minimize cyber terrorism. Especially instead of people in legal firms and politics, civilians might not read laws, gazettes at often, awareness of those relevant laws should be done through newspapers, TV programs and through twitter and Facebook platforms. There must be a penal code recognition for cyber terrorism and breach of cyber security and data protection by a cyber terrorist as well. Further, to prevent from anonymity of cyber terrorists, the new laws must be implemented to address the anonymous activities of cyber terrorist.

REFERENCES

Anon., 2011. *Computer Law.* 7th Edition ed. s.l.:Oxford university press.

Anon., 2023. *Center for Strategic & International Studies.* [Online]
Available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
[Accessed 13 6 2023].

Anon., 2023. *Fairleigh Dickinson University.* [Online]
Available at: https://online.fdu.edu/program-resources/cybersecurity-and-cyber-terrorism/
[Accessed 12 6 2023].

Anon., 2023. *Maryville University.* [Online]
Available at: https://online.maryville.edu/blog/cyber-terrorism/
[Accessed 17 6 2023].

Anon., n.d. *FEDERAL BUREAU OF INVESTIGATION.* [Online]
Available at: https://www.fbi.gov/investigate/cyber/major-cases
[Accessed 16 6 2023].

Bulathgama, T., n.d. Cyber Terrorism an Emerging Threat to Sri Lanka's National Security.

Computer Crimes Act No. 24 (2007).

Computer Fraud and Abuse Act, 18 U.S.C. 1030 (n.d.).

Cybersecurity Enhancement Act (2014).

Cybersecurity Information Sharing Act (n.d.).

Dr.J.N.Barowalia, n.d. *Commentary on the Right to Information Act.* s.l.:s.n.

Electronic Transactions Act No. 19 (2006).

Fedaral Exchange Data Breach Notification Act (2015).

Gopakumar, G., 2017. *mint.* [Online] Available at: https://www.livemint.com/Industry/jVF2Aw72w0DcBsUGseV0UP/Malware-caused-Indias-biggest-debit-card-fraud-Audit-repor.html [Accessed 13 6 2023].

Information Act (2009).

Lloyd, I. J., 2017. *Information Technology Law.* 8th Edition ed. s.l.:s.n.

Mallick, M. G. P., 2019. Cyber Attack on Kudankulam Nuclear Power Plant A wake up call. *Vivekananda International Foundation,* pp. 6-11.

National Cybersecurity Protection Advancement Act (2015).

Personal Data Protection Act No. 4 (2020).

Prevention of Terrorism Act No. 48 (1979).

Somya, S., n.d. Cyber terrorism and Laws in India. *Legal Service India.*

Telecommunication Act No. 25 (1991).

USA PATRIOT Act (2001).

Viswanathan, A., 2012. *Cyber Law Indian and International perspective on Key topics including data security, Ecommerce, cloud computing and cyber crimes.* 1st Edition ed. s.l.:s.n.

Yasas, W. R., n.d. Laws in Sri Lanka to prevent cyber attacks. *Analyzing whether those lawsare sufficient to prevent a cyber warfare in the future*, pp. 3-14.

ACKNOWLEDGMENT

Since these are fundamental ideas of IT law, we would like to sincerely thank Ms. Ayodya Jayasinghe for inspiring us to learn more about it. We are very grateful to Mr. Shevan De Silva for giving us unwavering advice, direction, and support throughout this comprehensive study . We also thank all the respected personnel for their assistance. Finally, we would want to express our gratitude to our parents and friends for their support and encouragement throughout this study.

AUTHOR BIOGRAPHIES

Ms. S. C. T. S. Fernando, the author, is a third-year law student at General Sir John Kotelawala Defence University. This is her first experience in research publication. Information Technology Law, Space Law, Criminal Law and Human Rights Law are her particular research interests.

Ms. W. M. R. K. Wijesundara , the author, is a third-year law student at General Sir John Kotelawala Defence University. This is her first experience in research publication. Humanitarian Law, Criminal Law, Human Rights Law, and Information Technology Law, are her particular research interests.

Ms. D.N.Y. Welaratne, the author, is a third-year law student at General Sir John Kotelawala Defence University. This is her first experience in research publication. Forensic Medicine, Information Technology Law, Criminal Law and Human Rights Law are her particular research Interests.