|  |
| --- |
| Name: Balage Prabhani Pinsari Silva. |
| Student Reference Number: 10707375 |



|  |  |  |
| --- | --- | --- |
| Module Code: PUSL 2001 | Module Name: IT Legalization and Ethics. | |
| Coursework Title: Individual Assignment. | | |
| Deadline Date: 07/01/2021 | | Member of staff responsible for coursework: |
| Programme: BSC. (Hons) Software Engineering. | | |
| Please note that University Academic Regulations are available under Rules and Regulations on the University website [www.plymouth.ac.uk/studenthandbook](http://www.plymouth.ac.uk/studenthandbook). | | |
| Group work: please list all names of all participants formally associated with this work and state whether the work was undertaken alone or as part of a team. Please note you may be required to identify individual responsibility for component parts.  ***We confirm that we have read and understood the Plymouth University regulations relating to Assessment Offences and that we are aware of the possible penalties for any breach of these regulations. We confirm that this is the independent work of the group.***  Signed on behalf of the group: | | |
| Individual assignment: ***I confirm that I have read and understood the Plymouth University regulations relating to Assessment Offences and that I am aware of the possible penalties for any breach of these regulations. I confirm that this is my own independent work.***  Signed : C:\Users\User\Desktop\EXAM 2nd YEAR\20201205_150324.jpg | | |
| Use of translation software: failure to declare that translation software or a similar writing aid has been used will be treated as an assessment offence.  I \*have used/not used translation software.  If used, please state name of software………………………………………………………………… | | |
| **Overall mark \_\_\_\_\_% Assessors Initials \_\_\_\_\_\_ Date\_\_\_\_\_\_\_\_\_** | | |

\*Please delete as appropriateSci/ps/d:/students/cwkfrontcover/2013/14

**IT LEGALIZATION & ETHICS.**

**10707375 - PLYMOUTH ID\_NO**

**BALAGE SILVA - PLYMOUTH ID\_NAME**

****

**18409 - NSBM ID\_NO**

**B. P. P. SILVA - NSBM ID\_NAME**

**Analyses the laws in Sri Lanka which prevents terrorist Propagandism via Internet.**

“Terrorist Propaganda constantly shift on to new and diverse platforms such as social media and the quantity of information exchanged, either publicly or in private spaces, is increasing. In order to face the evolving threats, any country needs to safeguard the country tightening its laws. Analyses the Cyber law of Sri Lanka whether the said laws are strong enough to curb cyber terrorism propagandism strategies. Specially focus on the Computer crime legislation, data privacy and cyber security legislation in Sri Lanka.

Are the Cyber Laws in Sri Lanka able to curb terrorism propogandism which happens via the internet?”

**CONTENTS.**

**Abstract.**

**Chapter 1 :- Introduction.**

* ***Objective.***
* ***Rationale for the Research.***
* ***Background and History.***
* ***Context.***
* ***Definitions.***

**Chapter 2 :- Literature Review.**

**Chapter 3 :- Methodology.**

**Chapter 4 :- Critical Analysis and Discussion of Findings.**

* ***Introduction of Cyber Warfare.***
* ***Intellectual Property Act No. 36 of 2003.***
* ***Computer Crimes Act No. 24 of 2007.***
* ***Cyber Security Act.***
* ***Electronics Transaction Act.***

**Chapter 5 :- Suggestions and Opinions.**

**Chapter 6 :- Conclusion.**

**Bibliography.**

**Abstract.**

What is the Cyber law?

Information Technology Law (also known as “CyberLove” deals with IT law, including computers and the Internet. It deals with legal information and controls the digital distribution of (digitized) information and software, both information security and e-commerce. Sections and what is described as “paper rules” for a “paperless environment”.

The advanced world is totally founded on data innovation. These new advance have made new criminal chances, known as cybercrimes.

In the present, these cybercrimes are at the level and has been spread the world over as digital fighting which represents a genuine thereat to public security. Sri Lanka is additionally a survivor of digital fighting. There are numerous laws and enactments in Sri Lanka with respect to network protection.

“Social media” should not play film of murder “(Australian Parliament) Both New Zealand and Australia passed the overall sharing Abhorrent Material Bill that bargains tremendous fines for online media associations and jail time for their bosses if they don’t rapidly take out “abominable furious material” from their establishment (Liza Vass, 2019).” Against this setting, it is a critical need to inspect whether the Laws of Sri Lanka are sufficient to control unlawful terrorizing in electronic media.

Analyzing history, online media has accepted a basic occupation in the jihadists’ operational procedure in Syria and Iraq and past. The spotlight in the unlawful terrorizing composing on the exhibition focus of mental aggressor spectaculars rules reality that fear mongers in like manner use the Internet for comparable reason each other individual does; for affiliation and organizing, changing over and redirection and to show the enthusiasts. Believe it or not, by far most of the online correspondence of dread based oppressors is regularly to the point of appearing to be innocuous.

* Is that via web – based media stages all substance looks pretty much the equivalent.
* This new media climate in Sri Lanka is likewise impervious to policing.
* Sri Lanka needs to set up new laws to ensure against the abuse of the correspondence networks that have arisen in the computerized age.

The cutting edge world is totally founded on information Technology. These new advancements have made new criminal chances, known as cybercrimes. In the present, these cybercrimes are at the pinnacle level and has been spread far and wide as digital fighting which represents a genuine danger to public security. Sri Lanka is additionally a survivor of digital fighting. There are numerous laws and enactments in Sri Lanka with respect to online protection. Yet it is safe to say that they are sufficient to confront the digital fighting that has been spread among the countries? This exploration is done to discover the response to the above inquiry by investigating the network protection laws in Sri Lanka. As the result of this examination, the per user will get a smart thought about cybercrimes, cyberwarfare and digital laws in Sri Lanka. What’s more, there will be an investigation of digital laws in Sri Lanka to see if they are sufficient to confront the cyberwar. The basic information and data sources are sites, books, diary articles and Acts in Sri Lankan law, that have been utilized to deal with this exposition.

**Chapter 1 :- Introduction.**

Today, the PC (Computer) has become one of the most popular and widely used means of communication technology in the world. This is not only a communication tool but also a tool or equipment system that guides the infrastructure and essential services of the government in developed countries today. Because of this, the computer today is used as a popular tool, but in many ways it is common in the past, but today we can see the following in a way that can not be limited or prevented in a very intelligent way.

* Taken for modern terrorism.
* Computer virus production.
* Phishing.
* Shocking..
* Crimes committed using the Internet.

“Cybercrime is any criminal activity carried out using computers or the internet. Cybercrime uses tools like phishing, viruses, spyware, ransomware and social engineering to break the law.” (Avast Academy Team, 2016)

Because of the Industrial Revolution, the human needed to confront numerous dangers. In this way, specialists have done numerous investigations on discouragement system focusing on a few later dangers. To begin with, those investigates were cantered mostly around discouragement among countries and atomic prevention. After the 9/11 assault, there has been more exploration zeroing in on different dangers the same psychological oppression, maverick states and ethnic clashes. These investigates convey a couple of clues. They are essentially remaining with an end goal to dissect how the significance of certain conditions that can be applied for successful discouragement, created under the foundation of the Cold War and are strategy situated to a degree, particularly focusing on the dangers remaining against Sri Lanka.

Types of Computer Crimes.

Illicit harassment can simply be interpreted as a computer crime through the use of a computer or a device belonging to it. This is because the likelihood of committing a crime is high and the ability to raid criminals using such computer is limited.

1. Using the Computer for modern terrorism.

At present we can identify that the computer is being used at a high level for terrorism. They use the computer for the following purposes.

* Recruitment of members.
* Fundraising.
* Launching mental warfare to defeat enemies through the Internet.
* Spreading their ideological objectives.

1. Computer Viruses.

This is a series of written computer that can damage the computer’s functionality and the information files it contains. Computer viruses are now written with the primary goal of disrupting the development of a country or organization and otherwise making a country or an organization lagging behind by destroying information.

1. Phishing.

This crime is the act of fraudulently obtaining and using information belonging to an individual or other important entity and using it to commit fraudulent activities.

1. Hacking.

This is often a sabotage. Unauthorized alteration of data and software and intrusion into computer system.

1. Crimes over the Internet.

Measures taken by various countries to protect against computer crimes.

Computer crime has become a cancer all over the world today. As a result, computer crime has grown beyond the control of the world. The magnitude of the frauds taking place in the United States can be attributed to the fact that Sri Lanka has a higher value than the World Bank. This can be illustrated by the situation with credit card fraud in the United States.

Sri Lanka.

* Computer Crimes Act No. 24 of 2007.
* Rules contained in Article 100 of the Evidence Ordinance.
* Tech Search Institute.

America.

* 1982 Computer Crime search in Washington.
* Describing computer crimes in the Federal criminal code on computer crime.

India.

* Information Technology Act, 2002.
* Steps to take to protect yourself from computer crimes.
* ***Objective.***

The fundamental target of this exploration is to illustrate, understanding and investigate the lawful system in Sri Lanka that forestalls cyber warfare and its pertinent issues.

* ***Rationale for the Research.***

The primary explanation behind this examination is the digital assaults happened as of late which menacingly influenced public security and Sri Lanka being a casualty of cyberwarfare. In the present, the generally ground breaking and precise data source is the web. “As indicated by the International Media Transmission Union (ITU), the particular organization for date and correspondence advances of the United Nations, in 2013 more than 2.7 billion individuals routinely utilized the we.” (Buono,2014) For instance, web based banking, charge installments, web based shopping and so forth likewise, every country utilizes PCs and distributed storage to store all their classifieds data. Thus, programmers, psychological oppressors, rival nations attempt to take this data. It is a major danger to the world’s security. In the present circumstance, it is imperative to do an investigation on ‘the laws of digital protection’ particularly in Sri Lanka to lead local people to contemplate laws and their ability of forestalling Cyber Warfare. The principle explanation behind this subject to be examined in this work is to research, investigate and examine whether Sri Lanka law is sufficient to defend the country from digital fighting. There is new, as of late found data did in this examination. In this way, for additional scholarly/non-scholastic purpose including lawful activities, this work can be utilized viably and productively.

* ***Background and History.***

Returning to late years, we heard the news with respect to numerous digital assaults. As per the investigations, the most infamous cyberattack in late was WannaCry Ransomware which harmed around 200,000 PCs around the globe including a few medical clinics, manufacturing plants and so on (Kaspersky,2019) besides in Sri Lanka there were some new digital assaults which made the Sri Lankan government ponder data security. A few sites including Rajarata University and Tea Research Institute had been presented to digital assaults by a fear monger bunch as of late. What’s more, there were some disinformation crusades, utilizing online media after 21/4 assault that influenced more to the security in Sri Lanka. (Hewage,2019) Referring to the digital law, the main worldwide show on cybercrime was the ‘Budapest Convention on Cybercrime.’ Sri Lanka is additionally an individual from the show and that show was the fundamental motivation to present Computer Crimes Act No. 24 of 2007 in Sri Lanka. Be that as it may, in the present, there are numerous acts viewing cybercrimes, for example, the Electronic Transactions Act, cyber Security Bill, Media transmission Act and so on from limited scope organizations to significant enterprises (governments), digital assaults are developing quickly in extension and recurrence across the globe. Since the advancement of innovation, the digital assaults additionally started to rise step by step. The latest occurrence identified with the subject is the Cyber assaults on Sri Lanka that have been led in May 2019. Around 10 of the Sri Lanka homegrown sites with public spaces for example, .com and .lk including the site of the Kuwaiti Embassy working in Sri Lanka were assaulted and it was an incredible danger to the country. (Fernando,2019)

* ***Context.***

This exploration is basically zeroing in on the Sri Lankan legitimate system to forestall digital fighting. As in the point, the principle purpose behind this examination is to acknowledge, regardless of whether the digital laws in Sri Lanka are sufficient to confront the digital fighting in the cutting edge period. There will be a short audit of past explores, that had been finished centering IT laws and enactments, to introduce a plan to the per user about digital difficulties, laws to forestall them and how the general public should remain against digital fighting. At that point there will be an examination of Acts in Sri Lanka with respect to online protection.

Eg:- IP Act No. 36 of 2003, Computer Crimes Act No. 24 of 2007. As an outline, this exploration will experience numerous regions, principally the IT business, cybercrimes and dangers. Sri Lanka digital laws and how they can assist with forestalling digital fighting. This is nitty exploration about digital fighting, breaking down the legitimate system of Sri Lanka and see whether they are adequate to protect the country from digital fighting.

* ***Definitions.***

According to the Oxford Dictionary “Digital fighting” signifies “the utilization of PC innovation to assault the data frameworks of a state or association, keeping them from completing significant exercises.”

**Chapter 2 :- literature Review.**

Ms. Aparajitha Ariyadasa (2019) has noted that there is no possible evidence mentioned to prove the intention of a person, although it is said that accessing unauthorized data/ information with the intention is a cyber-crime in the ‘Computer Crime Act No. 24 of 2007.’ As espionage is spying and obtaining information without the knowledge or the permission of the holder of the information or the data, this is a negative point found in Sri Lankan law against the cyber-warfare. (Aparajitha Ariyadasa,2019)

Ms. Aparajitha Ariyadasa (2019) has cleared out much information in her comparative analysis of the Computer Crimes Act of Sri Lanka. It is clearly mentioned that it has not interpreted the terms such as cyber-crime and other technical phrases with legal terms or descriptions in the Computer Crime Act. So, it is a loophole of the act which is responsible for carrying the legalizations related to computer crimes including cyber terrorism. (Aparajitha Ariyadasa,2019)

“Even though Computer Crimes Act covers some areas of computer crime, the gaps in data privacy, Data misuse, hate speech by social Media, Cyberbullying, Cyberstalking etc. Must be filled by the legislature as soon as possible.” (Aparajitha Ariyadasa,2019)

Social media which is a part of the cyberspace also has a dark side and according to the study of Ms. Aparajitha Ariyadasa (2019), Cyberbullying, Cyberstalking, Addictive use, Trolling, Online witch hunts, fake news and privacy abuse can be mentioned as examples. It is mentioned that there is no legislature present in Sri Lanka which addresses ‘Cyber-bullying’ and because of that the citizens are unprotected on this issue. (Aparajitha Ariyadasa,2019)

Ms. Aparajitha Ariyadasa (2019) has clarified how unfair advertising which goes under the category of propagandism, misleads the consumers. The analysis shows that propagandism or unfair advertising is being done by many agencies or companies in order to gain financial benefits. This study has pointed out that there is no relevant law in Sri Lanka to protect consumers from these types of issues. “Sri Lankan legislature does not introduce a proper state to protect consumers, competitors and the general public against misleading advertising.” (Aparajitha Ariyadasa,2019)

“Digital wrongdoing alludes to any criminal behavior that happens in the virtual universe of the internet.” (Jayasekara,2015) The article distributed by Ms. Dinithi Jayasekara has pointed out some significant realities concerning cybercrimes in Sri Lanka.

* What are the cybercrimes in Sri Lanka?
* Challenges in cybercrime in Sri Lanka.
* Analysis of recent cases in Sri Lanka and recommendations.

As per her article phishing, malware, email badgering, counterfeit records (fake accounts), sites hacking and youngster erotic entertainment (child pornography) are a few cases that have been spread among society. What’s more, most cases were identified with fake accounts on Facebook, Instagram. In any case, in Sri Lankan law it isn’t considered as a cybercrime. Consequently, Ms. Dinithi jayasekara has proposed to change criticism laws and acquaint digital maligning laws with keep away from these violations. (Jayasekara,2015) In her article, she has likewise recommended presenting an individual information security act. Sufficiently which was presented by the Ministry of Digital Infrastructure and information Technology (Data Protection Bill 2019) in 2019 (4 years after her article) (MDIIT Admin,2019) Therefore, recommendations and feelings in this research are satisfactory when we need having proper laws to forestall cybercrimes in Sri Lanka. Additionally, we need to end these cybercrimes to keep Sri Lanka from being a survivor of cyberwarfare. What is cyberwarfare? What causes cyberwarfare? There is an ideal response to these inquiries in the article Cyberwarfare and Implications’ composed by Sourav Mukherjee. “Cyberwarfare encompasses the action by any international organization to attack and try to cause damage to another nation’s infrastructure, computers or information systems through computer viruses or denial-of-service (DOS) attacks.” (Mukherjee,2019) comparing to Ms. Dinithi Jayasekara’s article the distinction among cybercrime and cyberwarfare is that cybercrime is any IT related criminal behavior while any cybercrime that hurts public security can be added to cyberwarfare. As indicated by this investigation a few gatherings hesitant to consider it a war. However, I think there is a gigantic likelihood of beginning a battle among countries in view of cyberwarfare.

**Chapter 3 :- Methodology.**

This examination is never really answer for three principle questions,

* What is Cyberwarfare?
* What are Sri Lankan laws?
* Are the Sri Lankan laws adequate to defend the country from cyberwarfare?

Subjective approach was utilized in the whole exploration to discover answers to the abovementioned questions. Utilized techniques, Secondary Sources, Websites, Journal Articles, Blogs, Books, Legislations. Referring to Style: Harvard. These technique were picked identifying with past investigates on cybercrimes, cyberwarfare and digital law. Examinations depend on thoughts of specialists identified with cybercrimes and ongoing contextual analyses associated with cybercrimes and law. The techniques utilized in the exploration are basic and straightforward. Absence of past investigates on cybercrimes was a major issue when gathering data utilizing this procedure. This examination is subjective exploration dependent on a hypothetical premise. It is finished by dissecting the Sri Lankan enactment including, Computer Crimes Act No. 24 of 2007, Electronic Transactions Act No. 19 of 2006, Evidence (Special Provisions) Act No. 14 of 1995, Cyber Security Bill Information Protection Bill, Intellectual Property Act No. 36 of 2003 and Payment Devices Frauds Act No. 30 of 2006. This examination has followed auxiliary sources for example research articles, reports, diary articles and digital books taken from e-networks specifically, SSRN ResearchGate, Google Scholar, Taylor and Francis and so forth etc.

**Chapter 4 :- Critical Analysis and Discussion of Findings.**

* ***Introduction of Cyber Warfare.***

“Cyberwarfare includes activities carried out by a state or a global association to attack. For example, attempting to damage PCs or data networks in another country abandonment of Provincial Council Infections or Administrative Assaults. (Rand.org,2020) We talked earlier describes different types of cybercrime. These digital attacks are meant to undermine the public. There is a place with cyber wars for the security of a nation. In a Mechanical Period, Public Privileged Intelligence, Financial reports, military reports etc. are kept in the Provincial Council information Base Services of a Nation. Similarly, approved meetings can actually be closed or used by air guards, use of radar, rockets, nuclear weapons and PCs. However, think of a time when someone hacked them. Provincial Councils that control information camps and military weapons? Certainly, it would be a big accident for the important nation. Fear-based oppressive associations, for example have used ISIS, AI Qaeda and so on. Programmers to obtain data from certain nations. Similarly when looking at virus war rival nations in a bid to retrieve each other’s group data, military privileged insights etc. in March 2010 WikiLeaks mysteriously presents a US security analysis report. That is a mainly printing for US security. Its counterparts, in turn, are a rejuvenation of the legal system to make it a secure internet. Is important in the ultra-modern period.

* ***Intellectual Property Act No. 36 of 2003.***

Intellectual Properties are the elusive or manifestations of the psyche. For instance, creative work, developments, abstract work and so on. There are two classifications in protected innovation:

* Industrial: licenses, brand names and so forth.
* Copyright: music, films, artistic works, ideas and so forth.

Protected innovation Act is acquainted with give legitimate rights to the proprietor who made the work. It permits the makers (specialists, artists, patent proprietors and so froth) to advantage from their manifestations. In this manner, nobody can duplicate or republish any protected innovation has a place with another individual without their approval as per the Intellectual Property Act. This demonstration is identified with the advanced reality where individuals concoct PC programming, mechanical technology and so on what’s more, this has diminished wrongdoings identified with protected innovation in Sri Lanka. Thusly, this energizes individuals for advancements and manifestations. What’s more, security of protected innovation has expanded our monetary rates and open positions in Sri Lanka. At the point when we associate this with cyberwarfare, different gatherings (psychological militant associations, nations) attempt to take ideas particularly military ideas from proprietors. In this way, the public authority should take severe rulings against licensed innovation violations to safeguard those advancements from cyberwarfare. IP act is the legitimate documentation of the laws identified with intellectual property rights.

* ***Computer Crimes Act No. 24 of 2007.***

CCA is accommodated the distinguishing proof, examination and counteraction of Computer Crimes. In this act predominantly the computer related wrongdoings and hacking offenses are being covered. In this demonstration, there are a few holes/provisos that should be covered. As referenced in the writing survey, in this demonstration, there is no technique portrayed to demonstrate the goal. In any event, for the reference, there are no applicable lawful words given in this represent digital wrongdoings and so forth despite the fact that it is stated, “risk or unavoidable peril is sufficient against the public security, public economy or public request” in the CCA, it is extremely unlikely to demonstrate the peril or haven’t referenced what the perils are or some other method to demonstrate the inescapable risks. In this demonstration, besides during the examination, they have given an administrative structure to secure basic liberties. This law assumes a significant job being used of information technology. This Act is acquainted with recognize cybercrimes, research and actualize them. Endeavors to unapproved admittance to Computers, software’s, projects and information and data are a few limitations made by this demonstration.

* ***Cyber Security Act.***

This act was drafted in 2019 to protect information and services from cyber attacks the purpose of the draft act is to establish a new body to provide identification and security. Computer systems that require “critical information infrastructure.” According to the a system will be created for the CII in the event of data loss, loss of functionality or data leakage the CII can do great damage to national security, the economy or services. Government or private the state owned CIA is overseen by ‘National Cyber’ Security Operations Center. Therefore, it will provide security to the Sri Lankan security forces. Terrorist organizations that seek to steal information about the economy, public health and security can be prevented by the laws of this Act.

* ***Electronic Transaction Act.***

This demonstration was authorized to kill the lawful hindrances and help both nearby and global online business by setting up a lawful sureness. This demonstration shows that in any e-correspondence, information protection assumes a significant job. In any case, there are no realities referenced about information protection or how to make sure about it. Likewise, this demonstration hasn’t referenced any detail identified with web bugs, treats and net spies in spite of the fact that they are dangers related in e-correspondence. Also, there is no data identified with e-correspondence wrongdoings or such encroachments can be found in this demonstration.

**Chapter 5 :- Suggestions and Opinions.**

After analyzing the rules and regulations, the recent cases 1 in Sri Lanka have made several suggestions it helps to provide more security to prevent Cyber Crime.

* Inform the society about Cyber Crimes and how to fight against them promotional campaigns and lectures.
* Outdated rules need to be updated regularly. Introducing Defamation Laws.
* Providing proper procedures for obtaining patents and copyrights to protect the rights of the owners Intellectual qualities.
* Inclusion of subjects in the school curriculum based on cybercrime and law for notification students learn how to escape cybercrime.
* The Cyber Crime government should train professionals in cybercrime and cyber law.

**Chapter 6 :- Conclusion.**

Laws assume a major job in forestalling digital assaults in a nation. There are numerous digital dangers in current culture. It is obvious to anybody while experiencing the discoveries of this research. Perhaps we don’t see being a survivor of a digit assault until everything sneaks away from our fingers. Subsequent to investigating the current laws in Sri Lanka against digital fighting. You can see the legitimate activity taken by the public authority to forestall digital wars in Sri Lanka. As proposed above, there are principally existing laws to forestall digital fighting. Recreation to give a superior shield to residents and the country. Digital Attacks and future cyberwars. The public authority ought to do as recently recommended in the event that it is conceivable to bring all the laws identified with network safety. It is a ground-breaking actuality for our country to face digital battle with one activity or the other. From the focuses talked about all through this instructional exercise, we can see that Sri Lankan law is adequate to shield the country from digital fighting. A few weaknesses that could represent a danger to future dangers/open entryways. As the last line of in this dissertation, I propose future research on the topic, ‘What are the laws of Sri Lanka?’, ‘Should data privacy be protected?’.

**Bibliography.**

<https://www.researchgate.net/publication/334712974_Physical_Layer_Security_for_the_Smart_Grid_Vulnerabilities_Threats_and_Countermeasures>

<http://www.dailymirror.lk/opinion/Social-Media-as-a-vector-for-Jihadists--Can-Sri-Lankan-law-combat-terror-in-internet-/172-167692>

<http://apoorwathwayensundarathwayak.blogspot.com/p/blog-page_9554.html?m=1>

Ariyadasa, A., 2019. CAN SRI LANKAN LAW COMBAT TERROR IN INTERNET?. [Online] Available at: https://www.pressreader.com/sri-lanka/daily-mirror-srilanka/20190523/page/14/textview [Accessed 17 12 2019].

Ariyadasa, A., 2019. Computer Crime Legislation in Sri Lanka: Comparative Analysis. [Online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3382666 [Accessed 08 12 2019].

ARIYADASA, A., 2019. Computer Crime Legislation in Sri Lanka: Comparative Analysis. [Online] Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=3382666 [Accessed 17 12 2019].

Ariyadasa, A., 2019. MISLEADING CONSUMERS BY UNFAIR ADVERTISING; COMPETITION LAW IN SRI LANKA (SL).. [Online] Available at: https://poseidon01.ssrn.com/delivery.php?ID=4700021180051030701260201020911040920960750 37082045007068103010085117003006092014029013055021115109098101086094017001080081 02005505803607604808711702910602909111903101801901302109003000912308600908907209 10750701 [Accessed 19 12 2019].

Ariyadasa, A., 2019. Protection of Copyright Owners and Authors Rights in the Internet: A Comparative Analysis of IP Law in Sri Lanka and EU Directives. [Online] Available at: https://poseidon01.ssrn.com/delivery.php?ID=9460991130930651090760761140290260900150220 28045089092075001067099001096109106113127011017012000106100015112100076023123082 07401005001209207209311306610802208502012005405301209912507308911502910106802908 80751230 [Accessed 17 12 2019].

Congressional Research Service, 2018. Electric Grid Cybersecurity. [Online] Available at: https://fas.org/sgp/crs/homesec/R45312.pdf [Accessed 18 12 2019].

Jayasekara, D. & Rupasinghe, W., 2015. Cyber-Crime in Sri Lanka. [Online] Available at: researchgate.net/publication/294725446\_Cyber-Crime\_in\_Sri\_Lanka [Accessed 17 12 2019].

Buono, L., 2014. Fighting cybercrime through prevention, outreach and awareness raising. ERA Forum, , 15(1), pp. 1-8.

Avast Academy Team, 2016. Avast. [Online] Available at: https://www.avast.com/c-cybercrime [Accessed 09 01 2020].

MDIIT Admin, 2019. [Online] Available at: http://www.mdiit.gov.lk/index.php/en/mtdi-news/item/68-data-protectionlegislation [Accessed 11 01 2020].

MDIIT Admin, 2019. [Online] Available at: http://www.mdiit.gov.lk/index.php/en/mtdi-news/item/68-data-protectionlegislation [Accessed 11 01 2020].

<http://www.gov.lk/>

<https://en.wikipedia.org/wiki/IT_law#:~:text=Information%20technology%20law%20(also%20called,information%20security%20and%20electronic%20commerce>.

Rand.org, 2020. Rand Corporation. [Online] Available at: https://www.rand.org/topics/cyber-warfare.html [Accessed 11 01 2020].

Rand.org, 2020. Rand Corporation. [Online] Available at: https://www.rand.org/topics/cyber-warfare.html [Accessed 11 01 2020].

Kaspersky, 2019. Kaspersky. [Online] Available at: https://www.kaspersky.com [Accessed 31 October 2019].

