IN PARTNERSHIP WITH PLYMOUTH UNIVERSITY

Name: Nilma Nuleni Dulyana Gunawardhana Liyanage
Student Reference Number: 10707256

Module Code: PULS2001	Module Name: IT Legislation and Ethics
Coursework Title: Laws in Sri Lanka to prevent cyber-attacks: Analysis of laws in Sri Lanka to prevent cyber-warfare in the future.	
Deadline Date:07 january 2021	Member of staff responsible for coursework: Mrs. Aparajitha Ariyadasa
Programme: BSC. (Hons) in Software Engineering- Batch 08	
Please note that University Academic Regulations are available under Rules and Regulations on the University website 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 : *Gunawardhana*	

Use of translation software: failure to declare that translation software or a similar writin
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

IN PARTNERSHIP WITH PLYMOUTH UNIVERSITY

IT Legislation and Ethics
PUSL2001

Coursework
2020–2021

Laws in Sri Lanka to prevent cyber-attacks:

Analysis of laws in Sri Lanka to prevent cyber-warfare in the future.

Nilma Liyanage

Laws in Sri Lanka to prevent cyber- attacks: Analysis of laws in Sri Lanka to prevent cyber-warfare in the future.

Abstract

Digital dangers are wherever in the internet today. Indeed, even through a spam email, you can be a casualty of a digital assault. In the event that those digital assaults occur in huge scope focusing on a country that is called as digital fighting. This is subjective exploration dependent on a hypothetical premise that examinations the current laws in Sri Lanka identified with digital protection, to see if those laws are adequate to shield the country from digital fighting. Many related assets for example, research papers, diary articles, reports, and Sri Lankan Acts of law have been dissected to accumulate the information needed to full fill the examination issue referenced previously**.**

Chapter 01- Introduction

1.1 Overview

It was a common topic among the researchers on preventing and taking stable strategies regarding the cyber warfare and threats. It is a duty of this experiment to see the Sri Lankan's law is suitable to prevent the cyber warfare. As well people should be aware of the knowledge to protect from the cyber warfare and threats.

1.2 Background

When we searched the history of cyber attacks. We could see cyber attacks have been increasing a among the small and large business ventures. With the development of the technology a rapid increase of cyber attacks can be seen. When we study the recent incidents regarding cyber attacks in Sri Lanka following occasions can be identified.

- On 18 and 19 of may 2019, the following days of Vesak festival 10 local websites with .lk and .com were attacked by a series of cyber attacks.
- As well the Kuwait web site in Sri Lanka was attacked and suffered heavily in 1920.
- Top level domains in Sri Lanka national websites with .gov and .com were faced with cyber attacks.
- As well a leading media website in Sri Lanka was attacked.
- The website of china Embasy and the website of sri Lankan's parliament were attacked. It is believed that this attacks were done by Tamil Elam cyber force.

Nilma Liyanage

1.3 Context

This is definite examination about digital fighting, dissecting the legitimate structure of Sri Lanka and see whether they are adequate to shield the country from digital fighting.

1.4 Definitions

KEY WORDS: CYBER WARFARE, CYBERCRIME, CYBER SECURITY BILL, THE IP ACT NO. 36 OF 2003, THE COMPUTER CRIMES ACT NO. 24 OF 2007.A “Crime”’ is an action or mission which constitutes an offence and is punishable by in Sri Lanka. Criminal offences are typically indicted by the state or the typically indicated by the state or the common health ,though it is ordinarily dependent up on a person to prosecute a common activity. It is likewise feasible for a person to start criminal procedures, yet this is exceptionally uncommon. A few issues, for example, attack, can be the two violations and common wrongs simultaneously. The casualty can make a common move to recuperate cash for any injury endured.

What is Cyber warfare?

Cyber warfare, as its name recommends, alludes to the utilization of the utilization of innovation to assault a country’s PCS or data organizations, making similar mischief real fighting be it harm passing or pulverization. Despite the fact that there are vanishingly couple of instances of genuine world digital fighting, it’s turning into a developing worry for some. Governments are turning out to be progressively mindful that we are currently dependent on PC framework to run everything from monetary administrations to move organizations, and that an assault against these framework could be similarly as harming as conventional military utilizing troops furnished with firearms and rockets.

1.5 Aim and Objectives

The point of this work is principally to investigate, break down and recognize the laws in Sri Lanka and forestall. Digital assaults , digital fighting by making the laws solid. Subsequently, it is important to investigate. The legitimate system in Sri Lanka forestalls digital fighting and its important issue and exhibit the agreement. Also , it is essential to perceive how the Sri Lanka law address. Digital fighting, while at the same time investigating the holes between the laws identified with the subject. Moreover it is important to discover what are the investigates that should be done later on make the country protected from digital fighting.

1.6 Research problem and Research questions

By achieving the above mentioned objectives, this research will be analyzed the research.

- What is a crime? , what is cyber warfare?, what are the existing laws?
- Issues, problems can Sri Lankan law safeguard the nation by preventing the cyber warfare?
- In the Sri Lanka against cyber warfare ? what are the legal actions taken from the government.
- To prevent cyber warfare? How do you prevent cyber warfare and how to make the existing cyber laws more strong to safeguard the nation from cyber warfare?

1.7 Rational for research

The principle purpose behind this subject to be examined in this work is to research, investigate and dissect whether Sri Lankan Law is sufficient to shield the country from digital fighting. There is new, as of late found data did in this examination. Thus, for additional scholastic/ non-scholastic purposes including lawful activities, this work can be utilized adequately and effectively.

1.8 Methodology

This is one of the qualitative researches done by following the subject related legal acts, research articles, journal articles and many other e-resources as well.

Chapter 02- Literature Review

2.1 Cyber Terrorism , Cyber Crimes

"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." (Ariyadasa,2019)

Aparrajitha 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 Crimes Act. So, it is a loophole of the act which is responsible for carrying the legalizations related to computer crimes including cyber terrorism. (Ariyadasa,2019)

Social media, which is a part of the cyberspace also has a dark side and according to the study of Aparrajitha Ariyadasa (2019), cyberbullying, Cyberstalking, addictive use, trolling, online witch hunts, fake news, and privacy abuse can be mentioned as examples. It is 5 | P a g e D i n u k a N a v a r a t n a 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. (Ariyadasa,2019)

Cyber-crime refers to any illegal activity that occurs in the virtual world of cyberspace." The article published by Ms. Dinithi Jayasekara has pointed, cyberharassment and cyber-crimes such as abuse privacy, e-mail harassment, social media fake account usage, intellectual property cases related to the subject, e-banking cases and child pornography cases have been taken for the explanations under cyber-crimes and, the study points out a negative fact as, "But under Sri Lankan law, defamation is not considered a criminal offence and it tantamount to a civil matter". (Jayasekara, 2015)

As it has been described in the 'Cyber Terrorism Research Review' by the The danger of a digital psychological warfare assault ought to accordingly not be downplayed as an arising danger, and therefore, safeguard and reaction capacities ought to be kept up and progressed. Contemporary society, so, is coming to understand that brutal radicalism, yet generally uncommon, is the 'new typical'. In spite of the fact that it could be hard to anticipate every particular occasion, we can be sensibly sure that at some future point, they will happen. (Australian National University Cybercrime Observatory 2017)

2.2 Propagandism

Aparrajitha Ariyadasa (2019) has explained how uncalled for publicizing which goes under the class of propagandism, deludes the shoppers. The investigation shows that propagandism or then again out of line publicizing is being finished by numerous offices or organizations to pick up monetary benefits. This investigation has brought up that there is no applicable law in Sri Lanka to ensure buyers from these sorts of issues. "Sri Lankan assembly doesn't present a legitimate rule to ensure customers., contenders and the overall population against deluding advertising..." (Ariyadasa, 2019)

2.3 Espionage

Aparrajitha 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 cyberwarfare. (Ariyadasa, 2019)

According to the facts describes in the report published by the National state cyber Espionage and its impacts , we can see Quite possibly the most troublesome issues with respect to digital fighting is characterizing digital undercover work. Numerous countries and worldwide bodies have made their own definitions however it has been hard to limit it down to a solitary agreement. Variables like the degree and nature of the harm brought about by the assault, the character of the assaults, and how the taken data is utilized all impact how digital surveillance is seen. One bunch of rules for country state digital fighting, the Tallinn Manual, endeavors to give definitions, systems, and rules administering global digital activities. This manual, distributed in 2013 because of a meeting facilitated by the NATO Cooperative Cyber Defense Center of Excellence in Tallinn, Estonia, characterizes digital secret activities as â€œan act embraced stealthily or under misrepresentations that utilizes digital capacities to assemble (or endeavor to accumulate) data with the aim of conveying it to the contradicting (Dana Rubenstein)

Undercover work, as indicated by Merriam-Webster, is "the act of spying or utilizing spies to get data about the plans and exercises particularly of an unfamiliar government or a contending organization." Bring this into the digital world, and the covert agents are multitudes of loathsome programmers from around the world who use digital fighting for monetary, political, or military addition. These purposely selected and exceptionally esteemed cybercriminals have the specialized ability to close down anything from government frameworks to monetary frameworks or utility assets. They have impacted the result of political races, made destruction at worldwide occasions, and assisted organizations with succeeding or fall flat.

2.3 Surprise Attacks

"In various cases, digital assaults stayed unrecognized for quite a while, frequently to the shock of the person in question." (Koch and Golling, 2019) When examining the examination done by Robert Koch and Mario Golling (2019), we can see that shock assaults, more often than not stay covered up and jumps out of nowhere doing extraordinary mischief. Besides, it has clarified that numerous digital assaults veil the real substance of the assault to delude the security system around the objective. It says the recognition of such assaults is troublesome as the noxious code more often than not explicitly intended for the objective where it can stay covered up inside the objective. (Koch and Golling, 2019) As per the Special Report Series of the Kaspersky Lab (2015), it is demonstrating how the digital assaults, for example, DDoS assaults cover themselves and emerge with shock assaults. " 74% of assaults that lead to a perceptible disturbance of administration concurred with an alternate sort of security occurrence, for example, a malware assault, network interruption or different sorts of assault."

(Kaspersky Lab, 2015)

Susan W. Brenner (2012) has drawn out an incredible case identified with shock assaults, where the wrongdoing was finished utilizing the digital wrongdoing method 'deception assault'. In 2009, $415,989 was extricated from a bank in the USA by crooks outside the nation, utilizing a diversion program named 'Zeus'. The program was subtly introduced into the PC of the Country Financier and through that, the hoodlums have taken the cash. This is an illustration of a shock assault where it influenced the economy and the network protection of the country. (Brenner,2012)

2.5 Electric Power Grid

Electric frameworks are intricate foundations. The electric networks are unmistakably more than creating stations, transformers, high voltage communicating lines lastly the circulation lines which are interface with the purchasers. There is a significant worry about digital protection with the expanded network. Since there is a significant level of availability, an elevated level of security is required (Monteagudo, 2019). The security of the data of the purchasers must be concerned and furthermore it is important to shield the framework from malware and noxious updates.

Chapter 03 - Purpose of methodology

This Research study is done to find answer for three main questions,

- What is Cyberwarfare?
- What is Crime?
- What are Sri Lankan laws?
- Are the Sri Lankan laws sufficient to safeguard the nation from cyberwarfare?

Qualitative methodology was used in the entire research in order to find answers to the above questions.

Used methods: Secondary Sources

- Websites
- Journal Articles
- Blogs
- Books
- Legislations
- Reports
- News Papers
- Youtube Videos
- Articles

Referencing Style: Harvard.

These methods were chosen relating to past researches on cybercrimes, cyberwarfare and cyber law. Analyzations are based on ideas of experts related to cybercrimes and recent case studies connected with cybercrimes and law. The methods used in the research are very simple and easy to understand. Lack of previous researches on cybercrimes was a big issue when collecting information using this methodology.

Chapter 04- Analysis

4.1 Analysis of Computer Crimes ACT No. 24 of 2007

The PC wrongdoing act has been set up to recognize the PC violations and in the event that it occurs, the techniques to be followed including management counteraction and the punishments for the activity. This is pertinent when a law has been penetrated, a PC or related offices has been utilized with the cycle, or a misfortune has been happened to an individual or a state. The punishments incorporate a fine, detainment or both of these activities. As indicated by this law, the accompanying kinds of cybercrimes are fined in the underneath referenced ways. Unapproved admittance to information fines at least 100000 or detainment of at least 5 a long time. Unapproved admittance to submit an offense fines at least 200000 or detainment of at least 5 years. Offenses against the state and public security reasons for a detainment quip under 5 years. Managing unlawfully got information fines 10000-300000 fines with a detainment between a half year to 3 years. As such the activities referenced to be an encroachment of the laws will fine or detain as indicated by the circumstance. Sri Lanka Computer Emergency Readiness Team (CERT) and the Information and Correspondence Technology Agency (ICTA) are incredible forward jumps that arose with this act.

4.2 Analysis of Intellectual Property ACT No.36 of 2003

Licensed innovation. act no.36. of 2003 was ordered for the cycle of enlistment, control what's more, organization of the licensed innovation and defending their responsibility for unique work. It covers the zones like security of patent right of the innovators, assurance of the trademarks a lot, insurance of the exchange plans and coordinated circuits as well as the copyright possession. The mechanical plans, reserve just as the business trademarks has been ensured by the licensed innovation act and it goes about as a wellbeing net for the planners in the ICT business. The protected innovation right is vested for an individual for a time of ten years.

4.3 Electronic exchanges act 19 of 2006

This is an exhibition to see and empower the improvement of arrangements, the creation and exchange of data messages, electronic reports, electronic records and various correspondences in electronic structure in Sri Lanka. The guideline objective of this act are to progress private and worldwide electronic exchange by evading legitimate obstructions and developing real conviction and to convince the use of strong and safe sorts of electronic business.

4.4 Analysis of Cyber Security Bill

The network safety act was ordered with the point of building up the online protection inside the internet and to make moves against the individuals who disregard the morals of PC systems administration and taking care of. As indicated by the network safety act, online protection is a bunch of exercises proposed to make the internet more free from any and all harm. The. fundamental. destinations. of this. act are; to guarantee the compelling and appropriate execution of the Sri Lankan National 12 network protection, To dispose of the dangers to the network protection in a proficient and powerful way, to begin the network protection office of Sri Lanka with the point of giving a more secure and tied down network safety climate to the clients just as to ensure the basic data foundation.

4.5 Cyber Security Bill 2019

This demonstration is containing the significant laws for the usage of the National Cyber Security Technique of the nation and to ensure the basic data framework. Forestalling/ reacting to future network safety dangers proficiently and viably, build up the Cyber Security Agency of Sri Lanka are likewise remembered for this new demonstration, which means this is set to make sure about the country from digital wrongdoings and digital fighting. Yet, in this bill, web-based media issues and both reconnaissance and observing media has not been covered. In any case, this bill conveys data about creating network safety strategies for the public authority, which is a stage taken to stay away from cyberwarfare.

4.6 Evidence (Special Provisions) Act. No.14 of 1995

This demonstration is identified with giving varying media chronicles or data contained in the modernized explanations identified with any considerate/criminal episode. The principle fallback of this demonstration is that it is obsolete, where the innovation is improved a great deal since the days this demonstration was set up. Yet, this demonstration is being used in Sri Lanka when gathering proof identified with a few cases. Indeed, in the Electronic Transactions Act, it has turned-down this demonstration. "Nothing contained in the Evidence (Special Provisions) Act, No. 14 of 1995 will apply to".

Chapter 05- Suggestions and opinions

As I would like to think, the current digital law framework isn't sufficient to have command over the cyberattacks and to forestall a future digital fighting. During past period, the specialists needed to block the Facebook and other online media even to control the individuals from spread of bits of gossip. So it is dubious whether the dependable specialists will have the option to deal with a circumstance like digital fighting in any event, when they neglected to control the network at a minor issue. In my perspective, the best specialists of the ICT field who are having both hypothetical and pragmatic information ought to be accumulated and a sound arrangement of laws and acts ought to be executed by refreshing the current digital laws and acts.

Without a value-based ward, controlling of cybercrimes isn't simple. A solitary person or on the other hand a state can't battle against these sorts of wrongdoings. It is conceivable to forestall the cybercrimes by getting together as nations. With the end goal of harmonization of cybercrimes, the Worldwide collaboration can be actualized. The predominant general set of laws in the nation have to be change to confront these issues in a transnational level with the assistance of different purviews. The foundation of rules and guidelines under Cyber Crime Act is in a very lower level in the nation. ICT Agency of Sri Lanka ought to recognize and initiate projects to create limit in the Police Department so that Police staff would be exceptional to research PC violations.

Human Resource of an association ought to be prepared every now and then to bring issues to light about the most recent assaulting technique. Lead normal danger appraisals and characterize weaknesses. Associations should now be data security cognizant and should create and actualize legitimate security controls based on the aftereffects of their interior danger appraisal and weakness evaluation.

Chapter 06 – Conclusion

In spite of the fact that there are some digital laws to control the digital fighting, there are a few restrictions inside the current structure. The accessible demonstrations must be altered further in a manner that suits the present status of the innovation. The degree of comprehension of the general population with respect to this issue is additionally not in a good level. The practicability of the current laws, guidelines and acts ought to be more dependable. Appropriately it very well may be presumed that the existing digital laws are not sufficient to forestall a digital fighting in future.

Chapter 07- Bibliography

Bibliography

Anon., 2017 april 17. THE EVOLUTION OF ONLINE TERRORIST PROPAGANDA. p. 3.

Anon., 2019 oct 04. *what translatio troubles can tell us about russian information warfare,* s.l.: s.n.

Anon., 2019 oct 09. *The emerging risk of virtual societal warfare,* s.l.: s.n.

Anon., n.d. *cyber terrorism is sri lanka readt?,* s.l.: 2020.

Ariyadasa, A., 2019 june 30. ISIS, Vitual terrorist propergandism and Sri Lanka. *Lanka Electricity Company(PVT) Ltd.*

Ariyadasa, A., 2019 may 23. Can Sri Lanka law combat terror in interent?. *Daily Mirror(Sri Lanka).*

Ariyadasa, A., 2019 may 25. Social media as a vector for jihadists can Sri Lankan law combat terror in internet?. *Daily Mirror(Sri Lanka).*

cavelty, M. d., 2012 may 9. *Cyber sercurity,* s.l.: 2012 may 11.

jurcut, G. M. &. A. D., 2020 . Insider threats in cyber security the enemy within the gates. february.

Lewis, J. A., 2013. The economic impact of cybersecurity and cyber espianage. 22 july.

Roderic broadhurst, H. w. s. D. M. ,. S., 2017. cyber terrorism. 12 june, p. 129.

Rubenstein, D., n.d. Nation state cyber espionage and its impacts.

Rukmaldeniya, K., 2020 january. *laws in sri lanka to prevent cyber attacks and an investigation on the capacity of these laws to prevent a cyber warfare in future,* s.l.: s.n.

Samuel zilincik, M. m. &. P. K., 2018 . Cyber power and control a perspective from strategic theory. 15 octomber, p. 301.

singh, V., 2020 january 06. *Introduction to digital security laws in sri lanka,* s.l.: s.n.

University, C. w. (. M., 2014 August. *Cyber threats to Critical Information Infrastructure,* s.l.: Landon springer swansea university.

yasas, R., 2020 january 10. *laws in sri lanka to prevent cyber attacks and an investigation on the capacity of these laws to prevent a cyber warfare in future,* s.l.: s.n.