Cyber Crimes within Social Networks and Efficacy of Domestic Legislations to Combat against Them

Dilshani Yapa

[1]*Faculty of Law, General Sir John Kotelawala Defence University, Sri Lanka*
dilshaniyapa@yahoo.com

Abstract - *As every coin has its two sides, Internet, also contains positives and negatives both. But for all the good it does to us, internet has its dark sides too. Out of all the newest and possibly the most convoluted trouble in the cyber world is Cyber-crime. Cybercrime is an umbrella term that covers a wide array of attacks and scams. Cyber-crime generally refers to criminal activity where a computer or network is the source, tool, target, or place of a crime. In recent times most of the above bizarre crimes are committed via Social Networks. For instance, Face book impersonation, Face book pornography, Blackmailing on Facebook, Hacking of passwords & stealing of information are some of them.*

In the domestic scenario throughout the last few years Sri Lanka has been experiencing relatively high rate of cyber-crimes supervised under Face book and other social networks. This situation has endangered the social life of the general public, adversely affect to the life of individuals and ultimately tarnish the image of the country. In order to mitigate there are several legislations passed by parliament recently the problem remains whether they are functioning effectively and whether the general public is aware of the existing laws. Sri Lanka is having a high risk in near future in this regard and for the time being this threat has not been a complicated one. But with the availability of resources and with the developing technology over time, there is a potential of being. But our government comparatively or totally hasn't acted in an effective manner to mitigate these risks. This paper is completely focused on cyber crime issue, trends and problem faced by International and Sri Lankan users and how cybercrimes can be minimized by formulating effective cyber crime laws in Sri Lanka and how it happened in other countries. The paper also includes Sri Lankan cybercrime Statistics and much latest news. In order to compare the situation in Sri Lanka with other countries this study further engages with selected jurisdictions of India, USA and China.

Keywords- Cyber Crimes, Social Networks, Domestic Legislations

I. INTRODUCTION

Almost everyone believes that technology has made life easier and more comfortable. Thus it has enabled us to perform tasks that we could not do otherwise. In the current time people can't imagine their life without technology. Emergence of computer is one of the most important reasons for the revolution of modern technology .Today computers have come a long way, with neural networks and nano-computing promising to turn every atom in a glass of water into a computer, capable of performing a Billion operations per second. Starting from the abacus, this is thought to be the earliest form of a computer, the era of modern computers, went until the analytical engine of Charles Babbage. Computer was earlier purely used for the good side. But currently people use computer for the bad side as well. Cyber crime is one such instance which is an evil, having its origin in the growing dependence on computers in modern life. These cyber crimes have assumed sinister implications since everything now is running on computers.

II. A CRIME

So often we experience an advance in technology that is so radical. It does not only change the way that societies interact, it also has a fundamental effect on the behavior of the criminal element within that society. Thus cybercrime has been the most recent radical change in criminal behavior. The term crime can be defined simply as "a positive or a negative act (Commission or an

omission) in violation of a Penal Law ". The Sri Lankan Penal Code has used the term "offence" to define such acts and omissions[7]. This definition extends to all offences under the Penal Code and other offences created by other acts of parliament.

III. A CYBER CRIME

A commonly accepted definition of this term is that a cybercrime is a "crime committed using a computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs" .New World Encyclopedia defines it as " a term used broadly to describe activity in which computers or computer networks are the tool, target, or place of criminal activity. These categories are not exclusive and many activities can be characterized as falling in one or more categories."[8] Though there are many different definitions of cybercrime they all have a few key concepts common. These key concepts are criminal activity and the use or abuse of computers. With these concepts in mind cyber crime can be easily defined as using a computer to commit a criminal act.

IV. A SOCIAL NETWORK

Simply it is a network consists of social interactions and personal relationships among people who, share interests, activities, backgrounds or real-life connections. It consists of a representation of each user (often a profile), his social links, and a variety of additional services. Most social network services are web-based and provide means for users to interact over the Internet, such as e-mail and instant messaging. Social network sites are varied and they incorporate new information and communication tools. Social networking sites allow users to share ideas, pictures, posts, activities, events, interests with people in their network. Popular methods now combine many of these, with American-based services such as Facebook, Google+, YouTube, LinkedIn, Instagram, Pinterest, Tumblr and Twitter widely used worldwide.

V. INTERNATIONAL CYBER-CRIMES DONE THROUGH SOCIAL NETWORKS

With the rapid diffusion of technology the number of crimes has increased dramatically. There's no doubt that Facebook which is the widest used social network has completely revolutionized the way people interact. But there's a dark side too. Criminals are finding new ways to utilize Facebook to commit new and disturbing crimes that authorities don't necessarily know how to police. That's why if someone wants to continue to enjoy social media, he should be aware of the common crimes committed on Facebook so that he can avoid becoming a victim. Most of the crimes fall under social bullying, defaming exercise and black mailing on face book. Following are some true incidents on this regard.

- Amanda Michelle Todd committed suicide at the age of 15 at her home in Port Coquitlam, British Columbia, Canada. Todd being blackmailed into exposing her breasts via webcam; bullied; and physically assaulted. The Royal Canadian Mounted Police and British Columbia Coroners Service launched investigations into the suicide. At the time of her death, Todd was a grade 10 student at CABE Secondary in Coquitlam.In response to the death, Christy Clark, the Premier of British Columbia, made an online statement of condolence and suggested a national discussion on criminalizing cyber bullying.
- Case of a New Jersey woman, Dana Thornton who could potentially face up to 18 months in prison for creating a fake Facebook profile for her ex-boyfriend to post pictures that intentionally defame his reputation.

- 23-year-old Nigerian Afolakemi Mojisola Adeniyi. She posted a picture of his ex-husband on Facebook and tagged him as a member of the Boko Haram, a violent jihadist terrorist group in Nigeria.

- In Staffordshire, a school bus driver used Facebook to attempt to groom a 14-year-old boy.

[7] Section 38 (1) of the Penal Code
[8] www.newworldencyclopedia.org/entry/Cybercrime

- A jilted boyfriend posted a naked picture of his former girlfriend, who was 17, on the site.

- In India Meghna Naidu too became the victim of cyber hack and she complained to the crime branch claiming her email account was hacked. The hacker allegedly tried to malign her by telling her friends on chat that she was pregnant and abused three other actors.

VI. LOCAL CYBER-CRIMES DONE THROUGH SOCIAL NETWORKS - THE SRI LANKAN EXPERIENCE

Sri Lanka too now has become a victim of the trend of cybercrimes done through social networks. There is a drastic increase regarding complaints on cybercrimes as reports reveal. As Chief Executive Officer of Sri Lanka Computer Emergency Readiness Team Coordination Centre (CERT CC) says "there were only about 200 complaints annually at the beginning of the Sri Lanka CERT CC. With the increase of Cybercrime related incidents, we have been receiving more and more complaints today. Now we receive about 2,000 complaints annually and about 200 complaints monthly. Most of the present complaints we receive are related to privacy breaching and hackings in Social Media Networks like Facebook"

Much reported cases were regarding face book bullying as done in international cases above, finally leading the victims lose their lives. At the same time face book black mailing through fake accounts. Also exercising defaming for the popular personalities now have become a common practice under cyber-crimes in Sri Lanka.

VII. ENACTMENT OF DOMESTIC LAWS REGARDING CYBER-CRIMES IN SRI LANKA

In Sri Lanka there is no any difference between domestic law and the international law regarding cyber-terrorism. However a computer crimes bill or a data protection act was not available in Sri Lanka until 2007.In 2007 the computer crime act was passed but we are still without a data protection law. A common problem that has been faced by many investigators and the prosecutors in almost every case relating to computer related crime is the absence of a specific law governing the area. As at today only piece of legislation in Sri Lanka which deals with some aspects of legislation in Sri Lanka which deals with some aspects of Information Technology is the evidence (special provision) Act, No 14 of 1995.

Computer Crimes Act (No. 24 of 2007) this is an act to provide for the identification of computer crime and to provide the procedure for the investigation and prevention of such crimes; and to provide for matters connected there with and incidental. The Sri Lankan Computer Crimes Act No. 24 of 2007 primarily addresses computer-related crimes and hacking offences. Content related offences are being addressed through a series of changes to the Penal Code and other statutory provisions. Sri Lankan Computer Crime act is content with 38 chapters. All those rules and regulation are discussed in the Computer Crime Act. Also by enacting the Computer Crimes Act No. 24of 2007, modeled on the Budapest Cyber Crime Convention and establishing Sri Lanka CERT as the National Centre to mitigate cyber threats and incidents at a national level the government has taken many policy initiatives to address this problem

The Sri Lanka Computer Emergency Readiness Team Coordination Centre (Sri Lanka CERT CC) established in 2007 to protect the country's information infrastructure and coordinate protective measures against cyber security, cyber threats and hacking. Sri Lanka CERT CC interacts with the Cybercrime divisions at the Police Department, Crime Investigation Department (CID) in Colombo and Moratuwa universities to combat cyber-crimes.

Microsoft Sri Lanka also works towards strengthening the capacity of law enforcement bodies when combating cyber crime. It is committed to increase its contributions to counter cyber crime by promoting the benefits of 'Clean IT' and healthy IT business practices around Software Asset Management (SAM), in partnership with IT stakeholders and government.

The special unit established at the Criminal Investigations Department (CID) to look into cybercrimes and Internet Crime Complaint Centre (IC3) which has been established at Police Headquarters with the collaboration of Criminal Investigation Department & Information

Technology Division to receive and investigate regarding criminal complaints in the rapidly expanding arena of cyber crime are other steps how SL government react.

VIII. ENACTMENT OF INTERNATIONAL LAWS REGARDING CYBER CRIMES – OTHER JURISDICTIONS

USA - along with its Cybercrime bill required authorities to investigate and prosecute individuals for internet-related crimes such as fraud, hacking and cyber-sex .Also this Act would expand the US Penal Code Title 18, Chapter 47, Section 1030, on Fraud and related activity in connection with computers. Also a Bill titled "Fostering a Global Response to Cyber Attacks Act" was introduced in the US Senate on July 10.2009.On the other hand, any person found guilty of cyber-squatting shall be punished with imprisonment of prison mayor or a fine of not more than P500,000 (or both); any person found guilty of unsolicited commercial communication with arrest mayor (imprisonment from one month to six months) or a fine of at least P50,000 but not more than P250,000 (or both); and any person found guilty of cybersex with imprisonment of prison mayor or a fine of at least P200,000 but not more than P1 million (or both).Meanwhile, any person found guilty of child pornography shall be punished according to Republic Act 9775 or the Anti-Child Pornography Act of 2009.Those who aid in the commission of any of the acts listed shall likewise be punished with imprisonment one degree lower than that of the main perpetrator of the offense or a penalty of at least P100,000 but not more than P500,000, or both depending on the court. Cyber law is also monitored and enforced by the United States Federal Bureau of Investigation - FBI Cyber Crime Division

INDIA-Information Technology (Amendment) Act 2008.This has been notified and enforced on 27th Oct, 2009.And this Act punishes various cyber-crimes including Cyber Terrorism.

CHINA- In 1994, the State Council issued the first law on computer crime, which is an Ordinance on protecting the safety of computer system. In 1997, 2000, 2009 China Criminal Law was amended to increase new Cybercrimes, in 2011 China Supreme People's Court and Supreme People's Procuratorate issued the judicial interpretation on Cybercrime. However China Criminal Procedure Law responses to Cybercrime slowly, now there is no rules on collecting electronic evidence or admissibility rules relating to electronic evidence, until 2011 Draft of amendments to China Criminal Procedure Law began to stipulate technical detection measures that include electronic surveillance. But China judicial practice already goes ahead of criminal procedure law, China Supreme People's Court and Supreme People's Procuratorate issued several judicial interpretations on electronic evidence. In the field of international judicial cooperation, there is no agreement between China and foreign countries on cooperation on combating Cybercrime, China does not join any international convention or treaty on Cybercrime also. The Chinese Defense Ministry confirmed the existence of an online defense unit in May 2011. Composed of about thirty elite internet specialists, the so-called "Cyber Blue Team," or "Blue Army," is officially claimed to be engaged in cyber-defense operations, though there are fears the unit has been used to penetrate secure online systems of foreign governments

IX. JURISDICTION DIFFERENCE

In Sri Lanka we can see that there is no any act or legislation which related to cyber-terrorism. But in Computer Crimes Act (No. 24 of 2007) it is mentioned some strong points, but in the act it is not mentioned clearly and we have to interpret it as we want. If any person did any cyber terrorism activity the punishment will be Rs. 50 000 or Rs. 100 000 or imprisonment. But this legislation does not specifically cover Cyber Crimes to meet the global standards where as India ,USA and China legislation have mostly addressed the Cyber Crimes issue. The Computer Crime Act of Sri Lanka deals primarily with computer related crimes and hacking offences. The Act does not deal with content related offences such as pornography and harassment perpetrated via ICT tools. So that it reflects the fact that Sri Lanka lacks sufficient laws to protect women and girls from cyber related violence and abuse. The 2006 UN Secretary General report on all forms of violence against women and girls recognized new forms of violence against women that have developed with the advent of the new information and communication technologies (ICTs). Incidents of ICT related violence against women and girls are also on the

rise in Sri Lanka. Women and girls therefore should take precautions when uploading pictures onto the internet for example via social networking sites, email or when sharing personal information via the internet. According to the Police Spokesperson SSP Ajith Rohana out of the 30 complaints received by the police last year, most of the cyber-crimes were committed from abroad and That does not fall under the jurisdiction of the Sri Lanka Police. While Sri Lanka does not have specific laws to deal with internet crimes, this act cannot be used to address crimes committed over the internet but it can be connected with some of the crimes to the criminal law and take action. However, though complaints have increased, prosecution and conviction of offenders appears to be minimal. Sri Lankan laws are apt to curb cyber-crimes, however, the prosecution process is lengthy which causes delays in reaching the end result.

Further in detail considering about the legislations which are available, very much important to highlight the Cyber Crime Bill passed by the senate. According to that Bill it required authorities to investigate and prosecute individuals for internet-related crimes such as fraud, hacking and cyber-sex. And also White House draft this Bill and it would expand the US Penal Code Title 18, Chapter 47, Section 1030, on Fraud and related activity in connection with computers. Also the Bill have proposals for cybercrime, including a series of criminal offences for cyber-attacks and confidentiality abuses. The Bill has also details on critical information security. And the important issue is highlighted from the section 06 of the Cyber Attacks Act. Apart from that there is a separate computer crime and intellectual property section function under authority of United States Department of Justice. Implementing the Department's national strategies in combating computer and intellectual property crimes worldwide is the responsibility of this section. This section has many roles. It prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts. A person using the internet in the United States could be subject to the cyber laws not only in the United States but also in other countries. This all depends on what the person in the United States is doing on the internet in relation to other countries. This is known as jurisdiction and entails the following: i. The laws of the state/nation in which the user resides ii. The laws of the state/nation that apply where the server hosting the transaction is located iii. The laws of the state/nation which apply to the person or business with whom the transaction takes place. Under the measure, any person found guilty of the acts in A and B shall be punished with imprisonment of prison mayor (imprisonment from six to 12 years) or a fine of at least P200,000 or an amount depending on the damage caused or both depending on the court. Meanwhile, any person found guilty of child pornography shall be punished according to Republic Act 9775 or the Anti-Child Pornography Act of 2009

Also china's attempt to defense cybercrimes by Blue Army which is a specialized online unit provide easy access for the general public to secure themselves from cyber warfare is appreciated. In India to solve cyber crime cases, Indian police developed cybercrime investigation cells all over India other than its statute. These Cyber Crime cell investigates in respect of cases pertaining to hacking, spread of virus, pornography, manipulation of accounts, alteration of data, software piracy, creation of false Web sites, printing of counterfeit currency, forged visas, theft of intellectual property, email spamming, denial of access, password theft, crimes with cell phones and palmtops, cyber terrorism etc.

X. KEY FINDINGS

Facebook and all the other social websites like twitter , flicker, Google+ now have become a favourite meeting place for people to keep in touch with friends on-line. As a result, millions of people (both young and old) are using them, so much so that if some one is not on using either one of them it's like he or she doesn't belong to the modern tech-savvy society. Sri Lankans most famous social web site is face book. According to Sri Lankan Facebook Statistics issued by social bakers, in 2013 May there are more than 1.5 million (1526360 users) Monthly Active Users (MAU) in Sri Lanka. Facebook users grew by more than 78200 in the last 6 months. According to their statistics, Facebook penetration in Sri Lanka is 7.09% compared to the country's population and 60.98% in relation to number of Internet users. More over Sri Lanka Facebook demographics the largest age group is currently 18-24 with total of 642 360 users, followed by the users in the age of

25-34. 68% of these users are male and 32% are female users(http://studentlanka.com/2014/04/30/facebook-users-in-sri-lanka) So that this proves the life blood of the new generation is internet. Day by day the use of internet is eating in to the lives of youth. Such a rapid growth in the use of internet inevitably brings in the growth of cybercrime activities. Cybercrime, in most cases, is not the stereotypical kid in some darkroom hacking away trying to get rich; these days, cybercrime is a well-organized, structured entity- almost like a company.

XI. PROPOSALS

The number, sophistication and impact of cybercrimes continue to grow and pose a serious and evolving threat to local individuals, businesses and governments today. This has gained tremendous attention nowadays due to the increasingly high amount of coverage being given to the subject by the media and various institutions especially those from the public and private sectors. The lack of implementation of already enacted policies and regulations which is being put up to regulate the illegal activities in cyberspace and the mitigate the misconducts is the major reason for Cyber-crimes in Sri Lanka to be a most effecting reason. Although, measures have been taken continuously to introduce necessary legislations, it is still below the standard of some Asia-Pacific countries. The matter is however there is a law regarding the combat of cyber-crimes in Sri Lanka, but many people don't know about the law or other security measures that exist. So that following steps can be proposed to improve this current situation.

The present public awareness programs regarding this area are not enough to educate the general population as most of them are being conducted targeting on organizations. So that creating more awareness amongst corporates on cyber security risks and how to mitigate those perils is a contemporary requirement.

Centralized bodies such as Sri Lanka CERT, Law Enforcement Agencies and the Legislature should focus on areas where it has particular competence, such as protecting critical infrastructure and coordinating legal structures, as well as regulating and working with business, consumer protection privacy, and anti-terrorism. Even though SLCERT is the national face of cyber security their contribution to the awareness programs is very low. The awareness programs should be attractive to the general public in a manner which would educate the public without any effort. They should be in a sense of a brand promotion campaign and Television advertisements should be telecasted at peak hours of usage. Further they should announce the people that they (SLCERT) were in contact with Facebook. So that all affected parties to can report abusive speech or comments on photographs directly to Facebook as well. According to their findings one of the main issues on Facebook's late reaction was the lack of understanding of the language since Some comments are either in Sinhala or transliterated, so the CERT, can educate them (Face Book) as to the content of the comments prior to them taking action.

Also Creating awareness on the importance of Cyber Security and to provide top officers in the government, private sector leaders and IT professionals, with the best practices in acquiring, implementing, managing and measuring information security postures of their organizations and countermeasures is required.

Supplementing the current intelligence picture of cybercrime and informing policy and operational responses to cybercrime by providing centralized aggregated data on cybercrime in Sri Lanka and improve understanding of its scope and total cost. This includes Streamline the process of referring cybercrime reports between law enforcement and other relevant government agencies directing cybercrime reports to the most appropriate agency, and provide a centralized point for advice on avoiding cybercrime. This would help in order to reduce confusion around how to report cybercrime. This gives lack of clarity victims about how and where different types of cybercrime should be reported

Develop capacity in the Police Department more so that Police personnel would be well equipped to investigate computer crime. The development of digital forensic labs and the setting up of the Computer Crimes Unit can also be implemented. Currently Internet Crime Complaint Centre (IC3) has been established at Police Headquarters with the collaboration of Criminal Investigation

Department & Information Technology Division to receive and investigate regarding criminal complaints in the rapidly expanding arena of cyber crime.

Also newly introduced programs like Computer Hacking Forensic Investigation (C|HFI) training programs using latest version released by the International Association of Electronic Commerce Consultants (EC-Council), USA should be expanded and can use to inculcate the public.

Also the need of proper investigation methodologies, proper set of investigation rules and regulations regarding the cyber based crimes are essential since speedy expansion of electronic and telecommunication equipment provide a good platform to the criminals to perform the offences without keeping physical evidences to examine and carry out the investigation process for the relevant crime.

The nation's cyber activities need to be coordinated on both the institutional, district and provincial levels as a responsibility of the government to ensure that national networks are secure and have not been penetrated. In order to take the message to the people that cyber security is compatible with individual rights, privacy and freedom of speech ,the national security policy would need to be extended to include a cyber security agenda that covers the length and breadth of the country.

Establish Public Private Partnerships is essential for governments to cooperate with the private sector, as the majority of web infrastructure is in private hands. All developed nations have identified this and are working closely with the private sector, and the private sector in return should reciprocate equally.

Educating the community to protect themselves - As with crime in the physical world, no amount of action by governments and the private sector can prevent every cybercrime. Those of us who use digital technologies have to take responsibility for our own security and safety online and exercise safe online practices. Governments and industry can assist users to understand these steps and to recognize the warning signs. Partnering with industry to tackle the shared problem of cybercrime is important in this regard.

Improving international engagement on cybercrime and contributing to global efforts to combat cybercrime; The interconnectivity of the internet means that Our agencies can face significant challenges in bringing cyber criminals in other countries to justice. Cybercrime is an international problem which requires a coordinated and cooperative international response. Differences in national laws and the capacity of local agencies to enforce those laws can create a barrier to effective international cooperation on cybercrime. We can improve this situation by encouraging as many countries as possible to strengthen and harmonize their domestic legislation on cybercrime and supporting them to build enforcement capacity.

Ensuring an effective criminal justice framework - criminal justice system must provide an effective framework for investigation and prosecution of cybercrime. This means that offences must account for the use of new and emerging technologies to commit crime; penalties must provide adequate deterrent and reflect the seriousness of different types of cybercrime. Procedural and evidentiary rules need to account for new forms of evidence and prosecutors and judicial officers must be well equipped to consider digital evidence. In addition to facilitating the investigation and prosecution of criminal conduct, the criminal law also plays an important normative role in shaping society's acceptance or non-acceptance of different forms of behavior. For this reason also, criminal laws need to continue to reflect society's views by appropriately criminalizing malicious online conduct and provide mechanisms for its punishment.

Assisting prosecutors and the judiciary to deal with cybercrime and digital evidence; Prosecution of cybercrime offences is an important part of the enforcement framework to deal with cybercrime and assists in creating and maintaining public confidence in our criminal justice system. In order for cybercrime offences to be prosecuted effectively, prosecutors and judicial officers need to be able to understand and evaluate technical digital evidence. While courts and the legal profession are becoming more accustomed to the use of new technology to commit crime, the admission of digital evidence can still be a technical process. As the use of technology in crime grows, prosecutors and judges will

increasingly be required to present and understand highly technical details in order to effectively administer the law. Governments can continue to assist prosecutors and the judiciary by providing the resources they need to respond to legal concepts associated with new technology and the facilities they need to analyse and consider digital evidence in a court setting. Providing training workshops for the legal community and developing mechanisms to improve the presentation of digital evidence in courts, particularly through the development of the eCourt facility would be innovative. Though this digital evidence matter is now in usage of Sri Lankan law the e court facility has not yet tried out.The e-Courts project was conceptualized on the basis of the "National Policy and Action Plan for Implementation of information and communication technology (ICT) in the Indian Judiciary – 2005.

XII. CONCLUSION

However it is obvious that above points stresses the fact that the existing legislation and litigation of Sri Lanka is not merely sufficient to overcome these ever increasing crimes while the prevailing ones are unknown to the society and further new security measures in addition to the existing ones to override the hackers and strengthen the computer systems from possible cyber-attacks in order to ensure the safety of the society should be implemented. There is no doubt that the impact of Face Book and other social media towards human lives is unavoidable phenomena. So standardizing and regulating the usage of them is essential in Sri Lanka. It is not clear yet that the jurisdiction regarding Face Book because even the company (Face Book) exercising minimum level of control over its users. In majority instances victims have no relief other than reporting to the company. The procedure of imposing criminal or delictual liability over the real perpetrators is not clearly defined yet and without the assistance of the company it is not achievable. So I think a precise mutual agreement between states and the company is the most appropriate mean. Recently state of India Asked Google Earth to delete the satellite images of Indian military bases and war ships from the particular application and company agreed on that. As the natives of the global village each of us acquire many more benefits from social media and we used to depend on them. It is essential to protect once liberty and freedom on the social media though no one should infringe others freedom.

REFERENCES

Fernando J. Cyber Crimes Legislation – Sri Lankan Update <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079if09pres-SriLanka_Jayantha.pdf > Accessed 9 August 2014

Cyber security , an Analysis of State Security in Sri Lanka http://www.slideee.com/slide/cyber-security- an-analysis-of-state-security-in-sri-lanka

Keerthisinghe, L. (2014) Prevention Of Cyber Crime In Sri Lanka .The Sunday Leader

(2014) Microsoft Sri Lanka partners with IT stakeholders on clean IT & cybersecurity:Colombo Gazatte.Review. [Online] Available from: http://colombogazette.com/2014/02/22/micr osoft-sri-lanka-partners-with-it-stakeholders- on-clean-it-cybersecurity/ [Accessed: 8 August 2014]

CyberSecurity, http://www.gov.lk/web/index.php?option=com_content&view=article&id=252&Itemid=273 &lang=en Aseef N. Cyber-Criminal Activity and Analysis < http://courses.cs.washington.edu/courses/csep590/05au/whitepaper_turnin/team2-whitepaper.pdf > Accessed 7 August 2014

Marcus D. Prospective Analysis on Trends in Cybercrime from 2011 to 2020 < http://www.mcafee.com/nl/resources/white-papers/wp-trends-in-cybercrime-2011-2020.pdf > Accessed 9 August 2014

Jaishankar, K., (2007). Establishing a Theory of Cyber Crimes. International Journal of Cyber Criminology, Volume 1, pp. 7-9.

Senevirathne A.(2013) Minimizing the impact of Cybercrime. Daily News

BIOGRAPHY OF AUTHOR

[1]Author is a 2nd year student at Faculty of Law, KDU. She is currently an active member of the KDU moot court & debating society. She has an interest in research under the theme of Cyber Crimes within Social Networks and Efficacy of Domestic Legislations to Combat against Them. This is her first research and KDU International Research Conference was her first attempt. Her Interest areas are Computer Law, Human Rights Law and Intellectual Property Law.