Journal of US-China Public Administration, October 2015, Vol. 12, No. 10, 759-763
doi: 10.17265/1548-6591/2015.10.003

Cyber-Crime in Sri Lanka

A. H. Dinithi Jayasekara, Wijayananda Rupasinghe
University of Kelaniya, Kelaniya, Sri Lanka

New media is a term meant to encompass the emergence of digital, computerized, or networked information and communication technologies in the later part of the 20th century. Most technologies described as “new media” are digital, often having characteristics of being manipulated, networkable, dense, compressible, interactive, and impartial. The internet is known as a kind of global meeting place where people from all parts of the world can come together and share information. According to Henson, Reyns, and Fisher, they define “Cyber-crime refers to any illegal activity that occurs in the virtual world of cyberspace”. This research studied the Sri Lankan cyber-crime and legal background about cyber-crime. In this research, it studied selected cases relating to cyber-crime in Sri Lanka. The authors examined the situation, evidence. In Sri Lanka, there have been four main acts which used in prevention of cyber-crime. Content analyzed these acts. In Sri Lanka, there is a challenge in preventing cyber-crimes. The growth of network-based crime has raised difficult issue in respect of appropriate balance between the needs of those investigating and prosecuting such crime, and the rights of users of such networks. Increasing the awareness about new media literacy is one way to minimize cyber-crime. Also, Sri Lankan legal system needs to be modified.

Keywords: cyber space, cyber-crime, internet, new media, law

The advancement of technology such as the internet has provided individuals and organizations with a means to both commit new types of crimes and adopt new methods of committing traditional street crimes. From online identity theft to cyber-stalking to viruses, millions of people worldwide are affected by online deviant behavior every day.

The origins of the internet can be traced back well over several decades to the early 1960s. Originally developed for military and educational applications, interlinked computer networks were designed to allow individuals and working groups to store and share information quickly and efficiently. The internet is based on single technical standards that allow global communication. This has the advantage of allowing the globalization of internet services (such as Facebook, Google, Yahoo, and others) that are operated in one country but can be accessed by users from all over the world. The internet has become important for daily life, education, work, and participation in society. A large majority of households and individuals make use of it today. Internet usage increased gradually all over the world. In 2000, 360,985,492 people used internet. At that time, 1,386,188,112 people in Asia used internet. In 2014, those values increased a lot. Currently, an estimated

Corresponding author: A. H. Dinithi Jayasekara, Master of Social Sciences in Mass Communication (MSSc), lecturer, Department of Mass Communication, University of Kelaniya, Kelaniya, Sri Lanka; research fields: media law, new media, and media impact. E-mail: dinithiuk85@gmail.com.

Wijayananda Rupasinghe, Master of Philosophy in Mass Communication (MPhil), senior lecturer, Department of Mass Communication, University of Kelaniya, Kelaniya, Sri Lanka; research fields: media policy, political communication, and media history. E-mail: wijeuk@yahoo.com.

3,035,749,340 people connected to the internet[1]. And its penetration was 42.3%. The technology has advanced so fast and has be more and more user-friendly; at the same time, people around the world have become more and more sophisticated in the use of technology.

Internet crime is quickly becoming one of the biggest and most threatening problems for both law enforcement and the public at large. “The computer is rapidly increasing society’s dependence upon it, with the result that society becomes progressively more vulnerable to computer malfunction, whether accidental or deliberately induced, and to computer manipulation and white-color law-breaking” (Weeramantry, 1998, p. 259). With the emerging use of computer technology, computer-related crime and cyber-crime have become a significant global challenge.

There are many definitions to cyber-crime. According to Henson, Reyns, and Fisher (2011), they defined “Cyber-crime refers to any illegal activity that occurs in the virtual world of cyberspace” (Henson, Reyns, & Fisher, 2011).

Gordon and Ford (2006) formulated an even more generic typology. Their typology includes any crime that is “facilitated or committed using a computer, network, or hardware device” (Gordon & Ford, 2006).

Most reports, guides, or publications on cyber-crime begin by defining the terms “computer crime” and “cyber-crime”. In this context, various approaches have been adopted in recent decades to develop a precise definition for both terms. Before providing an overview of the debate and evaluating the approaches, it is useful to determine the relationship between “cyber-crime” and “computer-related crime”. Without going into detail at this stage, the term “cyber-crime” is narrower than computer-related crimes as it has to involve a computer network. Computer-related crimes cover even those offences that bear no relation to a network, but only affect stand-alone computer systems.

From January 1, 2009 through December 31, 2009, the Internet Crime Complaint Center (IC3) website received 336,655 complaint submissions. This was a 22.3% increase as compared with 2008 when 275,284 complaints were received (*IC3 2009 Annual Report on Internet Crime Released*, n.d.). The costs of cyber-crime are difficult to measure, but by any reasonable standard, they are substantial and growing exponentially.

Threat posed by cyber-crime, including terrorism, but little has been done to protect against what has become the most costly form of such crime: transnational attacks on computers and the information infrastructure. Measures thus far adopted by the private and public sectors fail to provide an adequate level of security against these attacks. The internet and other aspects of the information infrastructure are inherently transnational. Transnational response sufficient to meet these transnational challenges is an immediate and compelling necessity.

The Convention on Cyber-crime is an international treaty that seeks to harmonize national laws on cyber-crime, improve national capabilities for investigating such crime, and increase cooperation on investigations.

Cyber-crime and cybersecurity are issues that can hardly be separated in an interconnected environment. The fact that the 2010 UN General Assembly Resolution on cybersecurity addresses cyber-crime as one major challenge underlines this (UNGA Resolution: Creation of a Global Culture of Cybersecurity and Taking Stock of National Efforts to Protect Critical Information Infrastructure, A/RES/64/211).

[1] Retrieved from http://www.worldstats.com.

Conceptual Framework

Communication Power by Manual Castells (2009) focuses on the role of communication networks in power-making in society, with an emphasis on political power making. Power in the network society is exercised through networks. Power relationships are the foundation of society, as institutions and norms are constructed to fulfill the interests and values of those in power. Each type of society has a specific form of exercising power and counter power. It should not surprise us that in the network society, social power is primarily exercised by and through networks.

According to Castells, he introduced concept "mass self-communication" in this book. This is mass communication because it can potentially reach a global audience and he refers to posting a video on YouTube, issuing a blog with RSS links and sending a message to a massive e-mail list. It is self-communication because the production of the message is self-generated, self-directed, and self-selected. This concept refers to important new forms of communication produced by digital media that should be located between interpersonal and traditional mass communication.

At that time, his view was that with networks we have created a machine that is dynamic, full of opportunities but controlled be no one. Castells keeps paying more attention to the relations between networks (both cooperation and competition) and to the exclusionary aspect of networks than to relations within networks, the remaining control of the far more important mass media by the regime and the attempts to censor the new media. Because of the power of networks, we have to face privacy, security, and surveillance issues. Theory of mass-self communication tells us the power of networks and it helps to commit cybercrimes. Then the authors used this theory for this research.

Problem of the Study

Currently, there are some legal enactments available in Sri Lanka to curtail internet related crimes, but they are not adequate.

Objectives

(1) Study selected cybercrime cases in Sri Lanka and internet related laws in Sri Lanka;

(2) Suggest new solution for minimizing cyber-crimes in Sri Lanka.

Methodology

(1) Primary data: interviews—communication specialist, lawyers, judges, police media spokesman, cyber-crime investigators, policy makers, media researchers, and senior engineers;

(2) Content analysis: Computer Crime Act—No. 24 of 2007, Electronic Transaction Act—No. 19 of 2006, Intellectual Property Act—No. 36 of 2003, Information and Communication Technology Act—No. 27 of 2003;

(3) Case studies: two child pornography cases, two e-mail related cases, one web site hacking case;

(4) Secondary data: websites, books, journals, and magazines.

Trends and Challenges in Cyber-Crime in Sri Lanka

In Sri Lanka, there have been number of cyber-crime reported to the Sri Lankan Computer Emergency Readiness Team and Cyber-Crime Unit in Sri Lankan police.

According to Sri Lankan police records, police mention normal crime rate decreased. But the study analyzes cyber-crime. This type of crimes gradually increased. Phishing, abuse privacy, malware, e-mail

harassment, fake accounts (Facebook), and intellectual property cases reported to the Sri Lankan Computer Emergency Readiness Team. In addition to this e-banking cases, website hacking, e-mail harassment, child pornography cases reported to Cyber-Crime Unit in Sri Lanka police (Jayasekara, 2015).

Most of the cases were about fake accounts in Facebook. But under Sri Lankan law, defamation is not considered as criminal offence and it tantamounts to a civil matter.

In Sri Lanka, there have been four main acts which used in cyber-crime prevention. 1997 computer crime act was really important. In this act, no definition about cyber-crime but computer crime is a term used to identify all crimes frauds that are connected with or related to computer and information technology. This act covers a broad range of offences and it can be divided into two categories. They were computer-related crimes and hacking offences.

In Section 3 to Section 10, the authors described the key substantive offences under computer crime act. Securing unauthorized access to a computer an offence, doing any act to secure unauthorized access in order to commit an offence, causing a computer to perform a function without lawful authority an offence, offences committed against national security and national economy and public order. And also about dealing with unlawful data and, unlawfully obtained an offence, illegal interception of data an offence, using of illegal devices an offence, unauthorized disclosure of information enabling access to a service also an offense. There is a provision in the act which enhances the scope of intellectual property provisions contained in the Intellectual Property Act 36 of 2003. An amendment made to the penal code in 2006 introduced an offence requiring all persons providing a computer service like a *cyber café* to ensure that such a service would not be used for offences relating to sexual abuse of a child.

In addition, information communication and technology act and electronic transaction acts are also specifically dealing with internet based crimes. Electronic Transaction Act facilitates to formation of contracts, the creation and exchange of data messages, electronic documents, electronic records. And Penal Code Amendment and Evidence (special provisions) Act (No. 14 of 1995) is also used to prevent these crimes. According to Penal Code Amendment: According to the penal code amendment 286(b), it has a provision in “Duty of person providing service by computer to prevent sexual abuse of a child”. These things help to protect children from illegal internet use.

Evidence Act is also helpful to avert cyber-crimes. After analyzed the selected cases and conducted interviews, the suggestions are:

(1) Introduce personal data protection act;

(2) Reform defamation laws and introduce cyber defamation laws;

(3) Awareness about new media literacy (especially in three languages);

(4) Internet safe guard method introduced to especially for the parents;

(5) Motivate to complain cybercrimes;

(6) Introduced not apolitical internet code of ethics.

Conclusions

In Sri Lanka, there is a challenge in preventing cyber-crime. The growth of network-based crime has raised difficult issue in respect of appropriate balance between the needs of those investigating and prosecuting such crime, and the rights of users of such networks, so there is a need to empower the coordination process. Prosecutor, investigator, and judger need to work in coordinating manner, experienced investigators need to

deal with cyber-crime. Awareness in new media literacy and information technology is one way of minimizing cyber-crime. Also, Sri Lankan legal system needs to be modified.

References

Abeyratne, S. D. B. (2008). *Introduction to information and communication technology law*. Rajagiriya: Golden Graphics.

Brysk, A. (Ed.). (2002). *Globalization and human rights*. Berkeley: University of California Press.

Castells, M. (2001). *The internet galaxy: Reflections on the internet, business, and society*. New York: Oxford University Press.

Castells, M. (2009). *Communication power*. New York: Oxford University Press.

Castells, M. (Ed.). (2004). *The network society: A cross-cultural perspectives*. UK: Edward Elgar.

Clay, W. (2008). *Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress, congressional research service*. Retrieved from http://fas.org/sgp/crs/terror/RL32114.pdf

Conn, K. (2002). *The internet and the law: What educators need to know*. Alexandria: Association for Supervision and Curriculum Development.

Connell, O. (2007). *Cyber-Crime hits $100 billion in 2007, ITU news related to ITU corporate strategy*. Retrieved from http://www.ibls.com/internet_law_news_portal_view_prn.aspx?s=latestnews&id=1882

Convention On Cyber-Crime in Europe. (n.d.). Retrieved from http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Creech, C. K. (Ed.). (2007). *Electronic media law and regulation* (5th ed.). USA: Elsvier.

Defleur, L. M., & Dennis, E. E. (1993). *Understanding mass communication: A liberal arts perspective* (5th ed.). Boston: Houghton Mifflin.

Dunne, R. (2009). *Computers and the law: An introduction to basic legal principles and their application.* New York: Cambridge University Press.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal of Computer Virology, 2*(1), 13-20.

Hattotuwa, S. (2010). *"Banning Sri Lankan porn online: A couple of months after", ICT for peacebuilding*. Retrieved from http://ict4peace.wordpress.com/2010/01/31/banning-sri-lankan-porn-online-a-couple-of- months-after/

Henson, B., Reyns, B., & Fisher, B. (2011). Internet crime. In W. Chambliss (Ed.), *Key issues in crime and punishment: Crime and criminal behavior* (pp. 155-168). Sage Publications. Retrieved from http://www.sagepub.com/haganintrocrim8e/study/chapter/handbooks/42347_10.2.pdf

IC3 2009 Annual Report on Internet Crime Released. (n.d.). Retrieved from http://www.lookstoogoodtobetrue.com/prdocs/ic32009report.pdf

Jayasekara, D. (2015). Internet and law (special reference to Sri Lanka). *The Social Sciences, 10*(6), 841-844.

Lunker, M. (n.d.). *Cyber law: A global perspective*. Retrieved from http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN005846.pdf

Sofaer, D. A., & Goodman, S. E. (2001). *The transnational dimension of cyber crime and security: The transnational dimension*. Retrieved from http://media.hoover.org/documents/08179

Weeramantry, C. G. (1998). *Justice without frontiers: Protecting human rights in the age of technology* (Vol. 2). The Hague: Kluwer Law International.