23 (3) 2015 IIUMLJ 415-438

LEGISLATING FOR CYBERCRIMES IN THE MALDIVES: CHALLENGES AND PROSPECTS

Fathimath Waheeda*

ABSTRACT

The growth of Information and Communication Technologies (ICT) has changed the way of life for many people in the Maldives. Unfortunately, with the benefits also comes the threats. The use of ICT have added new dimensions of threats such as online fraud and forgery, hacking into protected systems and dissemination of pornography. Hence, deterring cybercrime is crucial for the national security of the country. Adoption of an appropriate legislation to protect from abuse of ICTs for criminal purposes should be the highest priority for the legislators, as the speed of advancement of ICTs have challenged many areas of existing legislation. This article studies the legislative approaches used to regulate cybercrime, using the cybercrime offences highlighted in the Cybercrime Convention. The cyber laws of England and Australia are discussed comparatively in order to identify whether the existing law is adequate, needs to be modified or there is a need for new laws to be enacted in the Maldives. This article is divided into five parts. Part one makes a brief introduction to the existing Maldivian regulatory framework. The second part of the article discusses the need for reform in the country and the lacuna in the existing penal legislation. The third part will examine the areas where modification or new laws are required. This will lead to the fourth part of the article which identifies the legislative approaches that needs to be taken in order to regulate cybercrime by relying on the Cybercrime Convention as a guide. Finally, the fifth part of the article concludes by recommending new provisions or modifications whichever is necessary to adequately address the issue of cybercrime.

Keywords: cybercrime, cyber-security, ICT, the Maldives

* Department of Law, Faculty of Shari'ah and Law, The Maldives National University, email: fathimath.waheedha@mnu.edu.mv

MENGGUBAL UNDANG-UNDANG BAGI JENAYAH SIBER DI MALDIVES: CABARAN DAN PROSPEK

ABSTRAK

Perkembangan pesat dalam era Teknologi Perhubungan dan Informasi (ICT) telah merubah cara hidup kebanyakan rakyat Maldive. Malangnya, bersama kebaikan yang dijanjikan, terdapat juga keburukan. Penggunaan ICT turut membawa bersama bahaya pelbagai dimensi, contohnya penipuan dan pemalsuan yang dahulunya hanya boleh dilakukan secara bersemuka, kina berleluasa di alam maya. Di samping itu, bahaya penggodam computer turut membahaykan system computer yang mempunyai pelbagai maklumat sulit dan penting. Selain itu, bahaya pornografi turut menghantui ramai ibubapa dan menjadi masalah yang serius kepada Negara. Oleh sebab itu, pihak kerajaan perlu mengambil berat isu jenayah siber kerana ia boleh mengancam keselamatan rakyat dan Negara. Undang-undang yang sesuai perlu menjadi agenda tertinggi para penggubal undang-undang. Makalah ini mengkaji pendekatan undang-undang yang diambil oleh negara-negara seperti England dan Australia dalam menangani masalah jenayah siber di negara mereka. Diskusi perbandingan ini diharapkan akan dapat membantu dalam menentukan samada undang-undang sedia ada di Maldives memadai atau pihak kerajaan seharusnya menggubal akta baru yang menangani isu jenayah siber ini secara berasingan. Untuk itu, makalah ini terbahagi kepada lima bahagian dimana bahagian pertama membincangkan keaadan undang-undang semasa di Maldives. Bahagian kedua pula melibatkan perbincangan mengenai bahaya jenayah siber. Bahagian ketiga akan melihat apakah undang-undang yang sedia ada mencukupi untuk mengatasi permasalahan yang timbul. Ini akan membawa kepada bahagian ke tempat yang membincangkan tindakan yang perlu diambil berdasarkan Konvensyen Jenayah Siber, bagi mengatasi segala permasalahan yang berkaitan dengan jenayah siber dan makalah ini akan diakhiri dengan bahagian kelima dimana rumusan dan pendapat akan diberikan tentang bagaimana masalah jenayah siber ini harus diatasi.

Kata kunci: jenayah siber, keselamatan siber, ICT, Maldives

INTRODUCTION

The advancement of new forms of ICTs has transformed the way people live their lives. The impact of ICT and its benefits to the Maldives has been more than just involving the development of basic information infrastructure,[1] it has provided a more efficient means of communication, commerce and trade. For most developing countries ICTs have a huge developmental potential and in the Asia-Pacific region, it has been increasingly used as a tool for socio-economic development.[2] However, this opens an avenue for new threats such as online fraud, hacking and distribution of pornographic materials. The challenge is for governments to make the use of the internet safer without minimising the developmental opportunities. Deterring cybercrime is therefore, necessary for national security and protection of the information infrastructure. It is therefore a priority for legislators to adopt proper legislation to prevent the use of ICTs for criminal activities.

Background: Current Framework

The use of ICT is paramount to facilitate education, health and even e-commerce services. This is especially so for a country like the Maldives which has more than 1000 diversely spread islands. An example of the importance of the use of ICT in the Maldives is the use of Tele-medicine services which are provided through an internet connection to islands which do not have access to specialised medical care. Other services, such as judicial video conferencing and distance learning is also conducted. Recently there have been more online services available such as internet banking,[3] Billpay services,[4] online notice boards[5] and online shopping. In addition, the Government has

1 ISTAG, "Shaping Europe's Future through ICT" (Information Society Technologies Advisory Group, March), ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-shaping-europe-future-ict-march-2006-en.pdf.

2 "The Linkage Between ICT Applications and Meaningful Development" (United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development (APCICT)), accessed November 3, 2014, http://www.unapcict.org/ecohub/briefing-note-series/BN1.pdf.

3 Most Banks in the country provide online banking services which are quite popular. See for example, Bank of Maldives, Maldives Internet Banking, <http://www.bankofmaldives.com.mv/PBanking/MIB/Pages/default.aspx>.

4 Utility companies provide Bill pay services for convenience of their customers.

5 The most popular market place is the eBay website. Ads can be posted freely to

also established an E-government service platform, and additional services to provide online information and services to the public.[6]

Key Institutions

The key governmental institution that has the role of providing communication facilities and information technology is the Ministry of Transport and Communication, which was established in 2013 under the new regime of the President Abdulla Yameen Abdul Gayoom. The Communication Authority of the Maldives (CAM) has the mandate of regulating the communication sector, which includes, the telecommunications, post and information technology. The National Centre for Information Technology (NCIT) has the task of the development, promotion and propagation of information technology in the country.

Legal and regulatory environment for ICT Development

A telecommunication law has been drafted but has yet to be passed.[7] At present, the Telecommunication Regulation 2003 is the main regulation used. Although, this law does not directly deal with computer related laws, the need for cyber security regulation was identified in the telecommunication policy.[8] In the Legislative Agenda 2009 under the regime of the former President Mohamed Nasheed, information security related laws were identified, and a law related to Computer Misuse was drafted. The Data Protection and Digital Signatures legislation was considered as the appropriate law. The "Law on Copyrights and other related right was enacted on 21st October 2010.[9] The Legislative Agenda 2014 unveiled a 207 bill legislative agenda with 98 new bills being drafted; however legislation relating to computer misuse was not listed as a priority.

A new Penal Code Act 2014 (No. 19/2014) ("the Penal Code") was enacted in July 2015. The Act is quite comprehensive and resolves a majority of the issues faced in the previous code. This act is the main

sell and lease goods and property.

6 "National Centre for Information Technology - Home," accessed November 3, 2014, http://www.ncit.gov.mv/index.php/en/.

7 Patricia Brazil Arinto and Shahid Akhtar, *Digital Review of Asia Pacific 2009-2010* (IDRC, 2009).

8 "Maldives Telecommunication Policy 2006-2010," accessed November 3, 2014, http://www.cam.gov.mv/docs/policy/Telecom_policy_2006_2010_Eng.pdf.

9 Copyright and related Rights Act (Law No 23/2010) (Maldives).

regulation in which criminal activities will be prosecuted, including cybercrimes.

Recent Developments

Recently there have been initiatives to develop the sector, even though a comprehensive cybercrime policy has not been compiled. The NCIT conducted a feasibility study to cultivate an ICT industry. In order to facilitate access, they conducted a project to construct kiosks on the islands. Namely, there are two key reasons which support the development of the information sector.[10] Firstly, the establishment of a government E-platform which indirectly helps to "secure risk prevention measures and the user's awareness and promotes the development of cyber security as employers and users become more aware of security measures".[11] Secondly, as ICT becomes part of the Maldivian culture, security measures need to be developed as the government is forced to formulate policies to regulate the service providers and to protect the infrastructure.[12]

Although identified as an instrumental area of development, there has been little progress in developing a cybercrime framework or enacting the necessary legislation.[13] Maldives participated and signed the Ministerial Declaration for the ABBMN Forum[14] organised by the International Telecommunication Union (ITU) on Digital Inclusion.[15] This is an indication that the government is finally working towards establishing a much needed cyber-security framework.

The enactment of a suitable legislation is a crucial part of a country's cybercrime strategy. Regardless of how broad the policy is, the identification of substantive criminal provisions that prohibits the activities related to the misuse of ICTs, such as computer related fraud, illegal access, data

---

10 See "The Promotion of a Culture of Security for Information Systems and Networks in OECD Countries," *OECD Digital Economy Papers*, 2005, doi:http://dx.doi.org/10.1787/232017148827.

11 Ibid.

12 Ibid.

13 "Seventh National Development Plan 2006 -2010," *Department of National Planning* (Maldives), 87, accessed November 3, 2014, http://www.planning.gov.mv/en/images/stories/ndp/seventh_ndp.pdf.

14 Regional Forum on Digital Inclusion includes the countries: Afghanistan, Bangladesh, Bhutan, Maldives and Nepal (ABBMN).

15 "ITU Regional Forum on Digital Inclusion Boosts Regional Cooperation - Ministers of Afghanistan, Bangladesh, Bhutan, Maldives and Nepal Commit to Increased Regional Cooperation" (Maldives, August 5, 2010), http://www.itu.int/net/pressoffice/press_releases/2010/CM05.aspx#.VgEDvd-qqko.

interference, infringements or child pornography is required.

The remaining part of this article now continues to discuss the extent of the problem relating to cybercrime in the Maldives. It discusses the need for reform in the country the existing penal legislation and highlight areas where modification or new laws are required. This will lead to the third part of the article which identifies the legislative approaches that needs to be taken in order to regulate cybercrime by relying on the Cybercrime Convention as a guide. Finally, the fourth part of the article concludes by recommending new provisions or modifications whichever is necessary to adequately address the issue of cybercrime.

CYBERCRIMES IN THE MALDIVES

The criminal misuse of ICTs and the response towards it has been an ongoing debate over the years. The reason why the issue remains challenging is due the evolving nature of the technological development, as well as the change in the method and ways in which cyber offences are committed.The range of technology-enabled crime is always evolving, both as a function of technological change and in terms of social interaction with new technologies.[16]

New trends in computer and cybercrimes are constantly being discovered, with the latest methods of committing crimes such as phishing and botnet attacks discovered in the last decade.[17] The emerging and increased use of new technology makes it more difficult for law enforcement officers to investigate and prosecute cybercrimes. It is not only that the method used changes, but also the impact that it leaves on the society diversifies.

In this article cybercrime and computer crime is used interchangeably, although it can be argued that cybercrime is narrower than computer related crimes, as cybercrime involves a computer network rather than a standalone computer. There is no commonly accepted definition of cybercrime, although many approaches have been adopted to develop a clear definition of the term.

One common definition describes cybercrime as any activity where the computer is used as a tool, a target or a place of criminal activity.[18]

---

16 Gregor Urbas and Kim-Kwang Raymond Choo, *Resource Materials on Technology-Enabled Crime* (Australian Institute of Criminology, 2008), 5.

17 Marco Gercke, "Understanding Cybercrime: Phenomena, Challenges and Legal Response," *ITU, September-2012. Book Reference*, 2012.

18 Eric J Sinrod and William P Reilly, "Cyber-Crimes: A Practical Approach to the

The role of the computer can be characterised in three ways; (1) a computer system may also be the object of a crime, where an individual modifies, deletes or destroys information in a computer system or destroys the computer system physically; (2) a computer system may also be used as a tool to commit a crime, and (3) a computer system may also be used to store evidence of a crime. This article is confined to the substantive criminal law, therefore the central focus will be on the first two methods, and not the last method, as it involves a discussion on criminal procedural law.

The Computer as the Target of a Crime

In this category of cybercrime, a computer system may compromise the 'confidentiality, integrity or availability of computer data and systems'.[19] These threats may not be classified as new in the sense that it may be equivalent to stealing from an aging cabinet in a storage facility. But the risk involved in much higher, as the advent of technology increases the possibility of stealing or manipulating massive amounts of data at the click of a mouse. In general three types of crimes may be committed, which includes: unauthorised access, malicious software, and the denial of Service (DoS) attacks.[20]

The Computer as a Tool of Criminal Activity

Under this category of cybercrime, the traditional offences such as distribution of child pornography and copyrighted materials are increasingly conducted using the internet as a tool. Viber or Messenger or chat groups may be easily used to organise crimes, even serious crimes such as murder. In many cases the existing legislation intelligently used maybe sufficient to prosecute these crimes. To be on the safe side, legislators should review existing legislation to identify gaps, to ensure that virtual crimes may be prosecuted.

Application of Federal Computer Crime Laws," *Santa Clara Computer & High Tech. LJ* 16 (2000): 187.

19 Convention on Cybercrime, opened for signature 23 November 2001, CETS No.:185 (entered into force 1 July 2004). Referred in the Cyber Crime Convention, Chapter II, Section I, Title 1.

20 Jonathan Clough, *Principles of Cybercrime* (Cambridge University Press, 2010), 27.

The Need for Reform

The abovementioned cybercrimes are also present in the Maldives, where the reported cases of cybercrimes rose by 200 percent from 2010 to 2011. This is a huge concern, because a country without cyber laws will not have the capacity to investigate these crimes. The Maldives Police Services described cybercrimes as an "emerging and trending" issue for which a special unit has been formed. In 2011, continued DoS attacks on the server of Dhiraagu, the largest telecommunication service provider, disrupted internet services.[21] In 2012, more cases of hacking, internet financial scams and identity theft was investigated.[22] At the end of 2014, the Maldives Police Services cautioned the public on the increased prevalence of money-grabbing scams, using the mobile phone, which has amplified since then.[23] In the first week of September alone more than 25 cases were reported, with a total of Rf. 40,000. These numbers will keep on rising so long as there is no special legislation to deal with cybercrimes.

The challenge for the government is to assess whether traditional penal laws are adequate to accommodate cybercrimes. There is a wide spread assumption that cybercrime is a unique phenomenon which requires special protections. Brenner argues that cybercrime, rather than being a unique phenomenon, exploits ICTs to commit traditional crimes in new ways and to engage in new types if criminal activity to a limited extent.[24] Therefore a wide range of activities may fall under traditional penal laws, some may require amendment to the traditional penal laws and some may entail adoption of new penal laws.[25] One instance where the activity may fall outside the existing penal law is in the case of fraud offences as deception is at the heart of the offence. Deception is defined as: "inducing a man to believe a thing which is false, and which the person practising the deceit knows or believes to be false".[26] Applying this approach, a machine may not practice

---

21 DHIRAAGU has been receiving these kind of attacks since 2009 but the most recent being the worst.

22 There has been many more reported incidents such as hacking of twitter, viber or facebook accounts of political or government officials.

23 Scammers call victims, on behalf of stores and companies on promotional offers and mislead people into recharging or reloading phones, even to the maximum of Rf. 40,000.

24 Susan W Brenner, "Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law," *Retrieved January* 20 (2001): 2007.

25 Ibid.

26 See Re *London and Globe Finance Corporation Ltd* [1903] 1 Ch 728. It is the same for the theft offence in the Penal Code, as a 'person' is required to

deception.[27] In this case, the penalty depends on the value of the misappropriated or damaged property, on the basis that it is tangible.[28] But the cost of stolen or altered information or data may be impossible to evaluate.

Many jurisdictions have reformed the general law to include specialised regulation to prosecute cybercrimes. Flanagan argues that the requirement to legislate cybercrime depends on the degree or kind of activities.[29] In the first type, the nature of the crime remains the same while the scale within which it occurs increases. Meanwhile, in the second type, the nature of the crime changes because of the use of systems and networks.[30] If you take theft offences, using a computer will enhance the capacity and allows it to be committed in larger scale and across jurisdictions with relative ease. This is because, as any person with a computer or an email address can be targeted.[31] DoS attacks is a case where both issues of degree and kind may coincide on the basis that sending a single mail or communication may not be considered problematic, but it may be, where in a DoS attack, a person sends several mails or traffic to a specific target.[32]

LEGAL APPROACHES TO CRIMINALISING CYBERCRIMES

The Council of Europe's Convention on Cybercrime (or the Budapest Convention) was the first multidimensional instrument to regulate cybercrime.[33] The Convention provides a comprehensive response to and addresse issues of substantive offences, procedural laws

be involved in the process, which excludes automated processes.Theft by deception offence: 'a person commits an offence where he knowingly deprives another of property by deceiving such other person or another person'; s 212

27 It is the same for the theft offence in the Penal Code, as a 'person' is required to be involved in the process, which excludes automated processes.

28 Ibid.

29 Anne Flanagan, "The Law and Computer Crime: Reading the Script of Reform," *International Journal of Law and Information Technology* 13, no. 1 (2005): 98–117.

30 Ibid.

31 Ibid., Robert S Litt, "Crime in the Computer Age: The Law Enforcement Perspective," *Tex. Rev. L. & Pol.* 4 (1999): 59.

32 B B Gupta, Ramesh Chandra Joshi, and Manoj Misra, "Defending against Distributed Denial of Service Attacks: Issues and Challenges," *Information Security Journal: A Global Perspective* 18, no. 5 (2009): 224–47.

33 The convention opened for signature on 23 November 2001 and entered into force on 1 July 2004.

and international cooperation.[34] The Convention provides for four categories of offences: (1) offences against confidentiality, integrity and availability of computer and data systems;[35] (2) computer-related offences;[36] (3) content-related offences;[37] and (4) criminal copyright infringement.[38] The discussion below is arranged according to the categories of offences provided in the Convention. The discussion also looks at the Law in England and Australia in order to see how the Maldives could benefit from the way these two countries have used the Covention to develop their laws to address cybercrimes. This approach is possible as the Maldives is a common law country and has often looked at practices in other common law countries.

Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems

Access Offences

The offence referred to as hacking is considered to be most common and oldest computer related crime. In Australia the *C*ybercrime Legislation Amendment Act 2012 has repealed some sections in the Criminal Code 1995 (Cth). Under this legislation, if the restricted data is held in a commonwealth computer or on behalf of or caused by means of a telecommunication service, then it is an offence if a person intends or causes any unauthorised access to, or modification of, restricted data knowingly.[39] In England, the Computer Misuse Act 1990 contains a similar offence which states that it is a crime to "cause a computer to perform any function with intent to secure access to any program or data held in any computer" where the person knows it is unauthorised.[40] The aggravated circumstance occurs where there is an intention to commit a specified offence.[41] Since the current penal law does not include activities that considers an unauthorised access to a computer as a crime, it is recommended that such a crime is created should the Maldivian Government wish to enact a law addressing cybercrimes. In some jurisdictions, unauthorised access is not penalised if no harm is caused but additional elements such as proof of damage or intention to

34 Cybercrime Convention, Chapter III.
35 Ibid., Title 1.
36 Ibid., Title 2.
37 Ibid., Title 3.
38 Ibid., Title 4.
39 Criminal Code 1995 (Cth) (Australia), s 478.1(1).
40 Computer Misuse Act 1990 (UK); s 1.
41 Ibid., s2. Richard Walton, "The Computer Misuse Act," *Information Security Technical Report* 11, no. 1 (2006): 39–45.

cause damage needs to be shown.[42]

Impairment of Data

The Australian provision makes a person guilty of an offence if the person causes any unauthorised impairment of electronic communication to or from a computer while the person is aware that the impairment is unauthorised.[43] In addition to this, the electronic communication must be sent to or from the computer by means of a telecommunication service or a Commonwealth computer.[44] A person has committed a crime if 'the person does an unauthorised act in relation to a computer, knowing that it is unauthorised, and intends to do more of the following or is reckless as to the act will: impair the operation of the computer, prevent or hinder access to any program or data held in the computer and impair the operation of any such program or the reliability of any such data'.[45] This should also be included in the Maldivian context.

Misuse of Devices

In this category there are two main things: possession or control of data[46] and producing, obtaining or supplying data.[47] Possession is defined as; '(a) having possession of a computer or data storage device that holds or contains the data; (b) having possession of document in which data is recorded'.[48] This, being a low threshold, includes abuse of a computer and network or exploitation of weaknesses in systems. Nevertheless, intention still needs to be proven.

Meanwhile, producing, supplying and obtaining data includes; (a) producing, supplying or obtaining data held or contained in a computer or data storage, and (b) producing, supplying or obtaining a document in which the data is recorded.[49] In comparison, England has more offences. First, 'to make, adapt, supply or offer to supply any article intending it to be used to commit or to assist in the commission of an

42 Cybercrime Convention, Explanatory Report [49].

43 Criminal Code 1995 (Cth) (Australia), s 477.3(1).

44 Ibid.

45 Computer Misuse Act 1990 (UK), S3(1)-(3). Maximum penalty available under the Act, for these offences is 10 years imprisonment: s3(6).

46 Under s 478.3 it is an offence for a person to have possession or control of data within the intention that the data be used by the person or another person, in committing or facilitating an offence.

47 Under s 478.4 it is an offence to produce, supply or obtain data with the intention that the data be used, by the person or another person in committing or facilitating an offence against Division.

48 Criminal Code (Cth), s 478.3.

49 Ibid, s 478.4.

offence under section 1 or 3' is an offence.[50] Second, 'to supply to offer any article with belief that it is to be used to commit, or to assist in the communication of, an offence under subsection 1 or 3' is an offence.[51] Third, 'to obtain any article in view that it be supplied to commit or to assist in the commission of an offence under subsection 1 or 3' is an offence.[52]

Interception of data

The interception of data is also considered as a crime in the Convention. Data maybe intercepted whether through an email, an instant message or data transferred. In Australia, Section 7 of the Telecommunications (Interception and Access) Act 1979 (Cth), states that "a person shall not intercept or authorise, suffer or permit another person to intercept; or do any act or thing that will enable him or her or another person to intercept a communication passing over a telecommunications system".[53] In England, the offence is described as intentionally intercepting without lawful exercise and the communication to be in transmission through means of either public or private telecommunication.[54]

The concept of 'unauthorised' data is important and needs to be clarified as it is the basis of the abovementioned offences. The access to a program or data stored in a system is considered unauthorised if not subjected to control or consent.[55] In contrast, unauthorised data can relate to access by a person not entitled to cause the access.[56]

These offences are critical for an effective legal framework to control cybercrimes. In the eyes of the author, the Australian approach is more favourable, even though the provisions had been critiqued for being vague and over reaching, but the government has taken a restrained and conservative approach here.[57] The offence being easy to understand is quite beneficial for the Maldives being new to this type of laws.

---

50 Computer Misuse Act 1990 (UK), s 3A(1).

51 Ibid., s 3A(2).

52 Ibid., s 3A(3); Malcolm Highfield, "The Computer Misuse Act 1990: Understanding and Applying the Law," *Information Security Technical Report* 5, no. 2 (2000): 51–59.

53 Where a communication is no longer in transit, it may be considered 'stored communication' and is governed by s 108 (Telecommunications (Interception and Access) Act 1979.

54 *Regulation of Investigatory Powers Act* 2000 (UK) (RIPA). The maximum punishment here is 2 years imprisonment.

55 Computer Misuse Act 1990 (UK), s17(5).

56 Criminal Code (Cth), s 476.2(1).

57 E Eugene Clark, *Cyber Law in Australia* (Kluwer Law International, 2010), 371.

Computer-related Offences

Fraud and forgery are also offences covered in the Cybercrime Convention, this is due to the perception that adequate protection is not provided against these new forms of offenses.[58] Traditionally, the offence of forgery involves physical documents, not by the manipulation of computer data.[59]

Computer-related Fraud

ICTs may be used for fraud in a number ways such as in data entry, controlling programs that process data and altering data outputs. In England the relevant offences are; (1) fraud by false representation, (2) fraud by failing to disclose information and (3) fraud by abuse of position.[60] Both dishonesty and intention to gain or cause loss is an element, but it is not required to show an actual gain or loss. Under the Act the definition of property is extended to include intangible property[61] and article that includes 'any program or data held in electronic form'[62]. In contrast, the Cybercrime Convention provides specific computer fraud offences.[63] Similar to England, computer-related fraud focuses on the intention rather than the circumstances. It is more detailed in that different means of manipulation such as input, alteration, deletion and suppression and manipulation of hardware.[64] It disregards the economic benefits obtained and focuses on the fraudulent act.

Identity theft is where a person's identification details are obtained through disreputable means such as rummaging through contents of "personal data". At present this can be achieved easily by sending 'phishing' emails requesting a person to re-register their account details in a replicate website.[65] In 2005 a phishing scam involving eBay users, which included retail accounts worth £200,000 from fraudulent sales were discovered and brought forward.[66]

In identity theft cases, the offence is criminalised through penalizing

58 Cybercrime Convention, Explanatory Report, para 80.
59 Ibid.
60 Fraud Act 2006 (UK), ss2-4.
61 Ibid., s5(2).
62 Ibid., s8(1).
63 Cybercrime Convention, *Art 6.*
64 Ibid., Art 5.
65 Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, Inc., 2007), 115.
66 Emily Finch, "What a Tangled Web We Weave: Identity Theft and the Internet," in *Dot. Cons: Crime, Deviance, and Identity on the Internet*. (Cullompton, England: Willan, 2003), 87..

conduct that falls under any of the following categories, such as transferring, possessing, obtaining or using information for criminal purposes.[67] In England this is dealt as a different offence, depending on the form of 'identity theft'.[68] The existing penal law is unable to deal with misuse of identity related information effectively. This explicitly includes possession of identity related information or equipment required to create such information. The penalty is for possessing the information rather than using or committing a crime. The Identity Cards Act 2006 (UK) also additional provisions aimed at possession of fabricated 'identity documents'[69] and offering false information.[70] It is also prohibited the possession of an 'apparatus, article or materials which the person knows are or have been designed or adapted to make false identity documents'.[71] A second offence is mere possession without a reasonable excuse of identity related documents that are false, improperly obtained or relate to another person or apparatus, articles or materials.[72] A further offense of providing false information for the purposes of National Identity Register or an ID card requires the knowledge or belief that the person knows that the information is false, or the person is reckless as to whether not it is false.[73]

The Penal Code contains provisions for identity fraud, which penalises the unauthorised impersonation of others and manufacturing, transferring, selling or purchasing identification information.[74] Possession is not included in the offense, but selling, purchasing or transferring may not be achieved without possessing the information.

---

67 Marco Gercke, "Understanding Cybercrime. A Guide for Developing Countries," *International Telecommunication Union (Draft)* 89 (2011): 93.

68 Clare Sullivan, "Is Identity Theft Really Theft?," *International Review of Law, Computers & Technology* 23, no. 1–2 (2009): 77–87; Chris Jay Hoofnagle, "Identity Theft: Making the Known Unknowns Known," *Harvard Journal of Law and Technology* 21 (2007): 1.

69 Identity Cards Act 2006, s 26(1).

70 S Davies, I Hosein, and E A Whitley, "The Identity Project: An Assessment of the UK Identity Cards Bill and Its Implications," *London: LSE Research Online*, 2005. Possession requires evidence that the individual had an intention to use the documents to establish a 'registrable fact' in the National Identity Register; s 1(5) and (6)

71 Ibid., s 25(3), (4). The maximum penalty of 10 years' imprisonment; s 25(6)

72 Ibid., s 25(5).

73 Ibid., s 28(2).

74 Penal Code Act (Maldives, 2014), sec. 312 a. Identification information includes personal information such as name and birth date, personal identification numbers or codes, personal financial information and any information which can be used to identify a specific person; Ibid., sec. 312 b.

Content-related Offences

This category covers content that is illegal, including pornography, xenophobic material or insults related to religious symbols.

Erotic Materials and Pornography
The extent to which different countries penalise possession of pornographic material differs. The Maldives is a conservative Islamic state and the old Penal Code prohibits the viewing of pornography. The new Penal Code deals with the issue more comprehensively, where it also prohibits the production and distribution of pornographic materials altogether.[75] Alas, the Code does not make selling or distributing these materials through the internet as an explicit crime. Therefore, it is doubtful whether the section is broad enough to encompass such activities.

Child Pornography
The law distinguishes between general pornographic materials and child pornography. The malevolent side of internet and modern digital technology is that it expedites the production and distribution of pornography including child pornography and forms of child abuse. There was a 2,026 percent growth in the cases opened, between 1996 and 2005 recorded by the FBI as part of the 'Innocent Images National Initiative' in the United States.[76] The number of prosecutions involving indecent photographs of children increased from 93 to 1890 in the period 1994 to 2003 in England.[77] The internet provides a medium which allows distribution in 'large volumes, with minimal cost and relative anonymity'.[78] Leading jurisdictions have revised their laws to include the possession of such materials *per se*. McLachin CJ in *R v Sharpe*[79] argues that, penalizing the act of possession may reduce the market as it provides a deterrence.

The general nature of the offence is the 'sexual depiction of an under aged child' but the elements differ between jurisdictions.[80] The Cybercrime Convention considers a 'minor' as a person below the

75 Criminal Code s 88(29). Penal Code s 622.
76 "Online Child Pornography/Child Sexual Exploitation Investigations," *US Department of Justice*, accessed November 22, 2014, https://www.fbi.gov/stats-services/publications.
77 Clough, *Principles of Cybercrime*, 248.
78 Ibid 249.
79 *R v Sharpe* [2001] 1 SLR 45, 99.
80 Cybercrime Convention, Art 9(2)

age of eighteen years,[81] consistent with the practice in the Maldives.[82] Pornographic materials are defined according to the national standard. The medium of depiction, is described as 'materials' which can come 'in any form, or a combination of forms, capable of constituting a communication'.[83] Other jurisdictions use terms such as 'photograph', visual 'representation' or 'depiction' but may exclude some terms, leading to difficulty in proving the offence. If the term 'visual representation' is used, the prosecution has to prove that the image has been displayed, which may difficult where the images are found in a storage device. This issue is resolved by extending the definition of photograph broadly to include 'data stored on a computer disk or by other electronic means which is capable of conversion into a photograph'.[84]

Virtual child pornography is a new invention of the modern digital technology; an image of an adult is altered to represent a more childlike appearance. Both Australia and England, use the definition of 'child pornography' broadly enough to incorporate forms of virtual pornography.[85] In *R v Sharpe* it was argued that virtual pornography was as destructive as actual child pornography given that it 'fosters and communicates the same harmful, dehumanizing and degrading message'.[86] The offence in Article 9 of the Convention should be enacted in the Maldives, as there is no separate offence of child pornography and the problem is a serious issue deserving separate legislation. At present, it may fall under the offense of production of obscene materials as previously discussed. By enacting a separate law in the shadows of the Article 9 offense, it may be used to prosecute virtual pornography cases more effectively. However, it is not enough to only criminalise child pornography, it is also necessary to criminalise the supply and distribution of child pornographic materials. Both England and Australia has broad range of offences which includes, producing[87] making[88] or publishing child pornography.[89] Maldives

81 Ibid, Art 9(3).

82 Special Rules Regulating Conduct of Pedophile Act (Law No 12/2009), s 60(b).

83 Criminal Code (Cth), s 473.1. Communication includes text, speech, sound, visual images, signals, data or other forms or in any combination of forms.

84 Protection of Children Act 1978 (UK) s 7(4).

85 Criminal Code (Cth) s 473.1. The definition of child pornography under this section applies to materials 'which depicts a person, or a representation of a person'; s 473.1.

86 *R v Sharpe* [2001] 1 SLR 45.

87 Criminal Code (Cth), s 474.20 and 474.23.

88 Protection of Children Act 1978 (UK), s 1(1)(a).

89 Criminal Code (Cth), s 474.19(1)(a)(v).

should at least adopt this approach or abide strictly by Article 9(3) of the Convention which adequately addresses conduct that falls within this category by using terms such as 'producing', 'offering or making available', 'distributing or transmitting', 'procuring' or 'possessing' child pornography.

Copyright Crimes

Tools and software available on the internet enables users to copy and download music and movies, and to facilitate dissemination. Infringement of intellectual property is a common practice and frequently occurs over the internet. Article 10 of the Convention regulates the infringement of copyright and related rights. Infringements of copyrights are already criminalised in most countries and the elements includes, acts committed using a computer system and occurring at a commercial scale. The Maldivian Law on Copyrights and related rights criminalise infringements rights committed willfully or negligently,[90] but it fails to encompass the use of computer to mass distribute infringing rights of the holder. Although this type of cybercrime is addressed in Maldives, it is done through the Copyright laws.

Hate Speech, Racism and Religious Offences

Some countries criminalise hate speech and racism. Article 3 of the Conventions criminalises the dissemination of racist and xenophobic materials through computer systems. Articles 4 and 5 of the Convention mentions threats and insults committed intentionally without rights, through a computer, which attacks 'a person for the reason that they belong to a group distinguished by race, color, descent or national or ethnic origin, as well as religion'[91] or a group of people belonging to any of the abovementioned categories.

Religious offences may also fall under this category, as people of a certain religion may be protected as they fall into a certain group. The Maldives particularly prohibits the production, use, sale, offer, giving, or spreading of anti-Islamic materials,[92] therefore it is crucial that an offense that addresses the issue of committing the same crime over the internet be enacted as it may be more destructive when committed as a cybercrime.

---

90 Copyright and related Rights Act (Law No 23/2010) (Maldives), s 30.

91 Cybercrime Convention, Art 4 and 5.

92 Law Relating to the Protection of Religious Unity Act (Law No 6/94) (Maldives), s 4 and 6.

ANALYSING THE GENERAL CRIMINAL LAW FRAMEWORK

At present, computer related crimes is prosecuted under the Penal Code, as no special legislation relating to cybercrime exists.[93] This part aims to identify the gaps in the existing framework and identify areas where laws need to be amended or new laws be enacted. The following discussion shall be divided into the traditional categories of offences and the analysis which varies depending on the seriousness of the issue and the difficulty in applying the concept in the Maldives.

Offences Against the Person

Murder is defined as knowingly causing the death of another person.[94] It involves the physical confrontation of at least two individuals, leading to the belief that murder is not possible through the use of computer technology. A hospital computer system may be manipulated, to change hospital records and even the dosage of certain medicine causing death or probability of death to a patient or patients.[95] Therefore, if this happens then it may equate with the traditional offence of murder. The use of ICT is the tool which is used to cause harm or death.[96]

Assault is defined where a person, 'without the consent of another person, touches or injures or puts the fear of imminent bodily injury'.[97] The aggravated offence is where serious bodily injury is caused to another person[98] or the assault is instigated with a lethal weapon.[99] This has been extended to threats vocalised through phones and post. The use of ICTs has increased the ease in which criminals may harass and intimidate a person.

Cyber stalking has been a challenging area to regulate. Stalking has increased tenfold with the advent of ICTs as it increases the anonymity and ease in which a person can access private data. This is problematic

---

93 The new Penal Code was drafted by an American Professor Paul H. Robinson. Paul H Robinson, and the University of Pennsylvania Criminal Law Research Group, "Final Report of The Maldivian Penal Law & Sentencing Codification Project: *Text of Draft Code* (Volume 1) and Official Commentary (Volume 2)," vol. 1, 2006.

94 Penal Code Act, sec. 110

95 Brenner, "Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law," 9.

96 Susan W Brenner, "Is There Such a Thing as' Virtual Crime'?," *California Criminal Law Review* 4, no. 1 (2001): 1.

97 Penal Code Act, sec. 120.

98 Ibid., sec. 120 b (1).

99 Penal Code Act.

as many forms of activities may circumvent the threshold required for traditional offences. Therefore the legislators need to carefully evaluate and identify high risk areas and amend the law accordingly.

Sexual Assault is where one person commits a rape or criminal sexual contact.[100] No physical assault occurs in the context of sexual assault in cyberspace. Then how can it be prosecuted under traditional law? Even though where a case of virtual rape be made, it may be difficult to prosecute under general law.[101] However, the use of ICT could relate to the issue of the motive of a crime.

Property and Privacy Offences

The essence of theft offences is actual unlawful taking of another's property.[102] The Penal Code differentiates the theft offences by 'deception',[103] 'extortion',[104] and 'embezzlement' with the traditional meaning of theft.[105] The difference is that in the cyber world, theft occurs through manipulation of data, rather than the physical conduct.[106] Even a broadly drafted theft offence may be unable to accommodate all the aspects of theft in the virtual world. Hence, this needs to be addressed specifically by amending the existing Penal Code or to include it as a specific crime under the new cybercrime legislation.

In cyber extortion and cyber fraud, electronic transmission is used to convey threats and false information to another person.[107] There are cases in which the consequences differ, such as where the thief unlawfully access bank records and duplicates information. Issues arise because of the illegal breach but the Bank is not deprived of the information.[108] This is a problematic area in that the owners still possess the information, but this may be resolved by extending the

100 Ibid., sec. 130 & 131.

101 Brenner, "Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law," 8.

102 Theft offence: 'A person commits an offense if he: (1) knowingly takes or exerts unauthorised control over the property of another, (2) with the purpose of permanently depriving such other person of possession.' Penal Code Act s. 211.

103 Penal Code Act, sec. 212.

104 Ibid., sec. 213.

105 Ibid., sec. 215.

106 Brenner, "Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law," 8.

107 Ibid.

108 This is private and confidential information which was stolen, but can it be theft when the bank still has use of it. It may be explained in the sense that the owner does not have exclusive use anymore, and the dilution may lead to financial loss.

laws to include the misappropriation of intangible property.

The new Penal Code offers a broad range of offences, unlike the old code which dealt with forgery under theft, the essence of forgery being that, 'one person knowingly falsifies something to deceive someone'.[109] Cyber forgery may include manipulation of digital documents, forging of paper or electronic documents. The existing criminal law may be able to accommodate cyber forgery with minor amendments.

The above discussion of traditional offences being committed with ICT has been very enlightening but forms of new activities have also emerged. Hacking for example, refers to the unauthorised access of a computer system either by violating the password or evading the protection. Hacking is the first step to further commit crimes such as the alteration of data or sending DoS attack. Trespass maybe equated with hacking, as it means illegal entering to an area not accessible to the public. Therefore it may be possible to prosecute hacking under a trespass offence but it would be more effective to enact a special law as the conduct required for trespass in cyberspace is not the same.

Offences against Public Order, Safety and Decency

As seen in the discussion on child pornography above, computer technology may be used to facilitate the commission of existing offences against morality, including offenses like gambling, prostitution and dissemination of obscene material.[110] While countries may amend laws where they need to address specific issues, but it may not be an issue where the law is broad enough to incorporate these offences regardless of whether it is committed through the internet.

---

109 Penal Code Act, s. 310. Forgery is defined as follows:
"(a) Offense Defined. A person commits an offense if, with the purpose of deceiving another or concealing any wrongdoing, he knowingly: (1) makes, completes, executes, authenticates, issues, or transfers a writing so that it falsely purports: (A) to be the act of another, or (B) to have been executed at a particular time or place, or in a particular manner or numbered sequence, or (C) to be a copy of an original; or (2) creates or alters any object or writing so that it falsely purports to have a particular antiquity, rarity, value, origin, or authorship; or (3) utters, reiterates, or refers to any writing or object known to be a forgery under Subsection (a)(1) or (a)(2)."

110 John McMullan and Aunshul Rege, "Cyberextortion at Online Gambling Sites: Criminal Organization and Legal Challenges," *Gaming Law Review* 11, no. 6 (2007): 648–65.

Offences against Public Administration

ICTs may also be used as a tool to challenge the administration of justice. This may include offenses of creating or destroying evidence, changing or removing court records, threatening law enforcement officers and judges. These acts may fall under the offense of obstructing justice. The possibility of dealing with these types of crimes depends on how broad the existing penal law is and whether it will allow for the use of ICT in the commission of these crimes to also be considered as a crime.

Further, a new occurrence known as 'cyber vigilantism' has emerged in cyberspace. Vigilantism in the real world is punished based on the final offence which was committed. Dealing with cyber vigilantism in this manner is not advisable as it would not solve the online problem.

Crimes Against the State

Traditional offences under this category involve treason, espionage, sabotage, or dissemination of information and propaganda. It may be essential to re-examine the laws to explicitly address these offences conducted over the internet.

Challenges to Prosecuting Cybercrimes

Even where cyber security has been identified as a high priority, it may require time to regulate and address new cyber activities. The Penal Code has not given any special attention to cybercrimes. It is argued that computer crimes are just extensions of the general offences that already exist. Therefore, existing laws could be used to prosecute cybercrimes. Where the general law is used to cover cybercrimes, prosecutors may face problems in proving that the new activity falls within the confines of the offence. Aside from that, the judge may not be willing to accommodate new forms of conduct within the traditional offence. The primary problem would be to overcome the literal translation used by many judges when interpreting existing legal provisions. Next is the judge's inability to incorporate broad principles of law to understand and evaluate existing provisions, as many are not trained in law.[111]

[111] Marcus Enfield, "Strengthening the Maldivian Judicial System (June 2005)," accessed November 22, 2014, http://www.mvlaw.gov.mv/pdf/publications/9.pdf. See Paul H Robinson, "Report of the Criminal Justice System of the Republic of Maldives: Proposals for Reform," accessed November 22, 2014, http://www.unicef.org/maldives/Criminal_Justice_System_in_Maldives.pdf.

Finally, the judges may not be up to date with latest ICTs and they will have difficulty in comprehending how they are to be prosecuted.

Nevertheless, it may take time to legislate a new law. As such, while waiting for that to take place, some amendments need to be made to the existing Penal Code in order to accommodate cybercrimes. As for new legislations, it should be drafted broadly so as to encompass the many types of crimes that may be committed through the use of ICT. The offence needs to be specific in that legal and illegal conduct may be clearly differentiated by the public.

The law should reflect and be flexible enough to accommodate the societal values and preferences which results in sanctions which coincides with these interests. The enactment of new or amended legislation dealing with cybercrimes would be be the most effective method of addressing computer related abuse.

CONCLUSIONS AND RECOMMENDATIONS

In the case of non-sexual crimes, both homicide and threats can be accommodated under the traditional penal law. It is possible to commit homicide by hacking into a system and causing death; therefore this is a traditional offence of murder committed in a non-traditional fashion. Since the Maldivian penal law does not categorise homicide according to the weapon used to inflict death, there is no need to amend the law to include computer system as a tool. The same is true for threats, as previously discussed; if an offender uses a computer to communicate a threat, the computer becomes another tool to carry out the traditional offence. Alas, there are cyber activities such as cyber stalking, harassment or virtual sexual assaults which falls outside the scope of the traditional penal law. Therefore new provisions needs to be added to address these issues.[112]

Theft and forgery are traditional crimes that can be committed by using computer technology but what is unclear is the case of hacking and related offences. The primary distinctive factor of cyber theft is that it relies on the electronic transmission and manipulation of data rather than the acts in the physical world. The traditional theft accomplished through non-traditional means through cyberspace would therefore

[112] Brenner, "Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law," 9; S W Brenner and M D Goodman, "Cybercrime: The Need to Harmonise National Penal and Procedural Laws," in *International Society for the Reform of Criminal Law 16th Annual Conference, Technology and Its Effects on Criminal Responsibility, Security and Criminal Justice, December*, 2002, 6–10.

require no amendment to the existing Penal law, except where the Maldivian law of theft requires a person to take, to possess or to exploit according to the type of theft. This can be resolved by defining the person to include machines or systems that the person operates. The one area which is difficult to reconcile is in the nature of the property taken. In many cases cyber theft is not a zero sum offense and therein lies the problem. Therefore the amending legislation must be broad enough to incorporate the concept of stealing intangible property by making copies of it.

It is more difficult to place hacking into the traditional crimes even though it can be equated to criminal trespass at times if the law is broad enough. In the Maldives criminal trespass offence is broad enough; however, in the classification of the offense, it is a simple trespass if it does not occur in a dwelling and is treated as a misdemeanor, which fails to reflect the seriousness of the damage caused by the act of hacking. Therefore a new offence of "unauthorised" access to a computer must be created. "Hacktivisim" can be equated with real world vandalism, which is a type of attack on a website and should be addressed by laws which specifically address this type of activity. The last type of activity, DoS attacks, is an activity which needs to be regulated as it evades the traditional offence categories. Forgery offenses can be dealt with more easily under the traditional penal law, as the essence of the act is falsifying a document with the purpose of practicing deception.

In the case of offences against morality, ICT is used as a tool to facilitate the commission of traditional offences such as gambling, prostitution and the dissemination of obscene materials. Therefore there is no need to legislate for this type of offences.

Crimes against the administration of justice is an area where some activities may fall under existing penal laws and others may be outside the scope. If the laws in question are drafted very broadly that will be generally sufficient to accommodate this type of offences. New activities such as cyber vigilantism or cyber stalking of law enforcement officers needs to be addressed separately and legislation adopted accordingly.

Crimes against the state can take many forms such as treason, espionage, or dissemination of information and propaganda. This is not a category where new legislation is required if the traditional penal law is adequate to accommodate these offences conducted over the internet.

From the above discussions, it can fairly be concluded that although some cybercrimes may be addressed by relying on the existing Penal laws of the Maldives, it is not enough. There is a need to enact a cybercrime legislation to address specific criminal misconducts related

to ICTs, so as to protect the rights of persons and to defend information systems from being abused. Mostly for the government this remains a priority area as this relates to the basic infrastructure and violations may cause chaos and mayhem in the society.

ICTs offer opportunities for the development of the country by providing an avenue to raise the standard of living in remote islands through the use of ICT. Both direct and indirect benefits flow from an evolving information technology industry. Nonetheless since the establishment of the multiparty system, the country has been politically unstable and many of the issues have become very politically motivated. In the past, there has been a tendency to block certain legislation for political reasons, where the government is unable to maintain a majority in the parliament. High interest areas relate to the general administration of the government and business and public interest matters. In the promotion of cybercrime legislation, public interest may be created in relation to child pornography and other grooming offences that may cause the parliamentarians to pull together and pass the bill.

The parliament has been flooded with legislation lately as a result of recent changes in both political and legal environment. There is an exceptional amount of legislation waiting to be presented and to be passed. This leads to the conclusion that it may take time before any cybercrime legislation could be enacted and passed in the Maldives.