Countering Cyber Attacks in Malaysian Law: Assessing the Concept of Cyber Attacks and the Countermeasures

Ummi Hani Binti Masood

Submitted in accordance with the requirements for the degree of
Doctor of Philosophy

The University of Leeds
School of Law

March 2017

The candidate confirms that the work submitted is her own and that appropriate credit has been given where reference has been made to the work of others.

Acknowledgements

I am indebted to my supervisors Professor Clive Walker and Dr Henry Yeomans for their comments, suggestions and encouragement. The support I have received from them is invaluable. I am also grateful to Universiti Teknologi MARA for the chance to further my study. Lastly, I thank my family, friends and colleagues at the University of Leeds and Universiti Teknologi MARA.

Abstract

An examination of the nature of cyber attacks (meaning attacks on computer systems and the disruption of national security and order through online seditious and defamatory statements) and the appropriate countermeasures under the law of Malaysia and international law are undertaken in this project. This study explores the emergence of cyber attacks as a serious threat to security and a challenge to current legal norms. As such, it uses ontologies to encapsulate and analyse the existence and reality of the cyber attacks phenomenon. It provides an open-ended concept and categories of cyber attacks especially for countermeasures and criminalisation purposes.

This study posits that criminal law is a necessary reaction in dealing with cyber attacks in Malaysia on the basis of effectiveness and fairness alongside other non-criminal law measures. In doing so, it identifies non-criminal and criminal law approaches in countering cyber attacks. Apart from the position in Malaysia, this study investigates the emergence of international norms in relation to cyber attacks. It examines the effectiveness and fairness of the international law in dealing with cyber-attacks.

This study focuses on several approaches to draw out analysis of the effectiveness and fairness of the measures to counter cyber attacks. Besides doctrinal analysis and policy transfer, semi-structured interviews were also conducted with 32 participants in Malaysia including policymakers, law enforcement officers, deputy public prosecutors, legal practitioners and experts in cyber security from the public and private sectors. The results show that there are different variations in the perception of cyber attacks at the national and international level. In that socio-political culture of Malaysia influences the understanding of cyber attacks and countermeasures.

Table of Contents

List of Figures

List of Tables

List of Abbreviation

AFC	Asian Football Confederation
AGC	Attorney General's Chambers
APCERT	Asia Pacific Computer Emergency Response Team
APTs	Advanced Persistent Threats
ATM	Automated Teller Machine
ASEAN	Association of South East Asian Nations
BSC	British Society of Criminology Code of Ethics
CCA	Computer Crimes Act 1997
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CNI	critical national infrastructure
CNII	critical national information infrastructure
CSI	crime scene investigation
DDOS	distributed denial of service
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
FBI	Federal Bureau of Investigation
GCHG	Government Communications Headquarters
HITBSecconf	Hack in the Box Security Conference
IAB	Internet Architecture Board
ICC	International Criminal Court
ICCPR	International Covenant of Civil and Political Rights
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICT	Information and Communications Technology
ICTY	International Criminal Tribunal for the former Yugoslavia
ICP	Internet content provider
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IO	Investigating officer
IP	internet protocol
ISP	Internet service provider
ISMS	Information Security Management System
IT	Information technology
ITU	International Telecommunication Union
IDS	intrusion detection system
ISA	Internal Security Act 1960
JPN	Jabatan Pendaftaran Negara (Department of National Registration)
SKMM	Suruhanjaya Komunikasi dan Multimedia (Malaysia Communications and Multimedia Commission)
SOSMA	Security Offences (Special Measures) Act 2012
MAF	Malaysia Armed Forces
MYCERT	Malaysia Computer Emergency Response Team

MCMC	Malaysia Communications and Multimedia Commission
MAMPU	Malaysian Administrative Modernisation and Management Planning Unit
MACC	Malaysia Anti Corruption Commission
MLA	mutual legal assistance
MSC	Multimedia Super Corridor
NATO	North Atlantic Treaty Organization
NCCU	National Cyber Crime Unit
NSC	National Security Council
OIC-CERT	Organisation of the Islamic Cooperation Computer Emergency Response Team
OS	Operating system
OSA	Official Secrets Act 1972
OWASP	Open Web Application Security Project
PDPA	Personal Data Protection Act 2010
PDRM	Royal Malaysia Police
PO	prosecuting officer
SCADA system	Supervisory Control and Data Acquisition system
SCO	Shanghai Cooperation Organisation
SHAC	Safe Huntingdon Animal Cruelty
SIRIM	Standards and Industrial Research Institute of Malaysia
SMS	short message service
Telco	telecommunication companies
TNT	trinitrotoluene
TOR	the onion router
UDHR	Universal Declaration of Human Rights
UN	United Nations

Chapter 1

Introduction

This study is aimed at investigating the nature of cyber attacks and the appropriate countermeasures under the law of Malaysia and international law. The researcher came across this topic during the International Humanitarian Law Moot Court Competition organised by the International Committee of the Red Cross Malaysia in 2012. She was interested to assess the legality of the usage of cyber attacks during armed conflict and the extent to which they can be categorised as armed attacks under international humanitarian law. After extensive perusal of the literature on this topic, the researcher discovered that cyber attacks outside of armed conflict have not been sufficiently addressed by states especially in Malaysia. There are different views about the definition of cyber attacks. There is also an ongoing debate as to whether a large-scale cyber attacks can actually happen. There is a cyber defence policy but a lack of legal process under Malaysian law and international law. The researcher was interested to investigate the ways in which cyber attacks might be better regulated. This includes the usage of technological and legal measures and the extent to which these measures are effective and fair in dealing with cyber attacks. The complex nature of cyber attacks entails further investigation. The researcher decided to embark on this study for these reasons.

This chapter provides a brief explanation of the context of the debates and key issues surrounding the problem of cyber attacks. It acts as an introduction to the concept of cyber attacks and the appropriate countermeasures. It describes the thesis statement and the objectives of the research. This chapter also explains the significance and originality of the study and gives a brief overview of the methodology used in this study. An outline of the thesis structure is stated at the end of this chapter.

1.1 The Problem of Cyber Attacks

States have increasingly considered cyber attacks as a serious danger to national security and a challenge to the application of the existing legal norms especially the law of armed conflict.[1] Technocrats argued that 'the discovery of the stuxnet worm in Belarus in 2010 was a game-changer in the world of malware'.[2] It is one of the most sophisticated cyber attacks due to its ability to strike from long distance and the specificity of its attack. Iran disclosed that the stuxnet worm had damaged some of its nuclear centrifuges. Estonia also had been subjected to cyber attacks in 2007.[3] The country's banking, media and government websites were bombarded with distributed denial of service (DDOS) attacks. The culprits are suspected to have been pro-Russian hacktivists.[4] The attacks crippled the administration and banking system of Estonia for three weeks. This event led to the establishment of the NATO Cooperative Cyber Defence Centre of Excellence based in Tallinn, Estonia.[5] Georgia was subjected to cyber attacks before the actual usage of conventional weapons during the 2008 war with Russia.[6] The United States is constantly being exposed to cyber attacks. In response, President Obama declared that 350 million US dollars have been allocated to secure the United States' infrastructure and has proposed the possible enactment of the Cyber Security Act.[7] These

---

[1] Schmitt MN (ed), *Tallinn Manual on the International law Applicable to Cyber Warfare* (Cambridge University Press 2013) 3

[2] BBC, 'Researchers Warn of New Stuxnet Worm' (*BBC News Technology*, 19 October 2011) <http://www.bbc.co.uk/news/technology-15367816> accessed 14 January 2014; see also Taddeo M, 'Information Warfare: A Philosophical Perspective' (2012) 25 Philos Technol (2012) 25:105–120

[3] Schmitt MN, *Tallinn Manual* (n 1) 2

[4] Gallagher M, 'Web War II: What a Future Cyberwar Will Look Like' (*BBC News Magazine*, 30 April 2012) <http://www.bbc.co.uk/news/magazine-17868789> accessed 13 January 2014

[5] Schmitt MN, *Tallinn Manual* (n 1) 1; NATO Cooperative Cyber Defence Centre of Excellence <http://www.ccdcoe.org/> accessed 13 January 2014

[6] Handler SG, 'The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare' (2012) 48 Stan J Int'l L 209

[7] Office of the Press Secretary, 'Launch of the Cybersecurity Framework' (*The White House*, 12 February 2014) <http://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework> accessed 13 August 2014

incidents illustrate the impact of cyber attacks, which can paralyse a country's administration and damage the economy.

However, some scholars contend that the severity of cyber attacks and the vulnerability of the computer systems are created by 'sensationalistic excesses of tabloid journalism'.[8] Despite the fact that they may create panic, these sources may 'announce system flaws and potential opportunities for offending'. [9] According to Michalowski and Pfuhl, the ambiguity of new technology disturbs economic relations and established patterns of authority and dominance.[10] This is a plausible explanation for the attention given to cyber attacks. The purpose of this study is to conduct investigation in order to confirm that cyber attacks is not merely media hype and a term coined by politicians to garner the attention of the public.

Despite these doubts, governments and many organisations rely heavily on computer systems in their operations. Orphardt observes that 'the greater the network integration of a target country's infrastructure, the greater its potential vulnerability'. [11] Computer viruses such as ghostnet can easily penetrate the government's website, tampering with documents and destroying facilities. [12] The potential loss suffered by them is great if the system crashes.[13] Thus, cyber attacks epitomise a new dimension of waging war in the age of information.

1.1.1 The Impact of Cyber Attacks

The purpose of this section is to assess the perceptions and beliefs of the impact of cyber attacks. This study argues that cyber attacks are perpetrated by using malicious software and malware, which are designed to penetrate, alter and destroy the computer system and server. Apart from that, cyber

---

[8] Taylor PA, *Hackers* (Routledge 1999) 7

[9] Wall DS, *Cybercrime: The Transformation of Crime in the Informative Age* (Polity Press 2007) 27

[10] Michalowski RJ and Pfuhl EH, 'Technology, Property and Law: The Case of Computer Crime' (1991) 15 Crime, Law and Social Change

[11] Ophardt JA, 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield' (2010) 3 Duke L & Tech Rev 1, 2010

[12] Wasik M, *Crime and the Computer* (Clarendon Press 1991) 9

[13] ibid

espionage is perceived as cyber attacks as it poses a serious threat to the national security and economy. In addition, the findings of the study revealed that online sedition and defamatory statements with the intention to disrupt national security and harmony are perceived as cyber attacks in Malaysia. This study shall return to the perceptions of cyber attacks when it discusses the concept of cyber attacks in chapter 3. The nature of harm and impact of the attacks are important. Low threshold cyber incidents, which only cause inconvenience, should not be classified as cyber attacks. The term cyber attack should be reserved only for medium and high impact attacks. They may be classified as cybercrimes or war crimes.

However, the severity and the likelihood of the occurrence of high impact cyber attacks have been intensely debated. For instance, some scholars are sceptical about the existence of cyber attacks in the guise of cyber warfare. They argue that the Pentagon exaggerated the threat of cyber warfare for political reasons to convince the Congress to pass cyber security legislation and grant funding.[14] Thus, the scenario of a 'cyber Pearl Harbor' or a cyber 9/11 is an overstatement.[15] Bruce Schneier, chief security officer of BT, claims that the threat of cyber warfare is greatly exaggerated and is merely a power struggle involving a battle of metaphors.[16] In addition, Cavelty argues the description of cyber attacks rely heavily on hypotheses and the evidence is often anecdotal.[17]

Nevertheless, other scholars are convinced that the threat of cyber warfare is real. Cordula Droege, Head of the Operational Law Unit, Legal Division, International Committee of the Red Cross opines that cyber attacks during armed conflict is technically feasible.[18] Andrew Beckett, head of Cassadian

---

[14] Marcus J, 'Are We Really Facing Cyberwar?' (*BBC News Technology*, 5 March 2013) <http://www.bbc.co.uk/news/technology-21653361> accessed 13 January 2014

[15] ibid

[16] Shiels M, 'Cyber War Threat Exaggerated Claims Security Expert' (*BBC News Technology*, 16 February 2011) <http://www.bbc.co.uk/news/technology-12473809> accessed 14 January 2014

[17] Cavelty MD and Mauer V (eds), *The Routledge Handbook of Securities Studies* (Routledge 2010) 184

[18] Droege C, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2013) 94 International Review of the Red Cross

Cyber Security, a global defence and security provider, contends that even a small country has the capacity to engage in cyber attacks.[19] Eugene Kaspersky, founder and chief executive of Kaspersky Lab, warns that cyber criminals might decide to attack power plants to cause the entire nations to plunge into darkness.[20]

The majority of states perceive cyber attacks as a danger to national security and interest. The Ministry of Science, Technology and Innovation of Malaysia has issued the National Cyber Security Policy.[21] Malaysia acknowledges the alarming rise of premeditated attacks with potentially catastrophic effects to interdependent networks and information systems across the globe.[22] Significant attention must be paid to critical information infrastructure protection initiatives. The National Security Strategy of UK categorised cyber attacks as a Tier One threat to the national security alongside international terrorism.[23] UK has allocated £1.9 billion to implement the National Cyber Security Strategy 2016-2021.[24]

The steps taken by states in dealing with cyber attacks demonstrate the seriousness of this issue. The policymakers are faced with the task of formulating cyber defence strategy and military planning to protect critical

---

533

[19] BBC News Click, 'Trend of 2013', <http://www.bbc.co.uk/iplayer/episode/b03nnnpf/Click_Trends_of_2013/> accessed 6 May 2014

[20] Moskvitch K, 'The World's Five Biggest Cyber Threats' (*BBC News Technology*, 26 April 2012) <http://www.bbc.co.uk/news/technology-17846185> accessed 13 January 2014

[21] Kementerian Komunikasi dan Multimedia Malaysia, 'National Cyber Security Policy' <http://nitc.kkmm.gov.my/index.php/national-ict-policies/national-cyber-security-policy-ncsp> accessed 15 September 2016

[22] The position of cyber attacks in Malaysia will be discussed extensively in chapter 4 and chapter 5

[23] Office of Cyber Security and Information Assurance, 'Keeping the UK Safe in Cyber Space' (*Cabinet Office*, 12.12.2013) <https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace> accessed 14 January 2014

[24] Cabinet Office, 'National Security and Intelligence, National Cyber Security Strategy 2016-2021' (Policy Paper, <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 > accessed 1 February 2017

infrastructure from cyber attacks.[25] Arguably, cyber attacks are an unavoidable problem that must be addressed properly by states. Understanding the nature of cyber attacks and the appropriate countermeasures are crucial in addressing this phenomenon. As such, this study investigates the nature and attributes of cyber attacks as a phenomenon.

1.1.2 Governance of Cyberspace

This section analyses some of the challenges in dealing with cyber attacks at the international and domestic level. States are faced with an arduous task in regulating activities in the cyber world. This is due to the complex and resilient nature of the Internet. It consists of interconnected global networks of nodes. According to Castells:

> The information technology paradigm does not evolve toward its closure as a system, but toward its openness as a multi-edged network. It is powerful and imposing in its materiality, but adaptive and open-ended in its historical development. Comprehensiveness, complexity and networking are its decisive qualities. Thus, the social dimension of the information technology revolution seems bound to follow the law on the relationship between the technology and the society.[26]

The Internet has contributed significantly to the growth of administration, the economy and social relations at large. Nevertheless, it has also been used as a medium to commit illegal activities such as spreading obscene and racist content, theft, fraud, hate speech and online stalking.[27] Thus, the Internet is a powerful tool that can be used to influence or manipulate its users.

---

[25] Droege C, Get Off My Cloud (n 18) 2

[26] Castells M, *The Rise of the Netwok Society*, vol 1 (2nd edn, Blackwell Publishing 2000) 65

[27] Akdeniz Y, Walker C, Wall D, 'The Internet, Law and Society' in Akdeniz Y, Walker C, Wall D (eds), *The Internet, Law and Society* (Longman 2000) 5

The governance of the Internet involves 'a wide variety of public and private, state and non-state, national and international, institutions and practices'.[28] Managing the Internet has been difficult for all governments especially as their capability is limited due to the absence of physical territory in the cyber world. According to Loader:

> The possibility of cyberspace giving rise to new forms and expressions of governance: a paradigmatic change in the constellation of power relations between individuals, governments and social institutions. Such a contention arises from the transcending qualities of ICTs as a means to facilitate the demise of modernist forms of governance based upon territory, hierarchal managerial control of populations, and policing. Thus, nation state boundaries are said to be weakening both from the development of global economies where cyberspace is where your money is and also from the lack of control by national governments over communications in cyberspace.[29]

Due to the constraints and limits of the functions of the state, several issues need to be addressed. Can the law catch up with the progress of the development of technology? How should the law respond to the advancement of technology? Should public law regulate this or should it be left to the private bodies? Is the current regime sufficient to deal with this matter? The aims of governance are to regulate content and activities in the Internet. This may be achieved through the engagement between states and private actors.

The international character of cyber attacks has hindered attempts to sanction the perpetrators. Moreover, this problem has been intensified due to the absence of an international agreement between states. The efforts to create a common policy on cyber development have been fragmented and

---

[28] Ibid citing Hirst P and Thompson G, Globalisation and the Future of the Nation State' (1995) 24 (3) *Economy and Society* 408, 422

[29] Loader BD, 'The Governance of Cyberspace: Politics, Technology and Global Restructuring' in Loader BD (ed) *The Governance of Cyberspace* (Routledge 1997) 1

lacking in focus. All the major actors in cyberspace not merely governments need to be involved in forging an agreed approach.[30] It is argued even if there is legal instrument, how states will comply is a political issue.[31] Currently, there is no monitoring body being established to scrutinise the development of cyber weapons by states. Actions that can be taken against rogue states are limited. Some states may not even want to develop regulation on cyber attacks due to various reasons such as geopolitics. This is an obstacle that must be addressed by states in order to counter cyber attacks. This study aims to unravel the complex nature of cyber attacks and the responses to them. It explores the range of non-criminal law and criminal law measures by which cyber attacks might be regulated.

1.2 Thesis Statement and Research Objectives

This thesis posits that criminal law is a necessary reaction to counter cyber attacks alongside non-criminal measures on the basis of effectiveness and fairness. The primary purpose of this thesis, therefore, is to examine the concept of cyber attacks and the regime governing cyber attacks in Malaysian law and international law. This includes the current roles, values and potential of non-criminal and criminal law as a countermeasure. Accordingly, this thesis used doctrinal and empirical methods to analyse the implementation of non-criminal and criminal law measures to counter cyber attacks in Malaysia. Therefore, the main objectives of this thesis are as follow:

(1) The first objective is to identify the concept of cyber attacks by investigating the nature and attributes of cyber attacks as a phenomenon;
(2) The second objective is to assess the approaches to counter cyber attacks and to situate non-criminal and criminal measures within the strategy to counter cyber attacks in Malaysia;

---

[30] Stamp G, 'UK Seeks 'Consensus' at Cyberspace Conference' (*BBC News Politics*, 18 October 2011) <http://www.bbc.co.uk/news/uk-politics-15355739> accessed 14 January 2014

[31] Wuschka S, 'The Use of Combat Drones in Current Conflicts - A Legal Issue or a Political Problem?' (2011) 3 Goettingen J Int'l L 891

(3) The third objective is to assess the effectiveness and fairness of non-criminal law and criminal law measures in dealing with cyber attacks in Malaysia;
(4) The fourth objective is to ascertain the position of cyber attacks under international law and the measures used to address this problem at the international level.

1.3 Significance and Originality of the Study

This section assesses the extent to which the scholarly literature on cyber security and criminal law addresses the objectives of the thesis. Cyber attacks are situated at the crossroad of multi disciplinary studies including computer studies, information technology, media, communication and strategies studies. [32] According to Cavelty, other disciplines such as international relations in particular security studies 'have been very slow to come to grips with the challenge of the information revolution' and there are many 'unquestioned assumptions in both expert and official writings about the topic'.[33] Thus, scholars may contribute significantly in formulating the security policy related to this area.

Most scholars have tended to study cyber attacks in the context of the international humanitarian law and the use of force.[34] For instance, a group of international experts directed by Michael Schmitt was invited by NATO to prepare a manual on the law governing cyber warfare, which is known as the *Tallinn Manual*. The group proposed that general principles of international law applied to cyberspace and thus rejected any assertions that a new treaty law is required to govern cyberspace.[35]

---

[32] Cavelty MD, 'Cyber Threats' in Cavelty MD and Mauer V (eds), *The Routledge Handbook of Securities Studies* (Routledge 2010) 125

[33] ibid

[34] Li Zhang, 'A Chinese Perspective on Cyber War' (2013) 94 International Review of the Red Cross 801; Waxman MC, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 Yale J Int'l L 421; Tsagourias N, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012) 17 J Conflict Security Law 229; Brenner SW, Clarke LL, 'Civilians in Cyberwarfare: Conscripts' (2010) 43 Vand J Transnat'l L 1011.

[35] Schmitt MN, *Tallinn Manual* (n 1) 13

As for domestic law, Hathaway acknowledges that current 'domestic laws are not yet fully prepared to meet' the growing threat of cyber attacks.[36] Fafinski examined the compatibilities between the nature of computer misuse and the nature of English criminal law. He defined computer misuse as 'unethical or unauthorised behaviour in relation to the use of computers, programs, or data'.[37] He argued that 'since certain forms of behaviour involving the misuse of computer fall outside the boundaries of criminal law, then computer crime is but a subset of computer misuse. Computer misuse considers these particular behaviours to determine whether or not they fall within the criminal law and if not whether they should be dealt with via legal means or otherwise'.[38] The writer examined the usage of English criminal law in dealing with computer misuse, a similar theoretical framework to that adopted in this study.

Apart from Fafinski, other scholars including Wall and Yar have explored the key facets of cyberspace crime and policing cyberspace. They examine the concept of cybercrime and a wide range of issues related to cybercrime.[39] This includes the challenges of the enforcement of the law and policing online behaviour.[40] Their observations are relevant to this study. The aim of this study is to examine the application of criminal law and the problems of using this measure to counter cyber attacks in Malaysia.

To date, there is little research conducted on the measures to counter cyber attacks in Malaysia. Most of the scholars have been focusing on developing the technical tools and framework for cyber terrorism,[41] illegal activities in

---

[36] Hathaway OA and others, 'The Law of Cyber-Attack' 100 Calif L Rev 817, 27

[37] Fafinski S, *Computer Misuse. Responses, Regulation and the Law* (Willan Publishing 2009) 4 citing Wasik M, *Crime and the Computer* (Clarendon Press, Oxford, 1991) 3

[38] Ibid 6

[39] Wall DS, *Cybercrime: The Transformation of Crime in the Informative Age* (n9); Yar M, *Cybercrime and Society* (SAGE Publications, 2006)

[40] Wall DS, 'Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace' Police Practice and Research, Vol 8, No 2, May 2007, pp 183–205; Jewkes Y and Yar M, 'Policing Cybercrime: Emerging Trends and Future Challenges' in Newburn T (ed), *Handbook of Policing* (2nd edn, Willan Publishing 2008

[41] See Yunos Z, Ahmad R, Abd Aziz NA, 'Definition and Framework of Cyber Terrorism' (2013) 1 SEARCCT Selection of Articles 67, Yunos Z, Ahmad R, Suid

the Internet, Malaysia's cyber security policy[42] and the usage of the Internet by the public.[43] For instance, Olivia Tan Swee Leng scrutinised the general aspects of cyber terrorism in Malaysia.[44] The writer focuses on the strengths and weaknesses of cyber security by analysing the data provided by organisations and companies in Malaysia. Rabiah Ahmad and Zahri Yunos examined the methods that can be used to conduct research on cyber terrorism. They scrutinised the application of the mixed method in exploring the context of cyber terrorism, focusing on the attributes or components of cyber terrorism.[45] They also examined the usage of the focus group in analysing the phenomenon of cyber terrorism.[46]

The research done so far in Malaysia is different from this study, which aims to analyse the application of non-criminal measures and the imposition of criminal liability in detail from mainly a legal doctrinal perspective. Other scholars in Malaysia examine the issues related to cyber security from the perspectives of computer and political science. Furthermore, the finding of this study is supported by the data collected through fieldwork involving selected enforcement officers, experts in cyber security, national cyber institutions and prosecutors in Malaysia. The originality of the research is derived from the data gathered from the fieldwork. So far, there is little study conducted using such data with respect to non-criminal measures and criminal liability for cyber attacks in Malaysia. The data is also used to determine the effectiveness of the law regulating cyber attacks in Malaysia

---

SH, Ismail Z, 'Safeguarding Malaysia's Critical National Information Infrastructure (CNII) Against Cyber Terrorism: Towards Development of a Policy Framework' (Sixth International Conference on Information Assurance and Security, 2010)

[42] Hashim MSB, 'Malaysia's National Cyber Security Policy: The Country's Cyber Defence Initiatives', (IEEE Conference Proceeding, 2011) <eeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5978782> accessed 3 May 2014

[43] Salman A, Er AC, Wan Mahmud WA, Abdul Latif R, 'Tracing the Diffusion of Internet in Malaysia: Then and Now' (2013) 9 Asian Social Science 9

[44] Tan SLO, Khan S, Hossein RM, *Cybercrime and Cyber Terrorism: The Security Measures In Malaysia* (Lamber Academic Publishing 2012)

[45] Ahmad R, Yunos Z, 'The Application of Mixed Method in Developing a Cyber Terrorism Framework' (2012) 3 Journal of Information Security 209

[46] Ahmad R, Yunos Z, Sahib S, Yusof M, 'Perception on Cyber Terrorism: A Focus Group Discussion Approach' (2012) 3 Journal of Information Security 231

based on the socio-legal research. This contributes to the novelty of the methodology of the study. In addition, policy transfer is also being used to study the responses to cyber-attacks in Malaysia based on UK experiences, adding an extra layer of novelty and originality to the study and also widening the scholarly audience. This study has not offered an evaluative perspective on the power of the police, court processes, prosecution and the law of evidence, as the scale of the debate in these areas is extensive. The researcher intends to explore these areas in her future research.

1.4 The Structure of the Thesis

The study is structured as follows. To begin with, chapter 1 provides the focus and background information of the study. It explains the objectives of the study, background to the research, research methodology and the significance of the study.

Next, chapter 2 specifies the methods used in this study. This includes doctrinal analysis, policy transfer and empirical fieldwork study. This chapter illustrates the process of developing the interview guide, the selection of the participants, and analysis of data. It also discusses the problems in conducting the interviews and the measures to overcome the difficulties during fieldwork. After giving the scope of the research methodology, this thesis examines the four research objectives that frame the argument in each of the subsequent chapters.

The first objective is to identify the concept of cyber attacks by investigating the nature and attributes of cyber attacks as a phenomenon. Chapter 3 seeks to formulate the concept of cyber attacks. It investigates the nature and attributes of cyber attacks as a phenomenon through empirical study and doctrinal analysis. This is done by reference to the identity of the perpetrators, victims and targets, the method and impact of cyber attacks and the motives of the attacks.

The second objective is to assess the approaches to counter cyber attacks and to situate non-criminal and criminal measures within the strategy to counter cyber attacks in Malaysia. Chapter 4 discusses the strategy to deal with cyber attacks in Malaysia. This includes the usage of non-criminal

measures and criminal law. It also looks at various factors that affect the implementation of the strategy to counter cyber attacks including the values of the Malaysian legal system, the role of the government, the notion of fairness and effectiveness.

The third objective is to assess the effectiveness and fairness of non-criminal law and criminal law measures in dealing with cyber attacks in Malaysia. Chapter 4 explores the ways in which non-criminal measures are used in countering cyber attacks. This includes social prevention policy, situational crime prevention, the role of Computer Emergency Response Team (CERT), the involvement of private sector. Chapter 5 identifies the position of cyber attacks under the criminal law in Malaysia. It considers the obstacles and challenges in the enforcement of the law and possible reforms. Both chapters analyse the effectiveness and fairness of non-criminal measures and criminal law in managing cyber attacks in Malaysia.

The fourth objective is to ascertain the position of cyber attacks under international law and the measures used to address this problem at the international level. Chapter 6 assesses the position of cyber attacks under international law. It also analyses the measures in dealing with cyber attacks at the international level. This includes countermeasures, the principle of state responsibility, the development of international legal and non-legal framework and international criminal law.

Finally, chapter 7 provides the summary of the findings and outcomes of the study. It also considers several recommendations for future research.

This thesis has sought to state the law as at 31 December 2016.

Chapter 2

Methodology

2.1 Introduction

As stated in chapter 1, this study adopted socio-legal research approach in examining the measures to counter cyber attacks in Malaysian law. This methodology is used to address the questions about law by black-letter lawyers and to examine central issues in social theory.[1] Social science is perceived as an instrument that can be used to tackle legal concerns.[2] This is based on the notion that 'one must acknowledge a wider context to law and legal institutions, but without engaging with the many theoretical and political debates in sociology about how to understand society'.[3] Various methods can be used to conduct a socio-legal research Including: statistical analysis of survey research; analysing transcripts from tape-recording of judicial hearings; discourse analytic methods in studying legal texts; in-depth interviews and group discussion.[4] This study adopted doctrinal analysis, policy transfer and empirical fieldwork in examining the objectives of the thesis. More detail on the methodology used in this study is provided in this chapter.

2.2 Doctrinal Analysis

Doctrinal analysis was used to identify the latest developments and discussions on the background of the phenomenon of cyber attacks. This is necessary in order to delimit the parameters of the research as doctrinal analysis 'brings consistency and coherence to a set of rules that might

[1] Banakar R and Travers M, 'Socio-Legal Research in the UK' in Banakar R and Travers M (eds), *Theory and Method in Socio-Legal Research* (Hart Publishing 2005) 279

[2] ibid

[3] ibid

[4] Banakar R and Travers M, 'Law, Society and Method' in Banakar R and Travers M (eds), *Theory and Method in Socio-Legal Research* (Hart Publishing 2005) 17-18

appear at first glance to be an unrelated or jumbled mass'.[5] The researcher examined the documents from various disciplines including law, politic, sociology and computer science. Legal doctrinal analysis was used primarily for identifying the objectives of the rules and the values that they reflect upon. The legal system recognises individual rights including free speech, equality and due process.[6] In addition, the law has to comply with the demands of the inner morality of the law including coherence, clarity and publication.[7] They may serve a variety of the substantive aims of law with equal efficacy.[8] Fairness and effectiveness are an essential part of the doctrinal analysis in this study.

Several primary and secondary documents had been referred to in this study. They were selected due to their connection with the objectives of the thesis including the enforcement of the law in relation to cyber attacks. This study scrutinised primary data such as the Rome Statute of International Criminal Court, Charter of the United Nations, other relevant international instruments, policies adopted by regional organisations (EU and ASEAN), cases and legislations in Malaysia and UK. Secondary data such as articles, law reviews, journals, textbooks and other legal information were assessed in order to understand further the subject matter of this research. These data are also important sources in discovering the societal values and fairness.

The primary and secondary data were subjected to various canons of legal interpretation, to determine its scope, application and limitation. International instruments were downloaded from the websites of the United Nations, the International Criminal Court, EU and ASEAN. Cases and legislation in Malaysia and UK were found in online journal such as the Malayan Law Journal, Current Law Journal and LAWNET. Primary and secondary data were located in online databases such, as LexisNexis, Heinonline and Westlaw. The data was accessed through the browser of Leeds University

---

[5] Morris C and Murphy C, *Getting a PhD in Law* (Hart Publishing 2011) 31

[6] Dworkin R, *Taking Rights Seriously* (Duckworth 1997) 184

[7] Fuller LL, *The Morality of Law* (New Haven and London, Yale University Press 1964) 42

[8] ibid 153

Library and Faculty of Law Universiti Teknologi MARA Library. This study used the general principles in Oxford University Standard for Citation of Legal Authorities (OSCOLA) as the guide for the citation of the primary sources and secondary sources.[9]

2.3 Policy Transfer

This study assessed the feasibility of transferring the strategy to counter cyber attacks from the UK to Malaysia. The purpose of studying policy transfer is to examine the emergence and promotion of competing models to see how they can be connected to a particular problem.[10] The process starts with identifying the 'problem stream' that caused the concern of the policy makers and garnering responses from policy makers and politicians, which is also known as the 'policy stream'.[11] The adoption of a policy also depends on the 'political stream' or the structure of the political institutions of the state.[12] 'Policy instruments' which include the administrative and judicial organs are used to implement 'policy content' such as statutes, administrative rules and the court rulings.[13]

On the other hand, comparative legal analysis requires the researcher to 'confront any assumptions (often unconscious) about how legal systems should operate'.[14] Bell asserted that questions about the justifiability of differences, equality, and efficacy of the law are raised by looking at legal system of various states.[15] This approach was not adopted in this study, as it

---

[9] Meredith S and Nolan D, 'Oxford University Standard for the Citation of Legal Authorities Fourth Edition' (*Faculty of Law, University of Oxford*, February 2012) <https://www.law.ox.ac.uk/sites/files/oxlaw/oscola_4th_edn_hart_2012.pdf> accessed 15 March 2017

[10] Jones T and Newburn T, 'Comparative Criminal Justice Policy Making in the United States and the United Kingdom: The Case of Private Prisons' (2005) 45 Brit J Criminol. 58

[11] ibid

[12] ibid

[13] ibid

[14] Morris C and Murphy C, *Getting a PhD in Law* (n 5) 37

[15] Bell J, 'Legal Research and Comparative Law' in Hoecke MV (ed), *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline* (Hart Publishing 2013)

sought to identify the source of a policy transfer in order to improve and criticise the measures to counter cyber attacks in Malaysia.

Various laws from the UK have been transferred to Malaysia in the past. Therefore, this study analysed whether it is desirable for Malaysia to make further transfers with regards to policies relating to cyber attacks. The UK has been chosen in this study due to two main reasons. Firstly, Malaysia and the UK share common legal and administrative heritage. The Malaysian legal system is a mixture of the English common law, written constitution, Islamic law and local customary law.[16] The English common law is deeply embedded in the Malaysian law. [17] The penal system of Malaysia, Companies Act 1965 and Contracts Act 1950 are largely based on the British system. The application of the English law in Malaysia is governed under section three and section five of the Civil Law Act 1956. The common law of England and the rules of equity as administered in England on the 7 April 1956 are applicable in Peninsular Malaysia. [18] Even though the Malaysian legal system particularly the criminal law has developed its own jurisprudence, Malaysia still looks to England for its legal inspiration.[19]

Secondly, the UK is more advanced and powerful country especially in the area of cyber security. The UK is interested in becoming the forerunner in the developing cyber weapons and devising security measures against cyber attacks. Furthermore, cyber security is an issue that has attracted the attention of the policy makers both in Malaysia and the UK. There are convergences and divergences in the way both countries dealt with this problem. For instance, both countries rely on security professionals such as CERT to enhance their defence against future cyber attacks.

This study used doctrinal analysis to identify the strategy and the law in the UK that may be implemented in Malaysia in relation to cyber attacks. The selection was made on the basis of fairness and effectiveness. The adoption

---

[16] Sahamid B, *Jurisprudens dan Teori Undang-undang dalam Konteks Malaysia (Jurisprudence and Legal Theories in Malaysia)* (Sweet & Maxwell Asia 2005) 4

[17] ibid 27

[18] Section 3, Civil Law Act of Malaysia

[19] Hickling RH, *Essays in Malaysian Law* (Pelanduk Publications 1991) 251

of any foreign policies must be done carefully due to the different social and economic backgrounds of both countries. For instance, the UK and Malaysia may have different understanding of the concept of national security. In the UK, national security means protection against terrorism or foreign invasion. Whereas, in Malaysia, national security has a broader meaning in which it covers areas including maintaining racial harmony and protection of Muslim ideology. Despite those differences, Malaysia is receptive to emulate the measures adopted by UK due to the similarity of the administration of criminal justice.

2.4 Empirical Fieldwork

Empirical research is defined as 'the systematic collection of information and its analysis according to some generally accepted method'.[20] Socio-legal researchers may employ quantitative or qualitative methods or a combination of both methods. The main distinction between qualitative and quantitative methods is the usage of numerical data. In quantitative research numerical data is required whereas a qualitative researcher 'does not have to work with numerical data in his research project'.[21] Quantitative research 'involves choosing subjects, data collection techniques, procedure for gathering data, and data analysis techniques'.[22] The objective is 'to classify features, count them, and construct statistical models in an attempt to explain what is observed'.[23] On the other hand, qualitative researchers examine the participants' perspectives towards events, belief or practices.[24] In the context of legal research, it enables the researchers to obtain in-depth meaning of the experience of individuals and their perceptions of the justice

---

[20] Cane P and Kritzered HM (eds), *The Oxford Handbook of Empirical Legal Research* (Oxford University Press 2010) 4

[21] Awang ZH, *Research Methodology for Business and Social Science* (UPENA UiTM 2011) 83

[22] Singh P, Chan YF, Sidhu GK, *A Comprehensive Guide to Writing A Research proposal* (Venton Publishing 2006) 107

[23] Noor NM, *Writing Research and Thesis Proposals: Guidelines and Examples* (UPENA UiTM 2011) 156

[24] ibid

system.[25] The researchers may also learn how the participants interact with each other and their point of view pertaining to the events that happens around them.

This research adopted the qualitative methodology as it provides a deeper understanding of social phenomena particularly of the assessment of the legal norms concerning the articulation of cyber attack as crimes. The researcher was able to gain original information concerning cyber attacks, which cannot be found elsewhere. On that basis, in depth interviews involving thirty-two participants were done to obtain the required data for this study. The quantitative methodology is not so suitable, as numerical data only probably explains the incidence of cyber attacks. The researcher may only obtain a general and superficial understanding of cyber attacks by using quantitative methodology. Furthermore, cyber attacks are highly to be underreporting. In addition, due to time and financial constraint, the researcher cannot afford to extract data and from multiple sources.

2.4.1 Interviews

Interviews were chosen as the method for this study due to several reasons. Interviews are more pragmatic in comparison to other methods of collecting verbal data such as a focus group. Individual interviews allow the researcher to approach the participants face to face in order to gain vital information based on their experience. Webley argues that 'interviews are extremely effective at garnering data on individuals' perceptions or views and on the reasoning underlying the responses.'[26] Furthermore, interviews were more feasible in terms of logistic and time management as the fieldwork is conducted in the beginning of the third year of this study.

The semi structured interview was chosen as it gives the researcher the opportunity to explore in depth the subject matter of the research based on the opinion given by the experts. The results can still be compared even though the interviewer permits the participants to answer more on their own

[25] Webley L, 'Qualitative Approaches to Empirical Legal Research' in Cane P and Kritzered HM (eds), *The Oxford Handbook of Empirical Legal Research* (n 20) 928

[26] ibid 937

terms.[27] This method enabled the researcher to design the structure and the forms of the interview for the purpose of aiding the interviewee to articulate his or her view. In comparison to unstructured interview, 'the context of the interview is an important aspect of the process'.[28] Semi-structured interviews provide a balanced outcome due to the need to reflect the set agenda of the thesis and the need for comparability. Furthermore, the semi-structured interview is 'sufficiently structured to address specific topics related to the phenomenon of study while leaving space for participants to offer new meanings to the study'.[29]

Despite these advantages, there are several limitations in using interviews for gathering data. Firstly, the reactive effects during the interview may impair the findings of the fieldwork. The interviewees may act differently from what they said during the interview. They may be influenced by social desirability due to the presence of the interviewer and the interview questions. Thus, they tend to provide the expected answers during the interview. The researcher was aware of this issue. She overcame the difficulties by not relying on specific individuals in her sampling strategy. In addition, she compared the answers in order to check their credibility. She carefully constructed her questions to ensure that they were not leading. She did not make her personal opinion apparent at any point during the interview.

The next limitation is the tendency for the interviewees to be too much guided by the set agenda. The usage of semi-structured interview with a set of agenda may restrict the findings of the research. This can be solved through the inclusion of alternative questions in the interview guide or the elimination of confrontational questions from the interview.[30] The researcher used several measures to overcome this limitation. The Interview guide was devised to include some open questions. In addition, the researcher encouraged the interviewees to add points, which may depart from the

[27] May T, *Social Research: Issues, Methods and Process* (2nd edn, Open University Press 1997) 111

[28] ibid 112

[29] Galletta A, *Mastering the Semi-structured Interview and Beyond* (New York University Press 2013) 24

[30] Flick U, *An Introduction to Qualitative Research* (Metzler K ed, 5th edn, Sage 2014) 219

agenda of the interview. Besides that, different interviewing techniques were used to encourage responses from the interviewees. The researcher devised vignette questions to illustrate the different scenery or factual situations of cyber attacks. She also stipulated the different measures to counter cyber attacks on cards. The interviewees were asked to determine the rank of the measures by arranging the cards. They were also requested to compare and contrast the measures to counter cyber attacks. The researcher was able to discern the dynamics between criminal enforcement and other alternative measures by engaging the interviewees.

Another limitation is that the interviewer's bias may affect the interview. The interviewer's characteristics, behaviour and conduct during the interview may influence the responses of the interviewee. The interviewer may not even realise her peculiarity that affects the outcome of the interview. Personal bias may stem from various issues including race, gender, political sensitivity, culture of secrecy and confidentiality.

The interviewer's personal feeling should be set-aside during the interview. Rubin suggests that the researchers have to examine their own understanding and reactions continuously rather than pretending that the come into the situation without any biases.[31] Responsive interviewing emphasises that 'the interviewer and the interviewee are both human beings, not recording machines and that they form a relationship during the interview that generates ethical obligations for the interviewer'.[32] Understanding personal biasness enabled the researcher to be more cautious in conducting the interview and during the write up.

2.4.2 Interview Guide

The interview guide consists of a series of questions or a list of topics designed by the interviewer to elicit the interviewee's experience and knowledge in the subject matter of the research. The questions encompass all topics relevant to the research including the basic biographic information of the interviewer. In this study, the interview focused on the development of

[31] Rubin HJ and Rubin IS, *Qualitative Interviewing. The Art of Hearing Data* (2nd edn, Sage 2005) 31

[32] ibid 30

the concept of cyber attacks, the usage of non-criminal measures, the imposition of criminal liability for cyber attacks and enforcement mechanism for cyber attacks in Malaysia. These headings contain multiple research questions.

The aim of the interview was to elicit detailed, deep and nuanced answers. The detail was obtained by encouraging the interviewees to provide specifics and important information, which may initially be perceived as trivial matters. The interviewees were encouraged to provide nuanced answers. This is necessary in order to 'avoid yes or no, black or white responses'.[33] Probes are spontaneous interventions used by the interviewer to stimulate in depths information in the interview. [34] Probes were used to seek further clarification and stimulate in depth discussion. The sequence and forms of the questions can be changed to follow up the answers given and the stories told by the subjects.[35] The interview guide is attached in Appendix A.

2.4.3 Sampling Strategy

Purposive sampling 'involves deliberate selection of individuals for a particular purpose'.[36] The researcher uses his or her judgment based on a certain elements such as the uniqueness of the sample's position. [37] Purposive sampling was used in this study as it allows in depth understanding of the phenomenon of cyber attacks despite the restriction in terms of generalisation of the outcome. However, the findings are still highly significant as the purpose of the research is to explore and to gather the views of the experts on cyber attacks in Malaysia. Furthermore, the findings can be compared with the observations derived from doctrinal research and policy transfer.

Besides purposive sampling, snowballing techniques was used in this study. In snowballing sampling, the researcher was led or referred to more potential

---

[33] ibid

[34] Jupp V, *Methods of Criminological Research* (Routledge 1989) 208

[35] Kvale S, *Interviews: An Introduction to Qualitative Research Interviewing* (Sage Publications 1996) 124

[36] ibid

[37] Bachman R and Schutt RK, *The Practice of Research in Criminology and Criminal Justice* (5th edn, Sage 2014) 119

subjects by the interviewees. This strategy may be influenced by the participants' bias, as they tend to recommend people who share their thoughts on the subject of the research.[38] However, bias can be reduced by stipulating clear instructions on the characteristics of the participants sought for the interview.[39] Snowballing sampling was also employed in order to generate more subjects for the interview. This technique was useful due to the researcher unfamiliarity with the experts in this field. Furthermore, the recommendation given by the interviewees strengthen the credibility of the proposed subjects.

Several factors were considered in choosing the interviewees. The data were collected from interviews with individuals who are familiar with the concept of cyber attacks. They are also involved in cyber security and criminal enforcement in Malaysia. At the same time, the interviewees' diverse background contributes to the richness and enhances the credibility of the research. Thus, the interviewees' experience and professions are the essential criteria in selecting the sample. The complexity of responsive interviewing is portrayed through overlapping perceptions and nuanced understanding of different individuals.[40] In order to explore the issues related to the imposition of criminal liability and enforcement for cyber attacks, the sample comprises of the representatives from the policy makers, national policing and military, and security professionals.

Thirty-two participants from the public and private sectors were interviewed over a three-month period. The ratio of the participants from these sectors was balanced. The participants were selected based on the type of data and the ability to provide the required information for the research. They came from various field related to the cyber security and data users such as telecommunication, Internet service providers and private security companies. The number of participants allowed for in-depth assessment and alternative views on criminal enforcement measures against cyber attacks.

---

[38] King N and Horrocks C, *Interviews in Qualitative Research* (Sage Publications 2010) 34

[39] ibid

[40] Rubin HJ and Rubin IS, *Qualitative Interviewing. The Art of Hearing Data* (n 31) 67

The numbers were also feasible due to time and budget constraint as the interviews was conducted in the area of Putrajaya, the administration centre of Malaysia, and Kuala Lumpur, Malaysia. The number of interviews in each category is shown in Table 2.1.

Table 2.1-Categorisation of research participants (Malaysia)

Category	Number of interviews
Policymakers	4
Policing	3
Prosecution	4
Legal practitioner	4
Military	1
Security professionals	11
Public and private sector officers (IT, operation or security departments of critical infrastructure and services such as telecommunication.	5
	Total: 32 interviews

Several problems may arise in conducting expert and elite interviews. They may be too busy to talk or 'want to control what is said about them, and they have staff who buffer them'.[41] Another problem is the time pressure, as 'expert interviews often have to be calculated and run much tighter than other form of interviews'.[42] However, these problems were not major obstacles for the research. The researcher took several steps to overcome them including using the snowball sampling.

2.4.4 The Process of Gaining Access for Fieldwork

A formal request to interview was made to the subjects and the institutions. This is essential as a research may disturb and 'disrupts routines, with no perceptible immediate or long term-payoff for the institution and its members'.[43] For this study, the request was made through an official letter using the University of Leeds letterhead. The letter indicated the

[41] ibid 94

[42] Jupp V, *Methods of Criminological Research* (n 34) 231

[43] Flick U, *An Introduction to Qualitative Research* (n 30) 160

interviewer's interest in the work of the interviewee and guarantees that the information obtained is subjected to his wishes.[44]

Before the request was submitted, an enquiry was made on the procedural requirement of each institution for conducting interview. This includes the process of gaining access to the subjects of the interview. For instance, the consent of the Attorney General is required before interview can be conducted with the officers from the Attorney General's Chamber.

2.4.5 Data Analysis Strategy

Data analysis involves the 'process of moving from raw interviews to evidence-based interpretations that are the foundation for published reports'.[45]. The questions for the interviews were designed to encapsulate the objectives and aim of the research as indicated in the interview guide. The interviews were conducted according to the schedule stipulated in the interview guide. Upon completion, the results were analysed to understand the perception of the participants on the nature of cyber attacks, the measures that are used to counter this problem and the feasibility of criminal law in dealing with cyber attacks.

In this study, data analysis was performed in several stages, starting from recording, coding, sorting the data and finally theming. Notes and recordings are used to record the data during the initial stage. Audio recording is necessary in qualitative research to encapsulate ' a full, accurate record of what the participant said'.[46] The recorded data is then transcribed into text before being analysed. The main issue concerning transcription is 'whether you transcribe every second of every interview word for word (verbatim) and to what level of detail you need to transcribe'.[47] The level of the detail for transcription includes any 'information that might influence the interpretation, such as laughter or gestures of emphasis or puzzlement'. [48] Recording in

---

[44] Rubin HJ and Rubin IS, *Qualitative Interviewing. The Art of Hearing Data* (n 31) 94

[45] ibid 201

[46] King N and Horrocks C, *Interviews in Qualitative Research* (n 38) 47

[47] ibid 143

[48] Rubin HJ and Rubin IS, *Qualitative Interviewing. The Art of Hearing Data* (n 31) 204

verbatim is necessary for studies involving in depth personal experience using narrative and phenomenological approaches.[49] However, the process of transcribing is time consuming especially for studies involving a large number of interviews. Thus, the transcription for this study focuses on the selected areas of interest which have been identified after listening to the recording several times.

The fieldwork added the values to the research questions. The researcher looked for things that are frequently mentioned or emphasised by the interviewees. The data revealed certain themes that address the objectives of the research. The thematic patterns are often referred to as codes.[50] They were coded based on their relationship with the objectives of the research. The codes were also located in the relevant chapters of the thesis. They were further coded according to the categories of the interviewees. The study compared and contrasted the codes in order to develop commonalities and to generate meaning.[51]

2.4.6 Ethical Issues

This research was conducted in accordance with the University of Leeds Research Ethics Policy and the Code of Ethics of the British Society of Criminology.[52] The researcher is required to conduct her research with integrity and sensitivity; compliance with legislation; regard for vulnerable subjects and obtaining informed consent. The participants have the rights to give, refuse and withdraw their consent to take part in the research projects. Besides that, the researcher has to ensure and safeguard the security, safety and the anonymity of the participants. The participants must be given the opportunity to raise queries, concerns or complaints.

The main ethical issues, which arose in this study, are confidentiality and anonymity as some of participants are high rank government officers and hold top position in their respective organisations. They have been given the

---

[49] King N and Horrocks C, *Interviews in Qualitative Research* (n 38) 143

[50] Galletta A, *Mastering the Semi-structured Interview and Beyond* (n 29) 122

[51] ibid 126

[52] Code of Ethics for Researchers in the Field of Criminology *(British Society of Criminology)* <http://britsoccrim.org/docs/CodeofEthics.pdf> accessed 12 July 2014

responsibility to manage sensitive information relating to cyber security in Malaysia. Thus, for government officers, they are bound under their oath of secrecy not to reveal any information that may jeopardise the security of Malaysia. They also have to follow a certain code of practice set by the government, which dictate the types of information that can be revealed to the public. Similarly, for the interviewees who are working in the private sectors, they are bound by their contractual obligation not to disclose confidential information of the company. They are also at risk of being implicated as endorsing movements with a certain political agenda. Thus, several measures had been considered during the different stages of the interview, which includes informed consent, confidentiality and data protection.

2.4.7 Informed Consent

The researcher is required to inform the subjects about 'the overall purpose of the investigation and the main features of the design, as well as of any possible risks and benefits from participation in the research'. [53] The participation of the interviewees was voluntary. They were requested to fill in the consent form after they fully understand the nature and the repercussion of the research. The participants were entitled to withdraw within two weeks from the date of the interview. The duration is sufficient as the identities of the participants is not revealed and remain anonymous. Sufficient time was allocated to the subjects to reflect upon any information given to them.[54] The participants of this research were provided with an information sheet containing the aims and objectives of the study. A copy of the information sheet and the consent form are attached Appendix B.

2.4.8 Confidentiality and Data Protection

Researchers have the obligation not to reveal private data identifying the subjects. The subjects' consent must be obtained prior to the publication and the release of identifiable information.[55] Since this study involves a small

---

[53] Kvale S, *Interviews. An Introduction to Qualitative Research Interviewing* (n 35) 112

[54] Annex III: Policy Notes, The University of Leeds Research Ethics Policy

[55] Kvale S, *Interviews. An Introduction to Qualitative Research Interviewing* (n 35) 114

group of experts from the public and private sectors, there is a risk that they may be identified as not many people work in the area of cyber security. Thus, several precautionary measures had been taken in order to maintain their anonymity. For instance, details such as the name of the organisation and the city are not revealed.

The participants were assured that the information given is confidential and will be kept according to the university's regulation. All data obtained from the interview and questionnaires were anonymised and codified immediately. The researcher was using a digital voice recorder for the interviews. The records were kept in the researcher's personal computer before being transferred to her network drive at the University of Leeds. For safety purposes, the researcher installed encryption programme in her personal computer. The electronic storage system of the university is password-protected. Thus, all data generated from the interview including tape recordings, transcripts, personal address, emails, telephone numbers and faxes were stored on the university's network for security and to prevent unacceptable disclosure. Any printed material was kept in a locked filing cabinet and will be destroyed upon the completion of the research. The researcher will only reveal the gender, age and role of the participants for publication purposes, when the text requires direct quotation from the participants. The data obtained during the interview will be kept for three years from the date of her graduation and then destroyed.

2.4.9 Risk Assessment

A researcher must not overlook the importance of ensuring safe environment in conducting research especially if the fieldwork is done in unfamiliar surrounding. Potential risks need to be assessed before embarking on the fieldwork. The researcher took several precautionary measures during her fieldwork. For instance, she informed her supervisors and friends of the time and place of the interview. The Faculty of Education, Social Sciences and Law of the University of Leeds provides extensive guideline on risk assessment to researchers. The risk assessment form had to be submitted to the related department. In addition, the form had to be taken to the field so that any changes can be recorded.

2.5 Conclusion

This chapter elaborates the methodologies used in this study. Apart from doctrinal analysis and policy transfer, qualitative methodology is used as it enables the researcher to explore cyber attacks from various perspectives including the criminal justice system. Thirty-two participants had been chosen for the interview based on their background by using the purposive and snowballing sampling. The main criteria for selecting the participants were their knowledge of cyber security and the enforcement of the criminal law. Semi-structured interviewing was used in gathering the data as it provides the researcher with in depth knowledge on the area of the study.

The researcher faced several methodological challenges in conducting the empirical fieldwork. This includes the reactive effects during the interview and the tendency of the findings of the research to be restricted by the agenda of the interview. She overcame these challenges by taking practical steps including using different interview techniques, ensuring that the questions were not leading and devising open questions. As an example of the questions to be adaptive and flexible, the initial findings suggested that the law enforcement officers and some of the security professionals considered online sedition and defamation as cyber attacks. The researcher had not addressed this issue in her interview schedule. As a result, the supervisee was unprepared and had to make changes to some of the interviews. This discovery leads to the adjustment of the data collection and analysis especially on the conceptual framework of cyber attacks in chapter 3.

Apart from methodological challenges, ethical issues are very important in conducting empirical legal research. The researcher ensured the integrity and credibility of her research by complying with University of Leeds Research Ethics Policy and the Code of Ethics of the British Society of Criminology.

Chapter 3

The Concept of Cyber Attacks

3.1 Introduction

This chapter investigates the nature of cyber attacks especially in Malaysia. This is necessary for the purpose of policy-making, formulating the law and planning resilient measures. Scholars such as Ophardt acknowledge the difficulty in formulating the exact definition of cyber attacks.[1] Some argue that they exist as a separate category of security threat, whereas others categorise them based on the identity of the perpetrators; the motives; the targets and degree of harm.[2] Describing the phenomenon of cyber attacks is not straightforward due to the absence of a consensus on the definition of cyber attacks. The lack of definition may be intentional due to political considerations. For instance, the adoption of UN Security Council's Resolution 1373 depends on the absence of an agreed definition of terrorism. [3] However, the absence of a clear concept may affect the effectiveness of any programme of action.[4] Saul argued that criminal law 'shuns ambiguous or subjective terms as incompatible with principles of non-retroactivity and specificity'. [5] According to the EastWest Institute, the uncertainty in defining cyber attacks may obstruct the development of policy and may be 'clouding the application of existing legal system.'[6] Accordingly, this issue requires further clarification.

---

[1] Ophardt JA, 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield' (2010) 3 Duke L & Tech Rev 1, 2010

[2] ibid

[3] B Saul, *Defining Terrorism In International law* (Oxford University Press, 2006) 48, citing L Bondi, 'Legitimacy and Legality: Key Issues in the Fight against Terrorism', Fund for Peace, Washington, DC, 11 Sept 2002, 25

[4] Hathaway OA and others, 'The Law of Cyber-Attack' 100 Calif L Rev 817

[5] B Saul, *Defining Terrorism In International law* (Oxford University Press, 2006) 4

[6] Hudson A, 'Is Cyber-Warfare a Genuine Threat?' (*BBC Click*, 1 February 2011) <http://news.bbc.co.uk/1/hi/programmes/click_online/9393589.stm> accessed 15 January 2014

In the *Concept of Law*, Hart argues that a concise definition is not sufficient to encapsulate the underlying issues of the nature of law. He contends that definition is 'primarily a matter of drawing lines or distinguishing between one kind of thing and another, which language marks off by a separate word'.[7] Thus, definition cannot provide a satisfactory answer to the question of what is law. He suggests that the formation of a central set of elements in understanding the law would be preferable.[8] The concept of law may be used in understanding the connection between law, coercion and morality as 'types of social phenomenon'.[9] In this thesis, the concept of 'cyber attacks' represents the overview of the phenomenon of cyber attacks. Short sentence or phrase may not encapsulate the intricacy, complexity and various spectrums of cyber attacks. The government may use a concept in devising strategy and policy related to cyber security. However, it is not satisfactory to do so for legal purposes as criminal law 'shuns ambiguous or subjective terms as incompatible with principles of non-retroactivity and specificity'.[10] A precise definition is required for the imposition of criminal sanction and the creation of criminal offences.[11]

The analysis of the concept of cyber attacks is based on various instruments related to this study. In addition, the empirical data from the fieldwork is included to support the findings in this chapter. The participants were asked about the definition and constituents of cyber attacks. This chapter is structured as follows. Firstly, it conducts an ontological enquiry into cyber attacks. Next, it provides a summary of the concept of cyber attacks and then considers the categories of cyber wrongdoing.

3.2 Ontological Enquiry into Cyber Attacks

Cyber attacks connote the usage of cyberspace as the medium and platform to conduct hostile activities and confrontations. The word 'cyber' refers to the

[7] Hart HLA, *The Concept of Law* (2nd edn, Oxford University Press 1997) 13

[8] ibid 16

[9] ibid 17

[10] Saul B, *Defining Terrorism In International law* (n 5) 4

[11] *Del Río Prada v Spain* Application No.42750/09 (ECtHR, 21 October 2013)

characteristic of the culture of computers, information technology and virtual reality.[12] Cyberspace depicts the connection between computers and the people who use them. It portrays an abstract virtual space created in part by networks of interconnecting computers and in part by the human imagination.[13] It provides an electronically defined experience that renders human identity fluid, digitized, spatial, and integrated in non-physical realm.[14] Cyberspace is not just about machines and data. It has become an integral conduit of social interaction among the communities. Various official and private activities are conducted in cyberspace. This implies the existence of public and private realms in cyberspace.

Attacks denote strong opposition, aggressive and violent act against an entity. *A Dictionary of the Internet* defines attack as an attempt to overcome the security provisions of the network of a computer network.[15] Attacks can be active attack, which alter the data stored on the network, for example deleting a critical file, or passive attacks which just read sensitive data passing through transmission lines.[16] In addition, scholars such as Hathaway have adopted a narrow definition of cyber attack that focuses on the uniqueness of threat posed by cyber technologies.[17] She defined cyber attack as 'any action taken to achieve the objective of undermining the functions of a computer network for a political or national security purpose'.[18] Consequently, she argued that cyber attacks exist as a separate category from cyber warfare and cybercrime based on the objective of the attack.[19] The above interpretations of cyber attacks provide useful information in formulating the concept of cyber attacks. However, it does not encapsulate the full dimensions of cyber attacks.

---

[12] *The Concise Oxford English Dictionary* (11th edn, Oxford University Press 2008)

[13] Chandler D and Munday R, *A Dictionary of Media and Communication* (Oxford University Press 2011)

[14] Childers J and Hentzi G (eds), *The Columbia Dictionary of Modern Literary and Cultural Criticism* (Columbia University Press 1995)

[15] Ince D, *A Dictionary of the Internet* (3rd edn, Oxford University Press 2013)

[16] ibid

[17] Hathaway OA, 'The Law of Cyber-Attack' (n 4)

[18] ibid 5

[19] ibid

Therefore, this study examines the concept of cyber attacks through ontological enquiry. Ontology is concerned with the nature of existence and the categorical structure of reality.[20] Jacquette defines ontology as a 'method or activity of enquiry into philosophical problems about the concept or facts of existence'. [21] In *The Ontology of Cyberspace*, Koepsell examines cyberspace from an ontological point of view.[22] He defines legal ontology as 'a categorisation of legal objects as applied or embodied in legal system'.[23] He also argues that accurate ontology is important in guiding the common law and positive rule making to accommodate the challenge posed by rapid technological change.[24] Ontology is useful for the purpose of determining the factors in categorising objects including cyber attacks.

The variables for the classification of cyber attacks have to be identified in this enquiry. A particular act or thing can be identified by using 'common sense, knowledge of the general kind of things, appreciation of general character of the occasion and the kind of behaviour appropriate to it'.[25] Accordingly, the notion of cyber attack is predicated on the following variables: (1) the identity of the perpetrators, victims and the targets; (2) the methods, scale and impact of the attacks; (3) the motives of the attacks. These variables depict the general characteristics of cyber attacks and indicate the required responses to the phenomenon of cyber attacks.

3.2.1 The Identity of the Perpetrators

The first variable in formulating the concept of cyber attacks is the identity of the perpetrators. Results of the fieldwork revealed that the threats of cyber attacks might come from outside or inside of Malaysia. Security Professional 11 claimed that:

---

[20] Honderich T, *The Oxford Companion to Philosophy* (2nd edn, Oxford University Press 2006)

[21] Jacquette D, *Ontology* (Shand J ed, Acumen 2002) 3

[22] Koepsell DR, *The Ontology of Cyberspace. Philosophy, Law and the Future of Intellectual Property* (Open Court 2000)

[23] ibid 33

[24] ibid 122

[25] Hart HLA, *The Concept of Law* (n 7) 125

> In Malaysia, there has been claim by certain companies that the IP comes from US, Malaysia and China in the context of cyber attacks. However, cybercrimes mostly originate from Russia. It is the hotbed of illegal activities on cyberspace.[26]

Cyber attacks may be conducted through multiple identities using numerous computers connected by many networks residing in various countries.[27] The attackers may use web proxy services from Indonesia, China and Germany.[28]

The data also suggest that the attacks can be attributed to state and non-state actors. However, it is difficult to identify the identity of the perpetrators as everyone with a computer connected to the Internet can carry out harmful attacks for various purposes ranging from 'juvenile hacking to organised crime to political activism to strategic warfare'.[29] According to Policymaker 3:

> The sources of the attacks can be identified from the IP. Based on the IP, the attacks always come from outside. MYCERT and MCMC are responsible to monitor the attacks. However, we cannot distinguish whether state or non-state actors committed them.[30]

Despite numerous speculations, it remains unclear whether the attacks on Estonia, Georgia and Iran could be legally attributed to an identifiable entity.[31] Military Officer 1 argued that:

> Cyber activisms often come from a group located in multiple places around the globe. Cyber espionage, on the other hand, often relates to a specific state actor. There is a grey line

---

[26] Interview with Security Professional 11

[27] Caton JL, *Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations, And Response Implications* (United States Army War College Press, 2014)

[28] Interview with Security Professional 2

[29] Cavelty MD, 'Cyber Threats' in Cavelty MD and Mauer V (eds), *The Routledge Handbook of Securities Studies* (Routledge 2010) 45

[30] Interview with Policymaker 3

[31] Kessler O and Werner W, 'Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare' (2013) 26 Leiden Journal of International Law 793

> between state and non-state actors attributes. A government may employ free agents to launch its cyber campaign while a non-state actor may launch an attack in the name of a government. Attacker's profile may vary from script kiddies, cyber activists to advance persistent threat actors.[32]

The government has the duty to identify and investigate the sources of the attack.[33] Security Professional 11 argued that the government plays a vital role in tracing the perpetrators:

> If you are looking at it from top down, the government has the clearance and authorisation. It can be done at this level. The government may instruct the law enforcement agency and corporations such as the ISP to collaborate in order to trace the perpetrators.[34]

However, the enforcement of the law is difficult due to the anonymity of the perpetrators especially if the attacks originate from outside of Malaysia. Security Professional 10 asserted that:

> Preventive measures are more effective than criminal law in relation to the attacks from outside of Malaysia. It is difficult to identify the wrongdoer it the attacks are committed through a network outside of Malaysia.[35]

The difficulty in the enforcement of the law is reflected in the climate change incident. It was reported that the server of the University of East Anglia's Climatic Research Unit had been hacked.[36] Some emails had been published in the website of a company in Russia. Upon investigation, the IP address of the attacker has been traced back to Kuala Lumpur, Malaysia.[37]

---

[32] Interview with Military Officer 1

[33] Interview with Military Officer 1

[34] Interview with Security Professional 11

[35] Interview with Security Professional 10

[36] Black R, 'A Brief History of Climate Change' (*BBC News Science and Environment*, 20 September 2013) <http://www.bbc.co.uk/news/science-environment-15874560> accessed 14 January 2014

[37] Rainsford S, 'Hackers for Hire' (BBC World Service Assignment 14 March 2010) <http://www.bbc.co.uk/programmes/p006j7qf> accessed 14 January 2014

So far, no attempt has been made to contact the Malaysian authorities to investigate the incident further.[38] The perpetrators have not yet been arrested.

This demonstrates that cyber attacks may originate from outside or inside Malaysia. The former may be orchestrated by foreign entities such as governments and terrorists groups.[39] Meanwhile, individuals and corporations may commit the latter. Accordingly, this chapter now divides the potential perpetrators of cyber attacks into several categories: states, hackers and hacktivists, terrorists and other entities including criminals, corporation and insiders.

3.2.1.1 States

Cyber attacks have been increasingly acknowledged as a new technological method to wage war and pursue public policy goals. Caton predicts that the 'future trends are toward more destructive cyber conflicts with more disruptive, covert and offensive cyber operations'.[40] Possessing the most modern weapons available is perceived as the best guarantee for the security of the state.[41] The results of the study showed that most of the participants from all categories agreed that states may orchestrate cyber attacks. According to Deputy Public Prosecutor 1:

> When I think about cyber attacks, I would think of the access to our SCADA system such as water and electricity. It implies the involvement of foreign government or hostile foreign powers.[42]

States may use cyber attack as an instrument to further their political agenda. Deputy Public Prosecutor 2 argued that:

> Cyber attacks can be legal or illegal. Some people claimed that cyber attacks happened when the government shut down

---

[38] ibid

[39] GCHQ, 'Common Cyber Attacks: Reducing the Impact' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf> accessed 23.02.2015

[40] Caton JL, *Distinguishing Acts of War in Cyberspace* (27) 6

[41] Eijkelhof HMC and others, 'Weapons' (1982) 2 Bulletin of Science Technology & Society 1982 2: 59

[42] Interview with Deputy Public Prosecutor 1

> certain websites like the Sarawak Report. Cyber attacks are conducted through computers, the Internet and web applications. Shutting down online newspapers is legal cyber attacks as it is done upon the instruction of the government.[43]

States may also use cyber attacks to promote their foreign policy. Caton argued that the disruption of the Ukrainian communication networks by using DDOS attacks and the Snake malware was done to enable surveillance activities.[44] In addition, Stuxnet had been used by the US to halt the development of Iranian nuclear capability.[45]

Cyber espionage is done to gather information on the latest technology developed for commercial and military purposes by another country. Corrupted insiders and foreign intelligence services steal and transfer massive quantities of data while remaining anonymous.[46] It has been argued that the usage of malware for spying and exfiltrating data from a network is not considered as cyber attacks, as it does not cause sufficient harm.[47] However, cyber espionage has been considered as a threat to the national security and economy.[48] For instance, the theft of military technology can jeopardise a country's ability to export high-tech products and advanced materials.[49] Espionage via computer does not violate international law.[50]

---

[43] Interview with Deputy Public Prosecutor 2

[44] Caton JL, *Distinguishing Acts of War in Cyberspace* (n 27) 6

[45] Muti A, Tajer K and Macfaul L, 'Cyberspace: An Assessment of Current Threats, Real Consequences and Potential solutions in New Ways of War: Is Remote Control Warfare Effective' [2014] The Remote Control Digest

[46] Office of the National Counterintelligence Executive, 'Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage'< *2009-2011*, http://www.ncix.gov/publications/reports/fecie%5fall/Foreign%5fEconomic%5fCollection%5f2011.pdf> accessed 23.04.2015

[47] Rid T and Mcburney P, 'Cyber-Weapons' (2012) 157 The RUSI Journal, 157:1, 6-13; see also Hathaway OA, 'The Law of Cyber-Attack' (n 4)

[48] Home Office UK, 'A Strong Britain in an Age of Uncertainty: The National Security Strategy', <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf> accessed 23.04.2015

[49] McAfee and Centre for Strategic and International Studies, 'The Economic Impact of Cybercrime and Cyber Espionage [2013]',

However, cyber espionage particularly industrial espionage is a criminal offence in countries such as the US. This is elaborated in the following section.

3.2.1.2 Hackers and Hacktivists

Hackers are described as 'an inquisitive or perhaps malicious meddler who tries to discover information about computers by gaining unauthorised access to them and exchanging intelligence with other like minded people'.[51] Williams describes the invasion of private space on the Internet by hackers as cyber trespass.[52] However, Wall argued that this term 'does not carry the emotional and ideological baggage that comes with the term hacking'.[53] Thus, cyber trespass refers to a wider range of attacks upon the computer system.[54] Hacking is done for various reasons including self-enrichment.[55] The juvenile hackers may be involved in hacking due to problematic family backgrounds and peer association.[56] However, not all hackers are bad as some of them are bound by self-imposed ethics.[57] They would explore others' computer systems out of curiosity and share their findings.[58] Any damage to the computer system while hacking is perceived as unethical and incompetent.[59]

<http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime.pdf> accessed 24.04.2015

[50] Dunlap JC Jr, *The Law and the Human target in Information Warfare: Cautions and Opportunities* in Campen AD and Dearth DH (eds), *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict* (AFCEA International Press, 2000) 141

[51] Wasik M, *Crime and the Computer* (Clarendon Press 1991) 18

[52] Williams M, *Virtually Criminal: Crime Deviance and Regulation Online* (Routledge 2006) 22

[53] Wall DS, *Cybercrime. The Transformation of Crime in the Informative Age* (Polity Press 2007) 53

[54] ibid

[55] Williams M, *Virtually Criminal: Crime Deviance and Regulation Online* (n 52) 22

[56] Yar M, 'Computer Hacking: Just Another Case of Juvenile Delinquency?' The Howard Journal Vol 44 No 4 September 2005

[57] Taylor PA, *Hackers* (Routledge 1999) 26; see also Wall DS, *Cybercrime. The Transformation of Crime in the Informative Age* (n 53) 55

[58] Yar M, 'Computer Hacking: Just Another Case of Juvenile Delinquency?' (n 56)

[59] ibid

Unlike hackers, hacktivists conduct their activity in furtherance of political agenda. According to Taylor, hacktivists oppose the re-establishment of traditional values based upon physical property rights in the information society, which is supposedly 'predicated upon the bodiless transportation of data streams'.[60] They also object to the information-gathering activities by the government bureaucrats.[61] Hacktivists are not perceived as terrorists as they do not intent to kill, maim or terrify.[62] They usually carry out: virtual sits-in and blockades, automated e-mail bombs; web hacks and computer breaks-in; computer viruses and worms.[63] However, the police may exercise their power to determine whether a hacktivist fall within the purview of the terrorism legislation. [64] Furthermore, hacktivists may be classified as terrorists if they possess or published material that may endanger a person's life, or created a risk to the health or safety of the public.[65]

Hacktivists such as Anonymous have gained a reputation for orchestrating several attacks. Anonymous consists of hackers who share similar ideals and aims. However, they do not have organisational structure and operate loosely.[66] Anonymous is allegedly responsible for sabotaging the websites of MasterCard, Visa and PayPal for their refusal to process donations to anti-secrecy organisations including the WikiLeaks. [67] Anonymous is also infamously known for the Denial of Service attacks on the websites of the Church of Scientology. The attacks were done in response to the attempts by the Church of Scientology to prevent the spread of a video interview with

---

[60] Taylor PA, *Hackers* (n 57) 26

[61] ibid 26

[62] Weimann G, 'Cyberterrorism: How Real is the Threat?' (2004) The United States Institute of Peace Special Report 119

[63] ibid

[64] *Regina (Miranda) v Secretary of State for the Home Department and another (Liberty and Others intervening)* [2016] 1 W.L.R. 1505

[65] ibid

[66] The Telegraph 'Who are Anonymous?', <http://www.telegraph.co.uk/technology/internet/8653447/Who-are-Anonymous.html> accessed 1.03.2015

[67] The Telegraph 'WikiLeaks Cyber Attacks Like 'Nuclear Weapon'' <http://www.telegraph.co.uk/news/worldnews/wikileaks/8193134/WikiLeaks-cyber-attacks-like-nuclear-weapon.html> accessed 1.03.2015

Tom Cruise online.[68] This had been perceived by the members of Anonymous as an infringement of freedom of speech and 'unjustified privatization of information'.[69] It was reported that members of the group have been arrested, prosecuted and incarcerated for their involvement in the DDOS attacks.[70]

3.2.1.3 Terrorists

Terrorists may use cyberspace to disrupt and destroy computer systems, telecommunication and information infrastructure. Denning defines cyber terrorism as:

> Unlawful attacks and threats of attacks against computers, network and the information stored therein that are carried out to intimidate or coerce a country's government or citizen in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property or at least cause enough harm to generate fear.[71]

The impact and scale of the attack must be serious in order to constitute cyber terrorism.[72] Besides that, terrorists uses cyberspace for publicity, radicalisation, spreading ideology and propaganda, communication and conscription.[73] This study will examine cyberterrorism in the next chapter.

---

[68] The Telegraph, 'Anonymous': the Mysterious Hacking Group Which Made Name Targeting Church of Scientology' <http://www.telegraph.co.uk/technology/internet/8380612/Anonymous-the-mysterious-hacking-group-which-made-name-targeting-Church-of-Scientology.html> accessed 1.03.2015

[69] Taylor, *Hackers* (n 57) 61

[70] Kravets D, 'Guilty Plea in 'Anonymous' DDoS Scientology Attack' (*wired.com*, 26.01.2010) <http://www.wired.com/2010/01/guilty-plea-in-scientology-ddos-attack/> accessed 1.03.2015

[71] Denning DE, 'Cyberterrorism: The Logic Bomb versus the Truck Bomb' Global Dialogue; Autumn 2000; 2, 4, 29

[72] ibid

[73] Home Office UK, 'A Strong Britain in an Age of Uncertainty' (n48)

3.2.1.4 Other Entities

The perpetrators of cyber attacks may include criminals, corporations and insiders. They commit the attacks for various reasons such as to attain profit and malice. Deputy Public Prosecutor 2 contended that:

> There are three primary sources of criminal activities: Malaysians, foreigners in Malaysia and foreigners outside of Malaysia. The foreigners usually steal the password to your account and transfer your money to their account abroad. They can do that outside of Malaysia. So, the threats are everywhere.[74]

Moreover, corporations may conduct industrial espionage in order to gain advantage over their competitors. According to Policymaker 4:

> I consider industrial espionage where organisation stealing information from another organisation for industrial purposes as cyber attacks.[75]

McAfee, a security technology company estimated that the cost of cyber espionage and cybercrime for the US is about $70 billion to $140 billion in 2013.[76] This includes rectifying computer systems, which have been with tampered due to cyber espionage. Besides that, insiders such as employees posed high risk to the security of an organisation.[77] According to Deputy Public prosecutor 1:

> There was a case involving a disgruntled employee from an oil and gas company. He hacked the company's server, which is based in Malaysia. He installed a bug, which disrupted the company's servers in the country by alphabetic order. The attack emanated from outside of Malaysia.[78]

---

[74] Interview with Deputy Public Prosecutor 2

[75] Interview with Policymaker 4

[76] ibid

[77] McNamara MR, 'Dysfunction in Cyberspace: The Insider Threat' in Campen AD and Dearth DH (eds), *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict* (AFCEA International Press, 2000) 79

[78] Interview with Deputy Public Prosecutor 1

The insiders may be authorised to access the information system of the organisation. They may commit the attacks easily as they have control over the system.

3.2.2 Victims and Targets

The victims of cyber attacks may include specific individuals, public or private organisations. For instance, the Malaysian Armed Force is targeted in order to obtain classified strategic, operational and tactical information.[79] However, some of the victims may not realise that they are being targeted. According to Military Officer 1:

> Awareness is what separates the organizations or individual. Either they know they are being attacked or they never know that they are being attacked.[80]

Apart from individuals and organisations, the perpetrators may target the critical national infrastructure.[81]

Critical national infrastructure has been integrated with computer systems and must be assessed in a new context in the information age.[82] The US Department of the Homeland Security defines critical infrastructure as 'systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economy security, national public health or any combination of those matters'.[83] According to the Commission to the European Union, information and communication technologies, which include services and networks infrastructures, are an integral part of the

---

[79] Interview with Military Officer 1

[80] ibid

[81] S 130A of the Penal Code provides that essential services include: water; electricity; public health; banking and financial; fire; prison, postal, telecommunication including the communication infrastructure; telegraph; radio communication including broadcasting and television; port, dock and harbor; public transport; bulk distribution of fuel and lubricants.

[82] Kessler, 'A Study of the Tallinn Manual on Cyberwarfare' (n 31)

[83] US Department of Homeland Security, 'NIPP 2013 Partnering for Critical Infrastructure Security and Resilience', <http://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf> accessed 23.04.2015

European community and society.[84] The effectiveness of critical national infrastructures is enhanced by the usage of the computer system. However, they are increasingly vulnerable to disruption or failure.[85]

The destruction of critical information structure would have a devastating impact on the function of the society.[86] According to Tyrell, attacks on critical national infrastructure are not easily detected 'and even if noticed may be classified as system failure, software bugs or human incompetence'.[87] According to Security Professional 9:

> The perpetrators may use special code to manipulate or disrupt the Scada system of the critical national infrastructure. They may insert malicious code such as stuxnett that is capable of controlling the system.[88]

The British Computer Society and the Institute of Electrical Engineers identified the critical role of computers in various fields including water-treatment plants, the chemical industry, medical electronics, motorcar infrastructure, the nuclear industry and aviation. They emphasised the importance of monitoring the computer systems used in these fields, 'which threaten life if they go wrong'.[89] It was reported that a cyber security consultant discovered the vulnerability of software used in communications equipment, which enable the WiFi signal or inflight entertainment system to

---

[84] Commission of the European Communities, 'Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience', <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF> accessed 23.04.2015

[85] Dearth DH, 'Critical Infrastructures and the Human Target' in Information Operations in Campen AD and Dearth DH (eds), *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict* (AFCEA International Press, 2000) 204

[86] Commission of the European Communities, 'Protecting Europe from Large Scale Cyber-Attacks and Disruptions' (n 84)

[87] Tyrell PJ, 'Protecting the National Critical Infrastructure: The Human Dimension From a Government Perspective' in Campen AD and Dearth DH (eds), *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict* (AFCEA International Press, 2000) 212

[88] Interview with Security Professional 9

[89] Wasik M, *Crime and the Computer* (n 51) 12

be hacked for the purpose of disrupting the aircraft's navigation and safety system.[90]

3.2.3 Methods and Impact of Cyber Attacks

The second variable in determining the concept of cyber attacks is the methods and impacts of the attacks. Describing the phenomenon of cyber attacks may be difficult due to the divergent understandings of cyber attacks. According to Security Professional 5:

> People have different ways of using the term cyber attacks. It covers a wide area. For instance, my client considered hacking, phishing and spamming as cyber attacks. My company does not used this term for that reason. Usually, IT security is mainly concerned with confidentiality, integrity and availability (CIA). We considered any breach of these components as a threat. They must be secured.[91]

The study revealed that some of the participants from all categories do not used the term 'cyber attacks' due to its vagueness. Apart from that, the concept of harm is not universal and subjected to the social contract entrenched in the domestic laws.[92] Thus, certain acts are perceived as harmful in Malaysia due to its social and economic background. The same acts may be considered as less harmful in Western countries such as UK.

Prior to the study, the researcher had posted provisionally that cyber attacks might be described as:

> The use of malicious software and malware by states and non-state actors to penetrate, disrupt and destroy the computer and telecommunication system of their enemy. The purpose of the attack is to incapacitate the enemy during armed conflict by targeting their military objectives and/or to cause serious and widespread harm to victims, which include mental and bodily

[90] Finkle J, 'Hacker Says to Show Passenger Jets at Risk of Cyber Attack' (Reuters.Com 4 August 2014) <http://www.reuters.com/assets/print?aid+USKBNOG4OWQ20140804> accessed 8 May 2014

[91] Interview with Security Professional 5

[92] Doig A, *State Crime* (Willan Publishing 2011) 77

> injury, damage to critical national infrastructure and damage to objects which are critical to the economy and national security.[93]

However, the study revealed some interesting observations. Some of the participants from all categories considered that the concept above is too narrow. Legal Practitioner 4 argued that:

> The definition should be broaden; cyber attacks not only are done to disrupt and destroy but also to target and obtain the information and to control the network for instance by using the DDOS.[94]

Others thought that cyber attacks are not confined to situations of armed conflict. Deputy Public Prosecutor 2 observed that:

> The attacks are not confined to armed conflict. I was involved in a case where two ex-employees hacked the computer system of their employer. The company had to shut down the system, which cause huge losses.

Similarly, Legal Practitioner 3 observed that:

> Armed conflict? No way, I am sure the purpose of or the ill that you are trying to remedy is not confined to the situation of armed conflict. Cyber attacks are problematic even during time of peace. We have to ensure that it is an offence. It should not be confined to armed conflict. We can impose heavier punishment if the attacks affect national security especially when it comes to national infrastructure.[95]

Accordingly, cyber attacks may be committed outside the situation of armed conflict.

---

[93] Interview Schedule

[94] Interview with Legal Practitioner 4

[95] Interview with Legal Practitioner 3

The study also found that most of the participants agreed with the concept above that cyber attacks are done in order to disrupt computer systems. Military Officer 1 described cyber attacks as:

> Any types of deliberate attempt to gain unauthorized access, exploit, disrupt or damage a computer infrastructure, network or information system by means of malicious acts.[96]

According to Policymaker 3, the term 'cyber attack' may be equivalent to cyber security incidents.[97] The Malaysia's National Security Council had issued Directive No. 24 in 2011 to manage cyber crisis at the national level. The Directive defines a cyber security incident as: the loss of confidential information; disruption of the data integrity or system; disruption which is intended to cause failure to obtain information from the computer system and any breach of rules and regulations governing information security.[98] The Directive does not specify the types of attacks that fall within the ambit of this definition. However, the Directive emphasises the need for a guideline to protect ICT from virus, worms and malware attacks.[99]

Some of the participants in this study emphasised the usage of tools such as malware in order to conduct cyber attacks. This pattern contradicts that of scholars such as Hathaway. She argued that any means might be used to damage the computer including the usage of a regular explosive to sever the undersea network cables.[100] It is, however, noted from this study that some of the security professionals highlighted the usage of cyber tools to access the computer system in order to constitute cyber attacks. Security Professional 10 contended that:

---

[96] Interview with Military Officer 1

[97] Interview with Policymaker 3

[98] National Security Council, *Arahan No. 24 (Directive No. 24)* (National Security Council, Prime Minister's Department Malaysia, 2011) 2

[99] ibid 5

[100] Hathaway, 'The Law of Cyber-Attack' (n 4)

> I consider the access to the computer system using a 'third party tool' as cyber attacks. Without the tools, the attacks cannot be executed.[101]

Moreover, Security Professional 11 argued that:

> I will bring your attention to the phrase armed conflict. There is a conflict being waged right now but it is not armed conflict. It is waged on the cyber frontier. The armoury consists of the vulnerabilities. Real weapons such as guns are used on the physical frontier. However, the exploit kits are used on the cyber frontier. The aim of the attacks is to incapacitate the cyber frontier instead of the physical infrastructure.[102]

Most of the security professionals had corresponding views. For instance, Security Professional 10 observes that:

> 'Cyber attacks' are confined to attacks on computer system or server. The perpetrators use malware as a tool to perform illegal activities such as obtaining confidential information from the computer system.[103]

Policymaker 4 argued that:

> Cyber attacks may be committed in several forms. I don't think trespassing on the computer system as cyber attacks. I consider an incident as cyber attacks when there is action and impact. For instance, I deliberately placed APTs malware in the server. This amounted to cyber attacks, as there is an action. I also consider DOS as cyber attacks. I deliberately launched unauthored packets to your IP address in order to ensure that your website is not accessible.[104]

Policymaker 3 asserted that cyber security incidents might include virus attacks that cause the computer system to slow down and failure to access

---

[101] Interview with Security Professional 10

[102] Interview with Security Professional 11

[103] Interview with Security Professional 10

[104] Interview with Policymaker 4

the email due to the denial of service attacks on the server.[105] Viruses are programs built for the purpose of contaminating other computer programmes and data files.[106] Rid and Mcburney define cyber weapons as 'computer code that is used or designed to be used with the aim of threatening or causing physical functional or mental harm to structures, systems or living being'.[107] They classified cyber weapons into two categories.[108]

Firstly, there is generic and low potential malicious software that can influence a system from the outside but incapable of penetrating the system to create direct harm.[109] DDOS falls within this category. DDOS attacks are done to cause congestion to a server. It was reported that Russian Internet service providers had attacked Spamhaus, a site responsible for keeping ads for counterfeit Viagra and bogus weight-loss pills out of the world's inboxes. The attack was done after Spamhaus had blacklisted them.[110] The perpetrators had taken advantage of the weaknesses in the Internet's infrastructure to trick thousands of servers into routing a torrent of junk traffic to Spamhaus every second.[111] Secondly, there is high potential malware that acts as intelligent agent capable of penetrating protected system to inflict direct harm.[112] Stuxnet virus was allegedly used to destroy Iran's nuclear programme. Malicious software and malware designed for cyber attacks are capable of causing financial loss and destruction of property including the computer's hardware and software.

In addition, the results of the study shows that some of the participants argued that cyber attacks should lead to serious effects to the victims. Security Professional 9 distinguished cyber threats from cyber attacks:

---

[105] Interview with Policymaker 3

[106] Wasik M, *Crime and the Computer* (n 51) 58

[107] Rid T and Mcburney P, 'Cyber-Weapons' (n 47) 7

[108] ibid

[109] ibid

[110] Aljazeera, 'Huge Cyber-attack Causes Worldwide Disruption' (*Aljazeera*, 28 March 2013) <http://www.aljazeera.com/news/europe/2013/03/201332723173599565 3.html> accessed 19 April 2014

[111] ibid

[112] Rid T and Mcburney P, 'Cyber-Weapons' (n 47) 8-9

> We consider cyber threat or potential cyber attack as an attempt to attack our assets such as the public website. We use certain equipment and solution to prevent it from becoming an incident or an actual 'cyber attack'.[113]

Security Professional 10 argued that:

> I think cyber attacks should inflict personal damage to the victims including financial loss or loss of reputation. I don't consider a troll's postings as cyber attacks.[114]

Other participants considered the attacks as serious if they cause loss of data and destabilise the country's economy, security and politic.[115] On the other hand, some of the security professionals measured the seriousness of the attacks according to the security perimeter. According to Security Professional 5:

> Another factor that we look at is the security perimeter that protects the network. Normally, the perimeter is divided into three tiers. The first tier is the firewall. We consider the attack is serious If the perpetrator compromised the server through DDOS attack or packet that the send from outside. This may cause the server down and affect the company's performance.[116]

The above findings demonstrate that 'cyber attacks' refer to the attacks on the computer system and server using tools such as virus, worms and malware. In addition, the attacks may cause detrimental effects including physical damage and economic loss to the victims.

Within the context of cyber warfare, cyber attack has been defined as offensive or defensive cyber operation causing injury, death or destruction to objects.[117] The *Tallinn Manual* has been produced to assess the application

---

[113] Interview with Security Professional 9

[114] Interview with Security Professional 10

[115] Interview with Security Professional 2 and 3

[116] Interview with Security Professional 5

[117] Schmitt MN (ed), *Tallinn Manual on the International law Applicable to Cyber Warfare* (Cambridge University Press 2013) 106

of international law to cyber warfare specifically the use of force by states such as self-defence under article 51 of the UN Charter and the law of armed conflict. The *Manual* is not considered as a comprehensive guide in dealing with all the issues related to the cyberspace under international law. It does not cover situations below the threshold of the use of force and armed conflict.[118] The *Manual* defines cyber operations as the usage of cyber capabilities primarily to accomplish objectives 'in or by the use of cyberspace'.[119] Communications, storage and computing resources 'upon which information systems operate' have been listed under cyber infrastructure in the Manual.

Despite of its classification as a non-kinetic force, cyber attacks can trigger physical harm similar to conventional weapons such as the release of the floodgates on a dam and the explosion of nuclear centrifuges. It can also be concerned in theory as causing catastrophic scenarios, such as collisions between aircraft, the release of poisons from chemical plants or the disruption of vital infrastructure and services such as electricity or water networks.[120] During the Russian-Georgian war of 2008, cyber attacks were allegedly used against Georgia through the usage of non-kinetic operations.[121] The advancement of Russia's tanks into Georgia was made easier by cyber attacks, which destroyed and disrupted Tbilisi's command, control and communication systems.[122]

The methods of the attacks vary according to the objectives of the perpetrators. According to Private Sector Officer 3, the perpetrator may use social engineering to discover the victims' information:

---

[118] ibid 4

[119] ibid 15

[120] International Committee of the Red Cross, 'Cyber Warfare' <http://www.icrc.org/eng/war-and-law/conduct-hostilities/information-warfare/overview-information-warfare.htm> accessed 10 March 2014

[121] Handler SG, 'The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare' (2012) 48 Stan J Int'l L 209

[122] Arquilla J, 'Rebuttal Cyberwar is Already Upon Us' (2012) 192 Foreign Policy; Mar/Apr 2012; 192, 84

> The perpetrators are using social engineering before they can launch the attacks. They try to get information such as who is the owner of the IP address. Some of the details can easily be found on the Internet. They can google for my information and contact details from the website of my workplace. Then, they will attempt to access my computer system by sending me emails.[123]

Military Officer 1 asserted that:

> Malware is created using programming language, compiled as a program, conceal itself from being detected and use mistakes of security systems of operating environments, social engineering and other tricks.[124]

Moreover, not all malicious software and malware are created with the capability to inflict physical harm and destruction of property. Some of them are designed for spying and espionage. The Government Communications Headquarters of UK (GCHQ) has released the guideline, 'Common Cyber Attacks: Reducing The Impact' to organisations that are vulnerable to cyber attacks. According to the guideline, cyber attacks can be done using techniques such as phishing, water holing, ransomware, scanning, spear phishing, deploying botnet and subverting the supply chain.[125] These techniques are mostly used to commit fraud and financial crimes. It is to be noted that the purpose of this guideline is to help corporate entities to understand and identify cyber attacks. It is one of non-criminal enforcement measures adopted by UK in countering cyber attacks designed for business owners. Disruption of business and financial loss is perceived as the commonly intended harm for cyber attacks.

As demonstrated in the preceding paragraphs, the impact of cyber attacks on the computer system and server is divided into three types. The first type is cyber incidents, which do not cause substantial impact to the victims. They

---

[123] Interview with Private Sector Officer 3

[124] Interview with Military Officer 1

[125] GCHQ, 'Common Cyber Attacks: Reducing the Impact' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf> accessed 23.02.2015

may be classified as ‘cyber pranks’ as the degree of harm is so low that the law should not be used as a response. The victims may suffer inconvenience due to the attacks such as the inability to access their email account. The security of the computer system needs to be secured in order to counter this problem.

The second type is the medium impact attacks in which malicious software and malware are created and used to commit fraud, identity theft and financial crimes. The victims may suffer financial losses because of the attacks. The third type is the high impact attacks, which cause widespread and serious harm to the victims. Apart from the infliction of mental and bodily injury, the attacks threatened and disrupted the lifestyle of the people. For instance, the attacks on the banking system and government websites may jeopardise the economy and national security. The destruction of critical national infrastructure such as heath services may not cause immediate danger but people may die due to prolonged attack. The term ‘cyber attack’ should be reserved only for medium and high impact attacks. The focus of the study is to analyse the measures to counter these attacks.

Besides that, the findings of the study also revealed that some of the policymakers, law enforcement officers and security professionals considered online sedition and defamation as cyber attacks. This pattern is consistent with the concept of international information security adopted by the member states of Chinese led Shanghai Cooperation Organisation (SCO).[126] They consider that the content of the Internet should be regulated, as it is a potential security threat.[127] However, Western countries perceive that this interpretation may jeopardise human rights through censorship on the Internet and suppressing political organisations.[128] The use of social media by political activists and social protest movements may cause intensive and intrusive online surveillance by states.[129]

---

[126] CCDCOE ‘Shanghai Cooperation Organisation’ <https://ccdcoe.org/sco.html> accessed 20 January 2017

[127] ibid

[128] Hathaway ‘The Law of Cyber-Attack’ (n 4)

[129] Yar M, ‘E-Crime 2.0: The Criminological Landscape of New Social Media’ Information & Communications Technology Law Vol 21, No 3, October 2012, 207–

Individuals' liberties are more restricted in Malaysia in comparison to the Western countries. They can be prosecuted for making seditious and defamatory statements with the intention to disrupt national security. The term 'national security' usually connotes 'public order, racial and religious harmony, economic strength, social welfare, political stability and strong government'. [130] Deputy Public Prosecutor 1 contended that defamation should be included in the concept of cyber attacks:

> Cyber attacks include not only to disrupt and destroy the computer system but also to give bad image. You can use the Internet to defame someone. This can be considered as cyber attacks on the character of a person by using the Internet.[131]

Defamation and sedition are categorised as cyber attacks by the policymakers in Malaysia. According to Policymaker 1:

> The security dilemma in Malaysia is different compared to other countries such as UK. There is lack of racial harmony in Malaysia. The law is needed in order to prevent individuals from inciting racial hatred in order to disrupt racial harmony. For me, maintaining national unity is more important than attacks on the computer system. We have to look at the literal meaning of the word 'attack'. It should include statements that can disrupt national unity.[132]

The maintenance of racial unity is of the utmost security concern in Malaysia. Thus, the term 'cyber attacks' is not confined to attacks on the computer system and server. Police Officer 3 claimed that:

> I perceive negative publication including seditious and defamatory remarks on the Internet as cyber attacks. The Internet enables the perpetrator to publish negative statements on social media sites such as Facebook and Twitter for the

---

219

[130] Sani MAM, 'Balancing Freedom of Speech and National Security in Malaysia' Asian Politics & Policy Volume 5, Number 4 585–607, 586

[131] Interview with Deputy Public Prosecutor 1

[132] Interview with Policymaker 1

> purpose of attacking the victim's reputation. These attacks are classified as improper use of network facilities under s 233 of the Communications and Multimedia Acts 1998.[133]

Deputy Public Prosecutor 1 shares this opinion. He said that:

> I would say that much interest of the Deputy Public Prosecutors about this issues stem from the publication of seditious articles. This was way back in 2009 and until now. The majority of cases in which cyber related evidence has to be dealt with are related to sedition. When I think about cyber attacks, I would consider unauthorised access to our SCADA System as such, water and electricity. It implies the involvement of foreign government or hostile foreign powers such as cyber attacks on US by China. However, I don't see why it cannot be extended to ideological attack. So, seditious remarks are a form of cyber attacks if they are published online.[134]

In essence, the results of the interviews show that the notions of the consequence of cyber attacks are divided into two categories in Malaysia. The first category is attacks on the computer system and server. The second category is seditious and defamatory remarks published on the Internet particularly the social media sites such as Facebook and blogs. This category is classified as cyber attacks due to the interpretation of national security in Malaysia.

The concept of cyber attacks in Malaysia may differ from other countries at the international level. The perception of cyber attacks may vary across geographical boundary due to different culture, history and social differences between societies. Yet, despite the differences, the application of the law and the measures to counter cyber attacks must be done within the limit of the international human rights law. This includes the idea of fairness especially in the context of freedom expression.

---

[133] Interview with Police Officer 3

[134] Interview with Deputy Public Prosecutor 1

The perception of cyber attacks may vary at the national level. However, a uniform and universal concept of cyber attacks is necessary for the purpose of applying international law and philosophical or theoretical ideas. This is also pertinent in formulating the mechanism to deal with cyber attacks at the international level. Therefore, it is important for Malaysia to consider the global view for the purpose of establishing international cooperation, protection and mutual assistance in the area of cyber security. This study shall return to the question of international action for cyber attacks in chapter 6.

3.2.4 Motives for the Attacks

Cyber attack is premeditated, as it requires extensive planning and technical expertise. Bentham contended that the quantity of an individual's pleasure and pains resulting from his action is the quantum of sensibility.[135] Most criminals do not think that they can be caught easily. For them, the profit of the offence and the pleasure of wealth and power outweigh the pains of privation and ill name. According to Military Officer 1:

> Cyber attacks are socially or politically motivated attacks carried out by criminal or trained professionals primarily through the Internet.[136]

Thus, the motives for the commission of cyber attacks are generally divided into divided into private and public realms.

In the private realm the perpetrators are motivated by personal gains including commercial advantage, malice and to demonstrate their technical expertise.[137] For instance, the victims of ransomware have to pay the perpetrators to decrypt the malware in order to avoid from reformatting the

---

[135] Bentham J, *An Introduction to the Principles of Morals and Legislation* (Clarendon Press Oxford, 1996) 51

[136] Interview with Military Officer 1

[137] GCHQ, 'Common Cyber Attacks: Reducing the Impact' <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf> accessed 23.02.2015

computer.[138] In addition, cyber attacks may be done to obtain confidential information and data. According to Private Sector Officer 4:

> Our customers are from Europe and US. Their details have to be protected. I cannot disclose their information to my own colleague. Let's say someone manages to access the server and obtained their details. I consider this as cyber attacks. The operation of the company is affected, as people know that our computer system is not secured.[139]

Taylor conducted several interviews with hackers in the Netherlands in 1999.[140] He observed that hacking for monetary gain is done sparingly with the intention to fund their activities rather than for profit.[141] The pressure to commercialise their activity arise due to the increasing demand of their techniques by traditional criminal groups.[142] Besides financial gain, Taylor also identifies other reasons including boredom, lack of mental stimulation, peer recognition, relentless pursuit of power, curiosity, to escape from the contingencies of the real world and jacking (that is to see if it could be done).[143]

Furthermore, cyber attacks may be committed for public causes. During situation of armed conflict, the attacks are undertaken as part of offensive and defensive military strategy. Apart from state, non-state actors may conduct cyber attacks in pursuant of political, racial and religious ideologies. Private Sector Officer 1 contended that:

> Somebody sent a PDF file with malicious malware to one of the investigators of the MH370 incident. His laptop was infected. The spyware was used to record the meeting and released the information. He asked Cybersecurity Malaysia to investigate this matter. I consider this case as cyber attack. The perpetrator

---

[138] Interview with Private Sector Officer 3

[139] Interview with Private Sector Officer 4

[140] Taylor PA, *Hackers* (n 57) 22

[141] ibid

[142] ibid

[143] ibid

> tried to get first hand information. Although the attack was non-disruptive, it involved national security, as the public may question the integrity of the public officials.[144]

Military Officer 1 argued that:

> Political agenda is the most obvious contributor to cyber attack but there are many other reasons to spark cyber attack such as nationality. For instance, Indonesian football fans attack Malaysian websites after losing a game, etc. Evidence shows that MAF is being attacked by spear phishing email the during MH370 incident.[145]

The perpetrator of cyber attacks may be encouraged by the rational calculation of the risk of getting caught. The rate of prosecutions is low as cyber attacks are underreported. The chances of getting caught are low as the victims such as the banks are reluctant to report the attacks. As stated above, Anonymous have used cyberspace to further their political causes. In the Huntingdon Life Science incidents, the protestors claimed that the attacks were done in furtherance of public objectives and not for monetary gain. [146] The aim of the attacks was to save animals from being experimented and torture. The protestors alleged the government is partly responsible for allowing experiment to be conducted on animals. Extreme action against the company is necessary in order to affect policy change.

In practice, it may be difficult to distinguish acts committed for private and public reasons. Any act which tantamount to breach of law is considered as public issue and threat to the state. For instance, cyber espionage may be categorised as private and public acts simultaneously. Industrial espionage by a company against its rivals may indirectly harm the economy of the country.

---

[144] Interview with Private Sector Officer 1

[145] Interview with Military Officer 1

[146] *Eli Lilly & Company Limited & Others and Stop Huntingdon Animal Cruelty & Others* (2011) EWHC 3527 (QB)

3.3 Summary of the Concept of Cyber Attacks

Based on the discussion above, this study suggests that the perpetrators of cyber attacks can be states and non-state actors. Currently, cyber attacks are used by states during armed conflict alongside with other conventional method of warfare. States may also resort to cyber attacks outside armed conflicts for instance by providing direct or indirect support to their proxies in conducting sporadic attacks against other states or individuals. States may cyber attacks in order to further their political agenda or foreign policy. Non-state actors comprise of individuals such as hackers and hacktivists, terrorists, criminals, corporate organisations and insiders. They commit the attacks for public or acquisitive purposes. Cyber attacks are targeted at individuals, private or public organisations and critical national infrastructure.

The nature of harm and impact of the attacks are important. This study argues that cyber attacks are perpetrated by using malicious software and malware, which are designed to penetrate, alter and destroy the computer system and server. Apart from that, cyber espionage is perceived as cyber attacks as it poses a serious threat to the national security and economy. Low threshold cyber incidents, which only cause inconvenience should be differentiated and categorised as ‘cyber pranks’. The term cyber attack should be reserved only for medium and high impact attacks. They may be classified as cybercrimes or war crimes. In addition, cyber attacks also include online sedition and defamatory statements with the intention to disrupt national security and harmony.

Consequently, cyber attacks can be classified into four categories of cyber wrongdoing: (1) Cyber warfare/use of force/unlawful intervention under international law; (2) Cybercrimes; (3) Cyber espionage (4); Cyber terrorism. This is illustrated in figure 1. They may share similarities in terms of the method being used, impact and the targets or victims. However, the identity of perpetrators and motives of the attacks may be different for each category.

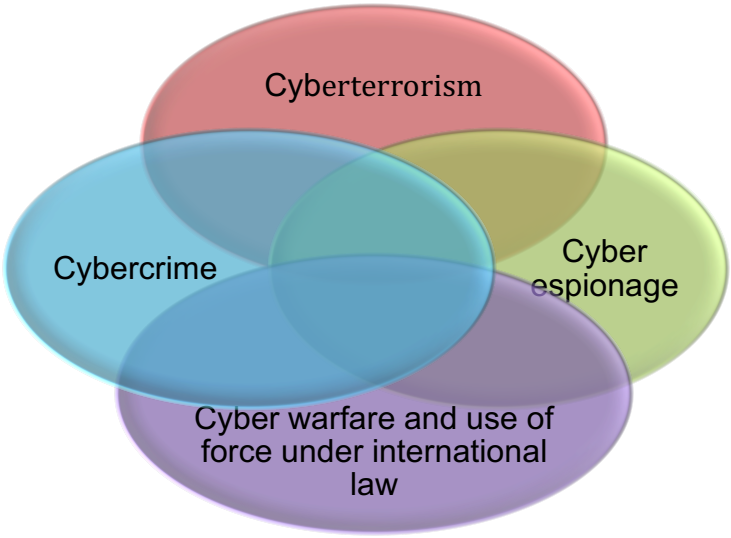


Figure 3.1: The categories of cyber attacks

3.4 Conclusion

There is no universally accepted definition of cyber attacks. Thus, this study identifies the concept of cyber attacks based on different variables including the identity of the perpetrators, the targets and victims, the methods in which the attacks are committed and motives of the attacks. The ontological features of cyber attacks are identified through empirical research and doctrinal analysis. The concept of cyber attacks may be utilised by the law enforcement agencies for tasking, training or budgeting purposes. In addition, it may be used to formulate the policy in relation to cyber security. The concept is also useful for the purpose of the application of non-criminal measures against cyber attacks. However, a specific definition is necessary in order to exercise policing powers and to apply criminal law due to the constraints imposed by human rights law. For that reason, this study classifies cyber attacks into four categories of cyber wrongdoings. Chapter 5 will examine the application of the criminal law in Malaysia in dealing with cyber attacks in the guise of cybercrime and cyberterrorism. Next, chapter 6 will assess the extent to which international law governs cyber attacks in the guise of cyber warfare, use of force and cyber espionage.

Chapter 4

The Strategy and Non-Criminal Measures to Counter Cyber Attacks in Malaysia

4.1 Introduction

The purpose of this chapter is to analyse the strategy to counter cyber attacks in Malaysia, which includes the usage of non-criminal measures and criminal law. It assesses the fairness and effectiveness of these measures. The analysis is based on various instruments including the Computer Crimes Act 1997 [Act 563], Penal Code 1936 [Act 574], Criminal Procedure Code 1935 [Act 573], Evidence Act 1950 [Act 56], Multimedia and Communication Act 1998 [Act 558], Personal Data Protection Act 2010 [Act 709] and directives issued by related governmental bodies.[1] This study also refers to the UK's Computer Misuse Act 1990, the 2001 Council's of Europe Convention on Cybercrime (Cybercrime Convention) and the directives issued by the European Union. Besides doctrinal study, this chapter incorporates a qualitative approach in analysing the application of the measures to counter cyber attacks in Malaysia. The empirical data from the fieldwork is included to support the findings in this chapter. This chapter is divided into two sections. Firstly, this chapter examines the strategic approach to counter cyber attacks in Malaysia. Secondly, this chapter analyses the usage of non-criminal measures in countering cyber attacks. Chapter 5 assesses the application of criminal law in dealing with cyber attacks in Malaysia.

4.2 Malaysia's Cyber Security Strategy

This section assesses the strategic approach to counter cyber attacks in Malaysia. It also examines the extent to which the government is involved in the implementation of the strategy. The Malaysia's National Cyber Security

[1] The sources are available to view at publicly accessed websites such as the official portal of the Attorney General's chambers of Malaysia http://www.agc.gov.my/agcportal/index.php?r=portal2/lom&menu_id=b21XYmExVUhFOE4wempZdE1vNUVKdz09

Policy was formulated in 2006 for the purpose of addressing the risk to critical national information infrastructure including: national defence and security; banking and finance; information and communications; energy; transportation; water; health services; government; emergency services; food and agriculture.[2] The policy contains eight thrusts: (1) effective governance; (2) legislative and regulatory framework; (3) cyber security technology framework; (4) culture of security and capacity building; (5) research and development towards self-reliance; (6) compliance and enforcement; (7) cyber security emergency readiness; and (8) international cooperation.[3] The National Security Council, the Attorney General's Chambers, CyberSecurity Malaysia, Ministry of Science, Technology and Innovation and the Ministry of Communications and Multimedia have been appointed as the drivers.

The National Security Council of Malaysia (the Council) is responsible to protect Malaysia's sovereignty and strategic interests including cyberspace.[4] This includes formulating the policies to safeguard critical national infrastructure from external and internal threats. The Council is in charge of strengthening the national CERT and in developing the mechanisms to report cyber security incident and disseminating vulnerability advisories and threat warnings.[5] The Council works closely with other government agencies to monitor and oversee the implementation of policies in relation to cyberspace.[6] CyberSecurity Malaysia is tasked with providing technical expertise and training in cyber crisis management.[7] Meanwhile, the Attorney General's Chambers of Malaysia is responsible for reviewing the laws, which address the dynamic nature cyber threats and harmonise the laws with the

---

[2] Kementerian Komunikasi dan Multimedia Malaysia, 'National Cyber-Security Policy' <http://nitc.kkmm.gov.my/index.php/national-ict-policies/national-cyber-security-policy-ncsp> accessed 8 December 2016

[3] ibid

[4] S 4 of the National Security Council Act 2016; National Security Council, 'Core Functions of the National Security Council' <https://www.mkn.gov.my/page/fungsi-teras> accessed 8 December 2016

[5] National Cyber-Security Policy (n 2)

[6] Interview with Policymaker 3

[7] National Security Council, *Arahan No. 24 (Directive No. 24)* (National Security Council, Prime Minister's Department Malaysia, 2011) 21

international treaties and conventions.[8] Accordingly, multiple agencies and governmental bodies are involved in ensuring the safety of cyberspace in Malaysia. However, Policymaker 3 argues that Malaysia does not have an extensive plan for cyber security at the national level, compared to other countries such as UK.[9] Pursuant to that claim, this study examines the UK's National Cyber Security Strategy 2016-2021.

The National Cyber Security Strategy 2016-2021 has been formulated to ensure that the UK is secure and resilient to cyber threats.[10] The strategy is divided into four main objectives: defend, deter, develop and international action. The first objective is to defend the UK against cyber threats. It requires effective means to respond to incidents and protect the networks and data system. The second objective is to deter all forms of aggression in cyberspace through detection, understanding, and investigation. In addition, pursuing and prosecuting the offenders are necessary in order to disrupt the hostile acts. The third objective is to establish an innovative cyber security industry. Lastly, international action is required for the purpose of advancing UK's wider economic and security interests. UK intends to improve its national cyber security by focusing on four broad areas: investing in innovation and supporting start-ups in the cyber sector; expanding intelligence and enforcement of the law against cyber activities by foreign actors, cyber criminals and terrorists; development and deployment of technology; and the establishment of a central body for cyber security at a national level. The National Cyber Security Centre is responsible to manage national cyber incidents and to provide expertise on cyber security.

This study suggests that Malaysia may improve its National Cyber Security Policy by incorporating and promulgating the 'defend, deter, develop and international action' strategies. The National Security Council of Malaysia is responsible to formulate the mechanisms and coordinate the effort to

---

[8] Kementerian Komunikasi dan Multimedia Malaysia, 'National Cyber-Security Policy' (n 2)

[9] Interview with Policymaker 3

[10] Cabinet Office, 'National Security and Intelligence, National Cyber Security Strategy 2016-2021 (Policy Paper)', <https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 > accessed 1 February 2017

manage any cyber crisis at the national level. Accordingly, the effort to counter cyber attacks in Malaysia is in fact divided into three main categories.

Firstly, non-criminal measures such as situational crime prevention are necessary in defending the networks and data system in Malaysia. This includes the development of technological measures such as encryption and electronic surveillance. In addition, civil remedies including injunctions may be invoked to dissuade the perpetrators from committing attacks. These measures are addressed in the next section.

Secondly, criminal laws are continuously improved in order to deter and punish the occurrence of cyber attacks. The laws should conform to international standard such as the European Convention on Cybercrime 2001. This is necessary due to political considerations including to attract foreign investment and to strengthen the confidence of trading partners. This study examines the role of Malaysia's criminal law in dealing with cyber attacks in chapter 5.

Thirdly, global partnership is needed to overcome the complexity of trans-national issues related to cyber security.[11] The divergences of criminal law, absence of prohibition and weak enforcement mechanisms against various cyber offences may lead to impunity.[12] Besides technological and legal measures, the Malaysia's National Cyber Security Policy 2006 and the UK's National Cyber Security Strategy 2016-2021 emphasise the need for international cooperation and action. The trans-jurisdictional character of cyber attacks renders resort to international law indispensable. International law provides solutions to issues such as the exercise of criminal jurisdiction of states and the surrender of fugitives. Moreover, it may be used to clarify the norms and standardise the procedures in dealing with cyber attacks. This study assesses the usage of international law in countering cyber attacks in chapter 6.

---

[11] 'Cybersecurity: A Global Issue Demanding a Global Approach' <http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html> accessed 11 April 2016

[12] Yar M, 'Sociological and Criminological Theories in the Information Era' in Leukfeldt R and Stol W (eds), *Cyber Safety: An Introduction* (Eleven International Publishing 2012) 52-53

This study explores the fairness and effectiveness of the measures to deal with cyber attacks in Malaysia. The background of the society and its material conditions shape the penal ideology and culture.[13] The principles of justice, liberty and democracy are the foundation of the establishment of the Federation of Malaysia. [14] Fundamental liberties including the right to life, equality of the law, freedom of movement and speech, prohibition of forced labour and slavery are entrenched in the Malaysian constitution.[15] However, the political system in Malaysia is ambiguous, as it is not based purely on democracy or authoritarianism. [16] Malaysia is not totally a liberal country as economic growth, political stability and national security have preceded individual liberty. The emphasis on the interests of society over individual rights reflects the influence of communitarianism in Malaysia. According to Shad Saleem Faruqi:

> Western attitudes towards freedom of speech are strongly influenced by the philosophy of individualism. In Malaysia, on the other hand, the value system emphasises duties as well as rights. It stresses the harmony of the socio-political order. It places a premium on the group over the individual and harmony and co-operation over disagreement. Maintenance of order and respect for hierarchy are cherished value. Our attitudes to nation, religion, culture, race, family and community are reverential. We place emphasis on communitarian goals.[17]

Some scholars argue that Malaysia employed authoritarian communitarianism especially during the administration of the former Prime

---

[13] Cavadino M and Dignan J, *Penal Systems: A Comparative Approach* (SAGE Publications 2006) 13

[14] The Proclamation of Malaysia on 16.09.1963 by By Prime Minister Tunku Abdul Rahman in the Stadium Merdeka in Kuala Lumpur.

[15] Article 5-13, Federal Constitution of Malaysia

[16] Mayudin G (ed), *Politik Malaysia: Perspektif, Teori dan Praktik (Malaysia's Politic: Perspectives, Theory and Practical)* (Penerbit Universiti Kebangsaan Malaysia 2008) 32

[17] Faruqi SS, 'Free Speech and the Constitution' [1992] 4 CLJ 1xiv

Minister of Malaysia, Mahathir Bin Mohamad. [18] Thus, the notion of communitarianism is important for Malaysia and within that notion religious values and custom are pertinent to the Malaysia society. Malaysia practices a limited form of democracy, as restriction of the media and freedom of speech is perceived as necessary to preserve national unity and racial harmony. The Parliament is permitted to impose necessary restriction in the interest of the Federation, public order and morality.[19]

Malaysia expressed the desire to embrace development via new technology and growth of the information society through Vision 2020. It aims to establish a scientific and progressive society, 'one that is not only a consumer of technology but also a contributor to the scientific and technological civilisation' by the year 2020.[20] Accordingly, the MSC Malaysia Bill of Guarantees ensures that there is no censorship of the Internet.[21] Sani argues that the current government 'practices comprehensive security' and has been overzealous in handling issues related to national security.[22] This could pose problems to the idea of freedom of the Internet. The prosecution of web operators under the media and libel laws has curbed the free cyberspace policy.[23] Consequently, the measures to defend national security may curtail the development of the knowledge - based society indicated in the Vision 2020. The notion of fairness should be specified in the strategy to counter cyber attacks in Malaysia.

Apart from the values of the Malaysian legal system, effectiveness is an essential criterion for the measures to deal with cyber attacks. As stated above, the effectiveness of the strategies to counter cyber attacks depends

---

[18] Etzioni A, 'Communitarian Revisited' Journal of Political Ideologies, 19:3, 241-260

[19] Article 149 of the Federal Constitution of Malaysia

[20] The Way Forward-Vision 2020 <http://www.wawasan2020.com/vision/index.html> accessed 8 December 2016

[21] MSC Malaysia Bill of Guarantee <http://www.mscmalaysia.my/bogs> accessed 8 December 2016; S 3(3) of the Multimedia and Communication Act 1998

[22] Sani MAM, 'Balancing Freedom of Speech and National Security in Malaysia' Asian Politics & Policy Volume 5, Number 4 585–607, 590

[23] ibid 591

on the intervention and cooperation by different agencies such as local government, probation and the police. According to Masum:

> Through effective and efficient mechanisms in place especially in the public sector institutions, we will be able to bring a measure of good governance to the people. This is based on the notion that good governance means that processes and institutions produce results that meet the needs of society while making the best use of resources at their disposal. Since the concept of efficiency in the context of good governance also covers the sustainable use of natural resources and the protection of the environment.[24]

The implementation of government initiatives might be hampered by the lacklustre performance of the public officials at a lower level.[25] Coordinated effort between various agencies may also be hindered by problems such as disparate policy initiatives and uneven allocation of resources.[26] The cost of updating IT equipment and computer system is high. The Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) is responsible for monitoring and evaluating the implementation of the ICT strategic plan for the public sector.[27] It spends millions of ringgit on improving cyber security in Malaysia.[28] However, Private Sector Officer 4 argued that:

> The budget allocated for IT infrastructure is low. The Internet connectivity in Malaysia is slow for a developing country. The government should improve the Internet coverage by investing

---

[24] Masum A, 'The Role of Good Governance in Protecting and Promoting Human Rights-A Case Study of Malaysia' [2010] 1 LNS (A) ii

[25] Interview with Private Sector Officer 2

[26] Young J, 'Left Realism and the Priorities of Crime Control' in Stenson K and Cowell D (eds), *The Politics of Crime Control* (Sage Publications 1991) 155

[27] ICT Strategic and Architecture Development <http://www.mampu.gov.my/en/role-mampu-department/ict-strategic-and-architecture-development> accessed 8 December 2016

[28] Interview with Private Sector Officer 2

> in fibre cable. I don't see how they can improve the strategies to tackle cyber attacks when they can't even do this.[29]

Security Professional 10 also made a similar observation. He contended that:

> I can see the initiatives by the government. The government is not serious in taking action. Just look at our network coverage. The security of our computer network is still at low level. The initiatives are merely empty rhetoric and politicised. Recently, they are talking about blocking Facebook in Malaysia. They should have done it if they are really serious. Not many people know that MCMC (Malaysian Communications and Multimedia Commission) has its own hotline number. The persons who control MCMC are not expert in IT. I cannot comprehend some of the advice given by MCMC. It was reported that MCMC had blocked 700 pornographic websites. However, I still can see them every day. I don't think the initiatives are effective.[30]

The social dependency upon state institutions and actors may be problematic, as they are 'increasingly alien, obscure and inaccessible to most people affected by the risk in questions'. [31] Some scholars argue that the police should lead the community anti crimes initiatives, as the government resources in preventing crimes primarily rest with them.[32] Yet, despite the effectiveness of the criminal process, it may contradict with fairness.

The effectiveness of the law might conflict with the notion of fairness especially in term of individual rights. Upholding communitarian principles through criminalisation may lead to legitimising authoritarian systems of law.[33] Harmonising the administration of justice with human rights norms is a

---

[29] Interview with Private Sector Officer 4

[30] Interview with Security Professional 10

[31] Beck U, *Risk Society: Towards a New Modernity* (SAGE Publications Ltd 1992) 4

[32] Rosenbaum DP, Lurigio AJ and Davis RC, *The Prevention of Crime: Social and Situational Strategies* (Wadsworth Publishing Company 1998) 174

[33] Wilson W, *Central Issues in Criminal Theory* (Hart Publishing 2002) 41

difficult task for the authorities especially in Malaysia. Individual freedoms must be balanced with 'national security in a multiracial, multicultural nation set in a region that is facing multiple challenges'.[34] At the same time, 'laws are shaped by the society in which they are applied'.[35] The policy makers in Malaysia are faced with arduous tasks to make necessary changes to the law in order to meet the requirements of both fairness and effectiveness.

Besides fairness and effectiveness, another factor that influences the implementation of the strategy to counter cyber attacks in Malaysia is late modernity. The main function of the government is to protect the people from present and future risk. This includes threats to the territory, economic security, infrastructure and way of life.[36] In Malaysia, the preservation of national security emphasises central control by the government. It seems that the idea of national security collided with a salient feature of late modernity, which is the 'hollowing out of the state', whereby the central administrative ability to coordinate and plan has diminished in the late modernity.[37] Decentralisation of power is widely seen as necessary to enable the government to perform its function effectively.[38] The decentralisation of the public sector management is likely to mean that more core functions of the government are delegated to distant agencies.[39] States are moving forward with their privatisation of the criminal justice and security systems especially in the West.

The role of the state is to control and design the context of the legal system. The shrinking size of government inevitably entails considerable use of non-

---

[34] Patail AG, 'Speech by the Attorney General of Malaysia, At the Opening of the Legal Year 2012' (2012) 1 MLJ cxiii

[35] Aziz SA, 'The Malaysian Legal System: The Roots, The Influence and The Future' (2009) 3 [2009] 3 MLJ xcii

[36] Prime Minister, 'National Security Strategy and Strategic Defence and Security Review 2015: A Secure and prosperous United Kingdom' (Cm 9161, 2015) ch 1

[37] Rhodes RAW, 'The Hollowing Out of the State: The Changing Nature of the Public Service in Britain ' The Political Quarterly Publishing Co Ltd 1994, 138

[38] Osborne D and Gaebler T, *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector* (Addison-Wesley Publishing Company 1992) 32

[39] Beck U, Giddens A and Lash S, *Reflexive Modernization. Politics, Tradition and Aesthetics in the Modern Social Order* (Polity Press 1994)

criminal measures in dealing with criminal activities. The limitation of the intervention by states renders an active role by the private bodies in managing the Internet. Thus, it can be inferred that the state is responsible for formulating the policy and the law relating to cyber security. Other fields such as enforcement can be negotiated and delegated to private sectors.

Despite these pressures, the decentralisation of the public sector management in Malaysia has advanced slowly compared to other countries such as UK. The size of the public sector and the extent of government intervention are indicated by examining the public spending, public ownership of industry and levels of government.[40] It has been reported that Malaysia's civil service relative to population is large, at more than double the average in the Asia-Pacific region by some measures.[41] It is estimated that 1.6 million people or 11% of the labour force are attached to the Malaysia's civil service.[42] There is less likelihood that the government would reduce the expenditure on the civil service as the civil service forms an important support base for the government and can usually be counted upon to show up and vote for the ruling party during elections.[43]

Apart from the civil service, the government linked-companies have immense corporate interests in the key economic sectors including property, trading, financial services, construction and plantations.[44] The privatisation of the criminal justice and security system does not exist in Malaysia. Consequently, the eradication of criminal activities primarily rests upon the government. Nonetheless, technical expertise is essential in countering cyber attacks compared to other conventional offences. A comprehensive

---

[40] Rhodes RAW, 'The Hollowing Out of the State' (n 37) 139

[41] Chong PK, 'Bloated Malaysia Civil Service Presents Headache for Najib' *Bloomberg* (10.08.2016) Bloomberg Markets <http://www.bloomberg.com/news/articles/2016-08-10/jobs-for-life-malaysians-hard-to-budge-as-najib-eyes-voter-risk> accessed 20.08.2016

[42] ibid

[43] ibid

[44] Aruna P and Inn TK, 'Fewer Political Appointees on GLCs' *The Star* (22.07.2016) Business News <http://www.thestar.com.my/business/business-news/2016/07/22/fewer-political-appointees-on-glcs/ >accessed 20.08.2016

strategy to counter cyber attacks in Malaysia necessitates the inclusion of the private sector.

This study suggests that the notion of late modernity in Malaysia differs from other modern countries. It entails greater public and private partnership instead of hollowing out of the state. The government agencies rely on the service of the private security firms especially in areas, which require technical expertise such as cyber security. The lack of technical expertise of the government agencies in this area transpired during the interview with Security Professional 11. He contended that:

> My company provides advice on how to improve cyber security to the government agencies. They seek our service especially for the purpose of gaining accreditation. The National Security Council warned the government agencies of the possible cyber attacks by Anonymous last year. The warning did not prompt sufficient action by the government agencies. For instance, some of the agencies decided to unplug the cable of the computer network during the day of which the attack was supposed to happen. This is not a real solution to the problem and obviously not an effective preventive measure.[45]

According to Policymaker 3:

> The security of the CNII (critical national information infrastructure) may be enhanced through partnership between the public and private sectors. There is a need to maintain good relationship with big companies, as the government cannot work alone.[46]

Policymaker 3 insisted that reliance on the private sector in cyber security should be done sparingly in order to protect the government's interests.[47] But, most of the critical national information infrastructures (CNII) in Malaysia

[45] Interview with Security Professional 11

[46] Interview with the Policymaker 3

[47] Ibid

are owned by the private sector.[48] Their role is significant in ensuring the safety of CNII. Thus, cooperation between the government agencies and private sector is needed in dealing with cyber attacks.

The National Security Council of Malaysia has issued Directive No. 24 in 2011 to deal with cyber crisis at the national level. The Directive emphasises cooperation between public and private sectors especially from the CNII in dealing with cyber crisis. They are implemented through concerted effort between public and private sectors.[49] Related ministries and government agencies lead each sector of the CNII. For instance, the Ministry of Science, Technology and Innovation and the Communication and Multimedia Commission are responsible for coordinating the strategies to counter cyber attacks for the Information and communication sector. The ministries and government agencies are obliged to adhere to Directive No. 24. Action can be taken against them for the failure to follow the directive.[50]

However, it is not clear whether Directive No. 24 is intended to be legally binding on the private sector. According to Policymaker 3, Directive No. 24 is extended to the private sector, but they are not compelled to follow it.[51] In the UK, the Civil Contingencies Act 2014 provides for the measures to be taken during situation that threatens serious damage to human welfare and security.[52] This includes the disruption of the system of communication, facilities for transport, health, supply of money, water, energy or fuel. A Minister of the Crown may by order permit or require the utilities and transportation providers to cooperate or provide information pertaining to the measures adopted in connection with an emergency.[53] Similar provision should be incorporated in Malaysia's Directive No. 24 to enable the National Security Council to enhance the cooperation between private sector and public sector.

---

[48] ibid

[49] National Security Council, *Arahan No. 24 (Directive No. 24)* (n 7) 8

[50] ibid 32

[51] Interview with the Policymaker 3

[52] S 1 of the Civil Contingencies Act 2004

[53] S 5 of the Civil Contingencies Act 2004; Schedule 1 of the Civil Contingencies Act 2004

To sum up, the aim of this section is to investigate the strategic approach to counter cyber attacks in Malaysia. The findings suggest that Malaysia does not have a detailed strategy in dealing with cyber attacks. The lack of strategy may lead to inconsistency of action or inaction. As a result, Malaysia is more vulnerable to cyber attacks. The Malaysia's National Cyber Security Strategy should be refined and improved in order to deal with the threats of cyber attacks. Therefore, this study suggests the incorporation of 'defend, deter, develop and international action' strategies into the Malaysia's National Cyber Security Strategy. The risk of cyber attacks may be alleviated by using non-criminal measures such as situational crime prevention, criminal law and global partnership. Furthermore, fairness and effectiveness should be the basis for the strategy in dealing with cyber attacks. The incorporation of these values into the strategy to counter cyber attacks is pertinent in order to ensure the development of a progressive knowledge-based society in Malaysia.

4.3 Non-Criminal Measures

This section discusses the application of non-criminal measures to counter cyber attacks. Reliance on criminal law is insufficient in combating crime. This is because it only addresses one factor in the commission of the crime that is the potential offender.[54] Questions have also been raised concerning the affordability, effectiveness and malpractice of the police and other enforcement agencies.[55] In addition, the prosecution of the perpetrator of cyber attacks is a field of expertise in which the law enforcement officers including police, prosecutors and judges may lack necessary skills. Moreover, the private sector may refuse to accept the government's intervention in the form of criminal law for various reasons such as not exposing their vulnerabilities to the public.

---

[54] Sutton A, Cherney A and White R, *Crime Prevention: Principles, Perspectives and Practices* (Cambridge University Press 2008) 19

[55] Ayres I, Braithwaite J, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992); Riesta I, 'Global Accounts of the Wrongfulness of Criminal Behaviour' (2011) 3 Contemp Readings L & Soc Just 110; Bright J, 'Crime Prevention: the British Experience' in Stenson K and Cowell D (eds), *The Politics of Crime Control* (SAGE Publications, 1991) 67

In light of these arguments, non-criminal measures are appealing to states and private sector since criminal justice system is no longer perceived as the ultimate mechanism to combat crimes. Early intervention is necessary in order to disrupt the commission of crimes. For instance, administrative infringement procedure is normally agreed to be less costly and faster than criminal procedure.[56]

In addition, protective security measures are vital in protecting the government's interests during the age of information warfare. Information warfare is instrumental in bringing about power and dominance by states in the age of information.[57] Taddeo defines information warfare as:

> The use of ICTs within an offensive or defensive military strategy endorsed by a state and aiming at the immediate disruption or control of the enemy's resources, and which is waged within the informational environment with agents and targets ranging both on the physical and non physical domains and whose level of violence may vary upon circumstances.[58]

Information technologies and communications networks are used as weapons together with techniques such as propaganda, public relations, misinformation campaigns and psy-ops to disrupt the enemies' activities and way of life.[59] During World War Two, the Government Code and Cypher School (GC&CS) and M16 played a vital role in cracking the Nazi Codes and ciphers.[60] A chain of wireless intercept stations was built across Britain for

---

[56] Lepage H, 'Study On Measures Other Than Criminal Ones In Cases Where Environmental Community Law Has Not Been Respected in the EU Member States' (*Milieu Ltd. and Huglo Lepage Associates*, 2004) <http://ec.europa.eu/environment/legal/crime/pdf/ms_summary_report.pdf> accessed 16 February 2014

[57] Schwartau W, *Information Warfare: Cyberterrorism: Protecting Your Personal Security in the Electronic Age* (2nd edn, Thunder's Mouth Press 1996)

[58] Taddeo M, 'Information Warfare: A Philosophical Perspective' (2012) 25 Philos Technol (2012) 25:105–120, 114

[59] Munro I, 'Defending the Network Organization: An Analysis of Information Warfare with Reference to Heidegger' (2009) <http://org.sagepub.com/content/17/2/199> accessed 10 August 2014

[60] Bletchley Park 'Intercept to Action' <https://www.bletchleypark.org.uk/content/hist/worldwartwo/inttoact.rhtm> accessed 18 February 2017

the purpose of monitoring the Germans' every move. The messages were sent back to Bletchley Park to be deciphered and translated.[61]

Cyber attacks are deployed by states for heterogeneous purposes including espionage and military action.[62] Protective security measures such as encryption and restricting the access to the government's information are pertinent in countering cyber attacks. Individuals and government officials such as Edward Snowdon should not be vested with unlimited access to confidential information. In addition, several organisations have been established in the UK to protect the government's information. The UK government's National Technical Authority for Information Assurance advises organisations on how to protect their data and information systems against today's threats.[63] In addition, the National Cyber Security Center (NCSC) provides advice, guidance and support on cyber security to the government and industry.[64] The NCSC's published guidance is aimed at helping the UK government departments, agencies, the critical national infrastructure and its supply chains protect their information systems.[65] It also has relevance for local government and the wider public sector.

Apart from that, private securities companies may be contracted as a supplement to the policing by public police forces especially in conducting surveillance and detective work. However, reliance on private security firms to manage critical information infrastructures must be done cautiously. The Intelligence and Security Committee of the UK Parliament released a report entitled 'Foreign Involvement in the Critical National Infrastructure: The Implications for National Security in 2013'.[66] The report indicated that Huawei, a Chinese telecommunications company was awarded a contract in

---

[61] ibid

[62] Munro I, 'Defending the Network Organization (n 59)

[63] CESG, 'Documents' <https://www.gov.uk/government/organisations/cesg> accessed 18 February 2017

[64] National Cyber Security Centre <https://www.ncsc.gov.uk> accessed 18 February 2017

[65] NCSC, 'Published Guidance' <https://www.ncsc.gov.uk/index/guidance> accessed 18 February 2017

[66] Foreign Involvement In the Critical National Infrastructure: The Implications for National Security (*Intelligence and Security Committee*, 2013), Cm 8629

2005 to supply some of the transmission and access equipment including routers across the network from January 2007. The Committee expressed its concern about the 'potential conflict between the commercial imperative and national security, as a result of increasing private ownership of critical national infrastructure combined with the globalisation of the telecommunications marketplace'.[67] There is the possibility that the Chinese Government may influence Huawei. This caused grave concerns as China is suspected to sponsor attacks for the purpose of gathering information and espionage.[68] Despite of its vehement denial, politicians in US and Australia have considered Huawei as a security risk.[69] The Committee suggested that the British Government establish a procedure to assess the risk and to clarify accountability in managing contracts involving critical national infrastructure and foreign investment. Profiling is perhaps a necessary measure to ensure the reliability of the firm contracted to guard the critical national infrastructure and enhance cyber security.

This section is structured as follows. After giving an assessment of the scope of preventive measures, this section examines the role of the Internet architecture, national CERT and private sector in managing cyber attacks in Malaysia. Next, this section assesses the extent to which civil action and remedy are used in dealing with cyber attacks.

4.3.1 Preventive Measures

Preventive measures are part of the holistic response to crime. Tranter contends that 'scholarship on law and technology is a thoroughly speculative activity'. [70] Lawyer-scholars 'need to state the worries, promises, risks, benefits and anxieties that are suggested by the chosen technology and in

[67] ibid 4

[68] ibid 5

[69] ibid 6

[70] Tranter K, 'The speculative Jurisdiction. The Science Fictionality of Law and Technology' 20 Griffith L Rev 817, 817

so make the case for law'.[71] The responses to cyber attacks are discussed in terms of preventive logic.[72]

The objective of preventive measures is to maintain social and public order by reducing or stopping the occurrence of criminal activities. The fundamental premise of preventive actions is that 'the centre of risk consciousness lies not in the present but in the future'.[73] Beck defines risk as a 'systematic way of dealing with hazards and insecurities induced and introduced by modernization itself'.[74] It entails anticipation of destruction 'that has not yet happened but is threatening and of course in that sense risk are already real today'.[75] The increase of threats has paralleled the rise of the interventionist policy of the state.[76]

As indicated above, the privatisation of the criminal justice and security system does not exist in Malaysia. Consequently, the government of Malaysia is vested with the task to implement crime prevention policies. It allows the government to exercise unrestricted central capability and full capacity to steer the system.[77] Rhodes argues that 'governance is not a choice between centralisation and decentralisation. It is about regulating relationships in complex system'.[78] According to Brenner and Clarke, the power of the government is necessary in order to create incentives to secure systems and to prevent cybercrime.[79] Malaysia has to identify the conditions under which the preventive policies can work in countering cyber attacks. According to Policymaker 3:

---

[71] ibid 821

[72] Kessler O and Werner W, 'Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare' (2013) 26 Leiden Journal of International Law

[73] Beck U, *Risk Society: Towards a New Modernity* (n 31) 34

[74] ibid 21

[75] ibid 33

[76] ibid 77

[77] Rhodes RAW, 'The Hollowing Out of the State: The Changing Nature of the Public Service in Britain' (n 37) 149

[78] ibid 151

[79] Brenner SW and Clarke LL, 'Distributed Security: Preventing Cybercrime' 23 J Marshall J Computer & Info L 659 2004-2005, 685

> Cyber security in Malaysia is always about preventive or proper protection. This is equivalent to eliminating trouble through risk management. Standard periodic assessment is necessary as cyber security is massive. Furthermore, the threats and risks keep on changing. Legal action is difficult in Malaysia due to the ambiguity of the facts of the cases. We carry out research in law based on the current cyber security environment.[80]

Preventive measures are generally based on three approaches: (1) the improvement of social conditions by creating employment and educational opportunities; (2) the reduction of the opportunity to commit crime by managing and modifying situations that allow the occurrence of crime; (3) the preventive effect of law enforcement and the criminal justice agencies.[81] These approaches should be an essential part of the strategy to counter cyber attacks in Malaysia.

4.3.1.1 Social Prevention Policy

Social prevention policy has become increasingly prevalent in curtailing serious offenses including terrorism.[82] Social prevention policy focuses on normative values. Etzioni contends that the advancement of social goods is necessary 'because they are good in themselves, not because they are likely to reduce crime significantly'.[83] There is a need to reinforce the involvement of every fabric of the society especially families and schools in order to minimise crime.[84] They play a vital role in reducing or precluding the opportunities for crime.[85]

Social prevention policy emphasises the interventions of the community to prevent the emergence of potential criminals by modifying the social

---

[80] Interview with Policymaker 3

[81] Bright J, 'Crime Prevention: the British Experience' in Stenson K and Cowell D (eds), *The Politics of Crime Control* (SAGE Publications, 1991) 62

[82] Walker C and Rehman J, 'Prevent Responses to Jihadi Extremism' in *Global Anti-Terrorism Law and Policy* (2nd edn, Cambridge University Press 2012) 243

[83] Etzioni A, *The Spirit of the Community* (Fontana Press London 1995) 190-191

[84] ibid

[85] Rosenbaum DP, Lurigio AJ and Davis RC, *The Prevention of Crime: Social and Situational Strategies* (n 32) 19

conditions that contribute to offending.[86] The community refers to a set of social ties that link individuals, religious clustering or groups a geographic area such as a neighbourhood.[87] Community prevention can be enforced through 'surveillance, verbal reprimands, rejection, warnings and other pressures to achieve conformity'.[88] A sense of wellbeing, security, belonging and values of connectedness is necessary in the creation of civil and secure environments. This can be achieved by investing in neighbourhoods, family, schools, voluntary associations, sporting clubs and places of worships.[89]

Social prevention policy to counter cyber attacks may be designed and directed towards potential offenders and potential victims. Prevention includes encouraging and educating individuals to discharge their responsibility to ensure the security of their computer system.[90] Risks can be avoided through education and attentiveness to information.[91] According to Deputy Public Prosecutor 2:

> The public will be more alert. They can take care of themselves based on certain guideline. An informed person is better protected. He knows about the law. What is wrong and right.[92]

The level of awareness among the potential victims, especially youths can be increased through education. They need to know the repercussion of being involved in organised cybercrime and to avoid from becoming a victim. Security Professional 10 asserted that:

> Education and campaigns take precedence over other measures. The public needs to understand this problem before

---

[86] ibid 9

[87] Rosenbaum DP, Lurigio AJ and Davis RC, *The Prevention of Crime: Social and Situational Strategies* (n 32) 35; Walker C and Rehman J, ''Prevent' Responses to Jihadi Extremism' in *Global Anti-Terrorism Law and Policy* (n 82)

[88] Rosenbaum DP, Lurigio AJ and Davis RC, *The Prevention of Crime: Social and Situational Strategies* (n 32) 37

[89] Sutton A, Cherney A and White R, *Crime Prevention: Principles, Perspectives and Practices* (Cambridge University Press 2008) 89

[90] Brenner SW and Clarke LL, 'Distributed Security: Preventing Cybercrime' (n 79) 678

[91] Beck U, *Risk Society: Towards a New Modernity* (n 31) 35

[92] Interview with Deputy Public Prosecutor 2

> installing anti virus and encryption software. They still can access the Internet even though their computer is not equipped with antivirus. The problem often arises in a situation where there is handshake between the Internet users and web servers that are used to transfer the malware or virus. For instance, I attach malware to some pornographic images. Afterwards, I send the images to a person. There is a handshake once that person clicks the image. He has inadvertently downloaded the malware to his computer. He is at fault in this situation. He has chosen to access materials that may not be good for his computer. The Internet users need to know the causes of the problem. In addition, they should know security measures such as the appropriate password for their computer or online accounts. It should contain 13 characters, which are a mixture of capital letters, numbers, and special characters.[93]

A person may become the victim of cybercrime due to a failure to take proper preventive measures. The victim suffers losses in the form of compromised files and information due to his own recklessness or negligence. [94] Security Professional 10 further contended that lack of awareness contributes to this problem. He said that:

> I blame cyber attacks on hackers and the public. My company was involved in several campaigns to raise awareness among students. I discovered that most students do not understand the security measures to protect their computer especially smart phones. For instance, most of them do not realise that the creation of ID such as Gmail account for Android and Apple ID is necessary to protect the data. They may delete the data remotely if their smart phones are stolen.[95]

---

[93] Interview with Security Professional 10

[94] Brenner SW and Clarke LL, 'Distributed Security: Preventing Cybercrime' (n79) 679

[95] Interview with Security Professional 10

Brenner and Clarke suggested the implementation of responsibility on civilians through the creation of disincentives for not preventing cybercrime.[96] They contended that 'assumed risk creates a disincentives by negating the expectation that law enforcement will redress one's victimization by apprehending and sanctioning the perpetrator'. [97] Furthermore, they argue that the imposition of a duty to avoid becoming the victim of cybercrime is necessary especially for those who negligently contributed to consequent victimisation.[98] The policymakers in Malaysia may explore these suggestions for preventing cyber attacks.

The majority of the interviewees from all categories agreed that education and campaigns are the most effective measures in countering cyber attacks. Government agencies and private security companies should take part in the campaigns to raise awareness among the public in Malaysia. Their focus should be to make the public responsible for the safety of their computer through target hardening. For instance, the objective of the cyber security awareness campaign organised by CyberSecurity Malaysia is to educate and enhance 'the awareness of the general public on the technological and social issues facing Internet users, particularly on the risks they face online'. [99] It provides online information about safe computing, virus and worm, spyware watch and password protection.[100]

Besides those initiatives, the Malaysian Communications and Multimedia Commission (MCMC) has initiated the 'click wisely', campaign targeting the people who are vulnerable to the threat of cybercrime including children, youths and parents. [101] The campaign emphasises the 'acculturation of

---

[96] Brenner SW and Clarke LL, 'Distributed Security: Preventing Cybercrime' (n79) 692

[97] ibid 693

[98] ibid

[99] Cybersafe Digest <http://www.cybersafe.my/about.html> accessed 10 December 2016

[100] Cybersafe Digest <Youth http://www.cybersafe.my/cyberyouth.html> accessed 10 December 2016

[101] Klik Dengan Bijak <http://www.skmm.gov.my/Media/Announcements/Klik-Dengan-Bijak.aspx> accessed 10 December 2016

national principles in the daily Internet use'.[102] It was reported that nearly 2 million people have participated in the campaign since 2012.[103] The head of the campaign, K Juslly Elis said that 24000 activities had been conducted so far throughout Malaysia. MCMC also co-sponsored the Hack in the Box Security Conference (HITBSecconf) until 2014. HITBSecconf is an annual two days conference held in Kuala Lumpur and Amsterdam. It provides a platform for the security researchers and professionals from around the world to discuss and disseminate issues related to computer security.[104]

However, the effectiveness of education and campaign depends on their impact and outreach. According to private Sector Officer 1:

> Apart from strengthening the laws and technical measures, I quite agree that education and campaigns are necessary. I think the MCMC (the Malaysian Communications and Multimedia Commission) conducted a few education programmes. We can use the media especially television to reach the public. However, the problem is the government only broadcasts these programmes on RTM TV1 (Radio Television Malaysia is an agency under the Ministry of Communication and Multimedia of Malaysia).*[105]*

Moreover, education and awareness campaigns should leave a lasting impression on the public especially the youth. This may be achieved through constant effort and continuous activities. Security Professional 11 opined that:

> MCMC partially sponsored a hard-core hacking convention. It went on for quite a few years. There are guideline, convention, seminars; a lot of things have been going on. However, the implementation of the guideline is not carried out. The support

---

[102] ibid

[103] Bernama, 'Lebih 2 Juta Sertai Program Klik Dengan Bijak SKMM' <http://www.skmm.gov.my/Media/Press-Clippings/Lebih-2-Juta-Sertai-Program-Klik-Dengan-Bijak-SKMM.aspx> accessed 9.09.2016

[104] HITB Security Conference <https://conference.hitb.org> accessed 10 December 2016

[105] Interview with Private Sector Officer 1

> does not last for long. The agencies only did it at that time. Security is a long lasting process. The biggest challenge to security is human. They need to be reminded constantly. I am not sure how to quantify the degree of the effectiveness of the guideline and procedure. Is it 10% or 20%? The guideline should not only look good on paper.[106]

Apart from the potential victims, education may be used to persuade the perpetrators, especially the youths, not to use their skills for illegitimate purposes. According to Private Sector Officer 4:

> The situation can be reformed through education. We have to explain to them what is cyber attacks. For instance, hacking the wireless broadband connection can be considered as cyber attacks. The victims may experience slower Internet connectivity and unexpected overage charges on the bill. They also incur cost to trace the perpetrator.[107]

The youths are seen as vulnerable to wrongdoing. Security Professional 11 developed his hacking skills since he was a teenager. He said that:

> I was involved in the hacking scene at the age of 15. I learned about hacking when the Internet started. I was myself a victim of hacking. It wasn't really disruptive. Somebody uploaded pornographic picture. I started looking at the measures to remedy this situation. The knowledge did not come from the classes I attended at the University; I was hacking from my room at the university.[108]

It is vital to instil strong ethical standards in using the Internet at a young age. They constitute 60% of the Internet users in Malaysia and are particularly prone to computer misuse.[109] As indicated in Chapter 4, crime prevention policies in Malaysia are influenced by the principles of communitarianism, which emphasise the need to balance autonomy and

---

[106] Interview with Security Professional 11

[107] Interview with Private Sector Officer 4

[108] Interview with Security Professional 11

[109] Bernama, 'Lebih 2 Juta Sertai Program Klik Dengan Bijak SKMM' (n 103)

common good in the creation of good society. Communitarianism stresses the inclusion and integration of the people with individual's membership of interest groups and other social groupings providing a vital link between the individual and the nation.[110] Religious institutions such as the mosques are strongly supported by the state in Malaysia. They try to inculcate the young people with moral values and decency.

In addition, government agencies including the MCMC aim to reduce the rate of offenders by instilling wariness of cybercrime among young people especially below 30 years old.[111] Apart from MCMC, the Royal Malaysia Police (PDRM) launched the 'Be Smart' campaigns in an effort to reduce cybercrimes. They work together with institutions of higher learning such as the Limkokwing University of Creative Technology in order to increase awareness on crime prevention.[112] According to Police officer 3:

> 'Be Smart' campaigns include activities such as public lecture on awareness at the universities. Besides working together with Limkokwing, PDRM established the Crime Prevention Department. They organise awareness campaigns. I think that the awareness campaigns are effective. Statistic shows that crime rates are going down ever since the 'Be Smart' campaigns were launched. The outcome prompted us to continue the 'Be Smart' programmes.[113]

Social prevention strategies are designed for known offenders and individuals who have not committed any offences from all stages of life. Most of the strategies are aimed at 'early or formative stages of life (infancy through to the late teenage years).'[114] According to Bright, strategies in the

---

[110] Cavadino M and Dignan J, *Penal Systems: A Comparative Approach* (SAGE Publications 2006) 17

[111] Bernama, 'Lebih 2 Juta Sertai Program Klik Dengan Bijak SKMM' (n 103)

[112] Letchumanan D, 'PDRM and Limkokwing Launch Cyber Crime Awareness Campaign' Limkokwing Newsletter <https://www.limkokwing.net/malaysia/news/article/pdrm_and_limkokwing_launch_cyber_crime_awareness_campaign> accessed 27 September 2016

[113] Interview with Police Officer 3

[114] Sutton A, Cherney A and White R, *Crime Prevention: Principles, Perspectives and Practices* (n 89) 23

UK, US, Canada and France indicate that one of the best long-term solutions in preventing crime is by investing in children and young people.[115] This includes organising anti crime education in schools; providing work training, increasing employment opportunities and coordinating youth activities.[116] Parents, schools and the communities have to work together in monitoring the activities of the young people. The inclusion of the young people in these programmes and community institutions may reduce the rate of offending.[117]

On the whole, the findings of this study indicate that social prevention policy is pertinent in dealing with cyber attacks. Most of the participants in this study asserted that education and campaigns are vital to prevent a person from becoming the perpetrator and victim of cyber attacks. Several organisations may be used in order to enhance the impact and outreach of the cyber security education especially among youths. The Youth Societies and Development Act 2007 [Act 668] was enacted in Malaysia for the purpose of promoting and facilitating the development of youth in Malaysia from the aspect of education, research and human resource. The Act refers to youth as a person aged between 15 to 40 years old. The Minister of Youth and Sports of Malaysia is vested with the function to formulate the policies in relation to youth development including inculcation of healthy lifestyle and attitude development.[118] The National Youth Consultative Council and the Malaysian Institute for Research in Youth Development were established in order to provide consultation and to make recommendations on youth activities.[119] The Malaysian Institute for Research in Youth Development (the Institute) has so far raised issues involving youths in the areas of politic and

---

[115] Bright J, 'Crime Prevention: The British Experience' in Stenson K and Cowell D (eds), *The Politics of Crime Control* (n 81) 80

[116] Young J, 'Left Realism and the Priorities of Crime Control' (n 26) 153-154

[117] Sutton A, Cherney A and White R, *Crime Prevention: Principles, Perspectives and Practices* (n 54) 34

[118] S 34 of the Youth Societies and Development Act 2007; Ministry of Youth Vision and Mission <http://www.kbs.gov.my/en/kbs-info/menu-misi-visi-objektif.html> accessed 10 December 2016

[119] S 35, s 36, s 55 and s57 of the Youth Societies and Development Act 2007

economy.[120] This includes the strategies to increase the levels of patriotisms and entrepreneurship among youths in Malaysia. However, these organisations are not actively involved in cyber security. The Institute should conduct studies to develop cyber security courses and syllabus for youth.

4.3.1.2 Situational Crime Prevention

Situational crime prevention can be an effective tool to counter cyber attacks. Various theories have been developed about situational crime prevention including rational choice theory, routine activity theory, criminal lifestyle analysis, crime as opportunity and the economic analysis of crime.[121] Situational crime prevention may be applied, as 'crime is a supply side phenomenon- a consequence of the production and delivery of opportunities to commit offences.' [122] It has been suggested that the decrease of crime in industrial societies has been due to the improvement of security including specific security devices.[123] For instance, the usage of electronic immobilisers and central locking system contribute to the reduction in motor vehicle theft in England, Wales and Australia. [124] Intervention strategies are designed to minimise the opportunities of the commission of specific offences.

The opportunities to commit specific kinds of crime may need to be blocked in highly specific ways.[125] These strategies are incorporated in the work done by architects, urban planners, and law enforcement agencies. [126] They lead to the proliferation of detailed technologies for deterring specific

---

[120] Research Info graphic <http://www.iyres.gov.my/index.php?option=com_content&view=article&id=1126&Itemid=531&lang=en> accessed 10 December 2016

[121] Garland D, 'Ideas, Institutions and Situational Crime Prevention' in Hirsch Av, Garland D and Wakefield A (eds) *Ethical and Social Perspectives on Situational Crime Prevention* (Hart Publishing 2000) 9

[122] ibid 217

[123] Farrell G and others, 'The Crime Drop and the Security Hypothesis' Journal of Research in Crime and Delinquency 48 (2) 147-175

[124] ibid

[125] Clarke RV, 'Introduction' in Clarke RV (ed), *Situational Crime Prevention: Successful Case Studies* (2nd edn, Harrow and Heston 1997) 4

[126] Rosenbaum DP, Lurigio AJ and Davis RC, *The Prevention of Crime: Social and Situational Strategies* (n 32) 238

crimes.[127] Repetitiveness or the expectation of the occurrence of similar events is necessary in devising preventive strategies. According to Eck and Clarke, offenders are likely to follow standardised routines or scripts out of habit, necessity or convenience.[128] Understanding the routine followed by the attackers and the ability to predict future attacks is necessary in the formulation of the measures to counter cyber attacks.

Target hardening involves the enhancement of the level of difficulty in reaching the targets. They include 'improving natural surveillance, controlling access to property and deflecting offenders from settings in which crimes might occur'.[129]. The offenders are dissuaded from pursuing the targets due to their failure to overcome the target-hardening device.[130] Target hardening is especially important as cyber attacks are premeditated and the criminals usually plan their moves. Besides technical devices, other strategies may be used such as ensuring that the IT appliances and computer system are being constantly updated and improved; controlling the link to username, protecting email and web equipment; and issuing circulars to restrict the usage of electronic devices on the premises of the organisation.[131] In addition, computer users have the responsibility to protect their computer system by installing software such as anti virus and encryption.

However, situational crime prevention is not without its flaws. Firstly, this approach ignores the role of social and economic inequalities in triggering crime.[132] In addition, the victim shoulders the main burden of preventing the occurrence of crimes. Secondly, situational crime prevention can displace

---

[127] ibid

[128] Eck JE and Clarke RV, 'Classifying Common Police Problems: A Routine Activity Approach' in Smith MJ and Cornish DB (eds), *Theory For Practice in Situational Crime Prevention* vol 16 (Willan Publishing 2003) 8

[129] Garland D, 'Ideas, Institutions and Situational Crime Prevention' in Hirsch Av, Garland D and Wakefield A (eds), *Ethical and Social Perspectives on Situational Crime Prevention* (n 121) 9

[130] Rosenbaum DP, Lurigio AJ and Davis RC: *The Prevention of Crime. Social and Situational Strategies* (n 32) 132

[131] Interview with Private Sector Officer 2

[132] Rosenbaum DP, Lurigio AJ and Davis RC, *The Prevention of Crime: Social and Situational Strategies* (n 32) 162

the crimes from potential victims to others.[133] It simply averts crime away from the people who can afford to pay the cost for protection. Thirdly, the policymakers may not be interested in using situational crime prevention as 'the best it could do is to dislocate criminal activity in time, space, method and type of offense'.[134] Apart from that, the implementation of situational crime prevention measures requires some costs and to a certain extent, may hinder freedom, autonomy and privacy.[135]

Situational measures to counter cyber attacks may not always work for various reasons. Clarke identifies several obstacles that may impede the success of situational measures: (1) technical or administrative ineptitude; (2) the measures may be easily defeated by the offenders; (3) the assumption of an active role on the part of guards or ordinary citizens; (4) the measures may be defeated by the carelessness or idleness of potential victims; (5) the failure to properly analyse the problem; and (6) insufficient thought to users' needs.[136] These obstacles may impinge the effectiveness of the situational crime prevention in countering cyber attacks in Malaysia. In the following sections, the extent to which these factors undermine the situational measures in dealing with cyber attacks will be discussed.

This study highlights five situational measures to counter cyber attacks: risk assessment; controlling the access to the computer system and server; the usage of anti virus software, anti spyware and firewall; encryption; and surveillance. They will be discussed in the subsequent sections.

4.3.1.2.1 Risk Assessment

Risk assessment is one of the mechanisms that can be used to protect a computer system and data. Regulation 15.1 (e) of the Directive No 24

---

[133] Duff RA and Marshall SE, 'Benefits, Burdens and Responsibilities: Some Ethical Dimensions of Situational Crime Prevention' in Hirsch Av, Garland D and Wakefield A (eds), *Ethical and Social Perspectives on Situational Crime Prevention* (Hart Publishing 2000) 25

[134] Rosenbaum DP, Lurigio AJ and Davis RC: *The Prevention of Crime. Social and Situational Strategies* (n 32) 164

[135] Duff RA and Marshall SE, 'Benefits, Burdens and Responsibilities: Some Ethical Dimensions of Situational Crime Prevention' in Hirsch Av, Garland D and Wakefield A (eds), *Ethical and Social Perspectives on Situational Crime Prevention* (n 133) 23

[136] Clarke RV, Introduction' in Clarke RV (ed), *Situational Crime Prevention: Successful Case Studies* (n 125) 26

imposes an obligation on the part of the agencies and organisation from critical national information infrastructure to implement Information Security Management System (ISMS) to reduce the risk of cyber security incident.[137] Standards and Industrial Research Institute of Malaysia (SIRIM) is authorised to certify ISO/IEC 27001 for information security management.[138] The purpose of the certification is to guarantee the reliability of the information system and to provide assurance to the customers and stakeholders that their information is secured from 'damage, loss and misuse'. [139] Risk assessment and treatment are included in the implementation of the ISMS.

Some of the interviewees were sceptical about the effectiveness of this measure to counter cyber attacks. Private Sector Officer 1 argued that:

> If you ask security researcher or the people who are doing the technical things, they will say that ISO ISMS is just a process. You have to update your documents based on certain guideline. The certification does not necessarily guarantee security.[140]

Similarly, Security Professional 11 asserted that:

> MAMPU compels the government agencies to perform security assessment at least once a year. However, some of them are not doing that. There is a website on the Internet that keeps track of other websites that have been hacked. You can search dot gov dot my. If you go through the list, some of the websites are quite critical. They are dealing with the data of the users. They are being hacked on daily basis. You can browse zone h [http://www.zone-h.org/?zh=1]. You will see on daily basis gov.my being hacked. It has always been like this since I started in 2009 until 2016. I have been doing security assessment for the same agency. The first time I came, I

[137] National Security Council, *Arahan No. 24 (Directives No. 24)* (n 7)

[138] Information Security Management SIRIM <http://www.sirim-qas.com.my/index.php/en/our-services/management-system-certification-related-services/isoiec-27001-information-security-management> accessed 5 May 2016

[139] ibid

[140] Interview with Private Sector Officer 1

> presented the finding. The second time I came, I presented the same finding, the third year also the same. There is no change. I am not sure what is lacking. I've been doing this since 2009. Has it changed? Not to the extent that I can say I am quite proud of the infrastructure.[141]

In addition, only large companies and organisations are capable of implementing the standard suggested by the ISO/IEC 27001 for information security management. According to Private Sector Officer 3:

> Usually large organisations such as banks and companies with huge budget are capable to implement the standard in order to obtain the certification. However, organisations that are involved in the CNI such as Tenaga National Berhad [Malaysia's largest electricity company] and the military are compelled to get the certification.[142]

Therefore, the certification is not required for small companies. According to Private Sector Officer 1:

> Small companies need to have at least somebody to manage the security services. In general, they need to ensure that the system is backed up for 6 months, the back up system is efficient, and their account is updated. They need to review their user account at least once a year.[143]

It can be inferred that, risk management sounds good on paper, but this measure may not actually work in reality. The implementation of risk management depends on the action taken by the organisation to remedy the situation.

To sum up, government agencies and critical national information infrastructure organisations are obliged to implement risk management in order to ensure the security of the information system. This is done by obtaining the necessary certification including ISO/IEC 27001. This measure

---

[141] Interview with Security Professional 11

[142] Interview with Private Sector Officer 3

[143] Interview with Private Sector Officer 1

is not compulsory for small companies as long as they constantly update their computer system. The findings of the study suggest that this measure so far has failed to ensure the security of the government's information system. This is due to the failure of the government's officials to implement the required procedure. For Regulation 15.1 (e) of the Directive No 24 to work, effective enforcement and sanctions must be in place. The government should develop not only strict rules on risk management but also the process of auditing the information system. Disciplinary action should be initiated against officials who fail to comply with the standard and security audits.

4.3.1.2.2 Controlling the Access to the Computer System and Server

Access control may be used to prevent potential offenders from entering places such as offices and factories.[144] Restricting the access to the computer system and server can prevent the occurrence of cyber attacks. According to Private Sector officer 3:

> Our defence system is one of the best. We hardened our website to restrict the entry to the outsiders. Some of our old websites had been subjected to web defacement. Those are seasonal websites that were used for conference purposes. We did not monitor those websites anymore.[145]

He described the measures taken to improve the security of the website:

> We use the web vulnerability scanner software to scan the system of the new websites before they are approved. This is especially if the websites are accessible to the users outside of the organisation. We have to make sure that the coding is safe. We will hold our approval if the report indicates the existence of high vulnerability such as potential exposure to injection. We ask the programmer to check the system again.[146]

---

[144] Clarke RV, Introduction' in Clarke RV (ed), *Situational Crime Prevention: Successful Case Studies* (n 125) 17

[145] Interview with Private Sector Officer 3

[146] Interview with Private Sector Officer 3

In addition, entry screening allows the management to detect the people who do not conform to entry requirements especially in relation to prohibited goods.[147] According to Private Sector Officer 2, visitors may be compelled to itemise their electronic devices before they are allowed to access the premises.[148] The entry requirements may be extended to the employees at the organisational level. Organisations usually require their employees to adhere to certain rules. According to Private Sector officer 4:

> Our company policy stipulates that whoever connects to the server without consent may be subjected to legal measures such as imprisonment or fine. This policy is imposed on staff and outsiders. I can be subjected to disciplinary proceeding for allowing someone to access the server. The warning is given every time we log in the system. Some of our clients impose restrictions before we can access their server. For instance, they require us to contact their engineer in order to get the entry code every time we want to connect to the server. They may allow us to access the server at specific directory. Some of them deny the access to their server. They will fix the problem on their own.[149]

Therefore, the findings suggest that access control is effective in reducing the opportunities for the commission of cyber attacks. This includes using certain devices to restrict the access to the computer system and entry screening to ensure the safety of the electrical devises. This measure should be made mandatory for government agencies and the critical national information infrastructure organisations.

4.3.1.2.3 Anti Virus Software, Anti Spyware and Firewall

Most cyber security agencies recommend the installation of anti virus software, anti spyware software and firewall in order to protect the computer

---

[147] Clarke RV, Introduction' in Clarke RV (ed), *Situational Crime Prevention: Successful Case Studies* (n 125) 19

[148] Interview with Private Sector Officer 2

[149] Interview with Private Sector Officer 4

system against cyber threats.[150] However, some of the interviewees are sceptical about the effectiveness of this measure. Private Sector Officer 4 ranked installation of anti virus software as the least effective measure in countering cyber attacks. She argued that the perpetrators of cyber attacks usually are good at spotting the vulnerabilities of anti virus software.[151] Security Professional 11 also shared similar opinion. He argued that:

> Anti virus does not detect the attempt to hack a website. It protects the operating system of the computer. This is OS and this is the web application; antivirus would be able detect to a certain extent what they are doing over here. However, there is a way to bypass anti virus. In some instances, the anti virus acted as the gateway. Anti virus does not guarantee your safety. If you use wrong antivirus, you will open another window for the attack to come in. [152]

In addition, some Internet users may lack the ability to identify and install genuine anti virus software. Security Professional 10 expressed his concern with the authenticity of the software. He contended that:

> We do not know for certain whether the anti virus software which are available on the Internet is genuine. Nobody can stop me from labelling spyware that I created as 'anti virus'. I can upload the spyware on the Internet. The Internet users may assume that it is anti virus programme and download it from the Internet. They don't realise that it is actually a malware. It is vital for the Internet users to be able to identify genuine anti virus.[153]

Furthermore, anti virus may be costly, and the users have to frequently update the software. According to Police Officer 3:

---

[150] Cybersecurity Malaysia, 'Cybersafe Digest' <http://www.cybersafe.my/cyberyouths-tips-virus-worms.html> accessed 10 December 2016

[151] Interview with Private Sector Officer 4

[152] Interview with Security Professional 11

[153] Interview with Security Professional 10

> I think anti virus software is important. However, there is no point in installing the anti virus, if the users don't update the software continuously. The computer is open to vulnerabilities and attacks after the expiry date. I rank the installation of anti virus among the most effective measures, provided that the users regularly update the software.[154]

Should the government consider imposing an obligation on the manufacturers or distributors to install anti virus programme before computers are sold to the customers? Such an obligation would be difficult to be implemented and enforced. According to Police Officer 2:

> The government may require the computer manufacturers to install anti virus in order to reduce the opportunities for cyber attacks. However, have they committed any offences if they fail to install anti virus especially if the computer is attacked? The rules should be inserted in which legislation? Who is going to implement the rules? Is it MCMC or Cybersecurity?[155]

Apart from enforcement, the imposition of the obligation to install anti virus may infringe the right to buy goods. Thus, intermediate ways of ensuring the installation of anti virus software on the computer may be used. For instance, at the organisational level, the employees may be required to ensure that their personal computers are equipped with anti virus.

To summarise, anti virus software, anti spyware and firewall should be used to protect computer system from cyber attacks. The findings revealed that the effectiveness of this measure depends on the ability of the Internet users to install genuine software and to ensure it is constantly updated. This study suggests that the government should educate the public on the importance of this measure. In addition, they may be given an incentive to improve the security of their computer system.

---

[154] Interview with Police Officer 3

[155] Interview with Police Officer 2

4.3.1.2.4 Encryption

Blocking the access to communications by using encryption may reduce the opportunities for cyber attacks. Cryptography is defined as 'a transformation of a message that makes the message incomprehensible to anyone who is not in possession of secret information (the key) that is needed to restore the message to its normal plaintext or clear text form'.[156] Cryptography is available for free download from the Internet. However, study shows that many people were unaware that encryption is available or did not know about cryptography.[157] Encryption is mostly used by corporate entities. Deputy Public Prosecutor 1 asserted that 'encryption is beyond the standard user to comprehend. It is targeted on corporate entity. Ideally, private users should have encryption for sensitive file'.[158] Encryption provides better protection for data 'with unbreakable codes' in comparison to firewalls.[159] However, some of the interviewees from all categories warned of the dangers of using encryption software manufactured by foreign companies. Police officer 3 argued that:

> You have to remember that when you install something, it creates vulnerabilities. We need to have solution such as decryption. The usage of encryption for normal computer including email is not problematic. However, it is different if an organisation such as the military, purchases encryption developed by a foreign company. There is probability that the people who are interested in the information will design a backdoor programme for the encryption. I think it is better to use encryption produced by our own specialists to prevent from any vulnerability.[160]

---

[156] Diffie W and Landau S, *Privacy on the Line: The Politics of Wiretapping and Encryption* (The MIT Press 2007) 13

[157] Dupont B, 'Hacking the Panopticon' in Deflem M (ed), *Surveillance and Governance: Crime Control and Beyond* (Emerald JAI Press 2008) 270

[158] Interview with Deputy Public Prosecutor 1

[159] Arquilla J, 'Rebuttal Cyberwar is Already Upon Us' (2012) 192 Foreign Policy; Mar/Apr 2012; 192, 84

[160] Interview with Police Officer 3

In addition, technological solutions such as encryption may hinder the attempts by the government to conduct surveillance for information and to protect national security. It may impede the state's ability to investigate and prosecute offenders. According to Police Officer 2:

> I investigated a case involving the unauthorised access of data by an ex-employee. He copied and encrypted the data. It was difficult for me to prove the existence of the data. The file name indicated that the data is there. However, I cannot open the file.[161]

In this way, it has been argued that encryption provides a 'means for tax evasion, money laundering, espionage, contract killings and implementation of data havens for storing and marketing illegal or controversial materials'.[162] Recently, a US magistrate court declared that Apple must build a tool to enable the FBI to access an IPhone owned by the San Bernardino shooters.[163] The government may not be in favour of encryption and may wish to start regulating it. However, any such attempt by the government may impede on the people's privacy and would not be welcomed by telecommunication companies such as Apple.

Some of the participants in this study argued that the access to the encrypted data is permissible in Malaysia on the basis of national security. Deputy Public Prosecutor 2 asserted that:

> Commenting on Apple vs FBI case is a tricky task. US values freedom of speech and expression, isn't it? The system in Malaysia is different. The encrypted information may be accessed on the pretext of eliminating threat to national security.[164]

---

[161] Interview with Police Officer 2

[162] Denning DE, 'The Future of Cryptography' in Loader BD (ed) *The Governance of Cyberspace* (Routledge 1997) 177

[163] *Order Compelling Apple, Inc to Assist Agents in Search*, No. ED 15-0451M, United States District Court for the Central District of California

[164] Interview with Deputy Public Prosecutor 2

Police Officer 3 also asserted that judges have the discretion to allow the access to the encrypted data, if the Apple vs FBI scenario happens in Malaysia. He said that 'judges should evaluate the evidence and decide whether the access to the information is necessary to bring those responsible to justice.'[165]

Several laws in Malaysia allow the access to computerised data including encryption and decryption codes by authorised persons for investigation purposes.[166] For instance, the Communications and Multimedia Act 1998 provides that a magistrate may issue a warrant authorising any police officer equal and above the rank of Inspector and officer of the MCMC to search and seize computerised data which contain or reasonably suspected to contain information pertaining to the commission of any offences under the act.[167] A police inspector is permitted to search and seize the computerised data without warrant if he has reasonable cause to believe that the evidence may be tampered with, removed, damaged or destroyed due to the delay in obtaining a search warrant.[168] The Act also empowers the police to seize the password of the encrypted data.[169]

All in all, this section discusses the main arguments concerning the application of encryption in dealing with cyber attacks. The findings demonstrate that encryption provides better protection for data and confidential information. Accordingly, the government should encourage the people to use this measure in order to safeguard their data. However, the findings also reveal several disadvantages of encryption. It may be used to facilitate the commission of criminal offences and to circumvent the law. Thus, legislative controls are necessary in order to break unscrupulous encryption schemes. S 49 of the Regulation of Investigatory Powers Act 2000 allows the government of UK to investigate electronic data protected

---

[165] Interview with Police Officer 2

[166] S 116B of the Criminal Procedure Code, S 81 of the Postal Services Act 2012, s 249 Communications and Multimedia Act 1998, S 79 Digital Signature Act 1997 and S 32 of the Strategic Trade Act 2010

[167] S 247 of the Communications and Multimedia Act 1998

[168] S 248 of the Communications and Multimedia Act 1998

[169] S 249 (2) of the Communications and Multimedia Act 1998

by encryption. Any person may be required by a judge to disclose information involving the interest of national security, to prevent or detect crime and to preserve the economic well being of the UK.[170] Notices requiring disclosure must be issued before the authorities can access the information.[171] The government of Malaysia may formulate powers and safeguards similar to s 49 of the Regulation of Investigatory Powers Act 2000.

4.3.1.2.5 Surveillance

Managing information is fundamental to the administration of the modern government.[172] Effective surveillance is necessary for the states to maintain both 'allocative resources (planning, administration) and authoritative resources (power and control)'.[173] States use surveillance systems to monitor public space in order to identify, apprehend and punish the offenders.[174] Surveillance is needed for the purpose of enhancing national security and preventing violence. On the other hand, private security officers use surveillance systems to enforce the internal rules of the organisation and informal rules of private justice.[175] Private Sector Officer 2 said that 'we use the surveillance cameras to monitor our staff. They can be subjected to disciplinary proceedings for doing unauthorised activities online'.[176] A breach of rules of the organisations usually entails warnings from the administration rather than criminal prosecution.[177]

---

[170] S 49 (3) of the Regulation of Investigatory Powers Act 2000

[171] S 49 (4) of the Regulation of Investigatory Powers Act 2000

[172] Webster F (ed), *Theories of the Information Society* (Routledge 1995) 124

[173] Giddens A, 'The Nation State and Violence: Volume Two of a Contemporary Critique of Historical Materialism' in Webster F (ed), *Theories of the Information Society* (Routledge 1995) 59

[174] Mccahill M, 'Plural Policing and CCTV Surveillance' in Deflem M (ed), *Surveillance and Governance: Crime Control and Beyond* (Emerald JAI Press 2008) 215

[175] ibid 215-216

[176] Interview with Private Sector Officer 2

[177] Mccahill M, 'Plural Policing and CCTV Surveillance' in Deflem M (ed), *Surveillance and Governance: Crime Control and Beyond* (n 174) 209

The main function of overt surveillance is to furnish a deterrent threat to potential offenders.[178] Electronic surveillance enables the police to infiltrate and intrude upon the interactions of a group of people who are involved in criminal activities. This is necessary, as many criminal activities especially organised crime such as drugs, prostitution and gambling do not have readily identifiable victims.[179] According to Police Officer 3:

> Surveillance can be divided into two types: people surveillance and programme surveillance. The computer will do the monitoring on our behalf. The information will be passed to the intelligence. When there is an issue, we already have the information. The police don't have surveillance power. However, we can perform lawful interception under s116C of the Criminal Procedure Code. Similar provision is provided under the Kidnapping Act. Lawful interception is extended to data. Lawful Interception is related to surveillance. This is because we can control the gateway; we know what happens and what has been mentioned on the Internet. MACC also perform similar function.[180]

Apart from the Malaysia's Criminal Procedure Code, the Security Offences (Special Measures) Act 2012 [Act 747] also permits interception of communications by the Police in relation to the commission of security offences.[181] The Public Prosecutor may require a Communication Service Provider to intercept and retain a specified communication.[182] Special investigative measures such as intercepting private communication are

---

[178] Clarke RV, 'Introduction' in Clarke RV (ed), *Situational Crime Prevention: Successful Case Studies* (n 125) 20

[179] Diffie W and Landau S, *Privacy on the Line: The Politics of Wiretapping and Encryption* (n 156) 129

[180] Interview with Police Officer 3

[181] S 6 (1) of the Security Offences (Special Measures) Act 2012; Chapter VI (offences against the State, Chapter VIA (offences relating to terrorism) and Chapter VIB (organized crimes) of the Penal Code

[182] S 6 (2) of the Security Offences (Special Measures) Act 2012

considered necessary by the government to fight terrorism and other challenges.[183]

Internet surveillance is challenging due to several factors. Firstly, it is difficult for a central authority to control the flow of data as 'the internet is built as a decentralised and distributed architecture with multi directional connections among all nodes in the networked information environment'. [184] The architecture of the Internet excluded the concept of centrality in order to increase the Internet's resilience in case of a major failure of the central node.[185] The Internet users may access and communicate with each other through a large number of simultaneous paths. [186] Police Officer 2 acknowledged this problem. He asserted that:

> Mycert monitors the attacks to the server and computer system. We only monitor the social media. We only monitor cyber attacks if a report is lodged to the police. We don't have the information about the attacks on dotcomdotmy websites. Anti virus companies usually keep track of the attacks on websites. Mycert is responsible to protect the security of the network in Malaysia. Most of the victims will lodge report to Mycert. They will advise the victims to report the incidents to the police. USA has the capability to infiltrate and scan the data that go through their gateway. Malaysia is considering this measure. However, this is difficult as we have a lot of gateways in comparison to other countries such as China. They have only one gateway. Malaysia has 6 or 7 gateway to allow the Internet access. Recently, the users of Celcom (Internet service provider) cannot access Malaysia Kini. However, those who are using Maxis can

[183] Patail AG, 'Speech by the Attorney General of Malaysia at the Opening of the Legal Year 2013' (2013) 1 MLJ ccxi

[184] Dupont B, 'Hacking the Panopticon' in Deflem M (ed), *Surveillance and Governance: Crime Control and Beyond* (n 157) 262

[185] ibid

[186] ibid

> still access Malaysia Kini. They only block Celcom's gateway. MCMC can instruct telcos to block certain websites.[187]

The government may reduce its enforcement burden by limiting the gateway to the arena where cybercrime flourishes.[188] This may be done through licensing of ISPs and restricting consumer access.[189] However, some of the interviewees argued that the usage of electronic surveillance by the police or state agencies is limited due to the disparity of laws between states. According to Security Professional 10:

> Surveillance is usually only effective in dealing with child pornography. You cannot find child pornography materials in any countries. Apart from that, you can obtain all kinds of data from the Internet. Some states prohibit certain searches; others allow all kinds of searches. There is disparity of the laws between countries. Recently, IS made threats of harm to Malaysia via a video posted on YouTube. Besides YouTube, they can upload the video on Dailymotion. They can also upload the video on Google and provide the link through SMS. You cannot watch the video that show people beheaded by IS in Malaysia. You can watch the video using US's IP address. A consensus view among states is necessary to put a stop to all this.[190]

Secondly, the subjects of surveillance may use several ways to evade Internet surveillance. They use blocking moves such as cryptography to block the access to communications where messages transit through several paths.[191] In addition, they can also use masking moves that allow users to surf the web anonymously.[192] Websites such as Greycoder offers

---

[187] Interview with Police Officer 2

[188] Brenner SW and Clarke LL, 'Distributed Security: Preventing Cybercrime' (n79) 700

[189] ibid

[190] Interview with Security Professional 10

[191] Dupont B, 'Hacking the Panopticon' in Deflem M (ed), *Surveillance and Governance: Crime Control and Beyond* (n 157) 270

[192] ibid 271

operating system that allows anonymous web surfing and encryption using anonymous Internet connection such as Tor.[193] According to Private Sector Officer 3:

> The perpetrators are mostly member of the open source gang. They use open source operating system without interface such as Linux. They will type command whenever they try to access anything.[194]

Masking tools such as TOR (the onion router), Freenet and Psiphone can be downloaded for free from the Internet.[195] They enable Internet users to thwart surveillance attempts by randomly routing the information through other Internet users.[196] Lastly, many Internet users do not look upon Internet surveillance with favour. Surveillance appears unfair as their privacy is infringed. In *Halford v United Kingdom*, the European Court of Human Rights held that telephone calls made from business premises as well as from the home may fall within the ambit of private life and correspondences under Article 8 of the European Convention on Human Rights.[197] The Court further held that:

> The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in and conditions on which public authorities are empowered to resort to any such secret measures.[198]

Private Sector officer 4 ranked surveillance by the police or state agencies as the most effective measures to counter cyber attacks. She is 'willing to sacrifice her privacy if the police are really doing their job'.[199] However, other

---

[193] Greycoder <https://greycoder.com/anonymous-linux-distributions/> accessed 10 December 2016

[194] Interview with Private Sector Officer 3

[195] Dupont B, 'Hacking the Panopticon' in Deflem M (ed), *Surveillance and Governance: Crime Control and Beyond* (n 157) 271

[196] ibid

[197] *Case of Halford v United Kingdom* App no 20605/92 (ECtHR, 25 June 2004*)*

[198] ibid

[199] Interview with Private Sector Officer 4

interviewees disagreed with this contention. Security Professional 11 argued that:

> I am a privacy advocate. I wouldn't want any form of surveillance to be applied here. The public doesn't know half of what the GCHQ is doing. We would argue that we know a lot more about FBI and the three related agencies from the Europe. What they are doing versus what GCHQ is doing. I would argue more towards the monitoring of the citizen. Even without monitoring all the IT, the law enforcement agency has detected most of the cases involving high-risk issues. This is more with regard to the flow of data information.[200]

Similarly, Legal Practitioner 3 emphasised that surveillance should be confined to habitual criminal:

> Personally I think this is hard. It requires intensive manpower. I am sure that the special branch is doing it. It's like asking whether the police are relevant. They need to be around. However, they cannot actively snoop on people. It is a balancing exercise. I am inclined to agree that you can actively survey someone is proven to be a habitual cyber criminal. Privacy is essential in Islam; surveillance is detrimental to Islamic principles.[201]

This section demonstrates the challenges in using Internet surveillance to counter cyber attacks in Malaysia. Surveillance is difficult due to the resilience of the Internet, the disparity of laws between states and the perpetrator's technical expertise. Although there is evidence to suggest that this measure is necessary to enhance national security, some participants argued that surveillance might be used to invade people's privacy. Chapter 6 provides further elaboration on the usage of surveillance under international law.

---

[200] Interview with Security Professional 11

[201] Interview with Legal Practitioner 3

4.3.1.3 The Role of the Internet Architecture

This section examines the role of Internet's architects especially the Internet Service Providers and computer manufacturers to counter cyber attacks in Malaysia. The architecture of the Internet has an important role to play in the development of a comprehensive strategy to counter cyber attacks. According to Lessig, 'code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed and the extent to which access will be guaranteed'.[202] Codes are not just a question of engineering; they represent values.[203] The code has its own norms which is reflected in its structures or in the rules it enforces.[204] Therefore, it is pertinent to look into the identity of the code writers, who controls them and how they use the code to regulate the Internet.[205]

According to Schewick, the texts on Internet policy define architecture as 'the software and hardware that make up the Internet.[206] Architecture influences human behavior by constraining the actors who 'will develop, produce or use the system, the relationships among them and the governance structures they use to interact with each other.'[207] The network architect of today's Internet classifies the roles of the participants during the exchange of information in three categories: (1) Internet Service Provider (ISP) who owns the physical network including cable, optical fiber, telephone line and satellite; (2) Internet Content (ICP) provider such as Google and Yahoo; (3) general users who use the internet to obtain information.[208] Brenner refers to the manufacturers of cyber related devices as the 'architects'.[209] She suggested that civil liability and criminal liability should be

---

[202] Lessig L, *Code Version 2.0* (Basic Books 2006) 79

[203] ibid 78

[204] ibid 62

[205] ibid

[206] Schewick BV, *Internet Architecture and Innovation* (MIT Press 2010) 19-20

[207] ibid 28

[208] Fu C and others, 'Study on the Contract Characteristics of Internet Architecture' Enterprise Information Systems, 5:4, 495-513, DOI: 101080/175175752011570457

[209] Brenner SW, 'Cybercrime: Rethinking Crime Control Strategies' in Jewkes Y (ed), *Crime Online* (Willan Publishing 2007) 24

imposed on 'architects' such as the software industry due to their role in creating and sustaining cyberspace. This includes the usage of criminal product liability to ensure that the product meets some threshold level of adequacy.[210]

The government is tasked with ensuring a secure cyber system to protect the interests of the public especially the Internet users. This includes engaging the services of Internet's architects such as ISPs to unravel the identity of the culprits behind cyber attacks. For instance, the US Congress enacted the Communications Assistance for Law Enforcement Act in 1994 to regulate the design of the network in order to preserve the ability of law enforcement to conduct electric surveillance.[211] Each telecommunication carrier has to ensure that the law enforcement officials are able to conduct electronic surveillance pursuant to court order or other lawful authorization on the equipment and facilities subscribed by their customers for the purpose of communication.[212] The law enforcement officers in Malaysia are not conferred with similar power. However, the Communications and Multimedia Act 1998 permits an authorised person to request the ISPs to provide records, accounts, computerised data and documents in relation to any offences under the Act.[213]

In addition, the government may impose obligations on the ISPs and computer manufacturers under the Communications and Multimedia Act 1998 to secure and prevent hardware and software from being affected by cyber attack. Private Sector Officer 1 argued that:

> Who should be responsible if somebody bought a modem that has vulnerability? It starts attacking other people. Who has the

---

[210] Brenner SW and Clarke LL, 'Distributed Security: Preventing Cybercrime' (n 79) 694

[211] Lessig L, *Code Version 2.0* (n 202) 63; Congress. Gov <https://www.congress.gov/bill/103rd-congress/house-bill/4922> accessed 15 January 2017

[212] Federal Communications Commission, 'Communications Assistance for Law Enforcement Act' <https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance> accessed 15 January 2017

[213] S 254 of the Communications and Multimedia Act 1998

> capability to stop it? Is it the ISP, the government or MCMC? The manufacturer has the responsibility to pre install the modem with anti virus. However, the manufacturer is outside of Malaysia. We have that dilemma. A brand is infected by DDOS. We can shut down the device, but we don't want to burden the customer. He will enquire why the ISP shut down his device? Can MCMC issue order to shut down the device? What is the definition of communication?[214]

Software has become essential in the national infrastructures; thus, a system must be devised to ensure that software manufacturers are taking adequate measures to ensure the reliability of their products.[215] Software companies such as Microsoft are capable of providing protection to software and encrypting emails. ICPs such as Google are also capable of detecting cyber attacks and warn the Internet users of the dangers of failing to improve their security system. According to Security Professional 11:

> In my opinion, cyber attacks can be sponsored by states. However, it takes a long time to coordinate attacks against huge agencies or organisation. Google, Yahoo, Twitter and Facebook may issue specific reminder or notification about the attacks. Google may notify that state sponsored hackers have attacked my email. However, they will not reveal how the attacks were discovered. They may use pop up notification to inform that there are cyber attacks and you are advised to take measures to rectify the situation. This is quite serious because the perpetrator is attacking the entire organisation.[216]

In addition, the government may monitor the production of the switch systems by companies such as Cisco. They could be compelled to install security software before selling their products.

---

[214] Interview with Private Sector Officer 1

[215] Brenner SW, 'Cybercrime: Rethinking Crime Control Strategies' in Jewkes Y (ed), *Crime Online* (n 209) 25

[216] Interview with Security Professional 11

The instillation of prevention into the design of services, products and systems perhaps is a 'cost effective means of tackling crime and can be directly influenced by the policymakers'.[217] Lessig argues that 'as code writing becomes commercial as it becomes the product of a smaller number of large companies - the government's ability to regulate it increases. The more money there is at stake, the less inclined business would bear the costs of promoting an ideology.[218] The government may take steps to 'induce the development of an architecture that makes behavior more regulable' to overcome the objections.[219] Although this approach can help in reducing cyber attacks, however, it is difficult to implement due to several reasons.

The ISPs and computer manufacturers prefer self-regulation instead of intervention by external bodies including government legislation. According to Security Professional 10:

> I think such obligation already exist at the organisational level. For instance, we developed the Internet penetration test. We used a pen tester to check the security of the system. This is necessary to ensure the system is safe before our customers can use it. It may be difficult to transform such obligation into legislation. Each system has different behaviour and purposes.[220]

Policymaker 4 made similar observation. He asserted that:

> I think self-regulation is prevalent in Malaysia. It is good to impose obligation on the ISPs. But, I don't think they will agree. Personally, I want them to be responsible. On the other hand, they don't want to be responsible. ISPs have the technology to ensure the safety of the Internet. However, it involves cost. They are commercially driven entities. Ultimately, the cost will

---

[217] Farrell G and others, 'The Crime Drop and the Security Hypothesis' Journal of Research in Crime and Delinquency 48(2) 147-175

[218] Lessig L, *Code Version 2.0* (n 202) 71

[219] ibid 62

[220] Interview with Security Professional 10

> be passed down to the end users. There are some issue with regard to this.[221]

In addition, ISPs and computer manufacturers may argue that the Internet should be free from any intervention and that regulatory measures infringe their commercial freedom and intellectual development. According to Private Sector officer 3, 'ISPs are profit-oriented companies. They cannot simply block any websites. They know what they stand to lose if they do that. Their customers will choose other ISPs.' [222] Furthermore, according to Private Sector Officer 1, the ISPs will try to avoid causing inconveniences to their customers. He said that:

> This is our business. We don't want people to get hassled with this kind of pop-up: 'your computer has been infected please clean it or use this antidote to clean it'. The idea is good and it has been implemented in Japan. A pilot study to test the pop-up should be implemented at the public sector. The focus right now is to ensure our customers are not particularly bothered about things such as pop-up. [223]

With regard to the implementation of Directives 24 issued by Malaysia's National Security Council, Private Sector Officer 1 asserted that:

> NSC issued Directive No 24 in 2011. There is no guideline on the implementation of the Directives. Who is going to do the audit? Where is the audit? There is no progress and success story. Which CNII comply with the Directive? ISP is included in the scope of the Directives. How about the subsidiary of the ISP? Is it the whole group or just a portion related to the Internet? [224]

Furthermore, some of the ISPs and computer manufacturers may incur financial burdens by implementing measures such as the storage of data. Private Sector Officer 4 claimed that:

---

[221] Interview with Policymaker 4

[222] Interview with Private Sector Officer 3

[223] Interview with Private Sector Officer 1

[224] Interview with Private Sector Officer 1

> From a consultant's point of view, we don't have the capability to store huge amount of data. We can keep the data for a maximum of three months. We have to examine his activities within that period. We will delete the data in order to free the space for other data. The cost of storing the data is high, as the company has to use a lot of servers.[225]

Security Professional 5 argued that the ISP's capability is restricted due to the different security level of the Internet users:

> The ISP provides services to many companies. They each have their own security level. It is based on their business. Banking and insurance companies have higher security level, as their data is more sensitive and highly confidential, whereas the security level for entertainment companies is low. The ISP only monitors and controls the access of the packet. I think this measure is not suitable as companies or the industry have different security level.[226]

Another problem with regulating the architecture of the Internet is that the computer network is operated in different places all around the world. Thus, states are only capable of imposing this regulation in their own territory. International organisation and agreement are needed to implement this regulation globally or to set the international standard on computer security. The International Telecommunication Union may perform this function; however this will not take place due to objections by member states such as US. This study shall return to this question in chapter 6.

4.3.1.4 National CERT and Private Sector

The purpose of this section is to analyse the role of the national Computer Emergency Response Team (CERT) and private sector in dealing with cyber attacks in Malaysia. The enforcement actions that can be taken by states may be limited due to financial constraints and limited human resources. Thus, the participation of the private entities and national CERT may

[225] Interview with Private Sector Officer 4

[226] Interview with Security Professional 5

alleviate the burden of the state in dealing with cyber attacks. The Ministry of Science, Technology and Innovation of Malaysia established the national cyber security specialist agency, which is known as CyberSecurity Malaysia. [227] This agency is given the task to prevent and minimise disruptions to critical information infrastructure.[228] It provides services such as the management of security quality and research. The Malaysia Computer Emergency Response Team (MyCERT) was formed in 1997.[229] The aims of MyCERT are to reduce attacks and to minimise any consequential damage. MYCERT handles cyber security related incidents such as intrusion, identity theft, malware infection and cyber harassment.[230]

It is noted that the Internet users may report computer security incidents to MyCERT through online form, email, short text messaging services, phone call, fax and mobile applications.[231] The statistics show that 38 Denial Of Service attacks, 33 content related incidents, 1714 intrusions, 303 intrusion attempts, 567 malicious codes and 22 vulnerabilities were reported to MYCERT in 2014.[232] They also reveal that 1525 spam containing virus, 1285605 botnet drones count by unique IP and 1486017 malware infection by unique IP were reported in 2014. The overall numbers of incidents reported to MYCERT have increased until October 2016. The statistics indicate that 33 content related incidents, 63 Denial of Service attacks, 2143 intrusions, 243 intrusion attempt, 338 malicious codes, 28 vulnerabilities and 4766 spam containing virus were reported to MyCERT. In addition, they also

---

[227] Cybersecurity Malaysia, 'About Us' <http://www.cybersecurity.my/en/about_us/corporate_overview/main/detail/2065/index.html>

[228] ibid

[229] MyCERT, 'Mission, Vision, Background' <http://www.mycert.org.my/en/about/about_us/main/detail/344/index.html>

[230] ibid

[231] MyCERT, 'Cyber 999 Help Centre' <https://www.mycert.org.my/en/services/report_incidents/cyber999/main/detail/443/index.html>

[232] MyCERT, 'MyCERT Incident Statistics <https://www.mycert.org.my/statistics/2015.php> accessed 15 January 2017

show 1681539 botnet drones count by unique IP and 986998 malware infection by unique IP were reported to MyCERT.[233]

The statistics demonstrated the sheer volume of the cyber security incidents and threats in Malaysia. Internet users especially small companies lodge the reports in order to seek technical advice and assistance.[234] MyCERT will verify and investigate the reports. It then provides technical support and analysis in order to prevent future attacks.[235] However, the complainers have to refer the incidents to the police if they want to recover their losses.[236] According to Security Professional 1, the complaints usually have not escalated into something serious which require the complainers to lodge report to the police.[237] Some of the participants from all categories considered that CyberSecurity Malaysia and MyCERT are more effective than the police in handling cyber attacks.[238] However, MyCERT is not equipped with the power to enforce the law. According to Deputy Public Prosecutor 2:

> CERT only deals with the technical aspect. However, there is no investigating officer; their function is limited. The job of a police is to secure the evidence. In order to apprehend the accused, the police needs to go to CyberSecurity Malaysia to find out what is inside the computer. Their roles do not supersede each other's.[239]

Other countries such as the US and UK have also established national CERTs to deal with cyber attacks. The CERT Coordination Centre US was established in 1988 in response to the Morris Worm incident. This organisation works together with the government, law enforcement and the academia such as the Carnegie Mellon University to develop advanced

---

[233] MyCERT, 'MyCERT Incident Statistics <https://www.mycert.org.my/statistics/2016.php> accessed 15 January 2017

[234] Interview with Security Professional 4

[235] ibid

[236] Interview with Security Professional 1

[237] ibid

[238] Interview with private Sector Officer 2

[239] Interview with Deputy Public Prosecutor 2

methods and technologies to counter cyber threats.[240] Pursuant to the National Cyber Security Strategy 2011, UK government established the UK National Computer Emergency Response Team (CERT-UK) in 2014. CERT-UK works together with the industry, government and academia to enhance UK cyber reliance.[241] This agency is responsible to manage the national cyber security incident, to provide support to companies in handling cyber security incidents and to promote cyber security awareness.

Cooperation between national CERTs is necessary in order to strengthen the defence against cyber attacks. States have developed frameworks to enhance cyber security especially at the regional level. For instance the Asia Pacific Computer Emergency Response Team (APCERT) was established for the purpose of improving the region's awareness and competency in relation to cyber security.[242] APCERT facilitates the exchange of information and technology among member states and the development of the measures to counter large-scale or regional network security incidents.[243] Apart from APCERT, the Organisation of the Islamic Cooperation also had established the OIC-CERT. The objective of OIC-CERT is to foster collaboration and partnerships in cyber security among member countries in order to strengthen their self-reliance in the cyberspace.[244] Malaysia is an active member of both organisations.

So far, this section demonstrates the role of a CERT in dealing with cyber attacks at the national and regional level. However, some of the interviewees claim that the CERT model is not without its flaws. The international cooperation between CERTs in particular failed to address cross boundaries attacks on information infrastructures. Private Sector Officer 1 argued that:

---

[240] Software Engineering Institute, 'About Us' <http://www.cert.org/about/> accessed 17 December 2016

[241] Ibid

[242] APCERT, 'Mission Statement' <http://www.apcert.org/about/mission/index.html> accessed 17 December 2016

[243] ibid

[244] OICCERT, 'Vision and Mission Statement' <https://www.oic-cert.org/en/missionstatement.html#.V9vFbRTKmII> accessed 17 December 2016

> Last November, we saw attacks moving toward Turkey through our networks. Turkey Internet system went down. DotgovdotTurkey domain was attacked by DDOS from all over the world. This happened because of the Russian plane was shot by Turkey. We saw huge attacks passing through our network, but we could not do anything. OIC-CERT should play a role in this situation especially in terms of technicality. We did not receive any instruction from Cyber Security Malaysia. OIC-CERT should escalate the attempt to inform ISP more about the attacks. Can we block the website? OIC-CERT can at least notify its members to block the access.

Apart from the national CERT, private entities have been substantially involved in dealing with cyber attacks. This includes the establishment of online groups such as the Open Web Application Security Project (OWASP). OWASP is an open community committed to improve the application security in areas such as people, process and technology problem.[245] OWASP local chapters including Malaysia were established in order to facilitate the discussion on cyber security at the national level.[246] OWASP Malaysia founded the MySecurity Community as a front line for cyber security in Malaysia.[247] According to Security Professional 8:

> The members of Mysecurity Community come from the government, the industry, academic, and security companies. Malaysia had experienced two massive cyber attacks in 2011 and 2014. Our involvement with the government was not significant in 2011. We have not set up the community yet. The community was not strong. We just shared silo information with the government. In 2014, we share information especially with regard to the motives of the attacks. The attacks were

[245] OWASP, 'About the Open Web Application Security Project' <https://www.owasp.org/index.php/About_OWASP#The_OWASP_Foundation> accessed 15 January 2017

[246] OWASP, 'Chapter' <https://www.owasp.org/index.php/OWASP_Chapter> accessed 15 January 2017

[247] OWASP, 'Malaysia Chapter' <https://www.owasp.org/index.php/Malaysia> accessed 15 January 2017

> committed by Anonymous Malaysia. We set up a cyber defence alliance with Cyber Security Malaysia.

Besides providing technical expertise, private entities may establish interests groups in order to influence the decision of the executive and to will formation in the political parties. According to Beck, 'Politics is said to have migrated from the official arenas parliament, government, political administration into the grey area of corporatism. The organised power of the interest groups is said to produce prefabricated political decisions, which others must defend as their own creations'.[248] Security Professional 8 explained the role of online communities especially in influencing the policymakers and the public in Malaysia. He said that:

> We are striving towards influencing the policymakers. Every day we have discussion on attacks to cyber security. CyberSecurity Malaysia is our middleman. We give them ideas and suggestions pertaining to cyber security. CyberSecurity Malaysia forwards our suggestions to the government. We use the media to disseminate information about possible attacks. The last event that we did together with CyberSecurity Malaysia was about stealing of information or data in the government and private hospitals. You can get the paper cutting from our Facebook homepage. Education, campaign and awareness are the primarily measures taken by OWASP. We are trying to show to the public that cyber security is not just about skills. You have to practice. Our community doesn't have the resources to enable us to do other activities compared to the government agencies. We provide the experts to talk about security upon request by the government agencies.[249]

Many large organisations have their own IT security departments. They are responsible to monitor and protect the computer system, server and database of the organisations.[250] In addition, security management firms and

---

[248] Beck U, *Risk Society: Towards a New Modernity* (n 31) 188

[249] Interview with Security Professional 8

[250] Interview with Private Sector Officer 4

contractors offer solutions, services and consultation on cyber security to public and private agencies. Recruiting private entities to assist in investigating cybercrime would enable the police to concentrate on arresting cybercriminals.[251] States have relied on these firms to strengthen their defence against future cyber attacks. For instance, Cassidian provides services such as cyber intelligence, crisis management assistance, incidents detection and maintenance of systems.[252] It also offers professional training courses on security solutions, cyber security awareness and reaction.[253] In addition, Internet companies such as Google provide information on cyber security to its users.[254]

It is nevertheless troubling to find that cyber security may only serve small portions of the private sector. According to Private Sector officer 1:

> It is possible that cyber security only cater a small portion of the industry. My company struggled to set up the CERT team. This is because the management is not ready. It is all about business unless the Prime Minister instructs us to do this. The government and GLC are ready. However, small companies are not prepared; they only think about profit and costs.[255]

The companies are not willing to invest in enhancing their cyber security. According to Private Sector Officer 1:

> Cyber security experts prefer to work abroad. We don't have a lot of experts. Usually they will send forensic analysis abroad. The government effort so far is not effective. Companies are reluctant to hire graduates. They claim that their security division is small and they have tools to do it. They are lacking in

---

[251] Brenner SW and Clarke LL, 'Distributed Security: Preventing Cybercrime' (n79) 672

[252] Services Overview <http://www.cassidiancommunications.com/services/overview.php> accessed 15 January 2017

[253] ibid

[254] Google, 'Next Steps in Cyber Security <Awareness' https://googleblog.blogspot.co.uk/2009/11/next-steps-in-cyber-security-awareness.html> accessed 15 January 2017

[255] Interview with Private Sector Officer 1

> awareness on the danger of cyber attacks. Some firms stopped providing training on cyber security due to lukewarm response.[256]

This demonstrates that actions taken by private entities and CERT arguably are not sufficient to deal with cyber attacks. According to Fafinski, 'Even though an ideal CERT network seems well suited as an extra-legal response to the problem of computer misuse, it must be recognised that CERTs cannot exist in a legal vacuum. The law still has the role of governing and informing the internal framework within which the CERT operates'.[257] For instance, Private Sector Officer 1 suggested improving the response mechanisms. He said that:

> CyberSecurity Malaysia sends notifications to ISP about potential attacks especially from abroad. However, the notifications were automated. Nobody read them. A better mechanism is needed to inform the users and response to incident in Malaysia. Without the laws, the top management will stick with business even though the threat is imminent. They will only act if Directives 24 compels them. However, the Directives are applicable in dealing with security issues at the national level. Strategic planning is needed. Perhaps MyCERT should be under regulatory bodies such as MCMC and not under CyberSecurity Malaysia. CyberSecurity Malaysia has the expertise but lack of enforcement mechanism.[258]

Therefore, private entities are not capable of enforcing the law against the people who pose serious threat to cyber security. They can merely assist in the investigation and production of evidence. Thus, they may lack the political will and the power to investigate trans-boundary attacks, which requires the assistance of the enforcement authorities of the state from which the attacks originated. The intervention by the government is still

---

[256] ibid

[257] Fafinski S, *Computer Misuse. Responses, Regulation and the Law* (Willan Publishing 2009) 260-261

[258] Interview with Private Sector Officer 1

needed especially in imposing liability and punishing the perpetrators. Legislation and prosecution are necessary to punish computer experts who cause destruction to the national infrastructure and severely disrupt the Internet service.

4.3.2 Civil Action and Remedy

The victims may consider initiating a civil action against the perpetrators of cyber attacks as an alternative to criminal proceedings. Civil liability is aimed at 'the compensation of a private party for the damages or injuries caused to persons or property, and therefore to protect private interests'.[259] The results of the study show that most of the law enforcement officers were sceptical about the effectiveness of this measure. The victims are more likely to face difficulties in preparing their case due to the complexity of the attacks and the need to identify the perpetrator.[260] Moreover, this approach is useless against young offenders especially if the victims are seeking monetary compensation.[261] Police Officer 2 claimed that:

> I am not sure the company can obtain compensation through civil action. Perhaps they can get their reputation back to normal. People usually lodge police report so that the perpetrator can be arrested and punished instead of a civil action.[262]

It appears that civil action has not been fully utilised in countering cyber attacks in Malaysia due to the reasons above. However, private actors such as the ISPs particularly in the US have successfully invoked this approach.[263] Therefore, this study examines the potential of civil action in countering cyber attacks.

The victims of cyber attacks must be able to satisfy the requirements for civil action. This includes identifying the appropriate cause of action before

---

[259] Lepage H, 'Study On Measures Other Than Criminal Ones' (n 56) 9

[260] Interview with Police Officer 3

[261] Interview with Security Professional 6

[262] Interview with Police Officer 2

[263] Hiller JS, 'Civil Cyberconflict: Microsoft, Cybercrime, and Botnets' 31 Santa Clara Computer & High Tech LJ 163

commencing the proceeding. It may be in the form of torts such as negligence and trespass to chattel, which include electronic intrusion or unauthorised use.[264] The requirement of intention is omitted from the tort of negligence. According to Legal Practitioner 1:

> From criminal law perspectives, Computer Crimes Act requires intention to commit the offences. On the other hand, civil law does not talk about intention. It talks about unauthorised access and unauthorised action by a person. It doesn't require intention to do harm.[265]

However, criminal aspects of cyber attacks may be used as the basis for obtaining compensation under the tort of breach of statutory duty.[266] For instance, the victims are permitted under the Computer Fraud and Abuse Act 1986 and the Electronic Communications Privacy Act 1986 of the US to initiate civil action against the violator in order to obtain compensatory damages, injunctive relief or other equitable relief.[267]

Apart from the appropriate cause of action, causation has to be established between cyber attacks and the loss suffered by the victims.[268] This is necessary as the perpetrators of DDOS attacks may rely on the defence of nova actus interveniens to avoid liability.[269] Liability may also be diminished due to the failure of an entity to take steps to prevent cyber attacks. The success of this claim depends on the foreseeability of harm; the duty owed by the entity to the plaintiff and the causal connection between harm and the failure of the entity to act.[270] Civil action is a viable recourse for private

---

[264] ibid

[265] Interview with Legal Practitioner 1

[266] Jougleux P and Synodinou T-E, 'Prevention of Cyber Attacks' in Iglezakis I (ed), *The Legal Regulation of Cyber Attacks* (Kluewer Law International BV, The Netherlands 2016) 50

[267] S 1030 (g) of the Computer Fraud and Abuse Act, 18 U.S.C.

[268] Jougleux P, Mitrou L and Synodinou T-E, 'Criminalisation of Attacks against Information Systems' in Iglezakis I (ed), *The Legal Regulation of Cyber Attacks* (Kluewer Law International BV, The Netherlands 2016) 50

[269] ibid 51

[270] Finch BE and Spiegel LH, 'Litigation Following a Cyber Attack: Possible Outcomes and Mitigation Strategies Utilising the Safety Act' 30 Santa Clara Computer & High Tech LJ 350

actors to seek compensation for their loss of profit and to re-establish their reputation. States may also initiate civil action to seek compensation for the destruction of any infrastructure caused by cyber attacks.

Civil action is also appropriate for situations involving theft of data. As indicated in chapter 3, the studies show that obtaining confidential information is one of the motives of cyber attacks. According to Legal Practitioner 1:

> Cyber attacks have become a serious concern from the commercial point of view. Businesses have been infiltrated for the purpose of obtaining information. Information such as credit card details is very valuable.

Apart from hackers, disgruntled employees may seek revenge against their employer by stealing or modifying confidential information. [271] The costs following data breach could be substantial, as a company has to bear the expanses of notifying potentially affected customers, hiring outside companies to assess the extent of stolen information, defending against potential lawsuits and fixing the security of the computer systems.[272] This leads to the development of insurance coverage that will protect businesses against the risk of cybercrime and mischief. [273] Civil liability may be established for the controller of the personal data and the supervisor of the employees pursuant to a data breach.[274] This includes the failure to inform their clients about security breaches of personal information.

The data subject may rely on the tort of negligence to cover losses due to the breach of data. The common law doctrine of tort liability for negligent cyber security measures has emerged as a measure by which companies

---

[271] Interview with Deputy Public Prosecutor 1

[272] Zelle AR and Whitehead SM, 'Cyber Liability: It's Just a Click Away' Journal of Insurance Regulation, 01/2014, Volume 33

[273] ibid

[274] Jougleux P, Mitrou L and Synodinou T-E, 'Criminalisation of Attacks against Information Systems' in Iglezakis I (ed), *The Legal Regulation of Cyber Attacks* (n 268) 53

are exposed to third-party lawsuits for damage caused by data breaches.[275] In *Lone Star National Bank v Heartland Payment Systems, Inc*, the US Federal Court of Appeals for the Fifth Circuit allowed a negligence claim by the appellants against the respondent for the losses that they suffered as a result of breach of data.[276] The respondent's data system was hacked and payment card information was stolen. The appellants claimed for the costs that they incurred in replacing the compromised cards and reimbursing customers for fraudulent charges. The court held that the respondent owe a duty care to the appellants to which it sends payment card information. The respondent had reason to foresee that the appellants would suffer economic losses due to its negligence. This study shall examine the imposition of criminal liability for cyber attacks under the PDPA in the next chapter.

Apart from procedural and substantive requirements, the victims must also consider the obstacles that may impair the success of the civil action against the perpetrators of cyber attacks. The biggest obstacle is the jurisdiction of the national court is limited with respect to the action initiated by an individual against a state and its organs. In *Jones v Saudi Arabia*, the House of Lords decided that Saudi Arabia and its agents are entitled to immunity in civil proceedings in UK.[277] In *Jurisdictional Immunities of the State (Germany v. Italy: Greece intervening*), the ICJ affirms this position. [278] In this case, the ICJ suggests that the principle of jurisdictional immunity does not affect the rights of individuals to seek other forms of redress besides the initiation of civil action. A state may initiate action on behalf of citizens against another state, which is involved in the commission of cyber attacks on the basis of diplomatic protection under international law.[279] This study shall return to the

---

[275] Weber R, 'Inside Cybersecurity' (Inside Washington Publishers) <http://0-search.proquest.com.wam.leeds.ac.uk/docview/1492017089?accountid=14664> accessed 6.10.2016

[276] *Lone Star Bank, et. al v. Heartland Payment Systems*, Case: 12-20648

[277] *Jones (Respondent) v. Ministry of Interior Al-Mamlaka Al-Arabiya AS Saudiya (the Kingdom of Saudi Arabia) (Appellants)* [2006] UKHL 26

[278] ICJ Report 2012

[279] 2006 International Law Commission Draft Article on Diplomatic Protection, ‹http://legal.un.org/ilc/texts/instruments/english/commentaries/9_8_2006.pdf> accessed 15 January 2017

question of state responsibility for cyber attacks when it discusses the application of international law in countering cyber attacks in the next chapter.

Apart from jurisdictional immunity, another obstacle is the reluctance on the part of the state to reveal information pertaining to the occurrence of cyber attacks, which may hamper attempts to initiate legal action. In Malaysia, the duty not to disclose confidential information is stated in the Official Secret Act 1972 and the Evidence Act 1950. They impose the obligation especially on public servants not to reveal any document, which has been classified as top secret, secret, confidential or secret by the government. The documents include cabinet papers, records of decisions and deliberations including those of Cabinet committees; State Executive Council documents, records of decisions and deliberations including those of State Executive Council committees; and documents concerning national security, defence and international relations.[280] Section 124 of the Evidence Act prohibits any action to compel any public officer to disclose communications that affect public interest. Next, section 162 provides that a witness, who has been summoned to produce a document in his possession, must bring it to the court despite of objection raised in its admissibility. The court has the jurisdiction to inspect the document to determine its admissibility unless it refers to the affairs of the state. In *Takong Tabari v Government of Sarawak,* the court held that:

> In this country, objection as to production as well as admissibility contemplated in s. 123 and 162 of the Evidence Act is decided by the Court in an enquiry of all available evidence. This is because the Court understands better than all others the process of balancing competing considerations. It has power to call for the documents, examine them, and

[280] Schedule of the Official Secret Act 1972; Section 123 of the Evidence Act 1950 provides that 'no one shall be permitted to produce any unpublished official records relating to affairs of State, or to give any evidence derived therefrom, except with the permission of the officer at the head of the department concerned, who shall give or withhold permission as he thinks fit, subject, however, to the control of a Minister in the case of a department of the Government of Malaysia, and of the Chief Minister in the case of a department of a State Government'.

> determine for itself the validity of the claim. Unless the Court is satisfied that there exists a valid basis for assertion of the privilege, the evidence must be produced. This strikes a legitimate balance between the public and private interest. Where there is a danger that disclosure will divulge, say, State secrets in military and international affairs or Cabinet documents, or departmental policy documents, private interest must give way.[281]

It can be inferred that the Government of Malaysia may rely on section 123 and 162 of the Evidence Act 1950 in denying any request to produce a document that will jeopardize the security of Malaysia. However, ultimately the court has the power to decide whether the disclosure of the document is prejudicial to the interest of the public and security of Malaysia.

In the UK, the courts may rely on the public interest immunity to prevent the disclosure of state secrets.[282] It is to be noted that the 2009 and 2010 decisions in the case of *Binyam Mohamed* illustrate a shift with respect to public interest immunity; the judgments did not show deference to the claims of the government. [283] In this case, the court granted him the access to the secret documents supplied by US to UK, which were subjected to confidentiality clause. This event led to the passing of the Justice and Security Act 2013. The Act restricts the production of materials related to the intelligence or security matters in civil proceedings. Any hearing involving secret documents may be conducted by closed procedure. The court has the jurisdiction to determine the sensitive nature of the documents and to allow the disclosure or non-disclosure of the document. In determining the status of the document, the court takes into consideration several factors such as the national security and to tilt the balance in favour of the government upon scrutinising the potential damage. Subject to the Court's approval, the UK

---

[281] *Takong Tabari v Government of* Sarawak (1995) 1 CLJ 405 citing *B.A. Rao & Others v. Sapuran Kaur & Anor* [1978] 2 MLJ 146

[282] ibid 88

[283] *Mohamed v. Secretary of State for Foreign & Commonwealth Affairs,* [2009] EWHC (Admin) 152, [14] (Eng.), *Mohamed v. Secretary of State for Foreign & Commonwealth Affairs* [2011] Q.B. 218 (Eng.)

government may invoke this provision against any request to disclose information concerning cyber attacks on the basis of security reasons during civil proceeding.

Besides damages, other remedies including injunction and restraining order may be used in countering cyber attacks. In 2010, a federal judge in the US District Court of Eastern Virginia granted Microsoft's request for temporary restraining order against 277 Internet Domains.[284] A group of criminals known as Waledac used these Internet domains to facilitate and continuously control the ability of the computers that make botnet to communicate with each other.[285] The Waledac botnet could send 1.5 billion spam emails per day to solicit fraudulent products, install malicious software and enlist more computers into the botnet.[286] Microsoft alleged that the registered owners of the domain names had violated the laws of the US including the Computer Fraud and Abuse Act 1986 and the Electronic Communications Privacy Act 1986. The restraining order enabled Microsoft to request the domain registry to shut down the domains that control the botnet.

A civil remedy such as injunction may be applied to cyber attacks in the UK. S 3A of the UK's Protection from Harassment Act 1997 provides for an injunction to restrain any person from pursuing conduct, which amounts to harassment. The victims of cyber attacks may use this remedy to stop the perpetrators from making their lives intolerable through constant intrusions to the computer system. In the case of *Huntingdon Life Sciences Group plc and others v Stop Huntingdon Animal Cruelty & others*, the claimant initiated action against the respondent for conducting an unlawful campaign to promote its closure. The claimant contended that the respondent is aiming of making live intolerable for its employees. An interim injunction was granted against the defendant. The court held that:

---

[284] *Microsoft Corporation v. John Does 1-27, et. al.",* Civil action number 1:10CV156; Microsoft 'Cracking Down on Botnets' <http://blogs.microsoft.com/blog/2010/02/24/cracking-down-on-botnets/#sm.001o0yokd9bpfml101y2ahi0cfwzt> accessed 15 January 207

[285] Hiller JS, 'Civil Cyberconflict: Microsoft, Cybercrime, and Botnets' (n 263)

[286] ibid

> If the Claimants are right all these Defendants are party to a ruthless and menacing campaign, which skilfully uses modern media and plays on the views and emotions of those who espouse or are sympathetic to the cause of animal rights. They are prepared to use criminal means to bring a company to its knees and deprive the community of the value of the work it does. The implications go beyond the world of medical research but strike at the foundation of society, namely the rule of law itself.[287]

The court will award the order for injunction on the balance of convenience if the claimants can demonstrate that they have a good arguable claim and serious questions to be tried.[288] In *Astraneca UK Ltd. V Vincent & Ors*, the accused was subjected to interim injunction instituted by Astrazaneca UK Ltd, a pharmaceutical company related to Huntingdon Life Sciences.[289] The claimant adduced materials in the form of Facebook entries to support its claim that the defendant will continue to harass the company in the future. The court granted the order to stop her from entering the claimant's land and pursuing any form of harassment within the ambit of the Protection from Harassment Act 1997.[290]

Civil liability of the perpetrator of cyber attacks needs to be more fully addressed by the legislator in Malaysia. In so far as the damages, s 426 (1a) of the Criminal Procedure Code vested the power of the court to award monetary compensation to the victims upon application made by the Public Prosecutor. The court has the discretion to order the manner in which the compensation should be made to the victims.[291] Civil remedy such as injunction or restraining order should be made available for the victims of cyber attacks in Malaysia. The Specific Relief Act 1950 provides for specific relief such as specific performance and injunction in Malaysia, However, the

---

[287] [2004] EWHC 1231 (QB)

[288] *Eli Lilly & Co Ltd v Stop Huntingdon Animal Cruelty* [2011] EWHC 3527 (QB)

[289] *Astraneca UK Ltd. V Vincent & Ors* [2014] EWHC 1637 (QB)

[290] ibid

[291] S 432 of the Criminal Procedure Code

Act stipulates that specific relief cannot be granted for the mere purpose of enforcing a penal law.[292] Temporary and perpetual injunctions may be granted by the court to prevent a party from doing something, which he is under an obligation not to do so.[293] Perpetual injunction may be granted when the defendant invades of threatens to invade the plaintiff's right or enjoyment of his property.[294] In addition, the court may also grant mandatory injunction in order to prevent the breach of an obligation or to compel the performance of certain acts.[295] For instance, the court may grant an injunction to restrain the publication of statements, which would be punishable under Chapter XXI of the Penal Code.[296] It seems that injunction may be granted to the Plaintiff on the basis that the perpetrator of cyber attacks interferes with his enjoyment to the property, which is the computer system. However, it is not clear the extent to which these remedies are applicable to enforce obligation under criminal legislation such as the Computer Crimes Act 1997.

Accordingly, this study proposes the inclusion of a civil remedy in the legislation related to cyber attacks including the Personal Data Protection Act 2010. Statutory provisions equivalent to the US's Computer Fraud and Abuse Act 1986, which allow for civil right of action may be considered by the legislator in Malaysia. Apart from that, a civil remedy such as injunction under the UK's Protection from Harassment Act 1997, should be introduced in Malaysia to address this problem.

4.3.3 Regulatory Measures and Financial Penalties for Data Breach

This section assesses the usage of regulatory measures and financial penalties against breach of data. A data breach happens when 'there is loss or theft of, or other unauthorised access to, data containing sensitive personal information that results in the potential compromise of the

[292] S 6 of the Specific Relief Act 1950

[293] S 4 (c) of the Specific Relief Act 1950; s 51 of the Specific Relief Act 1950

[294] S 52 (3) of the Specific Relief Act 1950

[295] S 53 of the Specific Relief Act 1950

[296] Illustration e, S 53 of the Specific Relief Act 1950

confidentiality or integrity of data'.[297] Regulatory action is perceived as necessary in order to send clear and consistent signals to the data controller of the repercussion of not complying with the information rights law.[298] This includes criminal prosecution, civil monetary penalties, non-criminal enforcement and audit.[299] Regulatory action is difficult to apply due to problems such as overlap of jurisdiction. Despite of that, it raises the security standard in which the data user is obliged to ensure that the personal data is not susceptible to cyber attacks. They could face stiff sanctions including financial penalties for failure to comply with the standard.

The Personal Data Protection Act 2010 (PDPA) regulates the processing of personal data in commercial transactions in Malaysia.[300] The Act defines personal data as any information that relates to a data subject including information in respect of commercial transactions, sensitive personal data and expression of opinion about the data subject.[301] Sensitive personal data consists of information such as: the physical or mental health; political opinions; religious belief and the commission or alleged commission of any offence.[302] The PDPA regulates any person who processes and has control over or authorizes the processing of any personal data in respect to commercial transactions (the data user).[303] However, the Act is not applicable to the Federal Government and State Governments.[304] They are governed by the Official Secrets Act 1972 and the directives issued by the related governmental bodies such as the Malaysian Administrative

---

[297] Froomkin AM, 'Government Data Breaches' 24 Berkeley Tech LJ 1019 2009, 1025

[298] ICO 'Data Protection Regulatory Action Policy' <https://ico.org.uk/media/about-the-ico/policies-and-procedures/1853/data-protection-regulatory-action-policy.pdf> accessed 22 January 2017

[299] ibid 1

[300] S 4 of the Personal Data Protection Act 2010 defines commercial transactions as 'any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investmnets, financing, banking and insurance'.

[301] S 4 of the Personal Data Protection Act 2010

[302] ibid

[303] S 2(1) of the Personal Data Protection Act 2010

[304] S 3(1) of the Personal Data Protection Act 2010

Modernisation and Management Planning Unit and the National Security Council. The data user may be held accountable for data breach under the PDPA. According to Legal Practitioner 1:

> Let's say a bank has been subjected to cyber attacks. It can be held accountable under the PDPA if appropriate security measures have not been taken. The bank has to show that it has done its part by implementing all the precautionary measures. The perpetrators have breached the PDPA by obtaining the personal data of the individuals through unauthorised access.

The data user is obliged to comply with the security principle stipulated under s 9 of the Act. This includes the duty to take necessary measures to protect personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. [305] Security measures have to be incorporated in operating the equipment in which the personal data is stored. The data user has to ensure the reliability, integrity and competency of the personnel who have been granted the right to access the personal data.[306] The user is also required to provide guarantees with respect to the technical and organizational security measures governing the data processing.[307]

The Personal Data Protection Commissioner is vested with the power to implement and enforce the personal data protection laws in Malaysia.[308] The public may lodge complaints in writing to the Commissioner about an act that may contravene the provisions of the Act.[309] The Commissioner has the power to refuse to carry out investigation on the grounds that the complaint is trivial, frivolous, vexatious or had been disposed previously.[310]

---

[305] S 9(1) of the Personal Data Protection Act 2010

[306] ibid

[307] S 9(2) (a) of the Personal Data Protection Act 2010

[308] S 48 of the Personal Data Protection Act 2010

[309] S 104 of the Personal Data Protection Act 2010

[310] S106 of the Personal Data Protection Act 2010

The PDPA only provides for criminal prosecution against any persons who contravene the provisions of the Act. It does not confer on the data subject the right to initiate civil action and to be notified of a data breach incident. According to Legal Practitioner 2:

> The PDPA does not include civil action and reporting obligation. These are among the complaints about PDPA. The company is not legally required under the PDPA to report if there is a breach, unless they are bound by the Bank Negara (Central Bank) guideline. The Commissioner of the Data Protection Department will decide whether to prosecute a person at fault including third party who took the information illegally.[311]

A data user is criminally liable for failing to adhere to the security principle provided in the Act and is liable to a fine not exceeding RM300,000 or to imprisonment for a term not exceeding two years or both.[312] The Personal Data Protection Commissioner is vested with the power to compound any offences committed by any person under the Act. The offender is required to pay not exceeding fifty per centum of the amount of maximum fine for the offences.[313] Failure to do so within the specified time will result in criminal prosecution. [314] Apart from compounding offences, the Personal Data Protection Commissioner does not have the power to impose financial penalty on the data user for failing to protect personal information.

Apart from the PDPA, the Financial Services Act 2013 regulates the information held by financial institutions in Malaysia. The Central Bank of Malaysia is vested with the power to ensure the soundness and responsible conduct of financial institutions.[315] This includes the safety, efficiency and reliability of the payment systems and instruments.[316] The Act does not expressly stipulate the duty to take precautionary measures to protect the

---

[311] Interview with Legal Practitioner 2

[312] S 5(2) of the Personal Data Protection Act 2010

[313] S 132(1) of the Personal Data Protection Act 2010

[314] S 132(2) of the Personal Data Protection Act 2010

[315] S 6 (a) (i) of the Financial Services Act 2013

[316] S 6 (a) (iii) of the Financial Services Act 2013

information of a customer. However, it provides that an authorised person is liable to imprisonment for a term not exceeding five years or to a fine not exceeding RM10,000,000 or to both for disclosing the information of any customer.[317] This provision should be invoked against insiders who commit cyber attacks for the purpose of disclosing a customer's information.

Unlike the Personal Data Protection Commissioner, the Central Bank of Malaysia is conferred with a range of regulatory actions to enforce the provisions of the Financial Services Act 2013. It has the power to investigate a person for committing an offence under the Act.[318] Besides criminal liability, the Central Bank of Malaysia has the power to impose monetary penalty on a person for breaching the provisions of the Act.[319] It may also institute civil action to seek for an order to restraint a person from engaging in any specific conduct; cease all breaches and take steps to mitigate the effect of non-compliance with the Act.[320]

In the UK, S 55A of the Data Protection Act 1998 confers the power to the Information Commissioner to impose monetary penalty for the failure of the data controller to comply with the data protection principles.[321] This includes the failure to take reasonable steps to prevent the data breach despite knowing there was a risk that it would happen.[322] This measure is imposed on every organisations, local authority and sole trader who is processing personal information in the UK (the data controller).[323] Organisations have been required to pay up to £500,000 for serious breaches of the Data Protection Act 1998.[324]

So far, the ICO have penalised several organisations for contravening the

---

[317] S 133 of the Financial Services Act 2013

[318] S 218 of the Financial Services Act 2013

[319] S 236 of the Financial Services Act 2013

[320] S 239 and s 242 of the Financial Services Act 2013

[321] S 4(4) of the of the Data Protection Act 1998

[322] S 55A (1)(3) of the Data Protection Act 1998

[323] S 1 of the Data Protection Act 1998; Privacy and Electronic Communications (EC Directive) Regulations 2003 and related laws

[324] ICO, 'Taking Action-Data Protection' <https://ico.org.uk/about-the-ico/what-we-do/taking-action-data-protection/> accessed 22 January 2017

data protection principles. It was reported that Staysure.co.uk Limited was penalised £175, 000 by the ICO for failing to update its software. The attacker was allowed to access and download over three millions customer record by installing a backdoor in the Staysure web server.[325] Besides that, the Ministry of Justice was fined £180,000 for failing to take technical measures to prevent the loss of portable hard drives containing prisoner intelligence information from 75 prisons.[326]

As well as the Information Commissioner, the UK's Financial Conduct Authority has the power to impose financial penalty on organisations for contravening financial regulation.[327] This power has been invoked against financial institutions that fail to take adequate measures to protect confidential information. In 2007, Nationwide Building Society was fined £980,000 for its failure to secure the confidential customer information.[328] Heavy fines are perceived as necessary in order to remind all firms about the importance of information security.[329]

Besides the failure to adhere to the principles of data protection, financial penalties may be used against organisations that fail to notify a breach of data. This measure is perceived as necessary in order to avoid 'identity theft, fraud, financial loss, damage to reputation and loss of confidentiality of personal data'. [330] The European General Data Protection Regulation

---

[325] Breach Watch, 'Breach Details' <http://breachwatch.com/2015/02/20/staysure-co-uk-limited/> accessed 22 January 2017

[326] Breach Watch, 'Ministry of Justice' <http://breachwatch.com/2014/08/26/ministry-of-justice-2/> accessed 22 January 2017

[327] S 206 of the Financial Services Act 2000

[328] Financial Services Authority, 'Final Notice to Nationwide Building Society' <http://webarchive.nationalarchives.gov.uk/20130403023549/http://www.fsa.gov.uk/pubs/final/nbs.pdf> accessed 22 January 2017;see also Techworld, 'The UK's 15 Most Infamous Data Breaches' <http://www.techworld.com/security/uks-most-infamous-data-breaches-2016-3604586/> accessed 22 January 2017

[329] The Guardian, 'Nationwide Fined £980,000 Over Stolen Laptop' <https://www.theguardian.com/money/2007/feb/14/accounts.business> accessed 22 January 2017

[330] European Union, 'The European General Data Protection Regulation' Official Journal of the European Union L119/17 <(GDPR) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL> accessed 24 February 2017 para 85

provides that the failure to notify a breach can attract fines up to 4 per cent of global turn over or up to €20,000,000.[331] This study shall return the question of the duty to report the occurrence of cyber attacks in Malaysia when it discusses the implementation of criminal law measures in section 5.4.1.

In light with the above discussion, this study suggests that the scope of the PDPA and the power conferred to the Personal Data Protection Commissioner should be reviewed. Firstly, the PDPA should be extended to all data users including the public sector organisations. They should be penalised for breaching the data protection regulations. The ICO observes that public sector such as the city council may lack sense of urgency in dealing with data protection concerns.[332] Some of the participants in this study argued that the government officials do not possess the required skills in protecting information. According to Security Professional 10

> The government officials lack the knowledge to protect the computer system. That is why there have been leakages of government's confidential information. I advised my client to lodge report to the Police. We have not heard any feedback for a couple of months now.[333]

Thus, PDPA should be extended to the government officials in order to ensure that they are accountable for data breach. This measure will heighten their awareness of the urgency of protecting the government data. However, the implementation of this suggestion is difficult due to several reasons. The governments determine the scope of the data breach and the remedies available for damages caused by these breaches.[334] Therefore, 'it is not

---

[331] ibid; see also O'Brien R, 'Privacy and Security: The New European Data Protection Regulation and It's Data Breach Notification Requirements' Business Information Review 2016, Vol 33(2) 81–84 DOI: 101177/0266382116650297, 82

[332] Progressive Digital Media Technology News London, 'Commissioner's Office to Detail Findings into Effectiveness of Financial Penalties on Public Sector Bodies' <http://0-search.proquest.com.wam.leeds.ac.uk/docview/1544883155?accountid=14664> accessed 24 February 2017

[333] Interview with Security Professional 10

[334] Froomkin AM, 'Government Data Breaches' (n 297)

surprising that the remedies available to victims of a government data breach are often less than those available to victims of private sector data breach'.[335] In addition, actions against civil servants are subjected to the provisions of the Government Proceedings Act 1956.

Secondly, relying solely on criminal prosecution is not sufficient in dealing with data breach. Compounding of offences usually happens when the parties have come to a settlement.[336] Thus, it is not equivalent to monetary penalty. Furthermore, the amount imposed on the offender which is not exceeding RM150,000 does not reflect the gravity and importance of adhering to the security principle. Therefore, this study suggests that the Personal Data Protection Commissioner should be conferred with the power to impose financial penalties. This measure may enhance the effectiveness of the PDPA in protecting personal information against cyber attacks. This study shall further examine the enforcement of criminal law and prosecution of the perpetrators of cyber attacks for stealing government's information and personal data in section 5.2.1.3.

4.4 Conclusion

The objective of this chapter is to assess the approaches to counter cyber attacks and to situate non-criminal and criminal measures within the strategy to counter cyber attacks in Malaysia. The National Cyber Security Policy was formulated for the purpose of addressing the risk to CNII in Malaysia. However, this strategy is inadequate due to the absence of detailed strategies to in dealing with cyber attacks in Malaysia. Therefore, this study suggests the incorporation of 'defend, deter, develop and international action' strategies in the Malaysia's National Cyber Security Policy. The Malaysia's National Security Council should be vested with the responsibility to monitor the implementation of the strategies to counter cyber attacks in Malaysia. The strategies to counter cyber attacks include non-criminal measures such as social prevention policy and situational crime prevention;

---

[335] ibid 1021

[336] Fook LC, Hassan CA and Bajury MSHM, *Introduction to Principles and Liabilities in Criminal Law* (2nd edn, LexisNexis 2012) 462

criminal law; and global partnership. They are required to meet the standard of fairness and effectiveness.

This study has used empirical findings to identify and assess the effectiveness and fairness of the non-criminal measures to counter cyber attack in Malaysia. Most of the participants rated cyber security education and campaigns as the most effective measures in addressing the risk of cyber attacks. They also agreed that situational crime prevention such as risk assessment and the usage of technological measures to restrict the access to the computer system and server may reduce the threat of cyber attacks. In addition, some of the participants argued that Cybersecurity Malaysia and MyCERT are more effective than criminal law in dealing with cyber attacks. These measures should be fully exploited and explored in Malaysia. Other measures such as encryption and surveillance may be used in dealing with this problem. However, the execution of these measures has been hampered by various factors including the perpetrators' technological expertise. Moreover, they may be in conflict with the notion of fairness.

Apart from that, this study gathered information about the role of the Internet architecture including ISPs, ICPs and computer manufactures in managing the risk of cyber attacks in Malaysia. Doctrinal analysis suggests that the government should regulate the Internet architecture including the imposition of sanctions and penalties to ensure the reliability of their products. However, the findings indicate that the Internet architecture prefer self-regulation instead of intervention by the government. Therefore, this measure may be difficult to be implemented in Malaysia due to the resistance from the Internet architecture.

Finally, this chapter considers the application of civil proceeding in countering cyber attacks. Most of the participants were sceptical about the effectiveness of civil action and remedy in dealing with this problem. Therefore, this measure has not been fully utilised and explored in Malaysia. However, theoretical analysis suggests that this measure has been invoked in other countries such as the US to shut down Internet domains that control the botnet. Moreover, civil action may be initiated against data holders for their failure to ensure the security of the data. Accordingly, this study

suggests possible reforms to encourage the usage of this measure in Malaysia. This includes the insertion of civil remedies such injunction and restraining order in the Personal Data protection Act 2010.

Chapter 5

The Imposition of Criminal Liability and Enforcement for Cyber Attacks in Malaysia

5.1 Introduction

As stated previously, non-criminal measures including preventive strategies and civil action may be used to counter cyber attacks in Malaysia. A comprehensive and proactive use of cyber security best practices are required in managing cyber attacks. [1] However, scholars such as Shackelford argued that existing measures to deal with cyber attacks are not effective.[2] Therefore, criminal law is still needed to regulate cyber activities performed by individuals, which cause harm to another. Criminal law serves several functions in dealing with cyber attacks. Firstly, criminal law may be a better option than civil law in dealing with online wrongdoings as it seeks to punish and deter aberrant conduct.[3] Civil law may not place the necessary restrictions on perpetrator's liberty to either prevent future attacks or reassure victims or wider community that justice has been done.

Apart from the deterrence effect, criminal law allows for early intervention through the criminalisation of preparatory acts or 'precursor offences'.[4] The state is obliged to take necessary measures to protect its citizens from future harm. This includes criminalising acts falling short of causing immediate harm.[5] According to Wilson and Kelling 'crimes are adventitious, not the

---

[1] Shackelford SJ, 'Toward Cyberpeace: Managing Cyberattacks Through Polycentric Governance' American University Law Review [2013] Vol 62 1273-1274, 1279

[2] ibid

[3] Lipton JD, 'Combating Cyber-Victimization' 26 Berkeley Tech LJ 1103 2011

[4] Walker C, 'The Impact of Contemporary Security Agendas against Terrorism on the Substantive Criminal Law' in Masferrer A (ed), *Post 9/11 and the State of Permanent Legal Emergency Security and Human Rights in Countering Terrorism* (Springer 2012) 129

[5] Ashworth A and Zedner L, 'Prevention and Criminalization: Justifications and Limits' (2012) 15 New Crim L Rev 542

result of inexorable social forces or personal failings'.[6] Therefore, catching and prosecuting lower level hacktivists and criminals, and making their activities harder could reduce the likelihood of cyber attacks.[7] The criminalisation of preparatory acts for cyber attacks may protect the people from actual harm in the future.

In addition, criminal law may be utilised to impose the duty on the public 'to help themselves and the state'.[8] For instance, the employees of the financial sectors are obliged to report their suspicion of terrorist financing to a central authority.[9] Criminal law may be used to persuade the public to report the occurrence of cyber attacks.

Apart from that, criminal law symbolises solidarity among the members of the international community in managing the risk of cyber attacks.[10] The Cybercrime Convention was formulated in order to overcome the inconsistencies of cybercrime legislation among states.[11] It is also instrumental in fostering cooperation among states to suppress cybercrime. The legal framework in dealing with cyber attacks should conform to international standards for various reasons such as to attract foreign investment and to strengthen the confidence of trading partners.

The perpetrators of cyber attacks should be denounced publicly through criminal law. The criminal law is publicly enforced in order to serve the interest of the public.[12] Tough sentencing is necessary in order to remind the offenders that cyber attacks are not to be tolerated by society. The cost of

---

[6] Wilson JQ and Kelling GL, 'Making Neighbourhood Safe' The Atlantic; Feb 1989; 263, 2: ABI/ INFORM Collection, 47

[7] 'Cyber-security: Problems Outpace Solutions' (*Security & Defence Agenda*, 2013) <www.securitydefenceagenda.org> accessed 13 March 2014

[8] Walker C, 'The Impact of Contemporary Security Agendas against Terrorism on the Substantive Criminal Law' in Masferrer A (ed), *Post 9/11 and the State of Permanent Legal Emergency Security and Human Rights in Countering Terrorism* (n 4) 139

[9] ibid 139

[10] ibid 143

[11] Calderoni F, 'The European Legal Framework on Cybercrime: Striving for an Effective Implementation' Crime Law Soc Change (2010) 54:339–357 DOI 101007/s10611-010-9261-6

[12] *PP v Loo Choon Fatt* [1976] 1 LNS 102

criminal enforcement may be high, however it 'offers a mean of controlling harmful activities that, if unchecked, would result in very high costs for victims and the wider community'.[13] Cyber attacks on financial and banking institutions can cause harmful effect to the economy of a state. They may hinder the development of the country especially the industry, which relies heavily on Internet due to the decrease of public confidence on the safety of the cyberspace and online transactions. Thus, criminal enforcement is necessary to ensure the public can use the Internet safely without harm.

This section is structured as follows: firstly, it provides an overview of the scope of cyber attacks under the law of Malaysia. Secondly, it examines the introduction of new offences to deal with cyber attacks in Malaysia. Thirdly, this chapter analyses the implementation of criminal law measures against cyber attacks in Malaysia. This includes the obstacles and reform of the criminal law in dealing with cyber attacks.

5.2 Cyber Attacks under the Criminal Law of Malaysia

The purpose of this section is to provide insight into cyber attacks falling under the Malaysian criminal law. The law enforcement officers in Malaysia do not officially use the term 'cyber attack'. Deputy Public Prosecutor 2 asserted that:

> It depends, we don't use the term cyber attacks; it is just cyber criminal cases. Cyber attacks can encompass cyber criminal activities or criminal activities related to the Internet. From the legal perspectives, at the Attorney General's Chamber we don't use the term cyber attacks, because it is a general term. There is specific definition for every offence.[14]

Deputy Public Prosecutor 1 argued that:

> I don't think that there is official classification with regard to cyber attacks-although you can refer to the classification by

[13] Bowles R, Faure M and Garoupa N, 'The Scope of Criminal Law and Criminal Sanctions: An Economic View and Policy Implications' (2008) 35 JL & Soc'y 389, 415

[14] Interview with Deputy Public Prosecutor 2

> cyber security experts. For me, this concept can be encapsulated by looking at the element of the offence. What is the meaning of access or unauthorised access?[15]

It may be inferred that the criminalisation of cyber attacks in Malaysia is explainable in the light of the typology of cyber attacks and the context of related statutory provisions. In Chapter 3, this study examined the typology of cyber attacks based on: the identity of the perpetrators and victims; the targets; methods; motives; scale and effect. It suggested that cyber attacks could be classified further into four categories: (1) cybercrime; (2) cyber terrorism; (3) cyber warfare/use of force/unlawful intervention under international law; and (4) cyber espionage. This section analyses the position of cyber attacks under the criminal law of Malaysia, in particular cyber attacks in the guise of cybercrime and cyber terrorism. This study shall return to cyber warfare and use of force under international law and cyber espionage in chapter 6.

5.2.1 Cyber Attacks in the Guise of Cybercrime

The distinctive feature of cybercrimes is the critical role of the Internet networks, which allows computers to be interconnected globally. [16] Cybercrimes can be divided into three groups: (1) computer integrity crimes; (2) computer related crimes; and (3) computer content crimes.[17] According to Deputy Public Prosecutor 1:

> It is important to distinguish cyber crime and cyber related crime. This is because 99% of the cases in Malaysia are cyber related crime. The Raja Petra case is an example of cyber related crime. The couple that hacked the 'Touch n Go' system recently is classified as cyber crime. This falls within the Computer Crimes Act 1997. I would say matters that falls under the Computer Crimes Act would be safely call as cyber crime.

---

[15] Interview with Deputy Public Prosecutor 1

[16] Walden I, *Computer Crimes and Digital Investigations* (2nd edn, Oxford University Press 2015) 12

[17] Wall DS, 'Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace' Police Practice and Research, Vol 8, No 2, May 2007, pp 183–205

> The Act is concerned with hacking for the purpose of unauthorized use and access.[18]

Accordingly, the distinction between different categories of cybercrimes is useful for the purpose of identifying the laws in relation to cyber attacks. Apart from the categorisation of cybercrimes, it is pertinent to reflect upon the general principles of criminal law. Cybercrimes in national laws are interpreted with reference to rules applicable to criminal offences including state of mind, defences, complicity, attempt and omission.[19] Different legal systems may use different concepts and definitions of these rules for cybercrime.[20] In the following sections, the elements of crimes for cyber attacks under these categories will be discussed.

5.2.1.1 Computer Integrity Crimes

Computer integrity crimes are concerned with the access, interception and modification or interference of the computer.[21] It encompasses offensive behaviour against network access mechanisms including hacking, cracking, vandalism and the usage of viruses.[22] The Malaysia's Computer Crimes Act 1997 defines a computer as:

> … an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices performing logical, arithmetic, storage and display functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related device.[23]

---

[18] Interview with Deputy Public Prosecutor 1

[19] United Nations Office on Drugs and Crime, 'Comprehensive Study on Cybercrime' (*United Nations* 2013) <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> accessed 20.10.2016

[20] ibid

[21] Walden I, *Computer Crimes and Digital Investigations* (n 16) 158

[22] Wall DS, 'Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace' (n17)

[23] S 2(1) of the Computer Crimes Act 1997

A device must be capable of performing logical, arithmetic, storage and display functions in order to qualify as computer within the ambit of the Act. The definition of computer under the Act covers wide-ranging devices including text messages from a cell-phone.[24] It also includes the usage of a debit card to access the Automated Teller Machine without authorization.[25]

The Computer Crimes Act 1997 was enacted in order to safeguard the computer programme against unauthorised access.[26] Stiff punishments including imprisonment and penalty are perceived as necessary in order to increase public confidence on the safety of the online transactions.[27] S 3(1) of the Act provides that a person can be punished for using a computer to access any programme or data of another computer without authorisation.[28] Dishonest intention is not required in order to justify criminal culpability. The mens rea for this offence is satisfied when there is intention to secure access to any computer program or data and the knowledge that the performance of the computer function is done without authorized access. S 4(1)(a) of the Act prohibits the unauthorised access with intent to commit or facilitate the commission of further offence such as fraud, dishonesty or to cause injury as defined in the Penal Code.[29] Deputy Public Prosecutor 1 asserted that:

> Crimes under the Computer Crimes Act 1997 can overlap with other legislation. The phrase 'for further unauthorised purpose' contemplates the commission of further offence in accordance to the law. The Computer Crimes Act 1998 criminalises the

[24] Peters M, 'Section 114A...A Presumption of Guilt?' [2012] 6 MLJ ciii

[25] *Basheer Ahmad Maula Sahul Hameed & Ors v PP* [2016] 9 MLJ 549 17 May 2016

[26] House of Representatives Deb 28 April 1997, 19, 15

[27] ibid

[28] S 3 (3) of the Computer Crimes Act 1997 specifies that a person can be fined not exceeding RM50 000 and imprisonment for a term not exceeding five years or both

[29] S 4 (3) of the Computer Crimes Act provides for the punishment of a fine not exceeding RM150 000 or imprisonment for a term not exceeding 10 years or to both.

> means but the means can be the end as far as the prosecution goes. As a result, the means is an offence by itself.[30]

The Act does not expressly specify any offence of illegal interception of non-public computer data. According to Csonka, interception appears to be related to the offence of unauthorized access to a computer system in some countries.[31] Therefore, illegal interception may fall within the ambit of s 3(1) of the Act. In addition, unauthorized interception and disclosure of communication are prohibited under the s 234 of the Communications and Multimedia Act 1998.

Apart from unauthorized access and illegal interception, s 5(1) of the Computer Crimes Act 1997 criminalises unauthorised modification of the contents of any computer including programme and data.[32] The requisite mens rea is the knowledge that the act will cause unauthorised modification of the contents of any computer. The Act defines a programme as data representing instructions or statements that when executed in a computer, causes the computer to perform a function; meanwhile, data is described as information or concepts prepared or have been prepared in a form suitable for use in a computer.[33] The Cybercrime Convention distinguishes system interference from data interference. The hindering of computer systems must be serious in order to be considered as criminal offence, whereas this requirement is not compulsory for data interference.[34]

The denial of service attacks and malicious codes that substantially slow the operation system are perceived as a serious hindrance to the computer system.[35] They significantly impair the ability usage of the system and

---

[30] Interview with Deputy Public Prosecutor 1

[31] Csonka P, 'The Council of Europe's Convention on Cyber CRime and Other European Initiatives' <http://www.cairn-int.info/article.php?ID_ARTICLE=E_RIDP_773_0473> accessed 22.06.2016

[32] S 5 (4) of the Computer Crimes Act provides for the punishment of a fine not exceeding RM100 000 or imprisonment for a term not exceeding 7 years or to both or RM150 000 or imprisonment for a term not exceeding 10 years or to both if the act is done with the intention of causing injury as defined in the Penal Code

[33] S 2(1) of the Computer Crimes Act 1997

[34] Article 4 and article 5 of the Cybercrime Convention.

[35] Csonka P, 'The Council of Europe's Convention on Cyber Crime and Other European Initiatives' (n 31)

communication with other systems. According to Deputy Public Prosecutor 5:

> DDOS is not specifically provided under the Computer Crimes Act. We can argue that it fall under unauthorised modification. It causes modification or the division of the computer. In addition, we consider the removal of files on the computer as modification. It affects the proper usage of the computer especially when it is done without authorisation. The Budapest Convention may serve as a cue to amend this provision to deal with programmes such as DDOS and Spam.[36]

Besides denial of service attacks, the perpetrators of web defacement may be prosecuted for unauthorised access with modification under the Computer Crimes Act 1997 even though the web operator does not suffer any serious harm including monetary loss.[37]

In the light of the observations above, this section analyses the extent to which cyber attacks may be categorised as computer integrity crimes within the ambit of the Computer Crimes Act 1997. As stated in Chapter 3, the findings of this study show that most of the participants from all categories described 'cyber attack' as an attack on the computer system and server using tools such as viruses and malware. The attack affects the function of the computer especially the hardware and includes disabling the access to the computer system and decelerating the performance of the computer. According to Police Officer 3:

> The CCA (Computer Crimes Act 1997) may be invoked against any person who carries malware and plants the malware without authorization. He has the intention to do something. He uses malware to commit cyber attacks. For instance, he can access the computer and plant the malware through DRT.EXE files. The malware will change the configuration of the computer system. This falls within s 5 of CCA, which is unauthorised access with modification. The malware can change the

[36] Interview with Deputy Public Prosecutor 5

[37] Interview with Deputy Public Prosecutor 1

> configuration of the computer including opening ports as a backdoor. The computer is vulnerable to attacks.[38]

Results also have revealed that most of the participants from all categories considered the impact of a cyber incident must be significant in order to be categorised as a cyber attack. They did not classify mere hacking, 'cyber trespassing' or modification of data as cyber attacks. Security Professional 10 asserted that:

> The law governing cyber criminal is vague. I don't consider modification of data as cyber attacks. The data is already in the computer. I can change it without using third party tools. I am concerned about the usage of third party tools to interfere with the computer and to remotely access the computer. Let's say, I send a hyperlink to your device. You click the link and then the device downloads malware. Technically, I am not modifying anything. You allow your device to be infected by virus when you click the link. You should be responsible. So far, the insiders such as employees committed the offences under the Computer Crimes Act. Most of them abused their power.[39]

Therefore, it is highly probable that cyber attacks fall within the ambit of s 5 of the Computer Crimes Act 1997, which involves unauthorised modification of the computer programme or system. Police Officer 2 argued that the Act is sufficient to deal with cyber attacks especially in terms of punishment:

> The punishment provided under the Act is severe which is imprisonment for a term not exceeding 7 years. The suspect can be charged every time he accessed the computer without authorization. He can be charged separately for accessing the computer at 8 am and at 8.05 a.m. He can be charged for 10 offences if he accessed the computer 10 times without authorisation. The punishment is sufficient. We can increase the punishment for the purpose of deterrent. However, we have to consider from the perspective of human rights. We cannot

[38] Interview with Police Officer 3

[39] Interview with Security Professional 10

> impose severe punishment for petty offences especially if teenagers commit them. I handled a case involving a university student who hacked the university's online bulletin using injection. He posted a false notification that a class has been cancelled. We arrested him but the university decided to drop the charge. They don't want his future to be affected.[40]

On the other hand, some of the interviewees acknowledged that a large-scale cyber attacks may not fall within the ambit of the Computer Crimes Act 1997. Deputy Public Prosecutor 1 argued that:

> Based on the scale of punishment, the Computer Crimes Act 1997 does not anticipate wide scale attack. The seriousness of the offence is reflected by the sentence. This may not be sufficient in situations where the Scada system is hacked resulting in deaths due to flood, water contamination and electricity blows up the building.[41]

Deputy Prosecutor 5 agreed that attacks against critical national infrastructure may not fall within the ambit of the Computer Crimes Act 1997:

> We are not going to charge the attacks on the CNI such as the hydroelectricity dam under the CCA. This is because the maximum punishment is 7 years. We do acknowledge that punishment must reflect the gravity of the offence. We are doing research on how to improve the law including the specific provision to cater for CNI. But, not everything that we look into will materialise. For example, the Budapest Convention requires us to criminalise offences to promote homophobic tendency. We don't agree with that provision.[42]

Some of the interviewees, particularly the law enforcement officers, argued that the perpetrators of cyber attacks should be charged with the offences under the Penal Code based on the outcome of the attacks. This includes

---

[40] Interview with Police Officer 2

[41] Interview with Deputy Public Prosecutor 1

[42] Interview with Deputy Public Prosecutor 5

murder, destruction to property or causing bodily injury. S 44 of the Penal Code defines injury as any harm whatever illegally caused to any person, in body, mind, reputation or property. According to Deputy Public Prosecutor 3:

> It doesn't necessarily fall within CCA. We can invoke the Penal Code. If the attacks on CNI caused loss of life, technically the perpetrator has committed murder. We can also prosecute him for a lesser charge such as destroying public property. We have to look at the result and specific provision in relation to that. The prosecutor will look at the heaviest tendency. This includes looking at the best evidence. Let's say, there is a cyber incident. Based on the facts and evidence, the offender can be charged under the Penal Code, CCA or preventive legislation. Cyber or computer is only the means. We didn't have computer before this. I think the laws to control these offences are sufficient. Apart from conventional laws and specific provisions for cyber, we also have the preventive laws. They can be detained under the preventive legislation.[43]

Similarly, Deputy Prosecutor 5 argued that:

> Cyber attacks may fall under different legislation including the Official Secret Act, Sedition Acts and Penal Code. Instead of using the CCA that carries the maximum penalty of 7 years, we can invoke the Penal codes, which may carry the death sentence. We have to remember that CCA is not enacted to deal with people who hack the system of the CNI. It caters for young offenders who hack the computer for instance to post malicious comment. We cannot impose harsh punishment to these low-end offenders in comparison to high-end offenders.[44]

According to Deputy Public Prosecutor 1:

> We don't have to amend the law. The current laws are sufficient in dealing with cyber attacks. There is no material distinction

[43] Interview with Deputy Public Prosecutor 3

[44] Interview with Deputy Prosecutor 5

> between cyberspace and conventional crimes. It is just the means. It is not necessary for an act to be confined to a particular statute. It can be considered as an offence under multiple statutes. Cyber attacks against CNII could be classified as waging war against the Yang Di Pertuan Agong (the Ruler of Malaysia) under the Penal Code. It is similar to the Al Maunah Case. However, I haven't done much research on these cases.[45]

As demonstrated above, some of the law enforcement officers in Malaysia tend to downplay the role of the Computer Crimes Act 1997 in countering cyber attacks. They contended that the perpetrators of cyber attacks might be prosecuted for committing offences under the Penal Code. Nevertheless, it may be difficult to prove culpability with respect to crimes committed in cyberspace using the Penal Code. Brenner and Clarke argued that cybercrime does not share the features of real-world crime as it can inflict individual harm and systematic harm.[46] A small group can commit cybercrime on a scale exceeding physical crimes. The current model of law enforcement including the Penal Code is based on the assumption that the police can react to discrete crimes, as they are committed on a limited scale.[47] Thus, the provisions of Computer Crimes Act 1997 are useful additions. However, the Computer Crimes Act 1997 has to be reformed in order to enhance its effectiveness in dealing with cyber attacks. The offences such as the modification of the contents of the computer may need to be defined with greater precision. This includes the criminalisation of the creation and compilation of hyperlinks, which are used to enable remote access to the computer. In addition, a specific offence for cyber attacks including the preparatory acts and distribution of materials to commit cyber attacks may be introduced. This study shall return to the question of new offences for cyber attacks in section 5.3.

---

[45] Interview with Deputy Public Prosecutor 1

[46] Brenner SW and Clarke LL, 'Distributed Security: Preventing Cybercrime' 23 J Marshall J Computer & Info L 659 2004-2005

[47] ibid

5.2.1.2 Computer Content Crimes

Malicious and harmful communications in cyberspace may be classified as computer content crimes. Malaysian society is often viewed as highly sensitive to issues such as race and religion.[48] Speaking about these matters is perceived as dangerous in Malaysia. However, the advancement of social media especially the anonymity of the Internet enables people to express their thoughts.[49] It was reported that a total of 20.62 million Malaysians had social media accounts as of January 2016.[50]

As discussed in chapter 3, most of the participants especially the law enforcement officers considered negative publication including seditious and defamatory remarks on the Internet as cyber attacks. Deputy Public Prosecutor 3 argued that:

> Cyber attack may include the attack on the institution of royalty. This is done to bring down the institution. Cyber is only the means of attack. Cyber attacks go beyond attacking the software of the computer.[51]

According to Deputy Public Prosecutor 2:

> The purpose of the attack is not only to disrupt and destroy but also to give bad image. You can use the Internet to defame someone. This can be considered as cyber attacks on the character of a person by using the Internet. You have to look at Computer Crimes Act and the Multimedia and Communication Act. These Acts are connected. They are created almost the same year during the establishment of the Multimedia Super Corridor. These acts govern the cyber industry. The Computer Crimes Act is for criminal activities and the Multimedia and Communication Acts governs the players in the industry and

---

[48] Nor MWH, 'Hate Speech on the Rise: Lacunae in Malaysian Law' [2016] 1 LNS(A) lxvii 1

[49] ibid

[50] '22 Charged With Misusing Social Media Since 2010 - Jailani' *Bernama* (Kuala Lumpur, 20.04.2016) < http://www.skmm.gov.my/Media/Press-Clippings/22-Charged-With-Misusing-Social-Media-Since-2010-J.aspx> accessed 28.10.2016

[51] Interview with Deputy Public Prosecutor 3

> provides for offences with regard to computer, if I am not mistaken under s 233 of the Act.[52]

Similarly Police Officer 3 asserted that:

> The definition of cyber attacks for me is wide. It includes the people who incited hatred, spread propaganda and tried to impose their own perception to the public especially against the government. These are not related to the Computer Crimes Act. They fall under s 233 of the Communications and Multimedia Act 1998. They misuse the network, which has been provided by the government. They use the network for unethical purposes such as persuading the people to do something against the government or to commit any offences under s 233 of the Communications and Multimedia Act 1998.[53]

Based on the contentions above, this section examines the Malaysian laws applicable to cyber attacks in the context of computer content crimes.

Content related crimes in Malaysia fall primarily within the ambit of the Penal Code, Sedition Act 1948 and Communications and Multimedia Act 1998. S 499 of the Penal Code provides that a person can be punished for making or publishing any imputation concerning a person with the intention or knowledge or reason to believe that it will harm the reputation and defame such person.[54] In addition, a person who knows and has reason to believe that a substance contains defamatory matter can be charged for printing and selling it.[55] The impact of defamation law is limited as it only protects victims against false statements that jeopardies their reputation.[56] However, it serves a 'larger regulatory purpose in terms of expressing social values more broadly'.[57]

---

[52] Interview with Deputy Public Prosecutor 2

[53] Interview with Police Officer 3

[54] S 500 of the Penal Code stipulates that the punishment for this offence is imprisonment for a term which may extend to two years or with fine or with both.

[55] S 501 and 502 of the Penal Code

[56] Lipton JD, 'Combating Cyber-Victimization' (n 3) 1134

[57] ibid

S 4 of the Sedition Act 1948 prohibits any person from uttering seditious remarks or to do any act, which has a seditious tendency.[58] The prohibition encompasses printing, publishing, selling, distributing and propagating any seditious publication. S 3 of the Act lists the seditious tendencies, which includes to excite disaffection against any Ruler; to raise discontent or disaffection among Malaysians; and to promote feelings of ill will and hostility between different races or classes in Malaysia. The Sedition (Amendment) Act 2015 amended s 3 of the Act by decriminalising seditious tendency against the government and inserting racial and religious hatred. In *PP v Param Cumaraswamy*, the court held that seditious intention is not a necessary element of the crime.[59] However, the prosecution is required to prove that the words have a tendency to achieve the objects stipulated in s 3(1) of the Act.[60] Seditious tendencies do not include any act or words that point out the mistakes made by the Ruler in any of his measures and errors or defects in any government.[61] Accordingly, a mere criticism of the government and the implementation of government policies and programmes is not sufficient to constitute sedition.[62]

The Sedition Amendment Act 2015 was enacted for the purpose of dealing with electronic communications especially the social media.[63] The amendment removed the imposition of fine for seditious offences; the offender is now subjected solely to custodial sentence upon conviction. The length of the imprisonment has been increased to not exceeding 7 years. In addition, a person is liable to imprisonment for a term of not less than three years but not exceeding twenty years upon conviction if the seditious act causes bodily injury or damage to property.[64] Besides punishment, the Sessions Court Judge is vested with the power to direct the officers specified

---

[58] S 4 of the Sedition Act 1958 provides for fine not exceeding RM5000 or to imprisonment for a term not exceeding three years or both for a first offence.

[59] *PP v Param Cumaraswamy* [1986] CLJ Rep 606

[60] ibid; S 3 of the Sedition (Amendment) Act 2015

[61] S 3(2) of the Sedition Act 1958

[62] Faruqi SS, *Document of Destiny: the Constitution of the Federation Of Malaysia* (Star Publications (Malaysia) Berhad 2008) 295

[63] House of Representatives Deb 9 April 2015, 20, 43

[64] S 4 of the Sedition (Amendment) Act 2015

under the Communications and Multimedia Act 1998 to prevent access to seditious publication by electronic means by a person who cannot be identified.[65] These provisions have been criticized as they remove the court's discretion to determine an appropriate sentence in lieu of imprisonment and infringe the rights of Malaysians to receive information and express themselves.[66]

The mandatory imprisonment for seditious remarks is unnecessary and disproportionate. To date, the common practice of the Malaysian judges has been to fine people for sedition. In *Karpal Singh Ram Singh v PP & Another Appeal (No 2)*, the accused, a prominent politician in Malaysia, was convicted under s 4(1)(b) of Sedition Act 1948.[67] He was sentence to a fine of RM 1,800 in default two months imprisonment. However, in *Hishamuddn Md Rais v PP & Another Appeal*, the accused was convicted of delivering seditious speech during a gathering in 2013.[68] He was alleged of instigating the public to topple the government through unlawful means and was sentence to nine months imprisonment. The court decided that the deterrent effect of prison sentence was necessary in order to prevent chaos, to safeguard national security and to protect the public interest.[69] Therefore, imprisonment was imposed only on grave seditious act that threaten the security of the country.

Apart from sentencing, the Sedition Act 1948 has been challenged on the basis of fundamental liberties. Statistics show that sedition cases have increased from 19 cases in 2013 to 42 cases in 2014.[70] The Human Rights Commission of Malaysia contended that the term 'seditious tendency' has been interpreted arbitrarily especially when the Act is invoked against

---

[65] S 10 of the Sedition (Amendment) Act 2015

[66] Suhakam, 'Human Rights Commission of Malaysia Annual Report ' (*Human Rights Commission of Malaysia*, 2013) <http://www.suhakam.org.my/pusat-media/sumber/laporan-tahunan/> accessed 23 August 2014, 66

[67] [2016] 8 CLJ 65

[68] [2016] 3 CLJ 256

[69] ibid para 43

[70] International Commission of Jurists 'Sedition Act 1948 Cases in Malaysia (2010-2015)' <https://infogram/sedition_act_1948_cases_in_Malaysia_2010_2015> accessed 20 January 2017

politicians, academicians and media representative who criticize the government and its policies.[71] A restriction must be formulated clearly so that individuals can act accordingly.[72] In addition, the government should ensure the tools are necessary and proportionate in order to achieve objectives such as to protect national security or public order.[73] The usage of the Sedition Act 1948 to block a news site and prosecute individuals for criticizing the government is not justifiable.[74]

In *PP v Azmi Sharom*, the defendant argued that s 4 of the Sedition Act 1948 contravenes freedom of speech, assembly and association provided under article 10(1) of the Federal Constitution.[75] The Federal Court held that s 4(1) of the Act is consistent with article 10(2)(a) of the Federal Constitution, which permits the parliament to impose restrictions in order to protect the security, public order or morality.[76] The restrictions imposed by s 4(1) are not too remote and sufficiently connected to the objects enumerated in article 10(2)(a) of the Federal Constitution.[77] However, in *Mat Shuhaimi Shafiei v Government of Malaysia*, the Federal Court ruled s 3 (3) of the Sedition Act 1948 unconstitutional as it removes any consideration or necessary finding on the issue of the intention of the accused. [78] This provision was a disproportionate restriction as 'mens rea was an essential ingredient to be proved in other criminal proceedings before a valid conviction was handed down'.[79] Accordingly, s 3 (3) of the Sedition Act 1948 contravened article 8 and article 10(2)(a) of the Federal Constitution.[80] Despite the validity of the rest of the Act, the Human Rights Commission of Malaysia urged the government to seek other laws or legal remedies in addressing seditious

[71] Human Rights Commission of Malaysia, 'Annual Report 2015' (n 66) 66

[72] Kaye D, 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression', General Assembly A/71/373

[73] ibid

[74] ibid

[75] *PP v Azmi Sharom* [2015] 8 CLJ 921

[76] ibid para 43

[77] ibid

[78] *Mat Shuhaimi Shafiei v The Government of Malaysia* [2016] 1 LNS 1119

[79] ibid para 35

[80] Article 8 of the Federal Constitution provides for equality before the law

tendency.[81] This includes the proposed National Harmony Bill, which is still considered and discussed at the House of Representatives.[82] The National Harmony Bill is not formulated in order to replace the Sedition Act 1948.[83] However, the proposed Act may be used to promote religious and racial harmony in Malaysia.

As indicated in the preceding paragraph, most of the law enforcement officers agreed that cyber attacks fall within the ambit of the Communications and Multimedia Act 1998. The Act was promulgated for the purpose of ensuring reliability and integrity of the information security and establishing a regulatory framework for the communications and multimedia industry.[84] According to Deputy Public Prosecutor 3:

> Computer Crimes Act is confined to the computer per se, whereas, the Multimedia and Communications Act covers wider scope. It can include software and the computer. It deals with social media activities especially if the content is objectionable or corrupt.[85]

S 233 of the Act provides for the offence of improper use of network facilities or network service. A person is prohibited from using the network facilities and service to make, create, solicit and initiate the transmissions of 'any comment, request, suggestion or other communication which is obscene, indecent, false, menacing or offensive in character with intent to annoy, abuse, threaten or harass another person'.[86] The prohibition is extended to communication using any applications service with or without the disclosure

---

[81] Human Rights Commission of Malaysia, 'Annual Report 2015', (n 66) 64; Thiru S, 'Speech by Steven Thiru, President, Malaysian Bar at the Opening of the Legal Year 2016' [2016] MLJ xxiv

[82] House of Representatives Deb 24 March 2016, 12, 122

[83] ibid

[84] S 3 of the Communications and Multimedia Act 1998

[85] Interview with Deputy Public Prosecutor 3

[86] S 233 (1)(a) of the Communications and Multimedia Act 1998; s 233 (3) provides that a person is liable to a fine not exceeding RM50 000 or to imprisonment for a term not exceeding one year or to both and also liable to a further fine of RM1000 for every day during which the offence is continued after conviction.

of identity.[87] Improper usage of network facilities or network service is not perceived as a trivial offence in Malaysia. In *PP v Muslim Ahmad*, the accused was charged for three offences under s 233(1) of the Act for posting offensive comments against the Perak state government's official portal; the court dismissed his application for probation of good conduct under s 294 of the Criminal Procedure Code.[88] It was held that:

> A binding over order would send the wrong message to would be offenders and the public at large that offensively uncontrolled and virulent comments can be indiscriminately posted on the Internet without any or serious repercussions, and that is not a message this court would like to send out.[89]

The prosecution is required to prove that the accused made the communication through a network facility and the act was done with the intention to annoy, abuse, threaten or harass the victim. In *PP v Rutinin Suhaimin*, the court held that:

> As for evidence in respect of intention, it is always a matter of inference. From the fact that an offensive remark pertaining to the HRH Sultan of Perak had been posted on the online visitor book, it can be inferred that the accused had intended to cause annoyance. It is also unnecessary to call the victim of the annoying remark to the witness stand. Section 233 (1)(b) does not say that the victim of the offence must actually feel annoyed or abused. The provision only says that the offender must have intention to annoy or abuse. Therefore it is sufficient if the communication in question has the tendency to cause annoyance or abuse to any person.[90]

The accused has to raise a reasonable doubt that he did not post the communication in dispute. He may argue that another person used his computer or his IP or Mac addresses had been spoofed. However, s 114A of

---

[87] 233 (1) (b) of the Communications and Multimedia Act 1998

[88] [2013] 5 CLJ 522

[89] ibid para 40

[90] [2013] 2 CLJ 427

the Evidence Act 1950 provides for statutory presumption in relation to fact in publication. S 114A (2) of the Act indicates that:

> A person who is registered with a network service provider as a subscriber of a network service on which any publication originates from is presumed to be the person who published or re-published the publications unless the contrary is proved.

The Evidence Act 1950 also provides that a person is presumed to have published the content of publication, which originates from the computer in his custody or control.[91] This provision was inserted in order to strengthen cyber laws and to overcome the problems caused by Internet Anonymity especially during criminal and civil proceedings.[92] Peters argued that this provision might affect Internet intermediaries including the operator and provider of online community forums.[93] They may not possess the technical expertise to rebut the presumption. Furthermore, the owner-onus principle may not be suitable in the context of technology, as access to the computer, website or Wi-Fi is more readily available. [94] Therefore, it is not difficult for anyone to impersonate another and perpetrate cybercrime. Police Officer 3 also noted that:

> Let's say I want to commit an offence; I will not attack the target directly. I will use other people's computer in case something happens later; it will not revert to me. I will use someone else as a middleman to spread the propaganda for me. In the end, the result is the same.[95]

However, Deputy Public Prosecutor 5 emphasised that s 114A of the Evidence Act 1950 is not simply a presumption of guilt:

---

[91] S 114A (3) of the Evidence Act 1950

[92] House of Representatives Deb 18 April 2012, 9

[93] Peters M, 'Section 114A...A Presumption of Guilt?' [2012] 6 MLJ ciii; Radhakrishna G, 'Legal Presumptions and the Burden of Proof: S 114A Evidence (Amendment) (No. 2) Act 2012' [2013] 1 LNS(A) lxxxv

[94] Peters M, 'Section 114A...A Presumption of Guilt?' [2012] 6 MLJ ciii

[95] Interview with Police officer 3

> We have the presumption of facts. I don't think there is any jurisdiction that shifts the presumption of guilt; it is just the presumption of facts. We have s 114A of the Evidence Act to cater for making false statement online. However, we have amended s 153 of the Criminal Procedure Code. Online publication such as defamatory statement is still an offence. This amendment was done because we had problem to prove where the comment was uploaded. So, the offence was committed at the places where the comment was heard or seen.[96]

S 153 (b) of the Criminal Procedure Code indicates that the place of the publication is where the publication is seen, heard or read by any person in relation to any person who is charged with an offence relating to publication by electronic means. In *Tong Seak Kan & Anor v Loke Ah Kin & Anor*, the court held that the presumption under s 114A(2) of the Evidence Act 1950 is not an irrebuttable presumption and does not finally determine the publisher's liability in a civil claim or guilt in a criminal prosecution.[97] However, once the presumption is invoked, the publisher has to provide the evidence in order to convince the court that he is not the author of the publication. The court noted that the registered subscriber has to prove on the balance of probability that he is not the author of the publication under the law relating to cyber publication.[98]

The presumption under s 114A of the Evidence Act and s 153 (b) of the Criminal Procedure Code are not applicable to offences under the Computer Crimes Act 1997. According to Deputy Public Prosecutor 5:

> They are not extended to hacking, as cyber criminals are really good at covering their tracks. For instance, we can use the IP address to trace them if they hack a server. However, we may lose their track especially if they use cloud computing. We cannot exactly trace where they physically committed the attack.

---

[96] Interview with Deputy Public Prosecutor 5

[97] [2014] 6 CLJ 904, para 22

[98] ibid para 18

Similarly, Police Officer 3 asserted that:

> Based on forensic evidence, let's say we discovered John's computer is the source of the vulnerability. We can invoke the presumption under s 114A. However, his computer may be used as a zombie. This may happen if John did not secure his computer; he did not have antivirus or firewall. How we are going to get the actual creator of the virus? [99]

This demonstrates that the presumption may not be invoked against cyber attacks in the context of computer integrity crimes due to the difficulty in tracing the perpetrators especially the creator of the malware.

Apart from the classification of cyber attacks as computer content crimes, this study examines the enforcement of the law in relation to the content of the multimedia applications especially the Internet in Malaysia. The Malaysian Communications and Multimedia Commission (the Commission) was established to supervise and regulate the communications and multimedia activities in Malaysia. The Commission is given the task of enforcing the communication and multimedia laws in Malaysia.[100] This includes the appointment of investigating officers to carry out inspection and investigation of any offence under the communications and multimedia laws. The police and the Commission have the jurisdiction to investigate computer content crimes in Malaysia.[101] According to Deputy Public Prosecutor 4:

> The prosecution would be considered on case-by-case basis. Let's say, a person posted a comment on Facebook or WhatsApp. The police will investigate whether the comment is seditious. At the same time, SKMM (the Commission) will be involved in investigating comment that harms or threatens the public. The investigations by the police and SKMM can be

[99] Interview with Police officer 3

[100] S 16 (1) of the Malaysian Communications and Multimedia Commission Act 1998

[101] S 246 of the Communications and Multimedia Act 1998

> conducted simultaneously. It is up to the Public Prosecutor to determine whether to proceed with the cases.[102]

The Commission cooperates with the police in monitoring, detection, information sharing and conducting digitals forensics to eradicate crimes and misuse of social media.[103] In addition, the Commission is empowered to regulate the content of the services. This includes preparing a content code and procedures for dealing with offensive and indecent content.[104] The service providers shall ensure that their services do not contain indecent, obscene, false, menacing or offensive materials.[105] They may be requested to assist the Commission and the police in preventing the commission of an offence in Malaysia.[106] Policymaker 2 noted that 'companies especially the ISPs are required to assist the Commission under s 263 of the Communications and Multimedia Act 1998 to protect the national interest and security.[107] However, Deputy Public Prosecutor 3 asserted that:

> The Malaysian Communications and Multimedia Commission can block the services provided online. There are issues pertaining to this measure. The politicians from the opposition parties argue that it may be used to block their opinions. How do you apply the discretion? You don't want to be perceived as crippling the opposition parties as contended by the western countries.[108]

Accordingly, the Commission must be unbiased and impartial in exercising its power to regulate the content of the services.

Some of the law enforcement officers claimed that the current laws are effective in dealing with cyber attacks in this category.[109] It was reported that

---

[102] Interview with Deputy Public Prosecutor 4

[103] MCMC Receives 403 Complaints on Offences Pertaining to Insults, Threats from January-May' *Bernama* (Kuala Lumpur, 20.06.2016)

[104] S 212 and s 213 of the Communications and Multimedia Act 1998

[105] S 211 of the Communications and Multimedia Act 1998

[106] S 263 of the Communications and Multimedia Act 1998

[107] Interview with Policymaker 2

[108] Interview with Deputy Public Prosecutor 3

[109] Interview with Police Officer 3

14 cases have been brought to the court under s 211 and s 233 of the Communications and Multimedia Act 1998 from January until August 2015.[110] 10 out of 14 cases have been prosecuted and sentenced by the court.[111] So far, 22 owners of social networking sites, websites and blogs were charged with misusing the medium for various purposes.[112] In addition, 403 complaints involving insults and threats were lodged to the Commissions between January and May 2016.[113]

On the whole, the empirical findings suggested that malicious and harmful communications including sedition is perceived as cyber attacks in Malaysia. They are governed by the Penal Code, Sedition Act 1948, Evidence Act 1950 and the Communications and Multimedia Act 1998. Statistics show that these laws have been used extensively to deal with the misuse of the social media and the Internet. However, as indicated in the previous chapter, the effectiveness of the law governing the abuse of the social media may contradict the notion of fairness. The Sedition Act 1948, in particular, has been challenged on the grounds that it has been used arbitrarily against politicians, academicians and social media operators. Thus, the decision of the court in *Mat Shuhaimi Shafiei v Government of Malaysia* has been hailed as a victory for freedom of speech. Nevertheless, the promulgation of the Sedition Amendment Act 2015, which provide for mandatory imprisonment may continue to undermine the fundamental liberties. Thus, a fair judicial process is necessary in order to protect the freedom of speech in Malaysia.

5.2.1.3 Computer Related Crimes

The section examines the prosecution of the perpetrators of cyber attacks for stealing government's information and personal data. Cyber attacks may be committed for the purpose of obtaining confidential information including

---

[110] '14 Kes Bawah Akta MCMC 1998 Dibawa ke Mahkamah Setakat Awal Ogos' *Bernama* (Kuala Lumpur, 13.08.2015) <http://www.skmm.gov.my/Media/Press-Clippings/14-Kes-Bawah-Akta-MCMC-1998-Dibawa-Ke-Mahkamah-Set.aspx> accessed 28.10.2016

[111] ibid

[112] '22 Charged With Misusing Social Media Since 2010 - Jailani' *Bernama* (Kuala Lumpur, 20.04.2016) < http://www.skmm.gov.my/Media/Press-Clippings/22-Charged-With-Misusing-Social-Media-Since-2010-J.aspx> accessed 28.10.2016

[113] MCMC Receives 403 Complaints on Offences Pertaining to Insults, Threats from January-May' *Bernama* (Kuala Lumpur, 20.06.2016)

official secrets, trade secrets and personal information. Policymaker 4 asserted that:

> I hacked your website and steal information; of course, I have committed a crime. We consider this as an intrusion. It is a part of cyber attack. Although it doesn't cause substantial damage, your data can be compromised. We consider industrial espionage as cyber attacks. This happens when a company steals information for industrial purposes. The perpetrator uses spyware; it is a malicious software.[114]

However, stealing of information may not be categorised as crime against the property under the Penal Code. According to Deputy Public Prosecutor 5:

> Cybercrime is a way of committing crimes. The crime is committed differently. For instance, from the point of law, theft is committed by taking somebody's possession. Cyber theft may be committed by stealing somebody's information. The perpetrator accessed the hard drive of the computer. Technically, such action is not considered as a theft under the Penal Code. Theft is taking the possession of movable property from somebody.[115]

Accordingly, this section examines the application of criminal laws to cyber attacks involving the loss of information or data.

As indicated in section 4.3.3, the Personal Data Protection Act 2010 is not applicable to government data. Therefore, the Official Secrets Act 1972 is instrumental in protecting the governmental confidential information against disclosure and acquisition. The protection is accorded to the following official information: any information and material concerning national security, defence and international relations; Cabinet documents; State Executive Council documents and materials that have been classified as 'Top Secret', 'Secret', 'Confidential' or 'Restricted' by the government officials specified in

---

[114] Interview with Policymaker 4

[115] Interview with Deputy Public Prosecutor 5

the Act.[116] An audit report that was tabled and deliberated upon by the Cabinet is classified as an official secret document.[117] Spying and espionage are considered as a serious threat to the government. Spies looking for intelligence, which is calculated to be useful to a foreign country, are punishable with imprisonment for life.[118] Similarly, the Penal Code provides for imprisonment for life for any person who commits espionage.[119] Most of the law enforcement officers asserted that the Computer Crimes Act 1997, the Official Secrets Act 1972 or the Penal Code might be invoked against the perpetrator of cyber attacks in this category. According to Deputy Public Prosecutor 5:

> The unauthorised access carries maximum punishment of five years. It covers criminals who hacked the banking system. It also covers somebody who walks into this room; opens a laptop; looks at the data and then exit the room. 5 years are enough for these offences. However, when somebody hacked into the system; access confidential materials and made it public; it falls under the CCA and OSA. These two acts are not at the same level. If he used that information to commit terrorist acts for example, it falls under section 130A of the Penal Code. It carries life imprisonment sentence. We cannot limit ourselves to the CCA. CCA covers specific offences including the offences provided under other legislation. If he hacked in order to get classified information, this is an offence under the OSA. We wouldn't charge him under the CCA because the punishment under the OSA is heavier.[120]

The Official Secrets Act 1972 is perceived as necessary in order to protect official secrets from cyber attacks. However, the Act may be used to restrict

---

[116] S 2 and the schedule of the Official Secrets Act 1972

[117] *Malaysian Trade Union Congress & Ors v Menteri Tenaga, Air dan Komunikasi & Anor* [2014] 2 CLJ 525

[118] S 3 of the Official Secrets Act 1972

[119] S 124M of the Penal Code; s 130A of the Penal Code defines espionage as 'an activity to obtain sensitive information by ulterior or illegal means for the purpose that is prejudicial to the security or interest of Malaysia'.

[120] Interview with Deputy Public Prosecutor 5

the access to information on matters of public interest. The expression 'official secret' and 'public service' are given wide definitions.[121] Masum argued that the 'catch-all provisions' do not fall within the permissible grounds stipulated in Article 10(2) of the Federal Constitution.[122] Ultimately the courts are vested with the power to ensure that the restriction to official secret is justifiable and permitted by the Federal Constitution.[123]

It can be argued that the application of the Official Secrets Act 1972 is difficult due to several reasons. Firstly, the government is focusing on the impact of the loss of data instead of prosecution of an individual. Prosecution is not a viable solution, as the government has to reveal the leak and the nature of the information that has been exposed. Secondly, the attempt to prosecute is futile especially if the accused fled to other country like Edward Snowdon. Moreover, a diplomat cannot be prosecuted for spying as they are protected under the 1961 Vienna Convention on Diplomatic Relations.[124] They can be declared as persona non-grata and expelled by the state.[125] For instance, Obama deported Russian diplomats for spying on the US.[126] Therefore, non-criminal measures such as encryption are more effective in protecting the government's information.

Cyber espionage is perceived as an attack on national security, economy and personal liberty in countries such as the US. It was reported that five Chinese military hackers were charged with cyber espionage against US corporations.[127] They were accused of masterminding government-led cyber

---

[121] Masum A, 'The Role of Good Governance in Protecting and Promoting Human Rights-A Case Study of Malaysia' [2010] 1 LNS (A) ii

[122] ibid

[123] Faruqi SS, 'Free Speech and the Constitution' [1992] 4 CLJ 1xiv

[124] Article 29 and Article 31 (1) of the 1961 Vienna Convention on Diplomatic Relations; see also Law Commission, 'Protection of Official Data A Consultation Paper', Law Com No 230, 2017) paras 2.110-2.111

[125] Article 9 of the 1961 Vienna Convention on Diplomatic Relations

[126] CBS News '35 Russian Diplomats Ordered Out by Obama Depart US, State Department Says' <http://www.cbsnews.com/news/35-russian-diplomats-ordered-out-by-president-obama-depart-us-state-department-says/> accessed 20 January 2017

[127] Cornwell R, 'US Declares Cyber War on China: Chinese Military Hackers Charged with Trying to Steal Secrets from Companies including Nuclear Energy Firm' *Independent* (19 May 2014) <http://www.independent.co.uk/life-style/gadgets-

hacking to steal significant trade secrets of energy and metal industries including nuclear power station manufacturer. United States acknowledges the need for coercive measures against the perpetrators of cyber attacks and cyber espionage.[128] Thus, the president of US signed the executive order April 2015, which allows the Federal Agencies to freeze financial assets of foreign individuals and barring cyber attackers from commercial transaction within US.[129] Similar measures may be implemented to counter cyber attacks in Malaysia. This study shall return to the question of cyber espionage under international law in chapter 6.

As stated in section 4.3.3, the data user is criminally liable for failing to take practical steps to protect the personal data from any loss. The Personal Data Protection Commissioner is vested with the competency to compound this offence under the Act. Apart from non-compliance with security principle, the data user and the perpetrators of cyber attacks may be held criminally liable for unlawful collecting or disclosing of personal data under the Act. This section assesses the application of this offence against the perpetrators of cyber attacks in Malaysia.

Most of the participants from all categories agreed that cyber attacks may be done in order to steal personal information. The perpetrators could reap profits from selling the information to a business competitor.[130] According to Legal Practitioner 1:

> Usually our client sought our advice in relation to the information involving customers who resided in Malaysia or the data of customers located in Malaysia. The information has

---

and-tech/us-charges-chinese-military-hackers-with-cyber-espionage-bid-to-gain-advantage-in-nuclear-power-9397661.html> accessed 13 May 2014

[128] BBC, 'US Raises Cyber Concerns with China' *BBC* <http://www.bbc.co.uk/news/world-us-canada-33264216> accessed 16 May 2016;

[129] House TW, 'Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"' (*The White House*, i April 2015) <https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m> accessed 16 May 2016; University Alliance, 'Presidential Order Clamps Down on Cyber Attackers' (*Florida Tech*, 26 May 2015) <http://www.floridatechonline.com/news/2015-headlines/presidential-order-clamps-down-on-cyber-attackers/> accessed 16 May 2016

[130] Interview with Police Officer 3

> been compromised when somebody hacked the computer system. They worried about the ramification of the data being compromised.[131]

S 130 of the Personal Data Protection Act 2010 provides for the offence of unlawful collecting, disclosing, selling or procuring the disclosure to another person of personal data that is held by the data user. A person is liable to a fine not exceeding RM500,000 or to imprisonment for a term not exceeding three years or both for committing this offence.[132] The intention to do harm is not specified for this offence. According to Legal Practitioner 2:

> The Act does not talk about what you are going to do with the data. You have breached the Act when you misappropriated the data in the way not consented to the by the original owner.[133]

Moreover, Legal Practitioner 2 noted that the Act primarily deals with the measures to protect personal data. It may not be intended for crime against property:

> Information is in a way can be considered as property, PDPA is limited to personal data. It is different from other law. It provides for the step to protect data and security such as the need for consent. It deals with individual's concern in relation to privacy. Why are you using my information for marketing?[134]

Results of the study have revealed that some of the participants contended that this offence is not effective in protecting personal information in Malaysia. This is due to the weakness in the enforcement and the lack of awareness of the data subjects of their rights. According to Legal Practitioner 1:

> The enforcement is slow. There is no strict enforcement. We haven't heard any news about the imposition of fine or imprisonment on the offenders. However, the Act is still new.

---

[131] Interview with Legal Practitioner 1

[132] S 130 (7) of the Personal Data Protection Act 2010

[133] Interview with Legal Practitioner 2

[134] Interview with Legal Practitioner 2

> We don't know about any internal investigation. Usually, this is between the Central Bank of Malaysia and the bank.[135]

Security Professional 10 argued that:

> I am sure that you are aware about PDPA. I don't think PDPA can control this. People are still receiving sms about sale from unidentified caller. There is lack of enforcement. I asked the audience about PDPA during one of my seminar. Most of them were layman. All of them ticked the box allowing their data to be used in the PDPA form. They didn't know the impact of their action.[136]

In addition, Private Sector Officer 1 argued that the data users failed to adhere to the obligation specified in the Act:

> The purpose of the PDPA is to protect personal data. However, small companies don't put their mind to it. I sent my documents to a bank last week. I asked the bank officer about the PDPA form. I need to sign it because the documents contained my personal information. Apparently, he had the form. However, he did not follow the policy. Who is going to enforce it? He cannot simply say I will keep it. My information can be stolen if the bank's computer is compromised.[137]

Accordingly, strict enforcement is necessary in order to enhance the effectiveness of the Act. Moreover, the Commissioner and the Department of Personal Data Protection of Malaysia should intensify their effort to increase awareness among the data users. They should constantly conduct systematic assessment of the implementation of safeguards provided under Personal Data Protection Act 2010 at site. In addition, they should organise frequent advisory visits to data subject and data user such as banks, local government, and healthcare facilities. An overview reports and monitoring

---

[135] Interview with Legal Practitioner 1

[136] Interview with Security Professional 10

[137] Interview with Private Sector Officer 1

reports should be produced in order to enhance the security of personal information.

Apart from that, self-assessment programme may be conducted to promote good personal data practice especially among small organisations. The ICO has conducted this programme in schools in order to raise awareness of data protection and the practicalities of complying with data protection legislation among youngsters. [138] The Department of Personal Data Protection of Malaysia may adopt similar measure in order to instil awareness among the data subjects.

On the whole, criminal law may be used to protect official secret and personal information against cyber attacks. The Official Secrets Acts Act 1972, the Personal Data Protection Act 2010 and the Penal Code may be invoked against the perpetrators of cyber attacks in this category. However, the usage of criminal law may be constrained by factors such as the risk of exposing the government's information during criminal proceeding and diplomatic row. Thus, the government may prefer to use non-criminal measures to deal with this problem. Moreover, the Official Secrets Act should be repealed in order to ensure that the legislation is fit for purpose in the digital era.[139] Finally, there is a need for the government to review the effectiveness of the enforcement of the Personal Data Act 2010 in protecting personal information.

5.2.2 Cyberterrorism

Terrorism poses a serious danger and risk to Malaysia. Malaysia is ranked number 49 in the Global Terrorism Index 2015 by the Institute for Economics and Peace.[140] Malaysia is on high alert following the attack on the ISIS stronghold in Mosul, Iraq in October 2016.[141] Moreover, there are growing

---

[138] ICO, 'Action We've Taken: Self- Assessment' <https://ico.org.uk/action-weve-taken/self-assessments/> accessed 21 January 2017

[139] Law Commission, 'Protection of Official Data Summary Com', No 230, 2017 para 2.37

[140] Institute for Economics and Peace, 'Global Terrorism Index 2015: Measuring and Understanding the Impact of Terrorism' START <http://economicsandpeace.org/wp-content/uploads/2015/11/2015-Global-Terrorism-Index-Report.pdf> accessed 1.11.2016

[141] Kanyakumari D, 'Zahid: 137 Detained so far Over IS Terror Links' *The Star*

concerns among Malaysians about cyber attacks on computer systems by terrorist groups.[142] Cyberterrorism is an attractive choice for terrorists due to the anonymity of the Internet, the potential to inflict serious damage, the psychological impact and the media appeal.[143] The computer technology may be used for preparatory acts such as providing financial support to launch cyber attack against an electronic system. The Internet is a useful tool for communication and instrumental purposes including disseminating lectures, and instruction manuals, data mining, recruitment and mobilisation.[144] Terrorist groups such as Daish and Al-Qaeda utilise computer technology to achieve their goals and to conduct their operation efficiently. They use the social media to spread their propaganda and to conscript new members. It was reported that the Royal Malaysia Police surveyed almost 1000 Facebook accounts, 100 Twitter Accounts and 50 websites and blogs related to ISIS and Al-Qaeda in Malaysia as at 6.04.2016.[145] This section examines the application of criminal law in dealing with cyber attacks in the guise of cyberterrorism in Malaysia.

Cyberterrorism is distinguished from cybercrime by reference to the components of terrorism.[146] S 130B of the Penal Code defines a terrorist act as an act or threat of action where: the act is done or threat is made with the intention of advancing a political, religious or ideological cause; and the act or threat is intended to intimidate the public or influence the Government or any international organization to do or refrain from doing any act.[147] A terrorist act includes the disruption or serious interference of any computer

---

Online (Kuala Lumpur, 18.10.2016) Nation <http://www.thestar.com.my/news/nation/2016/10/18/zahid-parliament-is/> accessed 1.11.2016

[142] House of Representatives Deb 6 April 2016, 18

[143] Weimann G, 'Cyberterrorism: How Real is the Threat?' (2004) The United States Institute of Peace Special Report 119

[144] Kennedy J and Weimann G, 'The Strength of Weak Terrorist Ties' (2011) Terrorism and Political Violence, 23:2, 201-212, DOI: 101080/095465532010521087

[145] House of Representatives Deb 6 April 2016, 18

[146] Stohl M, 'Cyber Terrorism: a Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?' Crime Law Soc Change (2006) 46:223–238, DOI 101007/s10611-007-9061-9

[147] S 130B (2) of the Penal Code

systems or services related to communication infrastructure, banking or financial services, utilities, transportation or other essential infrastructure.[148] Cyber terrorists use the information systems or other electronic means to target innocent people in order to cause a political change.[149] To achieve the terrorism element, the impact of the attacks must be significant. According to Policymaker 4:

> The scale and impact are very important. Crime and terrorism are two different things. If you are charged for committing act of terrorism, the punishment includes death penalty. Cyberterrorism includes the attack to the telecommunication network through cyberspace and the usage of stuxnet to attack nuclear power. The CNI may be damaged or people may die as result of the attacks.[150]

The potential threat from cyberterrorism is alarming as most critical infrastructure such as electrical power grids and emergency services are connected through computers.[151] In addition, cyberterrorism poses indirect threat of violence as it causes psychological impact on societies, which is 'as powerful as the effect of terrorists' bombs'.[152]

Most of the law enforcement officers argued that cyberterrorism is sufficiently covered by the Penal Code. According to Deputy Public Prosecutor 5:

> You can blow the dam by using a bomb or hacking the information system. It amounts to terrorist act and affects the

[148] S 130B (3)(h) of the Penal Code; s 130C of the Penal Code provides that the offender shall be punished with death if the act results in death or imprisonment for a term not less than seven years but not exeeding thirty years and fine in other cases.

[149] Yunos Z and Suid SH, 'Safeguarding Malaysia's Critical National Information Infrastructure (CNII) Against Cyber Terrorism: Towards Development of a Policy Framework' (Sixth International Conference on Information Assurance and Security, 2010)

[150] Interview with Policymaker 4

[151] Weimann G, 'Cyberterrorism: How Real is the Threat?' (n 143)

[152] Weimann G, 'Cyberterrorism: The Sum of All Fears? Studies in Conflict & Terrorism' Studies in Conflict & Terrorism, 28:2, 129-149, DOI: 101080/10576100590905110

> national security. It is sufficiently covered under our law, which is s 130 of the Penal Code. This provision provides for death penalty.

Apart from the Penal Code, the Security Offences (Special Measures) Act 2012 (SOSMA) may be invoked against cyberterrorism. SOSMA was enacted in order to protect Malaysia from serious threats especially terrorism.[153] The promulgation of SOSMA is justified as necessary in order to prevent Malaysia from being used as a terrorist haven.[154] SOSMA only regulates the trial of security offences; the offenders are punishable under the Penal Code.[155] SOSMA provides for special powers of arrest, detention and prosecution of security offences such as procedures in relation to sensitive information, protected witness and the admissibility of intercepted communications and surveillance information.[156]

However, the usage of executive based preventive measures especially preventive legislation, surveillance and deradicalisation programme are more prevalent than criminal law in dealing with terrorism in Malaysia. The Prevention of Terrorism Act 2015 (POTA) provides for detention without trial of up to two years by the order of an administrative board with the possibility of indeterminate extensions.[157] It was reported that 177 people were arrested under SOSMA, Prevention of Crime Act 1959 and POTA from 2013 until 24.03.2016 for their involvement with Daesh or ISIS.[158] In addition, the Home Ministry, Prisons Department and the Royal Malaysian Police have developed an Integrated Deradicalising for Terrorists programme. Malaysia's Deputy Prime Minister claimed that 240 detainees had been successfully deradicalised for the past 10 years.[159]

---

[153] House of Representatives Deb 17 April 2012, 3

[154] *Public Prosecutor v Yazid Bin Sufaat & Ors* [2015] 1 MLJ 571

[155] ibid para 23

[156] Part II, part IV, part VI of the Security Offences (Special Measures) Act 2012

[157] S 13 (1) of the Prevention of Terrorism Act 2015

[158] House of Representatives Deb 6 April 2016, 18

[159] BERNAMA, 'Tackling Daish More Difficult Than Tackling Communists - DPM' *Astro Awani* (1.11.2016) <http://english.astroawani.com/malaysia-news/tackling-daish-more-difficult-tackling-communists-dpm-121160> accessed 2.11.2016

The usage of executives order in dealing with terrorism is perceived as unnecessary as the provisions in the Penal Code and the SOSMA are adequate in the fight against terrorism.[160] Furthermore, the establishment of a special tribunal to handle cases related to extremism and militancy should reinforce the function of criminal law in dealing with cyberterrorism in Malaysia. The militant court/SOSMA was set up in order to hear cases involving Islamic State Militants and security matters. It was reported that 110 cases have been registered under SOSMA and 59 cases were disposed in 2015.[161] This study shall return to the usage of executive order in countering cyber attacks in section 5.3.3

So far, this study investigates the existing scope and role of criminal in dealing with cyber attacks in Malaysia. Cyber attacks are divided into: computer integrity crimes, computer content crimes and computer integrity crimes. Apart from cybercrimes, it also examines the application of criminal law in countering cyberterrorism. This study demonstrates the advantages and disadvantages of the Malaysian laws in managing cyber attacks. The findings suggest that the Computer Crimes Act 1997 is not adequate in dealing with a large-scale cyber attacks especially against the essential national infrastructures. In the following section, this study considers the introduction of new offences to enhance the effectiveness of criminal law especially the Computer Crimes Act 1997 in dealing with cyber attacks in Malaysia.

5.3 Potential New Offences Against Cyber Attacks in Malaysia

This study was designed to gather information about the creation of new offences for cyber attacks in Malaysia. There are varieties of offences that may be introduced in Malaysia in dealing with cyber attacks. However, this study considers the creation of an offence similar to s 3ZA (1) of the Computer Misuse Act 1990 in UK, precursor offences and executive order.

---

[160] Thiru S, 'Speech by Steven Thiru, President, Malaysian Bar at the Opening of the Legal Year 2016' [2016] MLJ xxiv

[161] Zakaria TAB, 'Speech by YAA Tun Ariffin Bin Zakaria, Chief Justice of Malaysia at the Opening of the Legal Year 2016' [2016] MLJ i

This section is structured as follows. Firstly, it discusses the reasons to justify the creation of a similar offence to s 3ZA (1) of the Computer Misuse Act 1990 in Malaysia. Next, this section examines the physical elements, degree of harm and fault elements for this offence. Then, this section assesses the main arguments that deal with the issue of the creation of precursor offences in Malaysia. Finally, this section examines the application of executing order in dealing with cyber attacks.

5.3.1 S 3ZA (1) of the Computer Misuse Act 1990

This section considers the introduction of extra offences that specifically deal with large-scale cyber attacks in Malaysia. The EU Directive 2013/40/EU on attacks against information systems emphasises the need to increase the protection of the critical national infrastructures against cyber attacks, which include the imposition of heavier criminal sanction.[162] Pursuant to this Directive, the UK's Computer Misuse Act 1990 was amended to include the creation of a new offence for the most serious cyber attacks and to provide heavier sentencing to reflect the gravity of this offences.[163] Besides that, the amendment confers the courts with extra-territorial jurisdiction and extends the scope of s 3A of the Computer Misuse Act 1990 to cover articles for personal use.[164] This amendment affirms the danger posed by cyber attacks; they can cause widespread and serious harm to the public. Large-scale cyber attacks may disrupt the economy through the interruption and alteration of information systems, communications and confidential information.[165] Such impacts necessitated the creation of a specific offence for serious cyber attacks. So far, these offences are not part of the criminal law of Malaysia, particularly, the Computer Crimes Act 1997.

As stated before, some of the interviewees from the law enforcement category acknowledged that a large-scale cyber attacks may not fall within

---

[162] European Parliament and the Council Directive 2013/40/EU of 12 August 2013 on Attacks Against Information Systems and Replacing Council Framework Decision 2005/222/JHA

[163] Home Office, 'Home Office Circular Serious Crime Act 2015' (Home Office, 2015)

[164] S 43 of the Serious Crime Act 2015

[165] European Parliament and the Council Directive 2013/40/EU (n 162)

the ambit of the Computer Crimes Act 1997 due to the inadequacy of the punishment. Consequently, they argued that other laws such as the Penal Code should govern these attacks. However, Legal Practitioner 1 suggested that the provisions of the Computer Crimes Act 1997 should be re-examined to cater for cyber attacks:

> The Penal Code provides for the offences against the state. It is designed for physical property or things. For instance, somebody steals your computer. However, stealing of data would be difficult to be proven under the Penal Code. The Computer Crimes Act can be paired with other legislation to cater for these offences. However, it can also be amended to incorporate more cyber attacks offences.[166]

Similarly, Legal Practitioner 3 argued that the Computer Crimes Act 1997 should be used as the prevalent law to deal with cyber attacks:

> We have a specific Act, which is the Computer Crimes Act 1997. It should be used to cater to those instances. Prosecution would be much easier as we focus on a specific Act. For instance, the Dangerous Drugs Act is enacted to deal with a specific situation. We get more sophisticated in term of how we are engaged with each other of the net and how we perform transaction on the net. As a consequence of that, as we progress, the law need to be updated from time to time.[167]

Despite the insistence on the application of the Penal Code, there was a hint from Deputy Public Prosecutor 2 that an attack on critical national infrastructure offence should be considered as viable in Malaysia:

> Currently, the attack on CNI is going to be implemented in the Multimedia Communication (Amendment) Act. It is under progress. I was involved in it. We have looked at several jurisdictions especially on the definition of CNI, There is a definition adopted by Cybersecurity Malaysia. All I can say, if

[166] Interview with Legal Practitioner 2

[167] Legal Practitioner 3

> you look at the UK, the answer is there. Cyber specific offences require cyber specific laws. For example, terrorists can fall within the ambit of terrorism legislation, but a normal person, who is not a terrorist, can infiltrate the computer system of the infrastructure and cause massive disruption, shut down the water supply system using the computer[168]

Deputy Public Prosecution 2 was asked about the insertion of the proposed offence in the Communications and Multimedia Act 1998 instead of the Computer Crimes Act 1997. He asserted that:

> We should have one law in order to simplify everything. However, in Malaysia we tend to converge to other things. It is weird; we have to look at other acts.[169]

The proposed offence would provide clarity especially with regard to the elements of crimes for a large-scale cyber attacks. According to Police Officer 2:

> In U.S, there are a lot of Acts for cyber. They do not contain many sections, but they are specific. In comparison, the legislation in Malaysia is drafted in broader and general terms. This allows us more leeway to interpret the laws. We can arrest the offenders and prevent the commission of crimes. We can open more cases. However, the drawback is in terms of the burden of proof. It is easier to prove the intention for specific offences. If he commits A, then we have to prove A. But, this is difficult for general offences. The Penal Code covers traditional crimes including cybercrimes, but with traditional element.[170]

Therefore, the proposed offence would provide for the degree of culpability and harm for a large-scale cyber attacks. This is necessary for the purpose discharging burden of proof and disclosure of evidence.

---

[168] Interview with Deputy Public Prosecutor 2

[169] Interview with Deputy Public Prosecutor 2

[170] Interview with Police Officer 2

Some of the interviewees from other categories acknowledged that the creation of a specific offence for serious cyber attacks is necessary for punitive purposes. According to Private Sector Officer 1:

> Specific offence is necessary to penalise the people who causes financial loss or disrupts the power plants and critical websites. However, I don't think it is required for defacing the websites of mudah.com.my and stealing information. This act is covered by the PDPA.[171]

Similarly, Security Professional 9 argued that:

> The unauthorised access to the computer system of the airport to cause flight delay perhaps is not covered under the Computer Crimes Act. Maybe, we have to look at other legislation. I think the prosecution is hesitant to charge the offender under the Computer Crimes Act because the forensic evidence is very fragile and difficult to prove. The success of the prosecution is low. However, we can propose the offence of the attack on critical infrastructure on the basis of its impact to the national interest. It is different from ordinary computer crimes. CNI is a critical subject; we frequently conduct drills with regards to the CNI.[172]

The proposed offence is necessary, as large-scale cyber attacks do not fit comfortably under the current legislation. Security Professional 11 noted that the creation of a new offence for cyber attacks against the critical national infrastructure may also be done for deterrence purposes:

> I am not sure how to comment about the CNI because currently, we are living in peaceful time. If there is a crisis looming; go ahead. However, I think that we should look at the intent, case-by-case basis; what you are doing is illegal. You have no business to access into the system; to do the illegal act. However, if your system is there; I can get into it; your

[171] Interview with Private Sector Officer 1

[172] Interview with Security Professional 9

> system is going to entice a lot of people. If you decide to connect the system to the Internet, it is your job to be proactive first. If you say that the law and prosecution is one of the mechanisms to deter people, you can go ahead.[173]

On the other hand, Police Officer 3 emphasised that this proposal may affect the law enforcement officers particularly in terms of their expertise. He asserted that:

> It is good to have this offence in our country. However, the enforcement agency including the police and the prosecution need to be equipped with the knowledge. Specific offences such as attack on CNI require more details and technical expertise. You need to know about the capability of the investigation officer and the prosecutor before you amend the Computer Crimes Act. The investigation department may not possess the knowledge about critical infrastructure, the intrusion detection or the disaster recovery plan. This information has to be understood by the IO and PO.[174]

Accordingly, the findings of this study suggest that the introduction of specific offence in relation to serious cyber attacks into the Computer Crimes Act 1997 may strengthen the application of criminal law in dealing with cyber attacks in Malaysia. The proposed offence is needed for several reasons. Firstly, the punishment provided under the Malaysia's Computer Crime Act 1997 is not adequate for a large-scale cyber attacks. The proposed offence provides for the appropriate punishment for the perpetrator of cyber attacks. Secondly, current legislation especially the Computer Crimes Act 1997 does not cater for a large-scale cyber attacks. Thirdly, the proposed offence clarifies the ingredients for the purpose of criminalisation of a large-scale cyber attacks. Finally, the proposed offence may be useful as a preventive measure in order to deter the commission of cyber attacks especially against critical national infrastructure.

---

[173] Interview with Security Professional 11

[174] Interview with Police Officer 3

Despite being a realistic threat, no spectacular disruption of service or serious damage to the critical national infrastructure caused by cyber attacks has been reported so far. The usage of the information infrastructures owned by the government and private entities by the public has not been eroded despite of the constant DDOS attacks.[175] Nevertheless, this offence is necessary as critical national infrastructures are essential especially for national security. The preservation of national security is vital for individual welfare and the community interests.[176] The next section investigates the degree of harm and culpability for this offence.

5.3.1.1 Physical Elements and Degree of Harm

S 3ZA (1) of the Computer Misuse Act 1990 provides that a person is guilty of an offence if he does any unauthorised act (including a series of acts) in relation to a computer which causes or creates a significant risk of and serious material damage in any place to: human welfare, the environment, the economy and national security.[177] The damage may be caused by an indirect act or the act needs not have to be the main cause of the damage.[178] The damage to human welfare is limited to: loss of human life; human illness or injury; disruption of a supply of money, food, water, energy or fuel; disruption of a system of communication; disruption of facilities for transport; or disruption of services relating to health.[179] The offence places great emphasis on the gravity of the cyber attacks. This is reflected in the imposition of heavier sentence. The offender is liable for imprisonment for a term not exceeding 14 years or to a fine or to both.[180] He is also liable for imprisonment for life or to a fine or both if the act causes serious damage to human welfare or national security.[181]

---

[175] Grant J, 'Will There Be Cybersecurity Legislation?' 4 J. Nat'l Sec. L.& Policy 103 2010

[176] Baker DJ, *The Right Not to be Criminalized* (Ashgate, 2011) 92

[177] S 3ZA (2) of the Computer Misuse Act 1990

[178] S 3ZA (4) of the Computer Misuse Act 1990

[179] S 3ZA (3) of the Computer Misuse Act 1990

[180] S 3ZA (6) of the Computer Misuse Act 1990

[181] S 3ZA (7) of the Computer Misuse Act 1990

As indicated in the preceding paragraph, the proposed offence requires the accused to have committed an unauthorised act to the computer.[182] The economy, environment, national security or human welfare are significantly damaged or at risk as a result of the unauthorised act.[183] Accordingly, the notion of harm for cyber attacks is wider than traditional criminal offences due to the potential damage caused by the attacks. Cyber attacks may be carried out remotely by using computer networks to destroy or manipulate the computer system of the critical national infrastructure. This may result in the destruction or disruption of facilities connected and controlled by computerised system such as health system or power plants. Any human casualties or economic loss caused by such attacks may be considered as indirect physical harm. Several questions arise pertaining to the extent of the damage for this offence. How do we determine the threat or harm to human welfare, economy and the national security? Can the disruption of lifestyle and erosion of public confidence be considered as harm? Should the impact of harm be felt immediately?

This study has noted the distinction between the nature of harm for the commission of unauthorised acts causing, or creating risk of, serious damage under S 3ZA of the Computer Misuse Act 1990 and the seriousness of harm for sentencing. Legal Practitioner 3 argued that:

> I don't think it matters if you attack one computer or hundreds of computers. Let's say, I choose to attack one computer. The computer may be essential to the operation of the entire bank. I don't think it is suitable factor to look at especially in determining the application of legislation. Is the scale of attack relevant? I think what amounts to an offence and what qualifies based on the scale of the attack are two different questions. If you are talking about the inconsequential impact of the commission of the offence; that relates to sentencing. Why full sentencing should be imposed on me? I am sure the magistrate will take that into account. The scale of harm is a matter for

[182] Home Office, 'Home Office Circular Serious Crime Act 2015' (Home Office, 2015)

[183] ibid

> sentencing. The seriousness of the offence depends on the infrastructure especially if it involves key infrastructure.[184]

This section focuses on the nature of harm for cyber attacks. This study shall return back to the role of sentencing in the next section and when it discusses the implementation of criminal law measures in Malaysia.

The severity of harm is important in order to justify state coercion. Greenfield and Paoli divide the severity of harms into five categories: catastrophic, grave, serious, moderate and marginal. [185] Death is categorised as catastrophic harm, whereas assault is rated as serious if the victim suffered serious injuries. [186] The categories of harms suggested by Greenfield and Paoli can be used to identify harms associated with a large scale cyber attacks. The attacks on the CNII may be classified as catastrophic. This situation necessitates a range of criminal law measures including executive order. However, Greenfield and Paoli acknowledge that the decision to label something as harm depends on a society's culture and socio-economic arrangements.[187] Accordingly, the role of the legislature is to identify the degree of harm in promulgating prohibitory legislation. According to Feinberg:

> The legislatures have to consider various factors including 'minor harms, moderately probable harms, reasonable and unreasonable risk of harm, aggregative harms, harms to some interests preventable only at the cost of harms to other interests irreconcilable with them, structured comparative harms, accumulative harm, imitative harms and so on.[188]

As stated in the previous chapter, Malaysia is not totally a liberal country as economic growth, political stability and national security have preceded

---

[184] Interview with Legal Practitioner 3

[185] Greenfield VA and Paoli L, 'A Framework to Access the Harms of Crimes' (2013) Br J Criminal (2013) 53 (5): 864-885 doi: 101093/bjc/azt018

[186] ibid

[187] ibid

[188] Feinberg J, *Harm to Others. The Moral Limits of the Criminal Law*, vol one (Oxford University Press 1984) 187

individual liberty. Consequently, there is a potential need for legislation if the facts warrant it.

The findings of this study suggest that harm caused by a large-scale cyber attacks may take various forms including financial implication and loss of reputation. According to Policymaker 3, the attacks on the Tenaga Nasional Berhad's electrical grid may cause the loss of a huge amount of money.[189] Similarly, Security Professional 8 asserted that the attack is serious when it involves loss of money, integrity and image.[190] Private Sector Officer 2 argued that web defacement might affect the user's reputation, business and income even though there is no physical damage to the users.[191] Other participants perceived cyber attacks as serious if they disrupt the harmony of the country, affect the community, and destabilise the politic and economy.[192] According to Policymaker 4:

> If the system of the critical infrastructure collapsed, it affects the country. It will create chaos. The people can go to the street to demonstrate. Stealing your information is cyber attacks. However, it doesn't affect national security. It only affects you as an individual or your company. The attacks against individual and company are still cyber attacks. However, damaging the CNI and objects critical to the economy are attacks against the country.[193]

Apart from that, the impact of the potential attack is also significant. According to Police Officer 3:

> Cyber attacks on the airport are related to national security. I would not classify the case under s 4 of the CCA. The attacks cause the entire airport collapse. The airlines such as MALINDO can sue the data centre for millions of ringgit. I cannot charge the perpetrator for offences in which the penalty

[189] Interview with Policymaker 3

[190] Interview with Security Professional 8

[191] Interview with Private Officer 2

[192] Interview with Security Professional 2

[193] Interview with Policymaker 4

> is RM5000. SOSMA may be invoked as the Act covers any acts that jeopardise the security of the country. The impact on the country is huge.[194]

Military Officer 1 divided potential attacks into several levels.

> The threat level is low if there is no unusual activity or beyond the normal concerns of cyber threats with insignificant impact to the MAF (Malaysian Armed Force). The threat is moderate if cyber threats exist or known exploits have been identified and has resulted minor impact to the MAF. Threat level caution is when there is detection of cyber incidents with potential of significant damage or disruption of MAF critical operation and has resulted moderate impact to the MAF. Threat level high is when exploitation created by cyber incident has impacted a wide spread level of damage or disruption of MAF critical operation and has resulted in major impact to the nation. Lastly, threat level critical happens when exploitation created by cyber incident has resulted critical impact to MAF critical operation and national cyber crisis has to be declared.[195]

This classification may assist in determining the level of harm anticipated for large-scale cyber attacks. Threat level high and threat level critical would constitute an offence of serious cyber attacks.

The finding of this study demonstrates that a serious cyber attacks can affect the public at large instead of a particular individual or entity. Apart from national security, the data revealed that the notion of harm for the proposed offence in Malaysia includes not only material harm or physical harm but also integrity and reputation. Most of the participants from all categories perceived the loss of reputation and integrity as serious. They also viewed that a large-scale cyber attacks would have grave repercussions to the economy of the country.

---

[194] Interview with Police Officer 3

[195] Interview with Military Officer 1

The extent of the economic and financial harm may be further elucidated by the Huntingdon Life Sciences cases. A group of activists known as Stop Huntingdon Animal Cruelty (SHAC) continuously disrupted the operation of a company and the life of its workers for several years.[196] In some instances, they deliberately took the workers' photographs and threatened to expose them to the public. [197] In *Halan Laboratories UK Ltd v SHAC*, the court held that SHAC was a vehicle used to terrorise ordinary traders engaging in lawful transactions.[198] One of the protestor, Deborah Vincent was convicted on 19.03.2014 for blackmailing the employees of the company through a campaign of terror involving improvised explosive and desecration of graves.[199] She is currently serving six years imprisonment.

Even though, Huntingdon Life Sciences is a small pharmaceutical company, this case garnered the attention of the public and government for symbolic reasons such as denunciation of illegal activities on the Internet. Several drugs company threatened to relocate their business outside of UK unless something is done to stop the activists in the form of new law.[200] The campaign spread for more than six years targeting individuals who are connected to the company including delivery vans. The police spent £3.5 million to conduct investigations to apprehend the mastermind of the campaign for duration of 2 years. The campaign has systematically carried out involving threats of violence, slanderous remarks and terrorising attacks.[201] The company suffered economic loss due to the refusal of banks

---

[196] The Guardian, 'Animal Rights Activist Jailed for Six Years For Huntington Life Sciences Plot' (*The Guardian*, 17.04.2014) <http://www.theguardian.com/uk-news/2014/apr/17/animal-rights-activist-jailed-six-years-huntington-life-sciences-debbie-vincent> accessed 5.10.2014

[197] ibid

[198] [2012] EWHC 3408 QB

[199] The Guardian, 'Animal Rights Activist Jailed for Six Years For Huntington Life Sciences Plot' (*The Guardian*, 17.04.2014) <http://www.theguardian.com/uk-news/2014/apr/17/animal-rights-activist-jailed-six-years-huntington-life-sciences-debbie-vincent> accessed 5.10.2014

[200] Laville S, 'From a Hampshire Cottage, Animal Extremists Plotted Campaign of Violence' (*The Guardian*, 23.12.2008) <http://www.theguardian.com/uk/2008/dec/23/ukcrime-animalwelfare> accessed 5.10.2014

[201] ibid

and insurance company to provide their services. It was forced to move its listing to New York as a result of continuous blackmail. Nevertheless, the company managed to obtain injunctions against the animal rights activist in several civil actions.[202] The economic impact illustrated in these incidents may be used as a reference for the nature of harm anticipated by s 3ZA of the Computer Misuse Act 1990.

On the whole, s 3ZA of the Computer Misuse Act 1990 was enacted in order to impose stiff punishment to individuals who uses the computer system to cause serious damage to human welfare, the environment, the economy and national security. This study investigates the nature of cyber attacks envisaged in section 3ZA of the Computer Misuse Act 1990. The findings suggest that this provision may be invoked not only against attacks on critical national infrastructure but other situations based on the *Huntingdon Life Sciences* cases. Some of the participants in this study argued that serious damage to human welfare includes not only physical harm but also damage to reputation, integrity and the economy of the country. Furthermore, the UK"s Law Commission suggests that this provision should be used against cyber espionage.[203] This provision may be inserted in the Penal Code or Computer Crimes Act 1997.

5.3.1.2 Fault Elements

The required mental element for the proposed offence would be divided into two parts. [204] Firstly, the accused must know that he is committing unauthorised act in relation to a computer. Secondly, he must intend to cause the harm or has been reckless as to whether such damage is caused.[205] With regard to the second part, the intention of the accused may be inferred from: the nature of the cyber weapon used; the place where the damage was inflicted; the nature of the damages caused and the

---

[202] ibid

[203] Law Commission, 'Protection of Official Data: A Consultation Paper Law' (Com No 230, 2017) para 2.7

[204] S 3ZA (1) of the Computer Misuse Act 1990

[205] Home Office, 'Home Office Circular Serious Crime Act 2015' (Home Office, 2015)

opportunity, which the accused gets.[206] The accused consciously shapes his conduct in order to bring about a certain event.[207] In contrast to recklessness, intention requires that the accused must have desired the commission of the offence.[208] It is noted that cyber attacks are premeditated almost all the time, as it requires extensive planning and technical expertise.[209] Most cyber criminals do not think that they can be caught easily.[210]

Besides intention, the proposed offence may be committed when the accused has been reckless. This could be satisfied by the 'subjective mental state of knowledge of a risk, or the objective standard of a failure to recognise an obvious risk'.[211] Recklessness is similar to rashness under the Malaysian Penal Code as they involve purely subjective mental states in which the accused knew of the possibility of harm happening.[212] Therefore, the accused may not have known that the cyber attack was likely to cause the damage as required under s 3ZA (1) of the Computer Misuse Act 1990, however there should be sufficient evidence that he knew of the probability of it causing the damage. This mental element may be extended to 'script kiddies' and hackers who commit cyber attack on the critical national infrastructure in order to test their skills. Private Sector Officer 1 argued that:

> Cyber attacks may be committed by the people who wanted to know about your weaknesses. They try to get the information from your workplace. It can become cyber crimes depending on the gravity of the attacks. The act may be done merely to test their skills; this is cyber attack but without the intention to commit crimes. For instance the script kiddies, they

---

[206] Fook LC, Hassan CA and Bajury MSHM, *Introduction to Principles and Liabilities in Criminal Law* (2nd edn, LexisNexis 2012) 145

[207] ibid 146

[208] *Yap Sing Hock v PP* [1992] 2 MLJ 714

[209] Interview with Security Professional 11

[210] Interview with Deputy Public Prosecutor 1

[211] Yeo S, Morgan N and Cheong CW, *Criminal Law in Malaysia and Singapore* (2nd edn, LexisNexis 2012) 102

[212] ibid 102

> downloaded tools from the network. They are in their high school years; they just want to test their skills and not to commit crime. They don't know the consequences such as to bring the company down financially.[213]

Similarly, Deputy Public Prosecutor 1 asserted that:

> I don't consider testing their skills as a crime. They merely disrupt the operation of the organisation. They just want to express their dissatisfaction. However, they have committed crimes if there is monetary damage. I think not all cyber attacks should be considered as crimes.[214]

According to Deputy Public Prosecutor 1:

> Let say, a minor playing with his computer and recklessly access government's website without authorisation. The Attorney General's Chamber has the discretion to charge him for committing an offence. However, we have to look at the evidence, the circumstances and the public interest.[215]

Therefore, 'script kiddies' and hackers who disrupt the computer system of critical national infrastructure may be prosecuted for committing serious cyber attacks. Although the attacks were done simply for gaining notoriety; they can still cause serious disruptive impact.[216] They may claim that the acts are done without the intention to cause harm. They have been reckless as it is known that attacking critical national infrastructure might harm human welfare, economy and national security.

5.3.2 Precursor Offences

The main objective of preventive legislation is to intervene and disrupt the preparatory acts before the commission of the crime. Preparatory offences, crime of possession and crime of membership are the examples of precursor

---

[213] Interview with Private Sector Officer 1

[214] Interview with Private Sector Officer 3

[215] Interview with Deputy Public Prosecutor 1

[216] Weimann G, 'Cyberterrorism: The Sum of All Fears? (n 152)

offences.[217] For instance, the UK's Terrorism Act 2006 criminalises the publication of statement to encourage terrorism and the dissemination of terrorist publications.[218] In Malaysia, among the offences that fall under this category is the possession of corrosive or explosive weapon and possession of arms and ammunition for unlawful purpose.[219] The Malaysia's Penal Code also provides for precursor offences such as the dissemination of information by electronic means to incite violence, disobedience to the law or any lawful order.[220] It also criminalises the membership of an organised criminal group.[221] In addition, the Penal Code provides for precursor offences in relation to terrorism such as providing training and instruction to terrorist groups and persons and inciting, promoting and soliciting property for the commission of terrorist acts.[222]

The degree of culpability and the intended harm for precursor offences differs from the paradigm of harm plus culpability.[223] The prosecutors are not required to prove tangible harm as the preventive legislation allows the presumption of future harm in the form of damage or injury. For instance, s 5 of the UK Terrorism Act 2006 provides that a person commits acts of terrorism by carrying out the preparatory acts. In *R v Kahar*, the accused was convicted of engaging in conduct in preparation for giving effect to an intention to commit acts of terrorism.[224] He was sentenced to five years imprisonment. The court held that the culpability of the offender is measured by various factors including the commitment to carry out the act, and the harm depends on the impact of the intended acts on the victims and the

[217] Ashworth A and Zedner L, 'Prevention and Criminalization: Justifications and Limits' (n 5)

[218] S 1 and s 2 of the Terrorism Act 2006

[219] S 3 of the Corrosive and Explosive Substances and Offensive Weapons Act 1958 [Act 357]; S 33 Arms Act 1960

[220] S 124H of the Penal Code

[221] S 130V of the Penal Code

[222] S 130F of the Penal Code; s 130G of the Penal Code

[223] Ashworth A and Zedner L, 'Prevention and Criminalization: Justifications and Limits' (n 5)

[224] *R v Kahar* [2016] EWCA Crim 56

public.[225] Similarly, intention is required for the possession of offensive weapons under the UK Prevention of Crimes Act 1953. Any individual who possesses offensive weapons could be prosecuted even if they have not been used. The mischief is followed by risk of harm.

Culpability for precursor offences is determined by the offender's present attitude toward the prohibited harm, as suggested in his mens rea and the preliminary acts that he has done.[226] This may be problematic as 'the criminal law is primarily concerned with proven acts and not prevention of future behaviour'.[227] Mill's harm principle requires the existence of definite damage or risk to an individual or the public in order to justify legal intervention.[228] However, this principle does not indicate when liberty ought to be restricted or the extent to which liberty may be sacrificed in the name of preventing harm.[229] Feinberg argues that the harm principle is based on the empirical generalisations of the likelihood of the effects of various threatening actions.[230] Consequently, the legislature needs to assess the degree of risk based on the magnitude and probability of harm in order to justify preventive coercion.[231]

Magnitude and probability of harm depend on the direct effect of the wrongful conduct on the society at large. Feinberg asserts that in this situation, 'the scales will surely tilt sharps away from liberty'.[232] He further contends that 'the greater the social utility of the act or activity in question, the greater must be the risk of harm for its prohibition to be justified'.[233] For

---

[225] ibid para 26

[226] Alexander L and Kessler KD, 'Mens Rea and Inchoate Crimes' The Journal of Criminal Law and Criminology (1973-), Vol 87, No 4 (Summer,1997), pp 1138-1193

[227] Yeo S, Morgan N and Cheong CW, *Criminal Law in Malaysia and Singapore* (n 211) 47

[228] Mill JS, *Utilitarianism and the 1868 Speech on Capital Punishment* (Sher G ed, 2nd edn edn, Hackett Publishing Company 2001)

[229] Ashworth A and Zedner L, 'Prevention and Criminalization: Justifications and Limits' (n 5)

[230] Feinberg J, *Harm to Others. The Moral Limits of the Criminal Law* (n 188)

[231] ibid

[232] ibid 191

[233] ibid 191

instance, the penalties for criminal preparation may be less than criminal attempts because the former has lower degree of defendant's culpability and risk to the public.[234] This argument can be used to justify the need for precursor offences in relation to drugs trafficking and terrorism. Planning and preparation are required for the execution of these offences. It could be argued that the rate of death from terrorism is lower than murder. However, terrorism poses a wider risk to the society as it is done for public purposes such as destabilising the country and engendering hostility between different groups. Consequently, precursor offences enable the law enforcement officers to effectively intervene before the commission of terrorism.

In the light of these arguments, this study discusses the creation of precursor offences for cyber attacks. It suggests regulating the possession of materials and the creation, distribution and procurement of materials to commit cyber attacks in Malaysia. In the following sections, the rationale for the creation of theses offences will be discussed.

5.3.2.1 Regulating the Possession of Materials to Commit Cyber Attacks

The crime of possession could potentially be used as a measure to counter cyber attacks in Malaysia. Article 6(1)(b) of the Budapest Convention on Cybercrime 2001 (the Cybercrime Convention) provides for the criminalisation of possessing devices such as computer programme and code that may be used illegally: to access the computer system; to intercept non-public transmissions of computer data; and to interfere with the computer data and system. This includes virus programmes, which are designed to access, alter, destroy or interfere with the operation of the computer system.[235] Member states have the discretion to determine the number of devices, which is required for the purpose of establishing the criminal intent. [236]

---

[234] Editorial, 'The Law Commission and Inchoate Offences' Crim LR 2008, 1, 1-2

[235] Committee of the Ministers of the Council of Europe, 'Convention on Cybercrime: Explanatory Report' ((ETS No 185), 2001)

[236] Csonka P, 'The Council of Europe's Convention on Cyber Crime and Other European Initiatives' (n 31)

Apart from proving the general intention and possession without rights, the prosecution has to show the specific intention to use the devices to commit the offences provided in Articles 2 until 5 of the Cybercrime Convention. This is necessary in order to prevent over criminalisation where the devices are produced for lawful reasons.[237] The expression 'without rights' entails the exemption of legal devices such as tools created for testing or protection of the computer systems from this provision.[238] States are allowed to reserve the application of this provision in their domestic law.[239] This is due to the different assessments of the need to apply misuse of devices to the computer offences stipulated in the Convention.[240] The crime of possession is not expressly provided in Malaysia's Computer Crimes Act 1997. The Act indicates that the accused is presumed to have committed an unauthorised access if he has the custody or control of any computer program, data or information without authorization.[241] It is relevant to observe whether this measure should be implemented in Malaysia.

The results of the fieldwork revealed that more than half of the participants from all categories think that criminalising the possession of materials to commit cyber attacks would be effective. Deputy Prosecutor 1 considered this measure especially effective against young offenders. He claimed that:

> It would be quite helpful. I think this works against category of hackers called as script kiddies; the one who commits unauthorised access via the use of pre written script by more established hackers. [242]

Furthermore, the creation of possession offences may enhance the enforcement of the law in dealing with cyber attacks. According to Police Officer 2:

---

[237] Committee of the Ministers of the Council of Europe, 'Convention on Cybercrime: Explanatory Report' (n 235)

[238] Csonka P, 'The Council of Europe's Convention on Cyber Crime and Other European Initiatives' (n 31)

[239] Article 42 of the European Convention on Cybercrime 2001

[240] Committee of the Ministers of the Council of Europe, 'Convention on Cybercrime: Explanatory Report' (n 235)

[241] S 8 of the Computer Crimes Act 1997

[242] Interview with Deputy Public Prosecutor 1

> Let's say we discovered a laptop containing numerous malware. We cannot apprehend and charge the owner of the laptop especially if there is no victim or complainer. However, we can do that if there is a specific provision of the law criminalising the possession of article to commit crime.[243]

The main purpose of possession offences is preventive. However, the extent of harm to be prevented is not usually specified in the description of the offences.[244] Therefore, some of the interviewees emphasised the function and effect of the malware for criminalisation purposes.[245] Nevertheless, other interviewees claimed that a person should not be penalised for merely possessing malware without further intention to commit any wrongful act. For instance, Deputy Public Prosecutor 2 argued that:

> You can get malware for free from the Internet. How are you going to regulate this? This law is not effective in reality. The culprits are mostly teenagers. I don't find this measure is effective especially if they are not doing anything but possession of malware.[246]

Deputy Public prosecutor 5 asserted that:

> We are not allowed to have software used for hacking according to the Budapest Convention. The problem is that a lot of software nowadays is designed for privacy purposes. Some of them are effective against forensic. Criminals cover their tracks using these software. So, we have to be very careful before we introduce this offence. Some people might download these programmes for certain purposes, which are not illegal in nature. However, due to this provision, they have committed an

[243] Interview with Police Officer 2

[244] Ashworth A and Zedner L, *Preventive Justice* (Oxford University Press 2014) 100

[245] Interview with Police Officer 3

[246] Interview with Deputy Public Prosecutor 2

> offence, which carries penal punishment including imprisonment.[247]

Criminalising the possession of materials to commit cyber attacks may alleviate the possibility of attacks especially by young offenders. However, as indicated by Deputy Public Prosecutor 2, the requirement of specific intent to commit further offence is essential. Criminal liability should be imposed for crime of possession only if the person has declared his intention to do further acts.[248] Furthermore, the effectiveness of this measure depends on halting the production and distribution of the materials especially on the Internet. This issue is addressed in the next section.

5.3.2.2 Regulating the Creation, Distribution and Procurement of Materials to Commit Cyber Attacks

This section examines the application of the law to regulate the creation and distribution of materials to commit cyber attacks in Malaysia. It could be argued that the criminalisation of the creation of instrument to commit cyber attacks is necessary as malicious software such as Botnets are capable of launching large scale cyber attacks.[249] They may cause serious damage to critical infrastructures. Directive 2013/40/EU and the Cybercrime Convention impose obligation on member states to criminalise the production, sale, procurement for use, import and distribution of tools or devices such as computer programme or data with the intention to be used to commit illegal: access the computer system; intercept non-public transmissions of computer data; interfere with the computer data and system.[250] The Cybercrime Convention refers to distribution as 'an active act of forwarding data to others' and making available as 'placing online devices for the use of

[247] Interview with Deputy Public Prosecutor 5

[248] Ashworth A and Zedner L, *Preventive Justice* (n 244) 112

[249] Committee of the Ministers of the Council of Europe, 'Convention on Cybercrime: Explanatory Report' (n 235)

[250] Article 7 of Directive 2013/40/EU; Article 6(1)(a) of the European Convention on Cybercrime 2001

others'.[251] This includes the creation or compilation of hyperlinks enabling access to the devices.[252]

The creation, distribution or procurement of the tools or devices must be done in relation to future cyber attacks. This is necessary in order to protect human rights and to exclude pure researchers from the offence.[253] Security professional 11 argued that:

> To some extent, this regulation would hinder creativity especially in the creation of codes. The quality of codes is going to be different. There is a need for clear-cut prohibition. People need to know that they have committed an offence. This prohibition should not be extended to dual-purpose devices and techniques. Is malware bad? This is an intricate issue.[254]

The Cybercrime Convention does not expressly exclude dual-purpose devices, as it could lead to difficulties of proof in criminal proceedings and it will render the provision applicable only in rare situations.[255] Consequently, this provision is restricted to cases where the devices are designed, distributed and procured with the intention to commit further offence as indicated in the Convention.[256]

Pursuant to Directive 2013/40/EU, the UK has enacted the Serious Crime Act 2015 to prevent individuals from obtaining tools such as malware for personal use with the intention to commit a cybercrime.[257] The Act also

---

[251] Committee of the Ministers of the Council of Europe, 'Convention on Cybercrime: Explanatory Report' (n 235)

[252] ibid

[253] Jougleux P and Synodinou T-E, 'Prevention of Cyber Attacks' in Iglezakis I (ed), *The Legal Regulation of Cyber Attacks* (Kluewer Law International BV, The Netherlands 2016) 104

[254] Interview with Security Professional 11

[255] Csonka P, 'The Council of Europe's Convention on Cyber Crime and Other European Initiatives' (n 31)

[256] Committee of the Ministers of the Council of Europe, 'Convention on Cybercrime: Explanatory Report' (n 235)

[257] Home Office and Ministry of Justice, 'Impact Assessment: Serious Crime Bill: Amendments to Computer Misuse Act 1990' 2014 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317527/2014-06-03_signed_IA_CMA_EU_Directive.pdf> accessed 25 February 2017; S 42 of the UK's Serious Crimes Act 2015

empowers UK law enforcement agencies to initiate action against UK citizens who commit cybercrimes whilst physically outside of UK on the basis of their nationality.[258] S 3A of the Uk's Computer Misuse Act 1990 provides that a person is guilty of an offence if he makes, supply or obtain any articles including any programme or data held in electronic form to be used or likely to be used in the commission of an offence under section 1, 3 or 3ZA. This provision enables the police to intervene before the occurrence of an attack, when the offender has procured the malware for their personal use.[259]

So far, it could be argued that the law in Malaysia does not cover the offences in relation to the production, sale, procurement, import and distribution of tools to commit cybercrime. S 240 of the Communications and Multimedia Act 1998 criminalises the distribution of devices including electronic or mechanical equipment used for the purpose of surreptitious interception of communications via mail or transported in national or international commerce. It seems that this provision does not include the distribution of computer programme and code especially through the Internet. Police officer 3 asserted that the spread of malware fell within the ambit of the Computer Crimes Act 1997:

> I think we already have such offence. We charge the person who spread the malware when they plant it in the computer. This amounts to unauthorised access with modification. However, specific offence for spreading is absent. But, we can classify the act as improper use of network or unauthorised access. Spreading and planting the malware may be considered as harming the computer.[260]

It appears that Police Officer 3 acknowledged the absence of the law regulating the distribution of malware in Malaysia. The transmission of malware may be classified as illegal system interference.[261] However, the

---

[258] ibid, S 43 of the UK's Serious Crimes Act 2015

[259] Home Office and Ministry of Justice, 'Impact Assessment: Serious Crime Bill: Amendments to Computer Misuse Act 1990' (n 257)

[260] Interview with Police Officer 3

[261] Jougleux P and Synodinou T-E, 'Prevention of Cyber Attacks' in Iglezakis I (ed), *The Legal Regulation of Cyber Attacks* (n 253) 104

creation of a virus and distribution of a virus tool kit should be distinguished from a mere transmission. It does not fall within the ambit of the Computer Crimes Act 1997. In the following paragraph, the need for the state to legislate for this offence will be discussed.

The findings of this study indicate that more than half of the participants from all categories agreed that the creation of offences to regulate the production and distribution of tools to commit cyber attacks would be effective. Security Professional 10 supported the implementation of this measure. He said that:

> This should be criminalised in Malaysia. There is a company in Bandar Sunway selling malware especially for interception. The company also sells spy cams. Most of these devices are used for private investigation. The company charges RM 9000 for installing malware on smartphones. I know a VIP who bought a phone infected with malware for his seconder from this company. He could find out anything done by his seconder. I can bring you there. It depends on the scenario. May be the company cannot be charged because we don't have this offence in Malaysia.[262]

Therefore, the prohibition is needed in order to disrupt the operation of black market in the production and distribution of hacker tools.[263] It also deters the growth of a black market in information including pin numbers of credit card; passwords to access online streaming services and email; and technical data.[264] According to Security Professional 11:

> There is always demand for malware in the black market. I can sell the information on ways to hack Windows to legal or illegal brokers. They will supply the information to anti virus companies. The anti virus companies will build the signature to counter this issue. This is how anti virus such as IDS is

---

[262] Interview with Security Professional 10

[263] Csonka P, 'The Council of Europe's Convention on Cyber Crime and Other European Initiatives' (n 31)

[264] Jougleux P and Synodinou T-E, 'Prevention of Cyber Attacks' in Iglezakis I (ed), *The Legal Regulation of Cyber Attacks* (n 253) 106

> produced and protected the user signature. The legitimate broker usually offers less than the black market. I can sell the way to exploit Windows to legal broker for 30 000 USD. But, I can sell it to the black market for 50 000 USD. It is purported that stuxnet would cost 200 000 USD in the black market.[265]

The security community and underground malicious hackers develop tools for the purpose of identifying and exploiting flaws in software.[266] Study shows that hackers are buying and selling devices to commit attacks or acquiring information through a compromise.[267] The markets for cybercrime tools and stolen data have become more accessible and lucrative. Transactions can be done using online stores, bulletin-board-style web forums, email or instant messaging platforms.[268] Some of the web-hosting providers revealed that their servers are located in Malaysia and other parts of Asia.[269] Therefore, criminalisation of the distribution and procurement of tools to commit cybercrime in Malaysia is highly recommended. This may alleviate the creation of safe havens for malware writes and hackers where they appear to have impunity from arrest.

However, other participants were sceptical about the effectiveness of this measure due to several reasons. One reason why this measure may not work is the fact that most offenders do not create the tools to commit cyber attacks. According to Police Officer 2:

> We have many experienced hackers in Malaysia. Once they reach certain level, they no longer do this. However, those who lack skills cause the problems. But, they don't create their own script. They use custom-made malware. I don't think we need to

---

[265] Interview with Security Professional 11

[266] Holt TJ, 'Examining the Forces Shaping Cybercrime Markets Online' Social Science Computer Review 31(2) 165-177

[267] ibid

[268] Ablon L and Libicki M, 'Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data' Defense Counsel Journal; Apr 2015; 82,2; ABI/INFORM Collection pg 143

[269] Chu B, Holt TJ and Ahn GJ, 'Examining the Creation, Distribution, and Function of Malware On-Line: Executive Summary' NCJRS <https://www.ncjrs.gov/pdffiles1/nij/grants/230112.pdf> accessed 12 November 2016

> have this offence. So far, we don't have situations involving the distribution of malware outside of Malaysia. We don't even have many incidents involving unauthorised access. But, I admit that Computer Crimes Act is not adequate in dealing with this matter.[270]

Some of the participants argued that the enforcement of this offence is challenging due to the complexity of cyber attacks and the difficulty in identifying the creator of the malware. Security Professional 8 claimed that:

> Malware attacks are complex. It takes more than a couple of weeks to trace the creator. There is a doubt about the practicality of the enforcement.[271]

Security Professional 5 also shared a similar view. He argued that:

> It is hard to find the creator of the malware. We know the behaviour of the malware in order to prevent it from affecting the system. But, we don't know who creates it and how he creates it. Perhaps the malware is created by the anti virus company.[272]

Furthermore, the distributor of the malware may feign ignorance of the final purpose of the tools in order to escape from liability.[273] This may impair the effectiveness of the offence. According to the Deputy Public Prosecutor 5:

> Another problem is the offenders may use the defence that they do not know it is wrong. We looked at the offences under the Budapest Convention. A lot of the offences catch hold of the people who lack awareness; they can say 'we do not know this is wrong'.[274]

---

[270] Interview with Police Officer 2

[271] Interview with Security Professional 8

[272] Interview with Security Professional 5

[273] Jougleux P and Synodinou T-E, 'Prevention of Cyber Attacks' in Iglezakis I (ed), *The Legal Regulation of Cyber Attacks* (n 253) 106

[274] Interview with Deputy Public Prosecutor 5

Policymaker 4 expressed his concern about the lack of knowledge of the Internet users especially the home users. He said that:

> We can have the law but how do we enforce it? If you are a home user and your computer has been affected by virus. Most probably you don't know or aware that the malware is using your computer as a launching pad to attack other computer system. We are facing this problem, for instance, we have a project with an industry in relation to home users who are not aware that their computers have been infected with malware. They may unintentionally distribute the malware.[275]

On balance, regulating the creation and distribution of materials to counter cyber attacks may not completely reduce the commission of cyber attacks. There is strong possibility that the enforcement of the law in this area would be problematic. Furthermore, law enforcement may not reduce the size of cyber black markets, as they are incredibly resilient.[276] Yet, this study suggests that there is a need to broaden the scope of S 240 of the Communications and Multimedia Act 1998 in order to include spyware and online distribution.

5.3.3 Executive Order

This section examines the potential usage of executive order against the perpetrators of cyber attacks in Malaysia. The aim of executive orders is to 'prevent, disrupt and counter' threats associated with serious crimes especially terrorism but with more limited proof or procedure than criminal justice systems.[277] The paramount duty of the government is to avert threat before it becomes worse.[278] The threats to security in Malaysia are mainly derived from domestic sources.[279] Racial tensions, extremism, corruption,

---

[275] Interview with Policymaker 4

[276] Ablon L and Libicki M, 'Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data' Defense Counsel Journal (n 268) 143

[277] Walker C, *Blackstone's Guide to the Anti-Terrorism Legislation* (Oxford University Press 2009) 212

[278] Kamarudin ARB, 'The Relevancy of Preventive Detention in Malaysia' (2005) 6 MLJ xcvii

[279] Abdullah KB, 'Emerging Threats to Malaysia's National Security' (2010) 5 Journal of Policing, Intelligence and Counter Terrorism 55

territorial integrity and cyber security are the utmost concerns of the government of Malaysia. Preventive legislation such as the Internal Security Act 1960 was used to counter any acts that were deemed to be prejudicial to the security of Malaysia.

The Internal Security Act 1960 has been replaced by the Security Offences (Special Measures) Act 2012,[280] which requires the accused to be tried by the High Court of Malaysia for committing security related offences and terrorism as specified under the Penal Code.[281] In addition, the Restricted Residence Act 1933 and Banishment Act 1959 were repealed in 2011. However, executive orders remain prevalent in Malaysia and UK especially in relation to terrorism, organised crime and drug trafficking. The Malaysian Parliament adopted the Prevention of Terrorism Act 2015 and the Special Measures Against Terrorism in Foreign Countries Act 2015.[282] The Prevention of Terrorism Board may order the detention of a person who has been engaged in the act of terrorism for up to two years.[283] The Malaysia's Prevention of Crime Act 1959 had been amended in 2015 to provide for the detention of undesirable persons including members of unlawful societies, smugglers of migrant, traffickers in person and persons who engage in the commission or support of terrorists acts.[284] The Prevention of Crime Board may direct the undesirable persons to be registered in the interest of public order or security.[285] Upon registration, the police will supervise them for a period not exceeding five years.[286]In addition, the Board may order them to be detained for a period not exceeding two years.[287] The Act restricts the

[280] This Act came into effect on 22 June 2012

[281] Offences against the State under Chapter VI of the Penal Code and Terrorism Offences under Chapter VIA of the Penal Code

[282] Sivanandram H, Keng YM and Carvalho M, 'Prevention of Terrorism, Special Measures Against Terrorism Bills tabled for First Reading' *The Star Online* (30.03.2015) <http://www.thestar.com.my/News/Nation/2015/03/30/POTA-Bill-tabled-first-reading/> accessed 19.06.2015

[283] S 13 (1) of the Prevention of Terrorism Act 2015

[284] S 12 and s 19A of the Prevention of Crime Act 1959 [Act 297]

[285] S 12 of the Prevention of Crime Act 1959

[286] S 15(1) of the Prevention of Crime Act 1959

[287] S 19A of the Prevention of Crime Act 1959

resort to judicial review to challenge decision made by the Board except in regard to compliance with any procedural requirement. [288]

In UK, Home Secretary may restrict the right of individuals who are suspected of involvement in terrorism in order to protect the public.[289] This includes requiring them to reside at a specified resident within a certain period of time and restricting them from leaving or travelling outside a specified area.[290] A notice under the Terrorism Prevention and Investigation Measures Act 2011 is in force for the period of one year and may be extended for another one year. The court is vested with the power to assess the decision to impose the measures on the individual.[291] The assessment is made based on the principles applicable for judicial review.[292]

Besides terrorism and organised crime, executive orders are also applied in other areas such as drug trafficking in Malaysia. The misuse of drug and trafficking of heroin are the main concerns among Malaysian.[293] Trafficking in dangerous drug is punishable with death penalty in Malaysia.[294] So, the Minister of Home Affairs may direct a person who is involved in trafficking dangerous drugs to be detained for a period not exceeding two years in order to protect the public.[295] The power to order the detention is different from the standard used to prosecute the drug trafficker in a court of law. The order can be issued even though the evidence is insufficient to initiate the case in court.[296]

In this study, the participants were asked to rate the effectiveness and fairness of executive orders such as detention with no access to computers

---

[288] S 15A of the Prevention of Crime Act 1959

[289] S 4 of the Terrorism Prevention and Investigation Measures Act 2011

[290] Schedule 1 of the Terrorism Prevention and Investigation Measures Act 2011

[291] S 6 (3) of the Terrorism Prevention and Investigation Measures Act 2011

[292] S 6 (6) of the Terrorism Prevention and Investigation Measures Act 2011

[293] Reid G, Kamarulzaman A and Sran SK, 'Malaysia and Harm Reduction: The Challenges and Responses' The International Journal on Drug Policy April 2007

[294] S 39B of the Dangerous Drugs Act 1952 [Act 234]

[295] S 6(1) of the Malaysian Dangerous Drugs (Special Preventive Measures) Act 1985

[296] Yeo S, Morgan N and Cheong CW, *Criminal Law in Malaysia and Singapore* (n211) 50-51

and the Internet. So far, the orders have not been issued against the perpetrators of cyber attack.[297] Deputy Public Prosecutor 3 argued that Prevention of Crime Act 1959 potentially could be invoked in this situation:

> Previously, we had ISA; it is a very powerful legislation. Now we have the preventive law, which provides for detention of certain groups that were involved in any activities that threatened the public order and public utility. They could be involved in several incidents. Instead of focusing on one incident, we can detain them without trial. This law can be invoked against any person who attacks the computer system, which cause harm to public security and order. Instead of charging him under the Computer Crimes Act or the Penal Code, we can detain him under the preventive law.[298]

Private Sector Officer 4 thought this measure might prevent cyber attacks. She asserted that:

> The suspects should be denied the access to any technology. They are capable of doing anything using their computer or telephone. I am just an ordinary IT Engineer, but I can access the server using my phone.[299]

Similarly, Deputy Public Prosecutor 1 agreed that this measure might be implemented in Malaysia. However, he was concerned about the repercussion of this measure especially on fundamental liberties. According to Deputy Public Prosecutor 1:

> This measure may well discourage the perpetrators. I am not sure whether it can be done in Malaysia especially under Security Offences (Special Measures) Act 2012. For instance, in the Adam Adli's case, he was charged with publishing seditious comment. One of the conditions of his bail is he cannot publish anything else. However, to restrict his access to computer or Internet might raise constitutional question of

[297] Interview with Police Officer 3

[298] Interview with Deputy Public Prosecutor 3

[299] Interview with Private Sector Officer 4

> freedom of movement. This measure has not been fully explored yet. [300]

Human rights implications must be taken into consideration in the administration of justice especially in the areas of criminal procedure. The Human Rights Commission of Malaysia has highlighted the inconsistency of some of the provisions of the Prevention of Crime Act 1959 with fundamental human rights stated in the Federal Constitution and Universal Declaration of Human Rights. [301] The Malaysian Bar has called for the Prevention of Terrorism Act 2015 to be revoked due to the potential abuse by the authorities. [302] In addition, legal practitioners have raised several issues concerning the provisions of the Security Offences (Special Measures) Act 2012. For instance, the Malaysian Bar has expressed its concern over the ouster of the jurisdiction of the court in the production of relevant evidence containing sensitive information certified by the Minister as prejudicial to the national security or national interest.[303] The interference of the Executive during the course of trial is considered as infringing the doctrine of separation of power.[304] Another issue that has been raised by the Malaysian Bar is the admissibility of evidence of protected witness without the presence of the accused during trial.[305]

Some scholars object to the severe deprivation of rights by the state without proof of intent to harm in committing an offence.[306] Preventive, civil and

---

[300] Interview with Deputy Public Prosecutor 1

[301] 'Annual Report 2015 Human Rights Commission of Malaysia' (*Human Rights Commission of Malaysia*) <https://drive.google.com/file/d/0B_iu0JnQlclBQW5OZTRhTF9XTnc/view?pref=2&pli=1> accessed 7 February 2017

[302] Sivalingam J, 'Bar Begins Campaign to Repeal Anti-Terror Law' (*The Malaysian Bar*, 16.05.2015) <http://www.malaysianbar.org.my/legal/general_news/bar_begins_campaign_to_repeal_anti_terror_law.html> accessed 19.05.2015

[303] Leong C, 'Speech by Christopher Leong, President of the Malaysian Bar at the Opening of the Legal Year 2014' (2014) 1 [2014] 1 MLJ

[304] ibid

[305] ibid

[306] Ashworth A and Zedner L, 'Defending the Criminal Law: Reflections on the Changing Character of Crime, Procedure and Sanctions.' (2008) 2 Crim Law and Philos 21

administrative hybrid orders are used in order to avert procedural requirements and human rights protections applicable to criminal process. [307] According to Zedner, the purpose of the order is to circumvent the need for prosecution and sidestepping the criminal process.[308] Ferzan argues that the application of presumption of innocence is necessary in preventive justice to avoid the misuse of power by the state. The state is obliged to discharge the onus of prove before a person's liberty can be infringed.[309]

On the other hand, to some extent, executive measures enable states to provide better protection to the population, as they are not required to meet the standards of criminal process.[310] Deputy Public Prosecutor 3 opined that:

> Sometimes, the evidence is not sufficient. You have all the information to support your case based on the intelligence. Unfortunately, you don't have eyewitnesses. Sometimes, the court declines the evidence. You don't have to discharge the burden of proof in court especially in relation to terrorism, security and public order by using the preventive laws. Preventive laws are quite useful tools, but we use it as last measures.[311]

Consequently, executive order against the perpetrator of cyber attacks should be used as the last resort due to human rights concerns.

It was reported that 10883 people had been arrested under the Internal Security Act 1960 from 1960 until April 2012.[312] Statistics also shows that 4461 people had been imposed with detention order under the Act.[313] The high rate of detainees reflects the lack of discernment and fairness in the issuance of executive order. POTA has been criticised for precluding judicial

---

[307] ibid

[308] Zedner L, 'Preventive Justice or Pre-Punishment? The Case of Control Orders' Current Legal Problems, 2007, Volume 60, Issue 1

[309] Ferzan KK, 'Preventive Justice and the Presumption of Innocence ' Crim Law and Philos (2014) 8: 505-525

[310] Walker C, *Blackstone's Guide to the Anti-Terrorism Legislation* (n 277) 299

[311] Interview with Deputy Public Prosecutor 3

[312] House of Representatives Deb 17 April 2012

[313] ibid

review of the detention order and allowing the possibility of indeterminate extensions. [314] Therefore, the government should develop tougher safeguards against overzealous arrest and detention. This includes the disclosure of the case and the setting up of an independent review of the detention. In addition, the executive order should only be extended for one or two years maximum.

Furthermore, Malaysia may consider conferring the power to High Court to grant certain types of prohibitions, restrictions or requirements against any persons who commit serious crimes upon application made by the Attorney General. This is based on the UK's Serious Crime Act 2007. The Act empowers the High Court in UK to make an order against a person who has been involved in serious crime in order to protect the public.[315] Computer misuse is classified as a serious crime under the Act.[316] The High Court may impose prohibitions, restrictions, or requirements on individuals including their financial, property, working arrangements, means of communication, access to premises and travel.[317] It could be argued that the Serious Crime Act 2007 ensures fairness in comparison to executive order, as the judge must satisfy that the person has been involved in serious crime and believe on reasonable grounds that the order would protect the public.[318]

Executive orders could be used against the perpetrator of cyber attacks alongside other preventive laws in Malaysia. Despite the difficulties over the formulation of the crime of possession and distribution of materials, it could be argued that executive order is necessary in order to avert serious threat through early intervention. As demonstrated in the preceding section, the government has significant roles in matters involving national security and public order. It may invoke this measure for the purpose of maintaining

---

[314] Thiru S, 'Speech by Steven Thiru, President, Malaysian Bar at the Opening of the Legal Year 2016' [2016] MLJ xxiv

[315] S 1 of the Serious Crime Act 2007

[316] Paragraph 11A, Schedule 1 of the Serious Crime Act 2007

[317] S 5 of the Serious Crime Act 2007

[318] CPS 'Serious Crime Prevention Orders Serious Crime Act 2007-Sections 1-41 and Schedules 1and 2, as amended by the Serious Crime Act 2015-Sections 46-50'<http://www.cps.gov.uk/legal/s_to_u/serious_crime_prevention_orders_(scpo)_guidance/> accessed 7 February 2017

public security and the safety of critical national infrastructure. However, this power may infringe personal liberty due to the dispensation of criminal conviction. Thus, it should be exercised sparingly and with utmost respect for human rights. In addition, Malaysia should consider prosecution before resorting to executive order for serious crimes including computer misuse and terrorism. Criminal justice is fairer, more open and effective. Executive orders must be used as a secondary option especially when prosecution is not possible.

So far, this study demonstrates that criminalising the possession of materials and regulating the creation, distribution and procurement of materials to commit cyber attacks may be invoked in dealing with this problem. The findings revealed that more than half of the participants from different categories agreed that these measures may enhance the effectiveness of criminal law in dealing with cyber attacks. They may alleviate the possibility of attacks especially by young offenders and disrupt the growth of a black market of information. Besides that, this study considers the usage of executive order in managing the risks of cyber attacks in Malaysia. Some of the participants argue that this measure is needed in order to protect the public. However, some of them expressed their concern that this measure may infringe fundamental liberties. Accordingly, this measure should be used sparingly and should only be invoked to protect essential services against large-scale cyber attacks.

5.4 The Implementation of Criminal Law Measures Against Cyber Attacks in Malaysia: the Obstacles and Possible Reforms

This section examines the implementation of existing criminal law measures against cyber attacks in Malaysia. It discusses some of the obstacles and possible reforms in the application of criminal law to counter cyber attacks in Malaysia. The effectiveness of criminal law depends on the enforcement mechanisms especially the capability of the law enforcement officers. The Chief Justice of Malaysia, YAA Tun Ariffin Bin Zakaria, acknowledged that

enforcement of the law is an issue in Malaysia.[319] He also suggested that a stricter enforcement regime to be implemented so that the public will take the law seriously.[320]

This study shows that some of the participants from all categories contend that there is lack of enforcement in dealing with cyber attacks. For instance, Private Sector Officer 4 argued that:

> I think the laws are not effective. After the bank refunded my money, I didn't see any initiatives to ensure that the incidents do not occur again. I made a police report as suggested by the bank officer. However, what is the purpose of police report if there is no action? Is it for documentation only?[321]

This section is structured as follows. After assessing the reluctance of the public to report the occurrence of cyber attacks, this section analyses the factors that hinder the enforcement of the law. This includes jurisdiction, technical expertise of the law enforcement officers. Next, this section reviews the sentencing for cyber attacks in Malaysia.

5.4.1 The Duty to Report the Occurrence of Cyber Attacks

This study next investigates the willingness of the public to report cyber attacks to the police and other authorities. This study reveals that half of the participants from all categories thought that cyber attacks remain underreported in Malaysia. The police rely heavily on the public in conducting the investigation to identify and apprehend criminals.[322] The reluctance of individuals and private institutions to report the occurrence of criminal activities to the police hampers the enforcement of the law. They may be hesitant to report the matter due to various reasons. According to Etzioni, corporations have been slow to act due to several reasons. Firstly, many corporate leaders maintain libertarian or conservative laissez-faire

[319] Zakaria TAB, 'Speech by YAA Tun Ariffin Bin Zakaria, Chief Justice of Malaysia at the Opening of the Legal Year 2016' [2016] MLJ i

[320] ibid

[321] Interview with Private Sector Officer 4

[322] Young J, 'Left Realism and the Priorities of Crime Control' in Stenson K and Cowell D (eds), *The Politics of Crime Control* (Sage Publications 1991) 154

approach. Their main commitment is to their shareholders and not the common good. They are free to follow their own directions. Secondly, the cost of implementing security measures is higher than the losses suffered by the corporations. Thirdly, business owners perceive that the duty to protect national infrastructure is the responsibility of the state. Furthermore, the imposition of regulations will impair their ability and flexibility to innovate.[323]

Individuals and corporations may be hesitant to report cyber attacks due to honourable motives such as to ensure the stability of the market and public confidence. The banks do not want the public to know that their computer systems are weak and vulnerable to any attacks. Security Professional 10 asserted that:

> I encourage my client to report the matter to the police. This is necessary in order to secure the evidence. Private companies will only report the incident to the Police if it involves serious data leakage. They want to preserve their reputation. They think that lodging police report is burdensome. Sometimes the laws may be prejudicial to the victims. For instance, in relation to politically motivated cases, somebody posted a comment on a website accusing the victims took bribes. He reported the matter to the Police in order to find the person who posted the comment. It can backfire on the victim. The Police will investigate him first to verify the accusation and then proceed with the report.[324]

Consequently, the victims may consider other options such as to hire private security company or CERT in addressing this issue. For them, this is a better choice as they can avoid unnecessary publicity that may affect their business and potential loss of profits. Security Professional 9 asserted that:

> I proposed each domain have its own CERT. They don't have to report the incidents outside of their domain. They may share the impacts, effort and challenges with other domains. They can

[323] Etzioni A, 'Cybersecurity in the Private Sector' (2011) 28 Issues in Science and Technology 58

[324] Interview with Security Professional 10

> maintain their reputation and their business will not be interrupted. Perhaps their CERT may report to MYCERT for the purpose of incident sharing but not the details of the company.[325]

Apart from preserving their reputation, the investigation may take a substantial amount of time. The companies do not want their business to be disrupted due to prolonged investigations. According to the Deputy Public Prosecutor 5:

> I wouldn't say that they are reluctant. Normally this type of investigation takes years. The victims will set up their own investigation first. They then hand over the matter to the police. The police needs to get second opinion. This is because the finding of the expert appointed by the company will be challenged in the court on the basis that he is not neutral. He may altered the findings to suit his client's interest. If the attacks involved server for example, the standard operating procedure for the police is that they have to take the server into their possession. So, this will disrupt the company's business. If the attacks affect significant number of the computers, the police take the computers away as evidence. During the course of the investigation, the police may discover that the attacks go beyond this one computer; it affected other computers. However, when they gather the other computers, it is too late. Work has been done on the computers; lots of evidence have been deleted and overwritten. They have to seize all the computers. Maybe, this is why they are reluctant to report to the police.[326]

However, the unwillingness of public to report cyber attacks may obstruct the attempt to arrest the perpetrators especially if they are extremely dangerous. This may impede the effectiveness of the criminal justice system in protecting the interest of the public. The perpetrators must be brought to

---

[325] Interview with Security Professional 9

[326] Interview with Deputy Public Prosecutor 5

justice and should not operate with apparent impunity. The compilation of the reports may also assist the authorities to determine the strategies to counter cyber attacks effectively. According to Security Professional 9:

> We have to share the information about the incidents. We need to know the root causes and how to prevent them from happening again.[327]

Accordingly, several measures may be implemented to overcome this problem. Some participants of this study suggested that the report should be kept confidential in order to protect the company's reputation. According to Legal Practitioner 1:

> Maybe the report should be kept confidential so that their business is not affected. The law enforcement officers can see how often it occurs and the measures that can be taken. Companies can be assured that the process is done privately and not publicised.[328]

However, other participants rejected this argument. Deputy Public Prosecutor 2 argued that different proceeding should not be used against corporate entities, as the law is equal to everyone. [329] Policymaker 3 insisted using diplomatic means to encourage the public to report cyber incidents to the authorities:

> We cannot dictate or force people to do things. They should do it voluntarily. The cyber security policy is based on diplomatic measures rather than using force. We have to make them understand the benefit of being on board.[330]

The role of the government is important in persuading the public to refer the wrongdoing to the authorities. They have to be reminded that cyber attacks may recur repeatedly due to their silence. On the other hand, some of the participants in this study suggested the promulgation of the law to oblige the

---

[327] Interview with Security Professional 9

[328] Interview with Legal Practitioner 1

[329] Interview with Deputy Public Prosecutor 2

[330] Interview with Policymaker 3

public especially corporate entities to report cyber attacks to the authorities. Private Sector Officer 1 argued that:

> I don't have the specific information. We don't have legislation similar to US in which the government's agencies and companies have to report security breach. So far, there is no news about data security breach in Malaysia. The mind-set of the people is do not tell. I think they should be compelled to do so.[331]

Similarly, Deputy Public Prosecutor 2 contended that:

> The policymakers have to decide whether to compel them to report. It should be made mandatory under the Central Bank's guideline. They have to report to the Police. I don't think we have this currently.[332]

Cyber attacks should be reported not only to the authorities but also to the customers. Security Professional 8 asserted that:

> There is a need for a legislation to compel all organisations to report. Fine should be imposed on them if they are reluctant to do so. In the US, companies have to inform the public every time they were attacked. They have to provide information pertaining to the attacks and the solution. They prepare a script to report the attacks. We need to have this in Malaysia. The public must be informed about the attacks.[333]

The obligation to report cyber incidents has been implemented in some states in the US. For instance, a business or state agency is required under the California law to notify any California resident and the Office of the Attorney General of a breach of the security system.[334] The state security breach notification laws in the US contain several standard elements: who must comply with the law; the definition of 'personal information' and 'breach

---

[331] Interview with Private Sector Officer 1

[332] Interview with Deputy Public Prosecutor 2

[333] Interview with Security Professional 8

[334] California Civil Code s 1798.29

of security'; the elements of harm in order for the notice to be triggered; the requirements for notice; exemptions and safe harbour; pre-emption and relationships to other federal laws; and sentencing, enforcement authorities and remedies.[335]

Apart from US, the European Commission has proposed that member states should oblige operators of critical infrastructures and public administrations to report serious incidents to the national authorities.[336] The security of the critical infrastructures such as banking, stock exchange, energy generation, transport, health and Internet services are vital to the functioning of the internal market.[337] This measure is perceived as necessary to enable the public authorities to react, take appropriate mitigating factors and set adequate strategies.[338] However, the proposal has been rejected by states including Sweden, Ireland and UK.[339] They are reluctant to share the information due to security reasons. Thus, the duty to report cyber incidents may be difficult to be implemented at the regional level especially for supranational institution such as EU. Also, it may not be enforced at the domestic level due to mistrust among local institutions.

5.4.2 The Regulation of Technical Expertise Among the Law Enforcement Officers, Prosecutors and Judges

This study identifies as crucial the capability and expertise of the Malaysian law enforcement officers in dealing with cyber attacks. It is noted that the Commercial Crime Investigations Department of the Royal Malaysia Police has established the Cybercrime and Multimedia Investigations Division. This unit investigates not only computer integrity crimes, computer content crimes

---

[335] Stevens G, 'Data Security breach Notification Laws' Congressional Research Service <as.org/sgp/crs/misc/R42475.pdf> accessed 9.11.2016

[336] Commission, 'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union' COM (2013) 48 final

[337] ibid

[338] ibid

[339] EurActiv.com, 'Member States See Digital Security as A National Issue', https://www.euractiv.com/section/digital/news/member-states-see-digital-security-as-a-national-issue/, accessed 15 December 2016

and computer related crimes but also traditional crimes that have a computer element. According to Police Officer 1:

> I investigate cases involving cheating. We don't have many investigating officers. I have to investigate other cases involving the usage of computer.[340]

Apart from investigation, this unit carries out forensic analysis, surveillance and monitors the content of the Internet in Malaysia such as sedition and national security.[341] Police Officer 3 explained the reporting and investigation process for cybercrimes in Malaysia:

> The reports are dealt with at two levels. The contingent (district level) investigate high interest cases, whereas, Bukit Aman investigates extremely high profile cases. The investigation officers at Bukit Aman provide technical support and gather cyber intelligence. The investigation officers at the district level investigate all cases involving cyber such as cheating. They will refer the cases to the specialist at Bukit Aman. Apart from that, we conduct Internet surveillance, operation and give public lecture.[342]

According to Police Officer 1:

> Let's say a complainer reported that he had been cheated. We will conduct the investigation and then submit the investigation papers to the prosecution. They will decide whether to prosecute under the Penal Code or the Computer Crimes Act or to use both laws.[343]

Deputy Public Prosecutor 1 described the factors that are taken into consideration in determining the prosecution of the offenders:

> There is no written guideline for the prosecutors. Evidentiary speaking, we have guideline under the Arahan Peguam Negara 2007 (Attorney General's Directive 2007) which says that we

[340] Interview with Police Officer 1

[341] ibid

[342] Interview with Police Officer 3

[343] Interview with Police Officer 1

> should prosecute only when we can prove a case beyond reasonable doubt based on the evidence. The policy concern is much wider, for example if someone publicised defamatory or seditious article, policy consideration may nevertheless works in favour of not charging, giving him a discharge or imposing a lesser sentence. This is subjective.[344]

The analysis results are mixed about whether the law enforcement officers have sufficient capability to respond to cyber attacks. Some of the law enforcement officers and participants from other categories considered that the police have sufficient capability in dealing with cyber attacks. According to Police Officer 3:

> Our capability is enough at the moment. Perhaps in 10 years, we have to catch up with the technology used by the hackers. We have to undergo a lot of training especially in relation to the laws, which is our core job. We have the technical skills related to computer. Most of our officers are provided yearly training. We conduct test in order to improve our technical skills and cyber issues. We established a platform to share our knowledge and conduct training for trainers.[345]

Deputy Public Prosecutor 5 noted the discrepancy between the competency of the officers at Bukit Aman (the Royal Malaysia Police's headquarter) and the contingent:

> The competency and capacity to investigate this crime is asymmetrical because most of the experts are located in Bukit Aman. The investigating officers at the district level do not commonly deals with this. I don't think they receive sufficient training. It would be difficult for him to decide where to begin.[346]

However, some of the security professionals asserted that the police do not have adequate expertise especially in conducting forensic investigation.

---

[344] Interview with Deputy Public Prosecutor 1

[345] Interview with Police Officer 3

[346] Interview with Deputy Public Prosecutor 5

They require assistance from other agencies such as MyCERT and MCMC. According to Security Professional 9:

> The forensic department of the Cybersecurity Malaysia assists them. I observe that they have the capability at the first level. However, they have to refer to Cybersecurity Malaysia at the second and third level. They have their own lab, however, they still need technical support from Cybersecurity Malaysia.[347]

On the other hand, Police Officer 3 compared the function of the police with other agencies including Cybersecurity Malaysia and MCMC:

> We are the law enforcement agency. We are not providing defence; we enforce the law. Cybersecurity and the military are responsible for defence. They have the capability to deal with the fraudsters. MCMC and Cybersecurity are at the same level with the fraudsters. So far, we managed to detect the attack.[348]

Nonetheless, Police Officer 3 asserted that the law enforcement officers have to change their attitudes toward the value of cybercrime training in order to effectively respond to the reports:

> We need to change the perception of the IO and PO. At least, they need to know and want to know about computer. If you don't know about the computer, then you will have a problem. Even if you have legal background, you cannot prosecute if you don't know about the computer. You need to change the perspectives of the PO and the IO. They need to understand and commit to their work. We don't have to amend the law because the current law can be used. The problem is the attitude of the PO and IO.[349]

Police Officer 3 also emphasized that the law enforcement officers should not succumb to their preconceived notions about the difficulties in investigating cybercrime:

---

[347] Interview with Security Professional 9

[348] Interview with Police Officer 3

[349] Interview with Police Officer 3

> I have to understand the cyber environment in order to investigate. For instance, an insider hijacks the computer system of the airport. It takes me a couple of weeks to understand this situation; I use my own initiatives. I managed to get the information from the site. However, I have to transfer the knowledge to the DPP. You need to act fast in investigating cybercrime. A couple of months delay will affect the investigation. I have to understand cloud computing today and malware during the next day. You have to continuously understand the terms.[350]

Apart from the police, some of the participants from all categories perceived that legal practitioners, persecutors and judges do not have sufficient knowledge of cybercrimes in Malaysia. According to Police Officer 1:

> The criminal process especially during trial needs to be improved. Sometimes lawyers and judges are not familiar with cyber terms. The judges tend to verify the terms a few times. Maybe this is due to the fact that cybercrimes are relatively new in Malaysia. They have to learn new things and increase their knowledge. We need to have more awareness programmes for judges and lawyers. The latest batch of deputy public prosecutors may have the knowledge. However, some of the deputy public prosecutors who are expert in this area quit their job to open their own firm.[351]

Similarly, Legal Practitioner 3 observed that:

> When you have a prosecutor who is not well conversed with the technical aspect, the charge won't be upheld because of his lack of experience in the subject matter. I was involved in a case. Some of the prosecutors were not specialised in computer related offences. You could see that they struggle a bit, except for the guys from cyber security.[352]

---

[350] Interview with Police Officer 3

[351] Interview with Police Officer 1

[352] Legal Practitioner 3

Police Officer 3 contended that:

> So far, the judges do not have clear understanding of cybercrimes. I conduct investigation and then the case is handed over to the DPP. I told the DPP about server, sqn injection or DDOS attacks. The DPP needs to know about these in order to prosecute the case. How many DPP understand the cyber terms? I have given lecture to some officers, but not many can adapt to the situation. Let's say they direct us to record the conversation with Yahoo or Google. This is nonsense; they are from the US. I heard that they are considering the establishment of cyber court. I think this may help in carrying out the prosecution.[353]

As for the judiciary, it was reported that the first special cyber court in Malaysia was activated on 1.9.2016.[354] The court specialises in cyber criminal cases such as hacking, spying, online gambling and defamation. The judges are to be trained in the field of cyber and computer cases. The jurisdiction of the court will be expanded to civil cases related to cyber.[355] The establishment of the cyber court may strengthen the application of criminal law in dealing with cyber attacks in Malaysia.

This section demonstrates that more efforts are need to improve the capability of the law enforcement officers, prosecutors and judges. Uniform training may help to increase their understanding on cybercrime. Training must be conducted at all levels especially the police at the district level as they may act as first responders. In addition, managerial support may change the law enforcement officers' attitude towards the challenges posed by cybercrime investigation.[356] It appears that there is a lack of investigation officers who are cyber security experts. Thus, staffing issues have to be

---

[353] Interview with Police officer 3

[354] Babulal V, 'Malaysia's First Cyber Court Begins Operations Today' *New straits Times Online* (Kuala Lumpur, 1.09.2016) <http://www.nst.com.my/news/2016/09/169883/malaysias-first-cyber-court-begins-operations-today?d=1> accessed 9.11.2016

[355] ibid

[356] Holt Tj, Burrus GW and Bossler AM, *Policing Cybercrime and Cyberterror* (Carolina Academic Press 2015) 125

resolved in order to deal with this matter more effectively. Besides that, the development of a specialised unit to investigate computer integrity crimes and forensic examinations is necessary in order to deal with cyber attacks.

Apart from the above recommendations, Malaysia may consider the establishment of a specialised law enforcement agency similar to the National Crime Agency (NCA) in the UK. It provides a range of specialist capabilities to prevent and disrupt the most serious criminal activities especially organised crime such as cybercrime, people smuggling, firearms and drugs.[357] The NCA officers come from different backgrounds, skills and experiences. They perform various tasks including investigations, intelligence, child protection, communications and finance.[358] The NCA works together with the police, public sector and private industry to tackle serious crime.[359] Besides enforcement measures, the police may be equipped with other arrays of legal weapon including civil remedy such as injunction as indicated in the previous chapter. The police should be able to actively implement reactive and proactive measures to counter cyber attacks in Malaysia.

5.4.3 Extra-Territoriality

As discussed in chapter 3, a majority of the participants from all categories acknowledged that the sources of the attacks might come from outside of Malaysia. Particularly salient is the difficulty in establishing criminal culpability and securing conviction for cyber attacks, which are committed or originated from the territory of another state. Although cyber criminals operate in cross-border, the law enforcement agencies are required to respect the sovereignty of other countries especially during investigation.[360] This study shows that the law enforcement officers and security

---

[357] National Crime Agency, 'Crime Threats' <http://www.nationalcrimeagency.gov.uk/crime-threats> accessed 15 February 2017

[358] National Crime Agency <http://www.nationalcrimeagency.gov.uk/about-us> accessed 15 February 2017

[359] ibid

[360] Csonka P, 'The Council of Europe's Convention on Cyber Crime and Other European Initiatives' (n 31)

professionals agreed that extra-territoriality is a major impediment in the application of criminal law against cyber attacks. The process of gathering the evidence is difficult due to extra-territoriality. According to Deputy Public Prosecutor 2:

> Let's say you commit an offence in the US. Are you being charged in US or Malaysia? This is one of the difficulties. How do you get the evidence to bring the accused in Malaysia? It is impossible physically to bring all the hardware to Malaysia. We can take the transcripts of the file and computer logs, but then this is difficult because of some judges. They are new to computer crimes. The Evidence Act does not mention about gathering evidence for computer crimes. It depends on how the lawyer and prosecutor argue their case.[361]

Apart from the production of evidence from outside of Malaysia, apprehending the offenders are problematic as the law enforcement officers are not allowed to exercise their power in the territory of another state under international law. Deputy Prosecutor 3 argued that:

> The problem is the prosecution. For instance the promoters of online gambling are in Taiwan. How do you catch them?[362]

Similarly, Deputy Public Prosecutor 3 asserted that:

> Recently, the Anonymous intruded the website of a local airline. I conducted the investigation. The attack came from abroad. We cannot proceed because the suspect was outside of Malaysia.[363]

The perpetrators may be apprehended through extradition or mutual legal assistance. The process is based on political consideration, as governments tend to increase procedural barriers for extradition and other forms of cooperation with less friendly countries.[364] Some of the law enforcements

[361] Interview with Deputy Public Prosecutor 2

[362] Interview with Deputy Public Prosecutor 3

[363] Interview with Police Officer 2

[364] Bassiouni MC, 'Policy Considerations On Interstate Cooperation in Criminal Matters' 4 Pace YB Int'l L 123 1992

officers described the difficulty in getting the assistance from their international counterparts. According to Police Officer 2:

> We tracked the origin of the attack; the IP address showed that it came from outside of Malaysia. We requested the police of that country to assist us through mutual legal assistance (MLA). It was difficult to rely on their help. They can reject our application. MLA is between the governments. They have their own regulation and laws. With regard to the intrusion of the website of the local airline, the police from the other country decided to do their own investigation even though the perpetrators attacked a Malaysian website. They requested us to provide the evidence through MLA. However, it takes time to entertain their request. In this case, we had the information in our server but it was not sufficient. They arrested the offender based on the forensic evidence from his computer. We had similar situation when we asked for assistance from Interpol. In 2008, the AFC Cup's website in Malaysia was hacked from Korea. Interpol did not entertain our request for assistance.[365]

This demonstrates that a foreign authority may dismiss the request for mutual legal assistance. According to Taylor, the foreign authority may allow the investigators to access the materials but refuse to disclose them to the defence.[366] Deputy Public Prosecutor 5 voiced his frustration at the extent of the cooperation from other countries:

> Malaysia has been accommodative with respect to the request for mutual legal assistance; other countries have not. Malaysia has received many requests; we have obliged to many of them. The term mutual legal assistance entails that I help you and you will entertain my request in the future. Sadly, that is not the case. Some countries had arm-twisted our government. In some cases, we have not received reply even after 5 years. We

[365] Interview with Police Officer 2

[366] Taylor C, 'Disclosure of Foreign Intelligence Material: CPIA, Norwich Pharmacal and the War on Terror' (2011) 15 Int'l J Evidence & Proof

> receive quick response in relation to cases that affect their national interest such as terrorism and child pornography. Other than that, the process is slow.[367]

The lack of cooperation among nations may hamper the investigation and prosecution of cyber attacks. Moreover, Internet regulators are bound by different moral codes and legal responses in different countries.[368] Security Professional 10 argued that:

> I don't see any cooperation between countries. They have their own rules and policy. They are concerned about data leakage. However, there is no consensus on the features of the protected data. For instance, there is consensus on the details such as age for child pornography. However, if I uploaded personal information about the CEO of Touch n Go in the US, they are not going to take action. He is not a US citizen or resident. U.S doesn't have any interest.[369]

The process of extradition depends on the existence of an agreement and other factors such as the principle of double criminality. Cooperation may be impossible when a state criminalise certain activities related to computers, whereas other states have not done so.[370] In particular, there is a conflict between states with a 'tradition of freedom of speech and those that are more repressive'.[371] Deputy Public Prosecutor 4 noted that:

> Dual criminality is big issue in cybercrimes. For example, someone posted a comment that amounts to defamation on Facebook, telegrams and blog. The server is in the US. It may not satisfy the dual criminality principle as the U.S has more

---

[367] Interview with Deputy Public Prosecutor 5

[368] Jewkes Y and Yar M, 'Policing Cybercrime: Emerging Trends and Future Challenges' in Newburn T (ed), *Handbook of Policing* (2nd edn, Willan Publishing 2008) 593

[369] Interview with Security Professional 10

[370] Csonka P, 'The Council of Europe's Convention on Cyber Crime and Other European Initiatives' (n 31)

[371] Jewkes Y and Yar M, 'Policing Cybercrime: Emerging Trends and Future Challenges' in Newburn T (ed), *Handbook of Policing* (n 368) 593

> freedom of speech. They will not assist us in getting the evidence.[372]

Deputy Public Prosecutor 5 asserted that:

> We have to prove dual criminality in order for that request to be successful. In some jurisdiction defamation is not a criminal offence; it is just a civil wrongdoing. They cannot assist us by revealing the owner of the IP address. Cyber attacks are offences under our laws and other jurisdiction. However, the process to get the information through MLA is slow.[373]

According to Deputy Public Prosecutor 2:

> Alvin posted comments on Facebook and blogs from the U.S insulting Islam and Muslims in Malaysia. We cannot extradite him, as it is not prohibited in the U.S.[374]

This demonstrates that the prosecution of cyber attacks in the guise of content related crime is difficult due to the principle of dual criminality especially if the perpetrators resided in the U.S. However, recently, US government agreed to exert pressure on the Internet companies such as Google and Facebook to remove materials that are related to terrorism and hate speech from their server in California.[375] It was reported that social media sites such as Facebook, Twitter and YouTube agreed to abide to the European Commission Code of Conduct on Illegal Online Hate Speech.[376] They are required to remove hate speech or disable access to the content

---

[372] Interview with Deputy Public Prosecutor 4

[373] Interview with Deputy Public Prosecutor 5

[374] Interview with Deputy Public Prosecutor 2

[375] Home Affairs Committee, 'Radicalisation: The Counter-narrative and Identifying the Tipping Point' (HC135, 2016-17); EURACTIV 'Google, Microsoft, Twitter and Facebook Agree to Remove Hate Speech Online' <www.euractiv.com/section/justice-home-affairs/news/google-microsoft-twitter-and-facebook-agree-to-remove-hate-speech-online/> accessed 20 February 2017

[376] European Commission-Press Release 'European Commission and IT Companies Announce Code of Conduct on Illegal Online Hate Speech' <http://europa.eu/rapid/press-release_IP-16-1937_en.htm> accessed 20 February 2017

within 24 hours after receiving notifications.[377] Nevertheless, this is not a feasible solution for Malaysia due the priority for freedom of speech in the US. These social media companies may not entertained the request to remove materials related to sedition and defamation in Malaysia. Furthermore, this measure is only available for transnationally shared offences such as terrorism incitement and child porn.

5.4.4 Sentencing

This section examines the role of sentencing and the application of sentencing guideline in countering cyber attacks in Malaysia. Sentencing is perceived as a process of censuring and labelling of the offender's bad behaviour.[378] Smith argued that 'punishment depends for its effect on the response of the individual and the audience, otherwise, as von Hirsch has observed, being sent to prison would be no worse than joining the crew of a submarine'.[379] In addition, punishment delivers 'genuine bindingness to the rule of law by providing significant incentives not to violate legal rules'.[380] The participants in this study were asked about appropriate form of punishment for the perpetrator of cyber attacks. The response to the function of sentencing for cyber attacks is divided into four forms.

Firstly, the perpetrators should be punished in order to deter future attacks. The utilitarian view asserts that punishment is needed for the benefits of the individual and the society at large 'including the possible deterrent effect which would follow from it'. [381] Criminal liability may deliver credible deterrence and carries public confidence.[382] According to Deputy Public Prosecutor 5:

---

[377] ibid

[378] Ashworth A, *Sentencing and Criminal Justice* (5th edn Cambridge University Press, 2010) 74

[379] Smith DJ, 'Less Crime Without More Punishment' 3 Edinburgh L. Rev. 294 1999, 309

[380] Riesta I, 'Global Accounts of the Wrongfulness of Criminal Behaviour' (2011) 3 Contemp Readings L & Soc Just 110, 111

[381] Faulkner D, *Crime, State and Citizen. A Field Full of Folk* (2nd edn Waterside Press, 2006) 89

[382] Roger Bowles MF, Nuno Garoupa, 'The Scope of Criminal Law and Criminal Sanctions: An Economic View and Policy Implications' (2008) 35 JL & Soc'y 389

> Criminal law is the most effective way to deal with this problem. It enables us to utilise 'full force' of the law. It means that the police can use their sources to identify the perpetrators. We can charge and send them to prison. We think this is the best way to remind everybody that the police will go all out to catch the perpetrator. The Attorney General Chamber will go all out to prosecute, secure conviction and ensure heavy sentence is imposed on the perpetrator. The law does not care whether the perpetrator pleads ignorance or has to support his family.[383]

Legal Practitioner 3 asserted that:

> Certain infrastructures attract heavier penalty. This includes key infrastructures for example public utility and military infrastructure. I think there is a need to ensure that strong deterrence sentence for those forms of cyber attacks so that no one attempts to do it. Maybe you can look at the legislation on other countries. We should distinguish infrastructures, which are pertinent to national security from commercial infrastructure. The latter should attract slightly different form of sentencing. I am a bit uncomfortable with the notion of life imprisonment, but we are talking about key infrastructures now.[384]

Bishop argued that 'the concept of deterrence is fundamentally premised on the notion that the infliction of a punitive sanction is capable of influencing the future conduct of potential lawbreakers'. [385] A range of sanctions including incarceration seems necessary to ensure the safety of the public. Capital punishment and lengthy incarceration are perceived as a mechanism to refrain a person from reoffending.[386] The imprisonment of the perpetrators of cyber attacks may reduce the occurrence of future attacks. However,

---

[383] Interview with Deputy Public Prosecutor 5

[384] Interview with Legal Practitioner 3

[385] Bishop P, 'Criminal Law as a Preventative Tool of Environmental Regulation: Compliance Versus Deterrence' (2009) 60 N Ir Legal Q 279, 281

[386] Ashworth A, *Sentencing and Criminal Justice* (n 378) 85

general deterrence and incapacitation will also affect the liberty of the offenders for the sake of the protecting future victims.[387]

Secondly, punishment for cyber attacks is more important for symbolic reasons including to strengthen public confidence and to reinforce moral values of the society. Denunciation is achieved by the severity of the sentence, which is a symbolic statement that the offence in question is not to be tolerated by the society.[388] Punishment may not deter future attacks, as the risk of getting caught for cyber attacks is low due to the perpetrator's technical expertise. Deputy Prosecutor 1 argued that:

> The advantage of criminal law is the deterrence effect of sentencing. However, it has to be measured against the risk of getting caught. This is due to the availability of software, which is created to maintain the anonymity of the perpetrators while they are online. I think the risk of getting caught is low if they do it properly. For instance, I go to a cyber café, and then I provide fake credentials to the cashier. I use anonymous software to publish seditious remarks. I don't see how the police can track me.[389]

Similarly, Private Sector Officer 1 argued that:

> You cannot simply accuse and penalise people when it comes to DDOS attack. The packets are here but the attackers are somewhere else. They can spoof packet to our country from abroad. It is really hard to identify the perpetrators mostly because of the anonymity. Should you be responsible for the attacks that come from your house? [390]

Clarke argued that it is more efficient to make the offender more fearful of being caught rather than increasing punishment. [391] This is due to the fact

---

[387] ibid 85

[388] *PP lwn Abdul Halim Ishak & Satu Lagi* [2013] 9 CLJ 559

[389] Interview with Deputy Public Prosecutor 1

[390] Interview with Private Sector Officer 1

[391] Clarke RV, 'Introduction' in Clarke RV (ed), *Situational Crime Prevention: Successful Case Studies* (2nd edn, Harrow and Heston 1997) 14

that the offenders pay closer attention to the immediate chances of getting caught than to the nature of the punishment they might receive later.[392]

Thirdly, the result of the interviews shows that some of the security professionals, prosecutors and private sector officers thought that the perpetrators should be punished harshly. Tough responses are essential for those who attack institutions of national importance. The retributivist argues that people deserve to be punished for committing offence as 'they do so of their own free will as individual moral agents'.[393] This view emphasises that the sentencing must be proportionate and consistent to the crimes committed. [394] The desert or proportionate theory provides the same perspective. This theory predicates that the offenders are capable of comprehending the evaluation of their conduct by the authority. The rule of law is respected through the imposition of proportionate sentence over the offenders.[395]

Finally, sentencing can be designed to rehabilitate the offender. Various programmes of treatment and facilities are devised to improve and tackle the attitude and behaviour of the offender.[396] Some of the security professionals, private sector officers and law enforcement officers suggested utilising the offender's skill to counter future attacks. Private Sector Officer 1 argued that:

> Imprisonment and fine should not be imposed on all perpetrators of cyber attacks. It depends on the seriousness of the attacks. If the attackers are below 20-year-old, I consider that is a talent. They commit the attack not for malicious purposes. For instance, a 17-year-old boy shows the vulnerability of TM's system. We can put him somewhere so that he can learn instead of punishing him.[397]

Similarly, Security Professional 10 contended that:

---

[392] ibid

[393] Faulkner D, *Crime, State and Citizen. A Field Full of Folk* (n 381) 89

[394] ibid

[395] Ashworth A, *Sentencing and Criminal Justice* (n 378) 89

[396] ibid 86

[397] Interview with Private Sector Officer 1

> If we put them in the prison, we are wasting their skills. They are not doing anything inside the prison. They should use the skills to serve the government including rebuilding the programme that has been disrupted or destroyed. Not everybody has the talent to write codes. However, this measure may not be applied to repeated offenders. The way we punish the perpetrator of cyber attacks should be different from other offences such as distributing pornographic materials. He does not physically attack the CNI. We spend millions of ringgit developing the security system, but he can single-handedly ruin it.[398]

This demonstrates that the government may consider a special programme for young offenders. Their talents may be used for the purpose of research in security area. They may help the authorities to identify vulnerabilities of the computer system of the public and private sectors in Malaysia.

Apart from the introduction of new offences for cyber attacks, Malaysia may consider the establishment of a sentencing guideline to determine the seriousness of cyber attacks. As stated above, the nature of harm is also significant for the purpose of sentencing. The fairness of the punishment for cyber attacks is dependent on the degree of harm suffered by the victims and the culpability of the offenders. The seriousness of the offences is determined by the offender's culpability and the degree of harm. The Overarching Principles: Seriousness Guideline issued by the Sentencing Guidelines Council of UK provides the standard in determining the seriousness of culpability and harm for the purpose of the imposition of punishment where the offender is aged 18 or over at the time of conviction.[399] The Guideline emphasises that the culpability of the offender should be the initial factor in determining the seriousness of an offence.[400] It

---

[398] Interview with Security Professional 10

[399] Sentencing Guidelines Council, 'Overarching Principles: Seriousness Guideline', http://www.sentencingcouncil.org.uk/wp-content/uploads/web_seriousness_guideline.pdf, accessed 15 December 2016

[400] ibid para 1.19

also provides for aggravating factors to indicate higher culpability and a more than usually serious degree of harm.[401]

However, there is no similar guideline formulated in Malaysia. According to Deputy Public Prosecutor 1:

> We conducted a research project on the need for sentencing guideline. Preliminary recommendation was to have it. This is because you can have sentences quite variant from each other, not only at the same district but the court in the same complex. Of course jurisprudence allows for judicial discretion. However, you have to explain to the accused why this court sentenced a person to one year, whereas, other court gave 5 months. Sentencing is based on practice. If I go to the court in PJ, I will look at who are the judges and the DPPs. [402]

Deputy Public Prosecutor 2 asserted that:

> Currently, they are working with MCMC to come out with a guideline; what should be considered as a serious and less serious offence so that the prosecutor will have an idea of the type of punishment.[403]

Based on the above observations, the establishment of a sentencing guideline in Malaysia is necessary in order to ensure that the punishment is proportionate. It is also pertinent for the purpose of maintaining uniformity and certainty. Furthermore, it can be used to differentiate the degree of culpability to ensure that the punishment is fair especially for script kiddies and hackers who commit cyber attacks in order to test their skills.

Malaysian policymakers may refer to the benchmark adopted by the UK's Sentencing Guidelines Council especially in determining the appropriate sentencing for cyber attacks. Judges may use the guideline to detect cyber attacks, to determine the seriousness of cyber attacks and to impose the corresponding sentencing. The elements to the offence of cyber attacks

---

[401] ibid para 1.22 and 1.23

[402] Interview with Deputy Public Prosecutor 1

[403] Interview with Deputy Public prosecutor 2

must be satisfied, whereas the sentencing guideline provides a spectrum of the seriousness of the offences for the purpose of sentencing. Thus, the guideline is a viable solution in dealing with cyber attacks through criminal law. It can be read together with the provisions of the Computer Crimes Act 1997. In addition, this measure may ensure the effectiveness and fairness of the sentencing for cyber attacks.

5.5 Conclusion

This study suggests that criminal law should be used as a reactive measure to counter cyber attacks in Malaysia. It can be argued that the imposition of criminal liability is a realistic option for countries like Malaysia, as it does not possess the military capability and technology to counter cyber attacks. Criminal law is essential in deterring the commission of cyber attacks and denounce the usage of cyberspace, which is against the norms and values of the Malaysian society. It may have not been fully utilised at this moment in dealing with cyber attacks in Malaysia. Non-criminal measures such as strengthening cyber security and preventive justice are more prevalent in countering cyber attacks in Malaysia. This may be due to the constraints of the criminal law in dealing with cyber attacks such as extraterritoriality, production of evidence and technical expertise This study provides suggestions to enhance the function of criminal law to counter cyber attacks in Malaysia.

Firstly, tough sentencing is necessary in order to remind the offenders that cyber attacks are not to be tolerated by society. This study suggests that Malaysia may enhance the effectiveness of the criminal law through the creation of a specific offence for serious cyber attacks. This includes the imposition of heavier punishment for the perpetrator of a large-scale cyber attacks. Therefore, it recommends the promulgation of an offence similar to s 3ZA (1) of the Computer Misuse Act 1990. In addition, the establishment of a sentencing guideline for cyber attacks may ensure certainty, uniformity and fairness of the punishment.

Secondly, this study suggests for the criminalisation of precursor offences including: the possession of materials; and the creation, distribution and

procurement of materials to commit cyber attacks. This is necessary in order to protect the public form actual harm caused by cyber attacks. In addition, these offences are provided under the Cybercrime Convention. They have been implemented in countries such as the UK. Thus, the implementation of this measure may ensure that Malaysia conform to international standards for various reasons such as to attract foreign investment and to strengthen the confidence of trading partners. It also shows that Malaysia is committed to manage the risk of cyber attacks at the international level alongside other members of the international community.

Thirdly, criminal la may be used to persuade the public to report the occurrence of cyber attacks. As indicated previously, the duty to report cyber attacks may be difficult to be implemented in Malaysia due to security reasons or mistrust among local institutions. However, some of the participants in this study argued that this measure is necessary in order to ensure that the perpetrators are brought to justice. In addition, it may prevent the commission of further attacks. Thus, the government should play an active role to persuade the public to report cyber attacks through education and awareness campaigns.

Finally, the function of the technical expertise among the law enforcement officers, prosecutors and judges should be enhanced in dealing with this problem more effectively. This includes more training, motivation and recruiting more cyber security experts. In addition, the creation of a specialist unit similar to the NCA may increase the effectiveness of the criminal law in dealing with cyber attacks.

Chapter 6

Countering Cyber Attacks Under International Law

6.1 Introduction

This chapter investigates the justification for using international law to counter cyber attacks. It analyses the emergence of international norms with regards to cyber attacks. States and non-state actors may commit cyber attacks in the situation of armed conflict and outside of armed conflict. Non-state actors may act independently or collude with states to commit cyber attacks. Besides analysing the actors, the aim of the present chapter is to examine the mechanisms that can be used to counter cyber attacks under international law. This includes the measures provided in the Charter of the United Nations, the principle of state responsibility and international criminal law.

This chapter is divided into several sections. Firstly, it examines the justification for applying international law in countering cyber attacks. Secondly, this chapter explores the main categories of cyber wrongdoings under international law, which include: (1) the prohibition of the use of force and the threat of use of force involving cyber attack; (2) cyber attacks under the law of armed conflict and (3) cyber espionage. Thirdly, this chapter examines the measures to counter cyber attacks at the international and regional level. The conclusion is provided in the last section.

6.2 The Justification for Applying International Law to Counter Cyber Attacks

This section examines the justification for using international law in countering cyber attacks. Norms are necessary in 'understanding the power to mobilise, to justify and to legitimate action'.[1] International legal norms ensure that the international community do or do not engage in a certain

[1] Hurrell A, *On Global Order: Power, Values and the Constitution of International Society* (Oxford University Press New York 2007) 18

state of affairs and course of actions.[2] Thus, the role of international law can be instrumental in countering cyber attacks at the international level. It addresses the fairness and effectiveness of the measures in dealing with cyber attacks. This will be discussed in the following paragraph.

International law emphasises the fairness of the approaches in dealing with cyber attacks. The Charter of the United Nations obliges states to resolve dispute peacefully, to respect the principle of the sovereign equality of states, to refrain from the threat or use of force against the territorial integrity or political independence of any state and not to intervene in the domestic jurisdiction of any state.[3] Consequently, international law should protect the interest of weak states from their stronger counterparts. It may be used as a heuristic devise to discourage states from using cyber attacks to disturb international peace. Moreover, it provides the standard of criticism and means of controlling powerful states.[4] The development of international standard is necessary to balance the interests of states.

Furthermore, the substance of international law is based on humanitarian values. International humanitarian law emphasises compassion, benevolence and preventing unnecessary suffering of the victims of armed conflicts.[5] These values are entrenched in various international agreements and customary principles on the laws of war. International law may deter states. Therefore, states are prohibited from conducting activities in cyberspace contrary to humanitarian values.

Aside from fairness, international law may ensure the effectiveness of the measures to counter cyber attacks. The codification of international criminal law provisions for cyber attacks may eliminate vagueness and create deterrence.[6] It also carries the authority of legitimacy and validates the

---

[2] Lefkowitz D, 'The Principle of Fairness and States' Duty to Obey International Law' 24 Can J L & Jurisprudence 327 2011

[3] Article 2 of the Charter of United Nations

[4] Koskenniemi M, 'What Is International Law For' in Evans MD (ed), *International Law* (4th edn, Oxford University Press 2010) 29

[5] Tasioulas J, 'International Law and the Limits of Fairness' EJIL (2002), Vol 13 No 4, 993–1023

[6] Stevens SR, 'Internet War Crimes Tribunals and Security in an Interconnected

international prosecution of the perpetrators of cyber attacks.[7] Accordingly, international law may be applied to dissuade states from disturbing international peace and security through cyber attacks. In addition, it may be used to standardise the laws and legal process among states in order to curtail trans-national crimes. These issues are addressed in the following sections.

6.2.1 Cyber Attacks as a Threat to International Peace and Security

This thesis considers cyber attacks as a threat to international peace and security. The UN Security Council would have to adopt a resolution to confirm that cyber attacks pose a major threat to peace, breach international peace or involve acts of aggression under Article 39 of the Charter before exercising enforcement measures.[8] The resolution requires unanimous support from the permanent members of the Security Council.[9] The Charter of the United Nations does not provide for the definition of threat to the peace, breach of the peace or act of aggression. The lack of definition was necessary for the purpose of conferring discretionary power on the Security Council.[10] In addition, the list of aggressive acts in the 1974 General Assembly Resolution 3314 is not exhaustive.[11] Aggression presumes the direct and indirect application of the use of force. It always constitutes a breach of peace.[12] Armed conflict between states and civil war are recognised as the paramount threat to the peace. Consequently, cyber attacks in the guise of armed attack may be categorised as a threat to peace. However, it is not clear whether cyber attacks outside of armed

---

World' (2009) 18 Transnat'l L & Contemp Probs 657

[7] ibid

[8] Sands P and Klein P, *Bowett's Law of International Institutions* (5th edn, Sweet & Maxwell London 2001) 51

[9] Article 2(3) of the Charter of the United Nations

[10] Sands P and Klein P, *Bowett's Law of International Institutions* (n 8) 51-52

[11] ibid

[12] Simma B and others (eds), *The Charter of the United Nations: A Commentary*, vol III (3rd edn, Oxford University Press 2012) 1293

conflict could trigger the application of enforcement action under Chapter VII of the Charter of the United Nations.[13]

Some states argue that non-military sources of instability in the fields of economic, social, humanitarian and ecology should be acknowledged as threats to peace and security.[14] This is reflected in the acknowledgement by the General Assembly of the United Nations of the possibilities of information technologies being used for purposes inconsistent with the objectives of maintaining international stability and security.[15] The General Assembly has commissioned three groups of governmental experts to analyse threats in cyberspace and the ways to counter them.[16] Scholars such as Dev suggest the inclusion of non-physical cyber effects in the definition of breach of peace under Article 39.[17] In addition, the leaders of states constantly announce the potential threat of cyber attacks. In 2015, UK Chancellor George Osborne warned of Islamic State's attempts to hack UK's critical infrastructure in order to cause serious harm and to kill people. He claimed that GCHQ is monitoring threats to 450 companies in areas including defence, energy and water supply.[18] Thus, there is potential connection between cyber attacks and international security.

The advancement of technology allows states and non-state actors to sabotage the critical infrastructure of another state by using cyber attacks. For example, it is reported that Ukraine is investigating cyber attacks on its

---

[13] The distinction between cyber attacks as an armed attack and use of force short of armed attack is explained in section 6.3.

[14] Simma B, *The Charter of the United Nations: A Commentary*, vol III (n 12) 1278

[15] 'Resolution adopted by the General Assembly on 2 December 2014' <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/69/28> accessed 11.04.2016; See also Germany: "Report on Developments in the Field of Information and Telecommunications in the Context of International Security" (RES 69/28) <https://unoda-web.s3.amazonaws.com/wp-content/uploads/2015/08/GermanyISinfull.pdf> accessed 11.04.2016;

[16] ibid

[17] Dev RP, '"Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Needs for Formal U.N Response' 50 Tex Int'l L J 381 2015

[18] 'Islamic State is Plotting Deadly Cyber-Attacks - George Osborne' *BBC News UK* (17 November 2015) <http://www.bbc.co.uk/news/uk-34839800> accessed 1 January 2016

power grid allegedly launched by Russian Security Services in December 2015.[19] International law is therefore needed in order to protect states from cyber attacks perpetrated by powerful states. However, it is to be noted that the Security Council is not a frequent enforcer of international law as it is subjected to the veto power of the five permanent members including Russia.[20] The Security Council does not have the obligation to make a determination under Article 39 despite the existence of a threat to or breach international peace.[21] Moreover, the absence of armed forces at its disposal is a major obstacle in addressing breach of international peace and security.

6.2.2 Trans-jurisdictional character of Cyber Attacks

The ability of crime to traverse borders and to evade legal enforcement has been greatly enhanced by the rapid development of communication technology and transportation systems.[22] Crimes in cyberspace span national territories as, the offenders, victims and targets may be physically situated in different countries and regions.[23] States are bound by the principle of state sovereignty, which prohibits them from exercising their policing powers in the territory of another state. Thus, inter-state cooperation in criminal matters and crimes with trans boundary elements have become the focus of international criminal law.[24] For instance, Malaysia's Special Branch Counter Terrorism officers detained Ardit Ferizi, a Kosovo national in September 2015 while he was trying to hack into confidential information about the US Security Forces. Malaysia plans to extradite him to US

---

[19] 'Ukraine to Probe Suspected Russian Cyber Attack On Grid' *The Star Online Tech News* (1 January 2016) <http://www.thestar.com.my/tech/tech-news/2016/01/01/ukraine-to-probe-suspected-russian-cyber-attack-on-grid/> accessed 2 January 2016

[20] Crawford J, 'Sovereignty as Legal Value' in Crawford J and Koskenniemi M (eds), *The Cambridge Companion to International Law* (Cambridge University Press 2012) 125

[21] Simma B, *The Charter of the United Nations: A Commentary* (n 12) 1275

[22] Broomhall B, *International Justice and the International Criminal Court: Between Sovereignty and the Rule of Law* (Oxford University Press 2004) 10-11; see also Wilkitzki P, 'Development of an Effective International Crime and Justice Programme-A European View' in Eser A and Lagodny O (eds), *Principles and Procedure for a New Transnational Criminal Law* (Freiburg im Breisgau 1992) 270

[23] Yar M, *Cybercrime and Society* (SAGE Publications Ltd London 2006) 16

[24] Broomhall B, *International Justice and the International Criminal Court: Between Sovereignty and the Rule of Law* (Oxford University Press 2004) 10

following the completion of necessary procedures.[25] Another example is the extradition of Babar Ahmad, a British cyber–jihadist to the US for supporting terrorism through the Internet.[26]

The association of criminals and organised crime rings across the borders is one of the factors that lead to the rise of transnational crime. Barak argues that harms have been 'transnationally invented and or reinvented as their new forms of crime and violence represent reconfigured social relations or acts involving perpetrators and victims located in, or operating through more than one country'.[27] Similarly, Kartha contends that the link between various non-states actors of different antagonistic groups across international borders leads to the proliferation of light weapons in South East Asia.[28] In addition, criminal behaviours have been transformed by the globalisation of crime opportunities and the rise of 'lone offenders who are enabled by networks technology to carry out incredibly complex and far-reaching tasks'.[29] Likewise, the connection between hackers in different countries has contributed to an alarming rate of cyber attacks in recent years. One of the participants in this study revealed the occurrence of several attacks committed by a group of hackers who called themselves as the Anonymous Malaysia.[30] The member of this group claimed that they are a part of the Anonymous United States.

---

[25] Zolkepli F, 'Long Wait to Extradite Hacker' *The Star Online* (18 October 2015) http://www.thestar.com.my/news/nation/2015/10/18/long-wait-to-extradite-hacker/ accessed 1 January 2016

[26] *Case Of Babar Ahmad And Others v. United Kingdom* Applications nos. 24027/07, 11949/08, 36742/08, 66911/09 and 67354/09 (ECtHR, 10 April 2012)

[27] Barak G, 'Towards an Integrative Study of International Crimes and State-Corporate Criminality: A Reciprocal to Gross HUman Rights Violations' in Smeulers A and Haveman R (eds), *Supranational Criminology: Towards a Criminology of International Crimes* (Intersentia 2008) 53

[28] Kartha T, 'Trans-national Crime and Light Weapons Proliferation: Security Implications for the State' <https://www.idsa-india.org/an-dec9-3.html> accessed 7.04.2016

[29] Wall DS, 'The Internet as a Conduit for Criminal Activity' in Pattavina A (ed), *Information Technology and the Criminal Justice System* (SAGE Publications 2005) 79-80

[30] Interview with Police Officer 3

Standardisation of laws and legal processes is a fair and effective way to counter trans-jurisdictional cyber attacks. This measure may curtail the acceleration of trans-national crimes.[31] This includes the process of extradition, the request for mutual legal assistance, an equivalent standard of proof and rules of evidence. The preservation of electronic evidence and data at the national level may be done within the framework of international cooperation. This is necessary due to the volatility of electronic evidence and the data may be transmitted through servers in several countries.[32]

Many states do not have sufficient capacities to tackle Internet related crimes.[33] They lack the capacity to investigate and to establish legal mechanisms to address international crimes.[34] Devising innovative strategies to enforce the law and the machinery to coordinate the development of policy in relation to trans-jurisdictional crime can solve this problem.[35] For instance, it was reported that the Justice Department of the US is planning to station a legal adviser in Malaysia in order to help the South East Asian countries to develop the laws and tools to fight hackers.[36] A regional Digital Counter-Messaging Communications Centre will be set up in Malaysia to deal with cross border hacking activities especially hackers who elude American prosecution.[37] In addition, states that have not acceded to the Cybercrime Convention including Malaysia may consider entering into bilateral agreement with a state party to the Cybercrime Convention.[38] This

---

[31] Elfstrom G, *International Ethics: A Reference Handbook* (ABC-CLIO 1998) 51

[32] Council of Europe, 'International Co-operation Under the Convention on Cybercrime'<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304352> accessed 3 January 2016

[33] Yar M, *Cybercrime and Society* (n 23) 17

[34] Elfstrom G, *International Ethics: A Reference Handbook* (n 31) 49

[35] Broomhall B, *International Justice and the International Criminal Court: Between Sovereignty and the Rule of Law* (n 24) 10-11

[36] Zolkepli F, 'Long Wait to Extradite Hacker' *The Star Online* (n 25)

[37] ibid

[38] Malaysia has not acceded to the Convention on Cybercrime. So far, only one member of ASEAN, which is the Philippines, acceded to the convention.

would enable them to request for assistance during investigation such as the preservation of stored computer data and the production of data.[39]

The standardisation of the law and legal process at the international level depends on cooperation among states. For instance, in *Babar Ahmad & Ors v United Kingdom*, the ECtHR decided that removal of detainees to countries that had a long history of respect of democracy, human rights and rule of law rarely violate Article 3 of the Convention except for crimes involving death penalty. Thus, the surrender of fugitives through extradition is accompanied by a guarantee that they are not to be subjected to death penalty or degrading treatment. The borderless nature of the cyberspace challenges the application of international law in terms of requiring consensus on what constitute cybercrime and how to punish the perpetrators.[40] Overcoming political hurdles is the key to successful implementation of the international legal framework. Recently US and China jointly denounced the resort to cyber attacks especially cyber espionage and cyber-enabled theft of intellectual property.[41] This signifies their willingness to compromise and to formulate common understanding in fighting cyber attacks.

To summarise, the application of international law is necessary due to the seriousness of the threat of cyber attacks to international peace and the trans-jurisdictional character of cyber attacks. The trans-jurisdictional character of cyber attacks means that nation states cannot counter this threat alone and international cooperation is essential. Therefore, the purpose of this chapter is to analyse the position of cyber attacks under international law and the measures used to address this problem. It also assesses the fairness and effectiveness of the actions in dealing with cyber attacks at the international level. The following section evaluates the extent to which cyber attacks are covered by the current international norms, particularly the use of force, the law of armed conflicts and cyber espionage.

---

[39] Article 16 Council of Europe Convention on Cybercrime

[40] Etzioni A, *From Empire to Community: A New Approach to International Relations* (Palgrave Macmillan 2004) 150

[41] Bejtlich R, 'To hack, or not to hack?' (*The Brookings Institution*, 28 September 2015) <http://www.brookings.edu/blogs/up-front/posts/2015/09/28-us-china-hacking-agreement-bejtlich> accessed 16 May 2016

6.3 Cyber Attacks Under International Law

The advancement of modern warfare especially cyber attacks targeting enemy infrastructures raises legal issues particularly in the application of the rules governing use of force and international humanitarian law. Scholars such as Roscini claim that the extension of existing rules and principles to cyber operations might be too general due to the failure to consider their uniqueness.[42] Similarly, the ICRC argues that, 'applying pre-existing legal rules to a new technology raises the question of whether the rules are sufficiently clear in light of the technology's specific characteristics, as well as with regard to the foreseeable humanitarian impact it may have'.[43] Erki Koda claims that international customary law does not deal with cyber attacks due to the lack of state practice and opinion juris.[44] Another scholar, Ruth Wedgewood contends that the current law of armed conflict is not suitable for electronic warfare.[45] Others suggest the designation of a specific standard or a new legal framework for cyber attacks in order to clarify their position under international law.[46] In the light of these contentions, this chapter investigates the extent to which international law deals with cyber attacks.

In general, many scholars acknowledge the applicability of international law to acts committed by states and non-state actors in cyberspace. They argue that existing international law norms prohibit state activities in cyberspace that cause certain effects.[47] Rubin asserts that the provisions of the 1949

---

[42] Roscini M, *Cyber Operations and the Use of Force in International Law* (Oxford Univerity Press 2014) 23

[43] 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (*The Red Cross and The Red Crescent*, 2011) <http://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf> accessed 10 March 2014

[44] Kodar E, 'Computer Network Attacks in the Grey Areas of Jus Ad Bellum and Jus In Bello' (2009) 9 Baltic YB Int'l L 133

[45] Wedgwood RG, 'Proportionality, Cyberwar, and the Law of War' (2002) 76 Int'l L Stud Ser US Naval War Col 219

[46] Stevens SR, 'Internet War Crimes Tribunals and Security in an Interconnected World' (n 6); Hollis DB, 'Why States Need An International Law For Information Operations' 11 Lewis & Clark L Rev 1023 2007

[47] Tubbs D, Luzwick PG and Sharp WGS, 'Technology and Law: The Evolution of

Geneva Conventions are applicable to 'all struggles for authority that turn violent' as they are regarded as 'definitive formulations of the substantive law binding as matter of general practice accepted as law even if not expressly accepted by formal ratification'.[48] The Tallinn Manual rejects the argument that new treaty law is necessary just because international law is largely silent on cyberspace.[49] The 2015 Group of Governmental Experts on Development in the Field of Information and Telecommunications in the Context of International Security acknowledges the application of the principle of state sovereignty and international norms that flow from sovereignty to ICTs related activities and infrastructure within states.[50] A state has the capacity to exercise state functions in its territory to the exclusion of other states and the ability to enter into binding agreement under international law.[51] Nevertheless, the elaboration of concepts for international peace and security in the use of ICTs at the legal, technical and policy level may be necessary to preserve the free and secure flow of information.[52] Therefore, following sections begin with the examination of the prohibition of the threat or use of force involving cyber attacks. Next, it reviews the application of the international humanitarian law to cyber attacks. Finally, this study analyses the extent to which international law is applicable to cyber espionage.

Digital Warfare' in Schmitt MN and O'Donnell BT (eds), *Computer Network Attack and International Law* (Naval War College Newport, Rhode Island 2002) 15

[48] Rubin AP, *Ethics and Authority in International Law* (Cambridge University Press 1997) 171

[49] Schmitt MN (ed), *Tallinn Manual on the International law Applicable to Cyber Warfare* (Cambridge University Press 2013) 3

[50] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (2015) <http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174> accessed 14 April 2016

[51] Crawford J, 'Sovereignty as Legal Value' (n 20) 1313-132; see also Declaration on Principles of International Law Concering Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations, A/Res/25/2625

[52] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (n 50)

6.3.1 Cyber Attacks and the Use of Force

This section examines the prohibition of the threat or use of force involving cyber attacks. States are obliged to refrain from the threat or use of force against the territorial integrity or political independence of any state under international law.[53] Nonetheless, they may exercise the right of individual or collective self-defence against armed attack by other states until the Security Council takes necessary measures.[54] Some authors suggest that that Article 2(4) of the Charter of the United Nations was never intended to address attacks against computer systems.[55] Opinion diverges widely as to whether or not information operations constitute a use of force and an armed attack for self-defence.[56] In the *Nuclear Weapons case*, the ICJ held that the Charter of the United Nations does not refer to specific weapons. Accordingly, the prohibition of the use of force is applicable regardless of the choice of weapons.[57] There is a growing consensus among states and scholars on the application of existing international law to activities conducted by states in cyberspace.

Several issues arise concerning the usage of cyber attacks by one state against another state. Firstly, can cyber attacks amount to use of force within the ambit of Article 2(4) of the Charter of the United Nations? Secondly, can cyber attacks constitute an armed attack to enable states to exercise the right of self-defence under Article 51 of the Charter of the United Nations? Thirdly, are states permitted to resort to force in self-defence if the cyber attacks are not carried out by or on behalf of a state? These issues will be discussed in the following sections.

---

[53] Article 2 (4) United Nations Charter

[54] Article 51 United Nations Charter

[55] Buchan R, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 J Conflict Security Law 211; see also Waxman MC, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 Yale J Int'l L 421

[56] Hollis DB, 'Why States Need An International Law For Information Operations' 11 Lewis & Clark L Rev 1023 2007

[57] *Legality of the Threat or Use of Nuclear Weapons,* ICJ Report 1996

6.3.1.1 Prohibition Against Use of Force Under Article 2(4) of the Charter of the United Nations

The clarification of the degree of gravity of the use of force is crucial to prevent states from classifying any criminal activity into a war and responding with high levels of force.[58] This is to avoid states from justifying the usage of violence under the pretext of self-defence in response to broad range of hostile and destructive physical acts.[59] In *Nicaragua v United States*, the International Court of Justice (ICJ) divided force into the gravest form that amount to armed attack and less grave forms.[60] The former is defined as not only action by regular armed forces across an international border, but additionally the sending by or on behalf of a state of armed bands or groups which carry out acts of armed force of such gravity as to amount to an actual armed attack conducted by regular armed forces or its substantial involvement. The ICJ further clarified that the scale and effect played a role in determining what constitutes an armed attack.[61] The term comprises: (1) the threat or use of force to violate the existing international boundaries of another State; (2) acts of reprisal involving the use of force; (2) forcible action which deprives peoples of equal rights and self-determination, freedom and independence; (3) organising or encouraging the organization of irregular forces or armed bands, including mercenaries, for incursion into the territory of another State; (4) organising, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts.[62] The distinction of different forms of force is necessary as the right of self and collective defences can only be exercised

---

[58] '"Between a Drone and Al-Qaeda": The Civilian Cost of US Targeted Killings in Yemen' (*Human Rights Watch*, 2013) <http://www.hrw.org/reports/2013/10/22/between-drone-and-al-qaeda-0> accessed 9 February

[59] Silver DB, 'Computer Network Attack as a Use of Force under Article 2(4)' in Schmitt MN and O'Donnell BT (eds), *Computer Network Attack and International Law* (Naval War College Newport, Rhode Island 2002) 83

[60] *Nicaragua v United States* ICJ Report 1986 paragraph 191

[61] ibid paragraph 195

[62] General Assembly Resolution 2625, Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations

in response to acts which constitute armed attack.[63] Nevertheless, the victim states are also permitted to adopt non-forcible and proportionate countermeasures in response to force short of armed attacks. The ICJ does not provide further clarification with regard to what exactly constitutes force short of armed attack. However, the Court acknowledges that this category includes supplying arms and other support to armed rebel.[64] Cyber attacks should potentially constitute an armed attack before states are enabled to exercise the right of self-defence under Article 51 of the Charter of the United Nations.[65] Apart from scale and effects, there is ambiguity in the criteria under which force amounts to armed attack.

The use of force amounting to armed attack can be interpreted in three ways.[66] Firstly, the instrumentality approach emphasises that force should resemble the traditional physical characteristics of military coercion, and, as such, the interruption of telegraphic, radio and other means of communications do not qualify as armed force.[67] Secondly, the target - based approach provides that attack on critical national infrastructure constitutes use of force notwithstanding the existence of destruction or casualties.[68] Thirdly, the consequentiality approach stresses that the effects of the attacks should be similar to kinetic force which include death or destruction of property.[69] Most scholars reject the application of second approach, as the presence of destruction or casualties is necessary for armed force.[70] So, this thesis examines the first and third approaches in

---

[63] *Nicaragua v United States* (n 60) 210

[64] ibid

[65] Hathaway OA and others, 'The Law of Cyber-Attack' 100 Calif L Rev 817

[66] Hollis DB, 'Why States Need An International Law For Information Operations' (n 56)

[67] ibid

[68] ibid

[69] ibid

[70] Melzer N, 'Cyberwarfare and International Law' (*UNIDIR*, 2011) <http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf> accessed 7 March 2014; Schmitt, *Tallinn Manual* (n 49) 48-51; Jupillat N, 'Armed Attacks in Cyberspace: The Unseen Threat to Peace and Security that Redefines the Law of State Responsibility' University of Detroit Mercy Law Review, Vol 92, No 2, 2015

determining the position of cyber attacks under Article 2(4) of the Charter of the United Nations.

The first approach is supported by resolutions adopted by the General Assembly including the 1970 Declaration on Friendly Relations, the 1974 Declaration on Aggression and the 1987 Declaration on the Use of Force.[71] This approach gives force a narrow scope, virtually limited to armed operation.[72] According to Silver, armed force as stipulated in Article 2(4) refers to the usage of instruments capable of producing violent effects (weapon) by states to exert coercion on another state.[73] 'Weapon' is defined as an instrument designed to injure, kill or to destroy property.[74] Hence, information operations such as shutting down civilian air traffic communication system, downing civilian aircraft and whereby killing hundreds of people may not qualify as use of force.[75] The incapacitation of computer networks and Internet equally may not amount to use of force under the first approach.

The consequentiality approach or direct effect approach provides that cyber attacks must cause direct destructive effects on property and persons equivalent to kinetic weapons to fall within the ambit of armed force.[76] Cyber attacks involve the manipulation of the vulnerabilities of the computer system, which are connected electronically to other system. This is done for the purpose of introducing malicious computer code into the computer system or network in furtherance of various ulterior motives.[77] The impact of cyber attacks can be divided into three categories: (1) the deletion,

---

[71] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 46

[72] ibid 45

[73] Silver DB, 'Computer Network Attack as a Use of Force under Article 2(4)' in Schmitt MN and O'Donnell BT (eds), *Computer Network Attack and International Law* (n 59) 84

[74] Brown D, 'A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict' (2006) 47 Harv Int'l LJ 179

[75] Hollis DB, 'Why States Need An International Law For Information Operations' (n 56)

[76] ibid 48

[77] Silver DB, 'Computer Network Attack as a Use of Force under Article 2(4)' in Schmitt MN and O'Donnell BT (eds), *Computer Network Attack and International Law* (n 59) 77

corruption or alteration of data or software of the attacked computer or the disruption of the computer system; (2) the partial or total incapacitation or destruction of the infrastructure operated by the attacked system; and (3) the loss of life or injury to persons due to the destruction or incapacitation of the infrastructure such as power plant due to cyber attacks.[78] Based on the direct effects approach, cyber attacks may amount to armed force if they cause physical destruction or incapacitation of property and consequently, causing the loss of life or injury to persons.

The direct effect approach has been applied by the group of experts in the formulation of the Tallinn Manual. [79] In the commentary, the group of experts stipulate that manipulation of Supervisory Control and Data Acquisition System (SCADA) to release dam waters resulting in the destruction to property, injury and deaths is an example of cyber attack.[80] The group of experts considered the infiltration of computer system by using malware tantamount to an attack once they are activated.[81] The assessment adopted in the Manual is similar with the instrument-based approach suggested by Graham.[82] This model is used to establish whether the damage caused by cyber attacks is similar to a kinetic attack.[83] Schmitt argues although cyber operations are considered as non-kinetic force, they may cause severe destruction and trigger the existence of international armed conflict.[84] Any operations, which lead to violent consequence, can be classified as an armed attack within the ambit of the law of armed conflict.[85]

As stated above, the scale and effect of force is important in determining the existence of armed attack. A series of minor attacks is not sufficient to

---

[78] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 53

[79] Schmitt MN, *Tallinn Manual* (n 49) 47

[80] ibid 107

[81] ibid 109

[82] Graham DE, 'Cyber Threats and the Law of War' (2010) 4 J. Nat'l Sec L. & Pol'y 2010 87

[83] ibid

[84] Schmitt MN, 'Classification of Cyber Conflict' (2012) 17 J Conflict Security Law 245

[85] ibid

constitute an armed attack.[86] In the commentary to the Tallinn Manual, the group of experts acknowledged that the law does not clearly indicate the extent to which death, injury or damage qualify as an armed attacks.[87] In *Nicaragua v United States*, ICJ held that certain incidents such as the laying of mines in internal or territorial waters, attacks in ports, oil installations and a naval base amount to the use force.[88] But, the ICJ does not provide further explanation of the gravity of harm or scale of attacks required for armed attacks. A majority of the members of the group of experts of the Tallinn Manual contend that cyber attacks in Estonia in 2006 were not classified as armed attack as these incidents did not reach the required threshold of the scale and effects.[89] They did not consider cyber activities such as cyber intelligence, cyber theft and brief or periodic interruption of non-critical cyber infrastructures amount to armed attacks. [90] However, some of them accepted that the stuxnet attacks on the Iranian nuclear reactor in 2010 had reached the level of armed attack due to the damage caused to the Iranian centrifuges.[91] This demonstrates that the incapacitation or destruction of a single critical infrastructure may be categorised as an armed attack. Nonetheless, recent attacks demonstrate cyber attacks have so far caused economic harm. Thus, the consequential approach leaves unregulated the very aspect that makes it so novel which is economic violence.[92]

Some scholars argue that the notion of armed force within the ambit of Article 2(4) should be interpreted broadly to include non-physical damage.[93] In the Tallinn Manual, the group of experts agreed that there is ambiguity with regard to 'actions that do not result in injury, death, damage or

---

[86] House of Lords House of Common Joint Committee on Human Rights, 'The Government's Policy on the Use of Drones for Targeted Killing. Second Report of Session 2015–16' (House of Lords and House of Commons, 2016)

[87] Schmitt MN, 'Classification of Cyber Conflict' (n 84)

[88] *Nicaragua v United States* (n 60) 227

[89] Schmitt MN, *Tallinn Manual* (n 49) 58

[90] ibid 55

[91] ibid 58

[92] Hollis DB, 'Why States Need An International Law For Information Operations' (n 56)

[93] Dev PR, "Use of Force" and "Armed Attack" Thresholds in Cyber Conflict (n 17)

destruction, but which otherwise have extensive negative effects'.[94] Dev argues that the adoption of the threshold based on the impact of a kinetic weapon within the ambit of the law of armed conflict, as suggested by the Tallinn Manual is not attainable due to several reasons.[95] Firstly, physical destruction or harm can only be discerned when kinetic weapons are used.[96] Secondly, 'in the cyber context, where attribution itself presents a complication, the physical harm or damage presents a more attenuated, proximate cause rather than a direct cause'.[97] The expansion of the notion of harm is perceived as necessary in order to tackle difficult issues such as whether the deletion, alteration or corruption of data is equivalent to physical property within Article 2(4).[98] Dev proposes examining the immediate financial repercussion and the total cost due to the loss of network connectivity to determine the violation of Article 2(4).[99]

Apart from economic harm, some scholars emphasise the impact of cyber attacks to the broader well-being of the society. Roscini argues that cyber operations fall within the ambit of Article 2(4) 'if the disruption caused is significant enough to affect state security or welfare of the nation'.[100] Article 2(4) should be interpreted to include factors such as the reliance of states on computer systems and network in providing critical service for the public.[101] Tsagourias contends that the manipulation of economic data could jeopardise a state's economic and political stability, although it does not cause instantaneous death or destruction.[102] In the light of these arguments, cyber attacks challenge the perceptions of the notion of harm associated with the use of force under international law. Unfortunately until now there

---

[94] Schmitt MN, *Tallinn Manual* (n 49) 56

[95] Dev PR, '"Use of Force" and "Armed Attack" Thresholds in Cyber Conflict (n 17)

[96] ibid

[97] ibid 390

[98] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 55

[99] Dev PR, '"Use of Force" and "Armed Attack" Thresholds in Cyber Conflict (n 17)

[100] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 55

[101] ibid 59

[102] Tsagourias N, 'The Tallinn Manual on the International Law Applicable to CyberWarfare: A Commentary on Chapter II—The Use of Force' in Gill TD (ed),

has not been adequate state practice to support or clarify the inclusion of non-physical harm in the use of force.

Although the adoption of a broader definition of force might be worthwhile for cyber attacks, in reality states are reluctant to extend non-physical damage within the realm of Article 2(4). This is based on the rejection of the inclusion of political and economic pressures within the ambit of Article 2(4) during the drafting of the Charter of the United Nations.[103] Caytas argues that 'manipulation of economic information and price levels, manipulation of the flow of political information or economic intelligence all fall short of sabotage in the proper sense that many will consider to qualify as an openly hostile act'.[104] The exclusion of economic damage due to cyber attacks from the ambit of force has necessitated a search for alternative recourse under international law.

This thesis demonstrates the difficulty in classifying as armed attack the non-disruptive effects of cyber attacks under international law, especially disruption to the economy. Should they be classified as force short of armed attack or unlawful intervention? It has been suggested military response may be used to deal with cyber operations that do not qualify as armed attack.[105] In the *Nicaragua Case,* the US was allegedly using indirect force through support of Contras during the armed intervention in Nicaragua.[106] Although they are not directly destructive, those activities are related to the use of weapons as they aim at enabling someone to use them.[107] Consequently, the supply of malware and training to carry out cyber attacks in the guise of armed attack could qualify as use of force short of armed attack.[108]

Year Book of International Humanitarian Law 2012 (15th edn, T.M.C. Asser Press)

[103] Harris D, *Cases and Materials on International Law* (7th edn, Sweet and Maxwell 2010) 723-724

[104] Caytas JD, 'Cyber Warfare as a Superficially Tempting Low-Level Engagement Strategy' <http://ssm.com/abstract=2348842> accessed 20 June 2016

[105] Schmitt MN, '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law' [2014] Virginia Journal of International Law 54

[106] *Nicaragua v United States* (n 60)

[107] Silver DB, 'Computer Network Attack as a Use of Force under Article 2(4)' (n 59) 84

[108] Schmitt MN, *Tallinn Manual* (n 49) 47

However, some element of violence is arguably necessary even for force short of armed attack. Thus, the disruption of the computer system of stock exchange and financial institutions for the purpose of causing economic harm may not be categorised as force short of armed attack.

The next issue is the determination of economic damage caused by cyber attacks as unlawful intervention.[109] The principle of non-intervention entails that a state has the right to conduct its affairs without outside interference.[110] Unlawful intervention occurs when states are coerced to do things against their own volition.[111] In the *Nicaragua Case*, the ICJ decided that the US contravened the principle of non-intervention under customary international law by supplying funds to the contras to wage war against Nicaragua.[112] This means that the assertion of economic pressure in order to affect change of government of another state may be classified as unlawful intervention. However, history suggests that economic interferences happen routinely among states. States frequently interfere in each other's economies through various means, including devaluing their currencies or imposing tariffs on imports. These actions entail some form of repercussion to the economy of another state. Thus, cyber attacks that incapacitate or interrupt the economy of another state could violate the obligation not to intervene in the affairs of another state, depending on the harm caused. States may initiate measures outside the scope of armed self-defence, such as countermeasures within the perimeter permitted by international law, in response to these attacks. Apart from unlawful intervention, states may be subjected to economic damages due to terrorism and cyber espionage. The impact of cyber attacks in the guise of terrorism is discussed in the previous chapter. This chapter shall return to the question of cyber attacks in the guise of cyber espionage in the subsequent section.

---

[109] Article 2(7) of the Charter of United Nations provides that United Nations shall not intervene in domestic jurisdiction of Members unless the matter falls within the enforcement measures under Chapter VII

[110] Gray C, 'The Use of Force and International Legal Order' in Evans MD (ed), *International Law* (4th edn, Oxford University Press 2010)

[111] Tsagourias N, 'The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II—The Use of Force' in Gill TD (ed), *Year Book of International Humanitarian Law 2012* (n 102)

[112] *Nicaragua v United States* (n 60) paragraph 227

6.3.1.2 The Right of Self-Defence Under Article 51 of the Charter of the United Nations

The second issue is to examine the exercise of the right of self-defence under Article 51 of the Charter of the United Nations in the context of cyber attacks. As demonstrated earlier, cyber attacks by a state that cause injury or death or destruction of property of another state might qualify as armed attack to trigger the application of the right of self-defence. The majority of the members of the group of experts in Tallinn Manual contend that anticipatory self-defence can then be exercised against imminent cyber attacks in the context of armed attacks. They propose the adoption of the 'last feasible window of opportunity standard' in exercising anticipatory self-defence. This standard entails that 'a state may act in anticipatory self defence against an armed attack whether cyber or kinetic when the attacker is clearly committed to launching an armed attack and the victim state will lose its opportunity to effectively defend itself unless it acts.'[113] Actions taken on the basis of self-defence are subjected to the requirements of necessity and proportionality. The response must not exceed the scale, scope, duration and intensity required to end the armed attack.[114] States are not permitted to resort to cyber attacks equivalent to kinetic weapon if passive cyber defences such as firewall can be used to thwart the attacks.

6.3.1.3 Self-Defence Against Non-State Actors

The final issue is to assess whether states can invoke the right of self-defence against cyber attacks by non-state actors situated within a foreign country. In *Congo v Uganda* case, ICJ found that where armed force cannot be attributed to a state, there is no right of self-defence against the accused sponsoring state.[115] States are expected to deal with non-state actors through domestic law enforcement instead of military action.[116] However, experts continue to divide over when states may lawfully resort to force in self-defence if the armed attack was not carried out by or on behalf of a

---

[113] Schmitt MN, *Tallinn Manual* (n 49) 64-65

[114] ibid 62

[115] *Congo v Uganda*, I.C.J Reports 2005, 148-165

[116] Hollis DB, 'Why States Need An International Law For Information Operations' (n 56)

state.[117] A majority of scholars assert that this right has increasingly been accepted by states.[118] Trapp argues that the decision of the ICJ in *Congo v Uganda* should not be read as absolutely precluding a use of force in foreign territory against armed non-state actors.[119] The unwillingness and inability of the host state to prevent and suppress international terrorism allows states to resort to defensive force against non-state actors.[120] The requirement for consent does not operate in these circumstances.[121] A state may exercise the right of self-defence to address an imminent or actual armed attacks by non-state actors.[122] This position is supported by states including the UK. [123] The continuous attacks on ISIL in Syria have led some to argue that the 'unwilling or unable' test to be crystallised into customary international law.[124] However, the use of force in self-defence must be proportionate and adhere to the principle of necessity. It must be necessary in order to prevent immediate threat of a terrorist attack of a suitable scale of threat. The use of force for self-defence should not be extended to lower-level terrorists attacks.[125] States should be unable to wait for the Security Council to act

---

[117] Thorp A, 'Drone Attacks and the Killing of Anwar al- Awlaqi: Legal Issues' (*International Affairs and Defence Section, House of Commons Library*, 20 December 2011) <http://www.parliament.uk/business/publications/research/briefing-papers/SN06165/drone-attacks-and-the-killing-of-anwar-alawlaqi-legal-issues> accessed 9 February 2014

[118] Schmitt MN, *Tallinn Manual* (n 49) 58-59; Paust JJ, 'Self Defense Targettings of Non-State Actors and Permissibility of U.S Use of Drones in Pakistan' 19 J Transnat'l L & Pol'y 237 2009-2010

[119] Trapp KN, 'Back to Basics: Necessity, Proportionality, and the Right of Self-Defence against Non-State Terrorist Actors' The International and Comparative Law Quarterly, Vol 56, No 1 (Jan, 2007), pp141-156

[120] ibid

[121] Bethlehem D, 'Self-Defense Against an Imminent or Actual Armed Attack by Non-state Actors' The American Journal of International Law, Vol 106, No 4 (October 2012), pp769-777

[122] ibid

[123] House of Lords House of Common Joint Committee on Human Rights, 'The Government's Policy on the Use of Drones for Targeted Killing. Second Report of Session 2015–16' (House of Lords and House of Commons, 2016)

[124] Flasch O, 'The Legality of the Air Strikes Against ISIL in Syria: New Insights on the Extraterritorial Use of Force Against Non-State Actors' Journal on the Use of Force and International Law, 2016 Vol 3, No 1, 37–69

[125] Odle J, 'Targeted Killings in Yemen and Somalia: Can the United States Target Low-Level Terrorists?' 27 Emory Int'l L Rev 603 2013

due to urgency of the situation. Non-fulfilment of this requirement would render the use of force as extrajudicial killing, which is forbidden under the human rights law. [126]

This view has been adopted to support targeted killings in response to terrorists' activities including recent cyber attacks conducted by non-state actors. Firstly, Junaid Hussain, a British-born Islamic State hacker, was killed in a US airstrike against ISIS in Raqah Syria.[127] He is believed to have helped Islamic State to establish attach cyber capabilities. Secondly, Siful Haque Sujan, a Cardiff based businessman who became computer hacker for ISIS was killed in a US-led coalition air strike in Raqah Syria.[128] Even so, uncertainty remains, as these events are not conclusive to indicate that the right of self-defence can be invoked against cyber attacks perpetrated by non-state actors. Some argue that imminent cyber attacks by non-state actors did not pass the threshold of armed attacks required under Article 51.

The ICRC considers extraterritorial use of force is governed by international humanitarian law or international human rights law and domestic law depending on the existence of armed conflict or not. [129] Due to the uncertainty of the invocation of the right of self-defence against non-state actors, the validity of the targeted killings of the perpetrator of cyber attacks outside of armed conflict may be determined by examining the domestic legal standard and human rights law. The lawfulness of the enforcement action is assessed based on several factors: (1) the use of force must be absolutely necessary; (2) the nature of threat; (3) the danger of imminent

---

[126] Ambos K and Alkatout J, 'Has 'Justice Been Done'? The Legality of Bin Laden's Killing Under International Law' 45 Isr L Rev 341 2012

[127] Ackerman S, MacAskillin O and Rose A, 'Junaid Hussain: British hacker for Isis believed killed in US air strike' *The Guardian* (27 August 2015) <http://www.theguardian.com/world/2015/aug/27/junaid-hussain-british-hacker-for-isis-believed-killed-in-us-airstrike> accessed 16 May 2016

[128] Burman J, 'British-Trained Islamic State Computer Hacker Wiped Out in Drone Strike' *Daily Express* (30 December 2015) <http://www.express.co.uk/news/world/630468/Islamic-State-ISIS-Siful-Haque-Sujan-US-America-Pentagon-Drone-Strike-Britain-Cardiff> accessed 16 May 2016

[129] House of Commons Defence Committee, 'Remote Control: Remotely Piloted Air System Current and Future UK Use', Tenth Report of Session 2013-14

attacks; (4) the absence of other countermeasures; (5) and lastly, the surrounding circumstances including planning and control.[130]

6.3.2 Cyber Attacks and the Law of Armed Conflicts

The aim of this section is to scrutinise the application of the law of armed conflicts to cyber attacks conducted by states. Cyberspace has been recognised as a potential battlefield due to the increase of cyber attacks launched by states.[131] Besides strengthening national cyber security, states are focusing on the establishment of cyber military units and military manual for cyber attacks.[132] Cyber warfare is perceived as a specialised form of military operation. Cyber force is established to conduct defensive and offensive operations in cyber battlefield. Cyber warfare differs from traditional military threats and shall be explained next.[133] For that reason, the UK's Defence Secretary, Philip Harmond announced the recruitment of computer experts as cyber reservist to enhance military capability in dealing with cyber operations. The Joint Cyber Reserve will work together with regular forces to protect UK's critical computer networks and vital data.[134] Other countries such as US have commissioned their soldiers to undergo basic cyber training.[135] The US Air Force has extended its operation to cyberspace by establishing the cyber military force under its 8th Air Force division.[136]

---

[130] *McCann & Ors v United Kingdom* (application no 18984/91)*; Armani Da Silva v United Kingdom* (application no 5878/08)

[131] Solce N, 'The Battlefield of Cyberspace: The Inevitable New Military Branch-the Cyber Force' 18 Alb LJ Sci & Tech 293

[132] The Tallinn Manual was prepared by an international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. The purpose of the Tallinn Manual is to provide clarity on the legal issues surrounding cyber operations specifically concerning the International Humanitarian Law and the law on the use of force.

[133] Dunlap CJ, 'Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors' 87 Neb L Rev 712

[134] Gov. UK, 'New Cyber Reserve Unit Created' <https://www.uk/government/news/reserves-head-up-new-cyber-unit> accessed 9 May 2014

[135] Meer H, 'Lessons from Anonymous on Cyberwar' (*Aljazeera*, 10 March 2011) <http://www.aljazeera.com/indepth/opinion/2011/03/20113981026464808.html> accessed 13 January 2014

[136] Solce N, 'The Battlefield of Cyberspace' (n 131)

According to Cavelty, cyberwar is a new form of command and control warfare targeting the opponent's military control. Military operations are conducted based on information-related principles, which aims to destroy and disrupt the adversaries' communication system. States may endorse the usage of ICTs for offensive or defensive purpose 'to immediately intrude, or control the opponent's resources' within the informational environment. The agents and targets come from physical and non-physical domains and the level of violence varies upon circumstances.[137] The manipulation and degradation of the information system of the critical infrastructures resulted in significance political and military advantage in comparison to physical destruction caused by kinetic weapons.[138]

The provisions of the Geneva and Hague Conventions as well as customary international law are applicable to military activities in cyberspace.[139] In the *Nuclear Weapons Case*, the ICJ held that the law of armed conflict applies to all forms of warfare and weapons.[140] The objectives of the international humanitarian law are to protect the victims of war and to regulate the means and methods of warfare.[141] These are provided in various treaties including the four Geneva Conventions 1949 and their Additional Protocols of 1977. The application of treaties regulating the aspects of warfare depends on the classification of the armed conflicts. The four Geneva Conventions of 1949 and Additional Protocol 1 of 1977 are applicable during situation of international armed conflicts. In comparison, non-international armed conflicts are governed by a rudimentary regime, which consists of among others Common Article 3 of the four Geneva Conventions of 1949 and Additional Protocol 2 of 1977. Henckaerts and Doswald-Beck argues that

---

[137] Taddeo M, 'Information Warfare: A Philosophical Perspective' (2012) 25 Philos Technol (2012) 25:105–120

[138] Tubbs D, Luzwick PG and Sharp WGS, 'Technology and Law: The Evolution of Digital Warfare' in Schmitt MN and O'Donnell BT (eds), *Computer Network Attack and International Law* (n 47) 18

[139] ibid 16

[140] *Legality of the Threat or Use of Nuclear Weapons* (n 57)

[141] Henckaerts J-M and Doswald-Beck L, *Customary International Humanitarian Law Volume 1: Rules* (Cambridge University Press 2005) xxviii

non-international armed conflicts suffer from a lack of rules and details.[142] The gaps in the regulation of the conduct of hostilities during non-international armed conflicts have been mostly filled through customary international law.[143] The treaties on international humanitarian law are applicable to the states that have ratified them. However, states that are not party to these instruments are obliged to adhere to customary international humanitarian law.

Several issues arise pertaining to the application of the law of armed conflict to cyber attacks. According to Kuehl, the conscription of hackers into the military activities challenges the traditional notion of warfare, which requires 'kinetic actions, destroying things or crossing physical boundaries with physical objects such as airplanes or tanks'.[144] Furthermore, the lawfulness of attacks on computer network system of the civilian telecommunications infrastructure during situation of armed conflict remains unclear.[145] The nature of cyber attacks further complicates the matter. Unlike conventional weapons, cyber attacks do not involve physical transfer of energy. Furthermore, cyber attacks may be conducted remotely and produce instantaneous effects. The remoteness of the operation leads to the difficulty in demonstrating the identity of the perpetrators and the organisation or states that commissioned the attacks and the purpose of the attacks.[146] The technology used to commit the attacks is accessible to anyone.[147] The aim of the present section is to examine these issues. This section analyses the elements that must be satisfied for cyber attacks to be classified as international or non-international armed conflicts. The classification is based

---

[142] ibid

[143] ibid

[144] Kuehl DT, 'Information Operations, Information Warfare and Computer Network attacks' in Schmitt MN and O'Donnell BT (eds), *Computer Network Attack and International Law* (Naval War College Newport, Rhode Island 2002) 54

[145] Tubbs D, Luzwick PG and Sharp WGS, 'Technology and Law: The Evolution of Digital Warfare' in Schmitt MN and O'Donnell BT (eds), *Computer Network Attack and International Law* (n 47) 17

[146] Boothby W, 'Some Legal Challenges Posed by Remote Attack' (2013) 94 International Review of the Red Cross 579

[147] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 167

on the nexus between armed groups and the state and the severity of the attacks. This section also addresses the rules of engagements for cyber attacks during international and non- international armed conflict.

6.3.2.1 Cyber Attacks During Situations of International Armed Conflicts

As indicated above, cyber attacks must be committed during the situation of international armed conflict in order to trigger the application of the Four Geneva Conventions 1949, the Additional Protocols to Geneva Conventions and customary humanitarian law in international armed conflict. Common Article 2 of the Geneva Conventions provides that situation of international armed conflict arise when there is armed conflict between states. Furthermore, it includes armed conflicts 'in which peoples are fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right of self determination'.[148] The declaration of war is not a prerequisite in order for international armed conflicts to exist. The principal focus of these instruments is to regulate hostilities between states normally involving cross border attacks using conventional weapons. However, states are no longer considered as the sole subjects of international law especially after 1945. Contemporary armed struggles involve variety organised armed groups driven by different interests.[149] This includes the existence of cyber militias and private military contractors offering diverse services related to cyber operations. The existence of international armed conflicts depends on the extent of relationship between states and these armed groups.

6.3.2.1.1 Virtual Organisations and Cyber Militias

The attribution of conduct by an entity to a state is important in determining the existence of situation of international armed conflict. Only lawful combatants are entitled to be treated as prisoner of wars under the

[148] Article 1(4) Protocol Additional to the Geneva Conventions of 1 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol 1).

[149] Steven H, 'The Nature of War and the Character of Contemporary Armed Conflict' in Elizabeth Wilhshurst (ed), *International law and the Classification of Conflicts* (Oxfor University Press 2012) 9

International Humanitarian Law.[150] Rebel groups, separatist movements and transnational groups are excluded from this category.[151] They may be subjected to the law of non-international armed conflicts provided in Common Article 3 of the Geneva Conventions 1949, Additional Protocol 2 of 1977 and human rights law. A lawful combatant is defined as a person who is 'a part of or closely related to the military apparatus' and has the access to the methods and means of warfare.[152] The belligerent nexus is established if harm is the effect resulting from the attacks committed by a belligerent against another.[153] Cyber attacks must be perpetrated by combatants on behalf or connected to the state's military apparatus to trigger the application of the law of international armed conflict. Furthermore, the attacks must be done pursuant to the military objectives and advantages. Consequently, there is a need to analyse the relationship between states and virtual organisations in the context of international armed conflicts.

It is often difficult to ascertain the existence of relationship between states and organised armed groups.[154] An organised virtual organisation is likely to posses several qualifications including: (1) the presence of leadership structure with the ability to coordinate activities such as the allocation of targets; (2) sharing tools to commit the attacks; (3) assessing the vulnerability of the computer system prior to the operation and the need for further attacks.[155] In the *Tadic* Case, the ICTY formulated the overall control test which provides that it is not sufficient for the group to be financially or even militarily assisted by a state, but it must be proved that the state wields overall control over the group, not only by equipping and financing the group, but also by coordinating or helping in the general planning of its military

[150] The status of belligerents is clearly stated in the Fourth Hague Convention 1907, the Article 4 of the Third Geneva Conventions 1949 and Article 43 of the Additional Protocol 1 of the Geneva Conventions.

[151] Thomson JE, *Mercenaries, Pirates and Sovereigns* (Princeton University Press 1994) 8

[152] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 127

[153] ibid 123

[154] Schmitt MN, *Tallinn Manual* (n 49) 80

[155] ibid 89

activity.[156] Based on this test, a state is required to control the acts of organised group of hackers or virtual organisations in order for the cyber operations to qualify as international armed conflicts. The test does not require the virtual organisation to meet physically in order to prove the existence of leadership structure.[157] The exercise of control is established when a state display the ability to instruct the group to launch a campaign against cyber infrastructures.[158]

6.3.2.1.2 The Degree of Harm for Cyber Attacks During International Armed Conflicts

Next, this section assesses the degree and scale of cyber attacks for the purpose of the application of the law of international armed conflict. According to Boer and Lodder, cyber operations may occur during international armed conflict in three situations: (1) a declaration of war preceded the cyber operations; (2) operations during a situation of international armed conflict; and (3) the cyber operations amounting to international armed conflict with or without the present of kinetic hostilities.[159] A composite armed attack comprising several low intensity attacks may also amount to armed conflict.[160] In the light of this argument, cyber attacks could be launched in combination with kinetic weapons during international armed conflicts or as a detached military manoeuvre. The evaluation of the threshold of harm is pertinent in order to identify the attacks within the ambit of the law of international armed conflict.

The law of international armed conflicts necessitates the existence of the collective application of means and methods of warfare.[161] However, there is no consensus on the degree of harm required to constitute cyber attacks. Scholars are divided as to whether the 2010 stuxnet operation that

---

[156] *Tadic Case* (IT-94-1-A)(ICTY), Appeals Chamber Judgment

[157] Schmitt MN, *Tallinn Manual* (n 49) 89

[158] ibid 80-81

[159] Boer L and Lodder A, 'Cyberwar' in Leukfeldt R and Stol W (eds), *Cyber Safety: An Introduction* (Eleven International Publishing 2012) 164

[160] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 109

[161] Schmitt MN, *Tallinn Manual* (n 49) 82-83

destroyed the centrifuges at the Iran nuclear plant at Natanz could constitute armed conflict.[162] Article 49(1) of Additional protocol 1 of 1977 defines 'attack' as acts of violence against the adversary, whether in offence or in defence. Cyber attacks that cause mere inconvenience and insignificant damage to military or civilian objects do not qualify as armed conflicts. The Tallinn Manual defines cyber attack as 'a cyber operation, whether offensive or defensive that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[163] The blockage of large-scale communications throughout the country such as email is excluded from the nature of harm in this definition.[164] The Tallinn Manual also excludes the shut down of national grid or the incapacitation of the banking system from the definition of attacks within the ambit of Article 49(1) of Additional Protocol 1 of 1977, as they do not involve any physical destruction. In contrast, other scholars, such as Roscini, suggest that the interpretation of attacks within the ambit of Article 49(1) of Additional Protocol 1 of 1977 should be expanded to 'include not only material damage to objects but also incapacitation of structures without destruction'.[165]

In the light of the arguments above, this study suggests that the presence of material harm or injury is essential for cyber attacks during international armed conflict. Accordingly, the use of force to cause material harm or damage might be necessary in order to trigger the application of the law governing international armed conflict. The Budapest Convention and the domestic criminal courts may be invoked against cyber operations that are not classified as armed attacks. Criminal law provides certain safeguards including fairness, disclosure and open court proceeding. However, the enforcement of criminal law is difficult for extra-territorial offences as it depends on the existence of an extradition agreement.

---

[162] ibid 83-84

[163] ibid 106

[164] ibid 109

[165] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 180

6.3.2.1.3 The Principles of International Humanitarian Law Applicable for Cyber Attacks

The principles of international humanitarian law govern the following aspects of warfare:(1) the distinction between civilians and combatants; (2) distinction between civilians and military objectives; (3) indiscriminate attacks; (4) proportionality in attack; (5) precautions in attack; (6) works and installation containing dangerous forces.[166] To qualify as a privileged combatant, the usage of cyber attacks during situation of international armed conflicts must be done according to these international legal obligations. The principle of state responsibility may be invoked against states for their failure to comply the obligations under international humanitarian law.[167]

6.3.2.1.3.1 The Distinction Between Civilians and Combatants

The distinction between civilians and combatants is pertinent during armed conflict. Combatants are entitled to immunity from criminal liability for killing the enemy forces or destroying legitimate military target. The immunity extends to cyber attacks but they must be considered as criminal acts if performed by a non-combatant.[168] In addition, combatants are entitled to be treated as prisoner of wars under the international humanitarian law. The distinction is also necessary to protect civilians from dangers resulting from military operations.[169] However, the protection shall cease if civilians take a direct part in the hostilities.[170] Civilians who commit cyber attacks can only be targeted under the laws of war if they are considered to be directly participating in the armed conflicts. Civilians may participate in the armed conflicts independently or by joining non-state armed groups such as militia or corps. According to ICRC, direct participation in hostilities entails the fulfilment of the following criteria: (1) the disruption of the military or military capacity or causing death, injury or destruction on persons or objects; (2)

---

[166] ICRC, 'Conduct of Hostilities' <https://www.icrc.org/en/war-and-law/conduct-hostilities> accessed 15 January 2017

[167] Sassoli M, 'State Responsibility for Violations of International Humanitarian Law' IRRC June 2002 VOL 84 No 846

[168] Brown D, 'A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict' (n 74)

[169] Article 51(1) of the Additional Protocol 1 of 1977

[170] Article 51(3) of the Additional Protocol 1 of 1977

direct causation between the act and harm; and (3) belligerent nexus.[171] Cyber attacks by civilians must satisfy these criteria in order to be considered as direct participation in hostilities.

The first criterion is the degree of harm. As discussed previously, the degree of harm for cyber attacks is essential for the purpose of determining the type of attacks to trigger the application of the law of international armed conflict. The degree of harm is also needed to justify targeting civilians due to their involvement during armed conflict. Direct participation in hostilities refers to specific hostile acts carried out by individuals to disrupt the military capacity or causing death, injury or damage to property during the armed conflict. This includes the usage of weapons or other means to conduct violence against enemy forces.[172] The second criterion is direct causation between the act and harm.[173] Direct participation in hostilities includes acts which are integral to the military operations such as 'identification and marking of targets, the analysis and transmission of tactical intelligence to attacking force and the instruction and assistance given to troops for the execution of a specific military operation'.[174] The last criterion is the existence of a belligerent nexus. The acts are done to support the party to the conflict for the purpose of harming the enemy force. The intentions of the immediate participants are irrelevant as the objectives of the acts are reflected in the design of the operation.[175]

The court in *Public Committee against Torture in Israel* discussed the notion of direct participation extensively.[176] The Supreme Court of Israel held that taking direct part in hostilities refers to civilian who assumes the function of a combatant. This includes: (1) a civilian bearing arms (openly or concealed)

---

[171] Melzer N, 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law' (n 70)

[172] Henckaerts J-M and Doswald-Beck L, *Customary International Humanitarian Law Volume 1: Rules* (n 141) 23

[173] Melzer N, 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law' (n 70)

[174] ibid 66

[175] ibid

[176] *The Public Committee against Torture in Israel v Government of Israel* HCJ 769/02

on his way to the place where he is using his arms against the enemy and on his way back from using it; (2) a person who collects intelligence on the army; (3) a person who transports unlawful combatants to or from the place where the hostilities are taking place;(4) a person who operates weapons which unlawful combatants use or supervises their operation, or provides service to them regardless of their distance from the battlefield; (5) a civilian who is driving the ammunition to the place from which it will be used for the purposes of hostilities; and (6) commanders who plan and decide upon the act.[177] The court further held that a civilian who provides general support such as selling food or medicine, general strategic analysis, logistical and financial support and distributes propaganda is taking an indirect part in the hostilities. Hence, direct participation in the context of cyber attacks can denote the usage of cyber weapons such as malware and computer viruses to cause physical harm or damage to the enemy forces. The opposing forces can therefore target civilians who activated the software and perform the attacks. Cyber attacks that negatively affect military operations of the enemy such as cyber espionage and disruption of military computer networks should amount to direct participation even though they do not cause physical harm or damage. The manipulation of computer networks may lead to serious impact on public security, health or commerce. However, it cannot be classified as direct participation in hostilities in the absence of adverse affect on military operations.[178]

Civilians can be targeted if they have been conscripted into cyber units that form part of the armed forces or non-state groups such as cyber militia or cyber corps. The criteria for 'belligerents' during situation of international armed conflicts are clearly stated in the Fourth Hague Convention 1907, the Third Geneva Conventions 1949 and the Additional Protocol 1 to the Geneva Conventions. [179] 'Rebel groups, separatist movements and

[177] ibid

[178] Melzer N, 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law' (n 70)

[179] Article 43 (1) of the Additional Protocol 1 provides that the armed forces of a party to a conflict consist of an organized armed force, groups and units which are under a command responsible to that party for the conduct of its subordinates even

transnational groups' are excluded from this category, as they are not state apparatus.[180] Unlike the state's armed forces, members of the non-state groups are considered as civilians participating directly in the hostilities. They are susceptible to attack while performing any combative function.[181]

Several elements must be satisfied to prove that cyber militia or cyber corps belongs to the state. Firstly, they must have acted on behalf and with the agreement of the state.[182] Non-fulfilment of this standard renders non-state groups as unprivileged actors who may be liable to criminal prosecution. They are not entitled to the combatant or prisoner of war status.[183] Secondly, the cyber militia and corps must be sufficiently organised and possess leadership structure. Thirdly, they are obliged to distinguish themselves from civilians.[184] The need to have a fixed distinctive sign recognizable at a distance and carrying arms openly.[185] These requirements are not applicable to cyber militias and corps who launch the attacks using their computer keyboard. Nevertheless, they are still regarded as part of the armed forces of the state as long as there is sufficient degree of military organisation.[186]

Cyber attacks may be included in the scope of direct participation of hostilities. The next issue is to determine the temporal dimension of the civilian who is directly involved in the hostility. According to ICRC, direct participation in hostilities begins when a civilian undertakes a physical displacement in order to perform a specific operation. It ends once the civilian has physically detached from the hostilities, for instance by laying

---

if that party is represented by a government or an authority not recognised by an adverse party.

[180] Thomson JE, *Mercenaries, Pirates and Sovereigns* (n 151) 8

[181] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 202

[182] Melzer N, 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law' (n 70)

[183] They are entitled to the fundamental guarantees under Article 75 of the Additional protocol 1 of 1977

[184] Article 44(3) of the Additional Protocol 1 of 1977

[185] Article 4(A)(2) of the Third Geneva Convention 1949

[186] Melzer N, 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law' (n 70)

down, storing or hiding weapons.[187] *In the Public Committee against Torture in Israel,* the court held that a civilian can be targeted for taking direct part in one single time or sporadically. The protection resumes once he is separated from the hostilities. He cannot be attacked for the acts of hostilities committed in the past. A civilian, who commits a chain of hostilities with short periods of rest between, loses his immunity from attack for such time. The court further held that the rest period between hostilities is nothing other than preparation for the next hostility.[188] Apart from deployment, direct participation in the hostilities includes preparatory measures aiming to carry out specific hostile act. General preparation to perform unspecified hostile acts is excluded from the scope of direct participation in the hostilities.[189] In the context of cyber attacks, the temporal dimension differs from attacks using conventional weapons such as guns. Cyber attacks can be done in remote area miles away from the battlefield provided that the military system is connected to the Internet. Infiltration is only necessary for instance, to install malware if the computer system is detached from the Internet. In this situation, instead of carrying arms and munitions, a civilian takes along tools such as flash drive containing malware. In addition, the effect of malware continues after the execution of the attack. There is no express prohibition on geographical limitation with respect to the attacks under international humanitarian law.[190] Thus, a civilian taking direct part in the hostilities by conducting cyber attacks during international armed conflicts can be attacked anywhere wherever they may be situated.

6.3.2.1.3.2 The Distinction Between Civilians and Military Objectives

Only military objectives can be targeted during armed conflicts. For that purpose, combatants are obliged to distinguish between civilian and military objectives. Military objectives are defined as objects, which by their nature,

---

[187] ibid

[188] *The Public Committee against Torture in Israel v Government of Israel* HCJ 769/02

[189] Melzer N, 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law' (n 70)

[190] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 214

location, purpose or use make an effective contribution to military operation. Party to the conflicts obtain definite military advantage by destroying, capturing or neutralising these objectives.[191] However, combatants are not allowed to target the object if they have doubts whether it is used for civilian purpose. [192] Military objectives include 'establishments, buildings and positions where enemy combatants, their materiel and armaments are located and military means of transportation and communication'.[193] Dual-use facilities such as civilian means of transportation, communication and economic targets may be attacked if they offer definite military advantage.[194] The presence of civilians within or near these objects does not preclude them from being attacked. However, combatants shall not use the civilians to shield military objectives from attacks.[195] The aim of the present section is to analyse the disruption and destruction of the Internet due to cyber attacks during international armed conflict.

The Internet is a vital instrument of communication and information for civilians and military. It comprises various physical and non-physical components including servers, fibre optic cables, satellites, web browser, email and command line.[196] Most of these components may be categorised as dual-use objects. Civilians and military use them for various purposes such as communication, dissemination of information and economic activities. Cyber attacks can be used to disrupt the Internet by targeting the hardware and software components. The attacks are legitimate only if they provide definite military advantage. Moreover, they are subjected to the principle of proportionality, which prohibits attacks that cause excessive incidental damage to civilians and civilians' property or outweighs the direct military advantage. Telephone relay stations, satellite and other communications hardware are not classified as cyber weapons. However,

---

[191] Article 52(2) of Additional Protocol 1 of 1977

[192] Article 52(3) of Additional Protocol 1 of 1977

[193] Henckaerts J-M and Doswald-Beck L, *Customary International Humanitarian Law Volume 1: Rules* (n 141) 32

[194] ibid

[195] Article 50 (7) of the Additional Protocol 1 of 1977

[196] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 185

they are amenable to attacks as they contribute to the military war fighting capability.[197] Military files and computer networks are categorised as military objectives. Thus, the deletion of military files and insertion of malicious code in military networks is permissible during armed conflict.[198]

6.3.2.1.3.3 Indiscriminate Attacks

The distinction between civilians and military objectives entails that combatants are prohibited from attacking randomly during armed conflicts. They are forbidden from using the means and methods of warfare that cannot be directed at a specific military objective.[199] For instance, the bombing of clear and separate military objectives in an area containing a similar concentration of civilian and civilians' objects is considered as indiscriminate attacks. Attacks that cause incidental loss of civilian life, injury to civilians, damage to civilians object that would be excessive in relation to the concrete and direct military advantage are not allowed under this principle.[200] In the context of cyber attacks, combatants are obliged not to use means and weapons of attacks that are indiscriminate. They have to consider various factors such as the nature, purpose and location of the objects before launching the attacks.[201] The embedding of malicious script on a public website is indiscriminate. The malicious script may infect the computer of anyone accessing the website.[202]

6.3.2.1.3.4 Proportionality in Attack

As stated above, combatants are not allowed to cause excessive damage to civilians' objects and loss of life and injury to civilians in comparison to the concrete and direct military advantage during the military operation. Civilians may be harmed if they live, work in or are passing by the military targets.

---

[197] Brown D, 'A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict' (n 74)

[198] Schaap AJ, 'Cyber Law Edition: Cyber Warfare Operations: Development and User Under International Law' (2009) 64 AF L Rev 121

[199] Article 51 (4) of the Additional Protocol 1 of 1977; Blank LR, 'After "Top Gun": How Drone Strikes Impact the Law of War' (2011-2012) 33 U Pa J Int'l L 675

[200] Article 51 (5) of the Additional Protocol 1 of 1977

[201] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 218

[202] Schmitt MN, *Tallinn Manual* (n 49) 156

They can only be considered as collateral damage if the attacks are matched by proportionate military advantages. The principle of proportionality also entails that a less harmful means should be chosen in attacking a civilian taking a direct part in hostilities. Combatants must choose the means that cause least harm to civilians; so, a terrorist taking direct part in hostilities by attacking civilians can be arrested, interrogated, and tried. [203] The principle of proportionality is centred on a values based test in which the attack is proportionate if the benefit stemming from the attainment of the proper military objective is proportionate to the damage caused to innocent civilians harmed by it.[204] In relation to cyber attacks, the destruction or disruption of computer system of dual purpose objects such as power plants may not be proportionate if they cause indirect effects including the death of many civilians in hospitals.[205]

6.3.2.1.3.5 Precautions in Attack

Combatants are obliged to take precautionary measures to spare the lives of civilians and damage to civilians' objects. The precautionary measures include verifying the status of the objects, using the means and methods of attacks to avoid excessive collateral damage and giving effective advance warning of attacks to civilian population.[206] In addition, combatants have to undertake measures to remove civilian and civilians' objects from the vicinity of military objectives. This is necessary in order to protect them from the effects of attacks resulting from military operation.[207] For instance, the military systems may be separated from infrastructures used by the civilian population. [208] However, this may seem impossible, as most of telecommunication infrastructures such as satellites, fibre optic cables and servers are owned by the private sectors and accessible to military and

---

[203] *The Public Committee against Torture in Israel v Government of Israel* HCJ 769/02

[204] ibid

[205] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 221

[206] Article 57 (2) of the Additional Protocol 1 of 1977

[207] Article 58 of the Additional Protocol 1 of 1977

[208] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 238

civilians.[209] Particularly salient, military commanders are obliged to assess the information from all sources available to them before executing an attack.[210] Precautionary measures must be exercised before the execution of cyber attacks especially if the attacks are done remotely.[211] The military commander is responsible to assess the legitimacy of the attacks in advance by ascertaining the cyber linkages between the sending and targeted computers, the effects of the attacks on the targeted computers and their dependencies and consequential damage to their users.[212]

6.3.2.1.3.6 Works and Installation Containing Dangerous Forces

Combatants are prohibited from attacking infrastructures containing dangerous forces such as dams, dykes and nuclear electrical generating stations.[213] The prohibition is necessary to prevent significant loss of civilians' life caused by the release of dangerous force from these infrastructures. However, the prohibition is not absolute as the infrastructures may be attacked if they are significantly and directly used to support military operations. Thus, cyber attacks on works and installations containing dangerous forces are prohibited unless they are directly used by the military. Precautionary measures must be exercised to ensure civilians do not suffer from such attacks.

6.3.2.2 Cyber Attacks During Situations of Non-International Armed Conflicts

The aim of this section is to identify the degree and scale of cyber attacks required for non-international armed conflicts and the criteria of the organised armed group during non-international armed conflicts. The determination of degree and scale of cyber attacks is pertinent in order to ascertain the presence of internal armed conflicts. Internal disturbances and tensions, such as riots, isolated and sporadic acts of violence are excluded

---

[209] ibid

[210] Henckaerts J-M and Doswald-Beck L, *Customary International Humanitarian Law Volume 1: Rules* (n 141) 54-55

[211] Roscini M, *Cyber Operations and the Use of Force in International Law* (n 42) 234

[212] Boothby W, 'Some Legal Challenges Posed by Remote Attack' (n 146) 579

[213] Article 56 (1) of the Additional Protocol 1 of 1977

from non-international armed conflicts.[214] In *Prosecutor v Tadic* (Appeal on Jurisdiction), the International Criminal Tribunal for the Former Yugoslavia (ICTY) affirms the existence of armed conflict 'whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organised are groups or between such groups within a state.'[215] Cyber attacks must be protracted and beyond internal disturbances to render the hostilities as non-international armed conflicts. However, the hostilities need not reach the magnitude of sustained and concerted military operations.[216] Consequently, sporadic cyber attacks including those that cause physical damage or injury do not amount to non-international armed conflict.[217] In addition, the deletion or destruction of computer data and Internet services such as defacing official websites are not categorised as non-international armed conflicts.[218]

The dissident armed forces or other armed groups must be sufficiently organised before a non-international armed conflicts can exist. Moir asserts that the level of organisation of the insurgents affects the application of common Article 3 of the Four Geneva Conventions 1949. The level is determined based on their capability to perform the obligations imposed by Common Article 3 of the Four Geneva Conventions 1949 that include according humane treatment to persons taking no active part in the hostilities.[219] Additional Protocol 2 of 1997 further requires the armed groups to possess chain of command and have control over a part of territory to enable them to carry out sustained and concerted military operations. Moreover, they must be capable of implementing the provisions of the Protocol.[220] Individuals who contribute to the general war effort of a non-state party are not classified as insurgents. Recruiters, trainers, financiers

---

[214] Article 8(2)(d) Rome Statute of International Criminal Court 1998

[215] *Prosecutor v Tadic*, Case No. IT-94-1-AR72

[216] Cullen A, *The Concept of Non-International Armed Conflicts in International Humanitarian Law* (Cambridge University Press 2010) 127

[217] Schmitt MN, *Tallinn Manual* (n 49) 86

[218] ibid 88

[219] Moir L, *The Law of Internal Armed Conflict* (Cambridge University Press 2002) 36

[220] Article 1(1) of the Additional Protocol 2 of 1977

and propagandists are not members of the organised armed unless they participate directly in the hostilities.[221] Accordingly, during non-international armed conflicts, virtual organizations or cyber militia must be sufficiently organised and able to perform the obligations imposed under the law of non-international armed conflicts including the principles discussed above.

The foregoing attributes of international humanitarian law discussed in section 6.3.2.1.3 regulate the commission of cyber attacks during non-international armed conflicts. These principles have attained the status of customary international law and are applicable during both international and non-international armed conflicts. [222] The application of customary international humanitarian law is necessary as Common Article 3 to the Fourth Geneva Conventions 1949 and Additional Protocol 2 of 1977 only provides minimum protection during non-international armed conflicts. These rules can be invoked when armed conflict occurs between armed forces of a state and dissident armed forces or other organised armed groups in the territory of the state.[223] International humanitarian law is applicable to the areas where the fighting occurs and the entire territory of the state involved in armed conflict.[224] In the context of cyber attacks, the transit of data through cyber infrastructure located outside a state during internal armed conflicts does not render the conflict as international armed conflicts.[225]

6.3.3 Cyber Espionage

This section examines the categorisation of cyber espionage as cyber attacks and the legality of cyber espionage under international law, especially under the international protection of the human rights regime. Intelligence gathering can be done covertly or by monitoring open sources

---

[221] Melzer N, 'Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law' (n 70)

[222] Henckaerts J-M and Doswald-Beck L, *Customary International Humanitarian Law Volume 1: Rules* (n 141) xxix

[223] Common Article 3 to the Four Geneva Conventions 1949

[224] Cullen A, *The Concept of Non-International Armed Conflicts in International Humanitarian Law* (n 216) 140

[225] Schmitt MN, *Tallinn Manual* (n 49) 86

such as newspaper and government proceedings.[226] The information is transmitted through human intelligence, aerial reconnaissance and electronic surveillance such as cyber espionage. This thesis so far suggests that cyber attacks are committed through unauthorised penetration of computer networks mainly for the purpose of inflicting harm and injuries on persons and properties. Similarly, the acquisition of unauthorised access to computer system is essential in conducting cyber espionage. This enables states to gather data or intelligence kept on another state's network or to analyse the configuration of the network.[227]

Some scholars argue that cyber espionage is not cyber warfare as it does not disrupt or destroy the computer system and networks.[228] Herr and Rosenzweig claim that malware which is capable to include a payload to create destructive effects should be classified as cyber weapon.[229] Thus, espionage tools and malware that create loss of confidentiality are excluded from this category, as they do not cause destruction to information or physical object.[230]

In contrast, Brown contends that the collection of intelligence through computer networks resemble cyber attacks.[231] The unauthorised access can cause the computer system to cease its intended function and decrease its effectiveness.[232] Furthermore, cyber espionage may be committed for reconnaissance and is a precursor of future offensive operations.[233] The computer system is subsequently compromised and vulnerable to upcoming attacks. Therefore, this thesis now considers cyber espionage as cyber

---

[226] Sulmasy G and Yoo J, 'Counterintuitive: Intelligence Operations and International Law' 28 Mich J Int'l L 625 2006-2007

[227] Schaap AJ, 'Cyber Law Edition: Cyber Warfare Operations: Development and User Under International Law' (n 198)

[228] ibid

[229] Herr T and Rosenzweig P, 'Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model' 8 J NAT'L SECURITY L & POL'Y ___ (forthcoming 2015)

[230] ibid

[231] Brown G, 'Spying and Fighting in Cyberspace: What is Which?' 8 J NAT'L SECURITY L &POL'Y ___ (forthcoming 2016)

[232] ibid

[233] ibid

attacks under international law. Moreover, cyber espionage may be categorised as a threat of use of force if it is conducted as a preparation for an armed attack.[234] An expansive view of cyber attacks may be necessary to accommodate cyber espionage due to its considerable impact and pervasiveness. This section analyses the accountability of states in cyber espionage under international law.

All Internet users leave digital footprints including 'the electronic record of their mouse clicks and keystrokes, the websites they visited, the sources they have run, the materials they have downloaded, the personal information they have entered, the words and images they have sent by email'.[235] These materials are collected and observed by Internet surveillance for various purposes.[236] States engage in cyber espionage during armed conflict in order to access vital information of their enemy. As a result, they gain considerable advantage that may be used to wage armed conflict successfully.[237] At the international level, cyber espionage may be viewed as acts of hostility, which can entail a military response.[238] Cyber espionage allows states to access computer system of other states from a remote location. This may undermine the deterrent effect of domestic law, which prohibits espionage activities. Traditional territorial limits have been increasingly undermined by the advancement of technology.[239] At domestic level, there is a tendency for Internet surveillance to intrude upon the personal liberties of Internet users especially the right to privacy and data protection. The position of cyber espionage under the domestic law of

---

[234] Forcese C, 'Spies Without Borders: International Law and Intelligence Collection' Journal of National Security Law & Policy 01/2011, Volume 5, Issue 1

[235] Yar M, *Cybercrime and Society* (n 23) 142

[236] ibid

[237] Boer L and Lodder A, 'Cyberwar' (n 159) 162

[238] Tubbs D, Luzwick PG and Sharp WGS, 'Technology and Law: The Evolution of Digital Warfare' in Schmitt MN and O'Donnell BT (eds), *Computer Network Attack and International Law* (n 47) 16

[239] Chesterman S, 'The Spy Who Came in From the Cold War: Intelligence and International Law ' 27 Mich J Int'l L 1071 2005-2006

Malaysia is discussed in Chapter 5. A reasonable balance has to be struck between national security and the interest of the Internet users.[240]

6.3.3.1 Cyber Espionage during Armed Conflicts

The Tallinn Manual defines cyber espionage as 'clandestine activities that use cyber capabilities to gather information with the intention of communicating it to the other party'.[241] The law of armed conflict does not prohibit espionage activities. However, spies are not entitled to the status of prisoner of war.[242] They may be punished under the domestic law of the state which is affected.[243] Despite the criminal sanction for the individual, the sending state does not incur responsibility under international law for spying during armed conflict.[244] Cyber espionage conducted by combatants who disguise themselves as civilians may breach the prohibition on perfidy.[245] Apart from spying on their adversary, states may gather information by engaging in Internet surveillance on civilians during armed conflict. This section assesses the legality of Internet surveillance during armed conflict under human rights law.

States are obliged to ensure respect for human rights and fundamental freedoms within their jurisdiction.[246] This obligation may be extended over an area outside the territory of a state party which it has effective control.[247] It is also applicable to area in which the state, through its agents, exercises control and authority over an individual.[248] The protection accorded by human rights conventions does not cease in the case of armed conflict save through the effect of provisions for derogation stated in Article 4 of the

---

[240] Yar M, *Cybercrime and Society* (n 23) 140

[241] Schmitt, *Tallinn Manual* (n 49) 193

[242] Article 46 (1) 1977 Geneva Protocol 1

[243] Schmittt, *Tallinn Manual* (n 49) 193

[244] Chesterman S, 'The Spy Who Came in From the Cold War: Intelligence and International Law ' (n 239)

[245] Schmittt, *Tallinn Manual* (n 49) 193

[246] Article 1 International Covenant on Civil and Political Rights; Article 1 European Convention on Human Rights

[247] *Bankovic and Others v Belgium and Others,* no 52207/99, ECHR 2001-XII

[248] *Al-Skeini and Others v The United Kingdom*, no 55721/07

International Covenant on Civil and Political Rights.[249] In *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, the ICJ held that 'some rights may be exclusively matters of international humanitarian law; others may be exclusively matters of human rights law; yet others may be matters of both these branches of international law'.[250] The law of armed conflict is considered as lex specialis. For instance, according to the ICJ the deprivation of life arbitrarily must be decided based on the law of armed conflict and not deduced from the provisions of the International Covenant on Civil and Political Rights.[251]

Certain rights are absolute and shall not be derogated even during situation of public emergency.[252] However, unlawful interference with a person's privacy, family, home or correspondences is not categorised as affecting non-derogable rights under the International Covenant on Civil and Political Rights.[253] Article 8 of the European Convention on Human Rights also permits the interference to privacy in the interest of national security, public safety and for the prevention of crime. Except for spying, the law of armed conflict is silent on Internet surveillance. It can be inferred that Internet surveillance is permissible under the law of armed conflict and human rights law during armed conflicts. However, the International Covenant on Civil and Political Rights requires state party to officially declare the existence of public emergency before the right to privacy can be derogated. This requirement is not indicated in Article 8 of the European Convention on Human Rights. Common Article 2 of the Four Geneva Conventions 1949 provides that the law of armed conflict applies even though the state of war is not recognised by a state party. It can be argued that proclamation of emergency is not necessary before Internet surveillance is conducted during armed conflict. The next section discusses cyber espionage outside armed conflict.

---

[249] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory,* ICJ Reports 2004

[250] ibid paragraph 106

[251] *Nuclear Weapon Case* (n 57)

[252] Derogation is not permitted from article 6,7,8 (paragraphs 1 and 2), 11,15,16 and 18 of the International Covenant on Civil and Political Rights

[253] Article 17 of the International Covenant on Civil and Political Rights

6.3.3.2 Cyber Espionage Outside of Armed Conflicts

Gathering Intelligence for the purpose of countering external threats from other states and internal threats such as organised crime and terrorism is prevalent in international community. Apart from state secrets, intelligence includes 'any information relating to an identified or identifiable natural persons'.[254] Edward Snowdon revealed that he was trained by the CIA and NSA to become highly skilled cyber operative in order to hack into the military and civilian systems of other countries.[255] The proliferation of transnational threats due to globalisation has led to cooperation in a broad range of issues among intelligence services.[256]

People responded critically to the revelation of extensive global surveillance and digital data collection by intelligence services including the US National Security Agency (NSA) and GCHQ.[257] Some argue that reliance on intelligence may undermine 'the legitimacy of multilateral institutions and process by the reality or the perception of unilateral influence'.[258] According to Greenwald, Internet surveillance would allow states to examine virtually all forms of human interaction, planning and thought.[259] However, some consider intelligence an effective tool to suppress the proliferation of threats

---

[254] Forcese C, 'The Collateral Casualties of Collaboration: The Consequences for Civil and Human Rights ' in Born H, Leigh I and Wills A (eds), *International Intelligence Cooperation and Accountability* (Routledge 2011) 73

[255] Greenwald G, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (Penguin Books 2014) 44

[256] Born H and Wills A, 'International Intelligence Cooperation and Accountability: Formidable Challenges and Imperfect Solutions' in Born H, Leigh I and Wills A (eds), *International Intelligence Cooperation and Accountability* (Routledge 2011) 277; Greenwald G, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (n 255) 101

[257] European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU Mapping Member States' Legal Frameworks* (Publications Office of the European Union, 2015)

[258] Chesterman S, 'Intelligence Cooperation in International Operations: Peacekeeping, Weapons Inspections, and the Apprehension of War Criminals' in Born H, Leigh I and Wills A (eds), *International Intelligence Cooperation and Accountability* (Routledge 2011) 140

[259] Greenwald G, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (n 255) 6

to national security, including terrorism, and to support the investigations of international criminal prosecution.

The legality of intelligence operation is scrutinised based on the domestic law of the target state, the domestic law of the acting state and international law.[260] The intelligence services have become increasingly legalised in many states under domestic law.[261] Each state also has the jurisdiction to expel diplomats and punish those who have engaged in spying under its domestic legal system. The prosecution of spies can also be an option for the purpose of protecting national interest.[262] However, international law does not expressly prohibit espionage activities. Espionage is not banned under customary international law, as it has become widespread state practice despite condemnation.[263] States freely engage in espionage and share information due to the absence of regulation under international law.[264] Nevertheless, extraterritorial spying tends to clash with state sovereignty and the principles of human rights.[265]

Intelligence activities are primarily constrained by international human rights law. As indicated earlier, states are prohibited from interfering with a person's privacy, family, home or correspondence.[266] Interferences with the right to privacy are only permissible in order to pursue a legitimate aim.[267] This entails the incorporation of safeguards and oversight mechanisms in

---

[260] Chesterman S, 'The Spy Who Came in From the Cold War: Intelligence and International Law ' (n 239)

[261] Born H and Wills A, 'International Intelligence Cooperation and Accountability: Formidable Challenges and Imperfect Solutions' in Born H, Leigh I and Wills A (eds), *International Intelligence Cooperation and Accountability* (n 256) 287

[262] Sulmasy G and Yoo J, 'Counterintuitive: Intelligence Operations and International Law' (n 226)

[263] Forcese C, 'Spies Without Borders: International Law and Intelligence Collection' Journal of National Security Law & Policy, 01/2011, Volume 5, Issue 1.

[264] Brown G, 'Spying and Fighting in Cyberspace: What is Which?' (n 231)

[265] Forcese C, 'Spies Without Borders: International Law and Intelligence Collection' (n 263)

[266] Article 17 International Covenant on Civil and Political Rights; Article 8 European Convention on Human Rights

[267] European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU Mapping Member States' Legal Frameworks* (Publications Office of the European Union, 2015)

national legislation and practices regarding surveillance of communications, interception and collection of personal data. [268] For instance, the authorisation of the law is needed before electronic surveillance of communications is conducted at home and workplace.[269] The right to privacy is usually enforced by an independent privacy agency, which is vested with the power to hear individual complaints and initiate investigations. [270] Moreover, data protection authorities are needed to safeguard the right to the protection of personal data.[271]

The discussion among scholars on the position of espionage under international law is divided into three categories: (1) those who view that espionage should be illegal under international law; (2) those who perceive espionage as legal; and (3) those who argue espionage as neither legal nor illegal.[272] The fundamental premise of the first category is that individuals have to be protected from potential abuses of power by the government.[273] The collection of information on individuals without their consent is a breach of liberal duty.[274] In addition, the accuracy of the data is questionable, as it may be wrongfully recorded, manipulated and interpreted. Consequently, reliance on the data may lead to wrongful surveillance, detention, deportation, prosecution and conviction. [275] On the other hand, the supporters of espionage argue that the regulation of intelligence activities at the international level is conducive to the emergence of more international

---

[268] Resolution 68/167, A/Res/68/167-The Right to Privacy in the Digital Age adopted on 18/12/2013

[269] Forcese C, 'Spies Without Borders: International Law and Intelligence Collection' (n 263)

[270] Bignami F, 'Towards A Right to Privacy in Transnational Intelligence Networks ' 28 Mich J Int'l L 663 2006-2007

[271] European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU Mapping Member States' Legal Frameworks* (n 267)

[272] Forcese C, 'Spies Without Borders: International Law and Intelligence Collection' (n 263)

[273] Bignami F, 'Towards A Right to Privacy in Transnational Intelligence Networks ' (n 270)

[274] ibid

[275] ibid

conflict.[276] Espionage is necessary in exercising the right of self-defence, as 'the mere knowledge that a neighboring state harbors hostile intentions does not sufficiently equip the threatened state with the requisite knowledge to defend itself'.[277] The third category of scholars proposes espionage as a tool to facilitate international cooperation and to broker international security agreements.[278] It may be used to verify the legitimacy of assurances provided by the neighboring states and to ensure their adherence with international obligations.[279]

These opinions demonstrate the uncertainty of the position of espionage in international relations. The second and third categories provide impetus to the continued practices of gathering intelligence by states. However, the development of standard setting is necessary to ensure states are accountable for the decisions and actions of security and intelligence agencies. Leigh suggests that international standards derived from UN Code of Conduct for Law Enforcement Officials, the Basic Principles on the Use of Force and Firearms by Law Enforcement Officials and the Council of Europe Code on Police Ethics may be partially applied to intelligence and security activities.[280] Intelligence services may be monitored by a combination of internal, executive, parliamentary, judicial and specialised oversight institutions.[281]

Judicial deference to security concerns and the invocation of state secret privilege may obstruct any attempt to hold government and intelligence services responsible for their actions.[282] In *Liberty (National Council of Civil*

---

[276] Sulmasy G and Yoo J, 'Counterintuitive: Intelligence Operations and International Law' (n 226)

[277] Baker CD, 'Tolerance of International Espionage: A Functional Approach' 19 Am U Int'l L Rev 1091 2003-2004, 1096

[278] ibid

[279] ibid

[280] Leigh I, 'Accountability and Intellligence Cooperation: Framing the Issue' in Born H, Leigh I and Wills A (eds), *International Intelligence Cooperation and Accountability* (Routledge 2011) 10

[281] Practice 6 of the UN Good Practices on Oversight Institutions.

[282] Born H and Wills A, 'International Responses to the Accountability Gap: European Inquiries into Illegal Transfers and Secret Detentions' in Born H, Leigh I

Liberties) v Government Communications Headquarters and Others, the tribunal held that the collection of information from electronic communication service providers and obtaining Internet communications under US court supervision do not violate Articles 8 or 10 of the ECHR.[283] Furthermore, in *Privacy International v Secretary of State for Foreign & Commonwealth Affairs & Another*, the tribunal examined the legality of computer network exploitation including hacking by GCHQ.[284] The tribunal held that a proper balance has been struck between protecting the public and individual's privacy through the issuance of the procedures to govern intelligence Service (draft EI Code). In *Human Rights Watch Inc v the Secretary of State for the Foreign and Commonwealth Office & Ors*, the tribunal examined the application forms prepared by Privacy International.[285] Ten claimants used the forms to submit their application that GCHQ had infringed their rights including the right to privacy. The tribunal held that 'an individual may claim to be a victim of a violation occasioned by the mere existence of secret measures or legislation permitting secret measures only if he is able to show that due to his personal situation, he is potentially at risk of being subjected to such measures'.[286] In addition, legal proceeding is difficult as intelligence operations are mostly operated covertly.[287] However, several measures may be undertaken to overcome these obstacles. These include convening specialised tribunal, allowing judges access to secret materials, relaxing

---

and Wills A (eds), *International Intelligence Cooperation and Accountability* (Routledge 2011) 73

[283] *Liberty (National Council of Civil Liberties) v Government Communications Headquarters and Others* [2015] UKIPTrib 13 77-H

[284] *Privacy International v Secretary of State for Foreign & Commonwealth Affairs & Another; Greennet Ltd & Others v Secretary of State for foreign & Commonwealth Affairs & Another* [2016] UKIPTrib 14_85-CH

[285] *Human Rights watch Inc v the Secretary of State for the Foreign & Commonwealth Office & Ors* [2016] UKIPTrib 15_165-CH

[286] ibid

[287] Leigh I, 'National Courts and International Intelligence Cooperation' in Born H, Leigh I and Wills A (eds), *International Intelligence Cooperation and Accountability* (Routledge 2011) 233

standard of proof, encouraging class actions and guaranteeing the safety of whistle-blowers.[288]

To sum up, the objective of section 6.3 is to ascertain the position of cyber attacks under international law. This study suggests that international law regulates cyber attacks in the guise of use of force, cyber warfare and cyber espionage. The findings showed that cyber attacks amount to armed attacks within the ambit of Article 2(4) of the Charter of the United Nations if they cause physical destruction, loss of life or injury to persons. States are permitted to exercise the right of self-defence under Article 51 of the Charter of the United Nations against such attacks. This right should also be invoked against cyber attacks perpetrated by non-state actors. However, the unwilling or unable test must be satisfied before military actions can be taken against them. This study suggests that non-physical harm such as economic and political instability should be categorised as a violation of the principle of non-intervention under international law.

Apart from use of force, international humanitarian law governs cyber attacks during situation of international and non-international armed conflicts. States are obliged to adhere to the principles of international humanitarian law in conducting their cyber operations. This includes the distinction between civilians and military objectives; proportionality in attack and precautions in attack. Civilians who directly participated in cyber operations during an armed conflict are not entitled to the protection provided under the international humanitarian law.

Finally, cyber espionage should be categorised as cyber attacks due to its considerable impact and pervasiveness. Cyber espionage may be conducted during armed conflicts and outside of armed conflicts. International law does not prohibit cyber espionage during armed conflict. Similarly, there is lack of regulation governing cyber espionage outside of armed conflict. However, intelligence activities are constrained by international human rights law and domestic law. This includes the right to privacy and protection of personal data. This study suggests that the

[288] European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU Mapping Member States' Legal Frameworks* (n 267)

development of standard setting is necessary to ensure that states are accountable for the actions of the intelligence agencies.

6.4 The Measures to Counter Cyber Attacks under International Law

The purpose of this section is to investigate the mechanisms to counter cyber attacks under international law. The integration of cyberspace leads to 'a conflict arising from individuals from different jurisdictions living together in one space while living in these different jurisdictions'.[289] Moreover, there is a growing consensus that cyber governance and sovereignty is an issue between governments instead of government and individuals.[290] Thus, concerted effort among states is necessary for developing the mechanisms to regulate cyberspace especially for cyber attacks. Unfortunately, until now states have failed to reach agreement on the appropriate form of governance for the Internet. Russia and China advocate the adoption of sovereign-based model of cyber governance that emphasises state control and centralised authority. They propose the adoption of multilateral model in which states ultimately decide the policy and permissible actions in cyberspace.[291] The United States and its allies contend that cyberspace should not be governed exclusively by states.[292] They argue that in addition to the government, all appropriate stakeholders including the private sector, civil society, academia, and individuals should be involved in the Internet governance.[293] Consequently, what is required now is perhaps a middle ground mode of governance to create a bridge between these opposing positions.

A common understanding and strategy for regulating cyberspace is necessary among states.[294] This includes the development of legal

---

[289] Lessig L, *Code Version 2.0* (Basic Books 2006) 300

[290] Eichensehr KE, 'The Cyber-Law of Nations' 103 Geo LJ 317 2014-2015

[291] ibid

[292] ibid

[293] ibid

[294] Lessig L, *Code Version 2.0* (n 289) 293

responses in the form of binding agreement among states.[295] However, the diversity of values throughout the world may hamper any attempt to conclude agreement between states. For instance, Mcquade argues that 'international agreements about managing crime are usually very difficult to establish because nations often have very different views as to what constitutes justice'.[296] In addition, consensus has not been reached on key issues such as the types of information that should be considered as weaponry.[297] Furthermore, the lack of support from states affects the normative legitimacy of a treaty.[298] Due to the divergence of opinion and a variety of vested interests among states, Eichensehr suggests the adoption of piecemeal treaties focusing on 'narrow issues or negotiated among like-minded groups of states and norms developed through unilateral, bilateral and multilateral declarations and evolving state practice'.[299] In the light of these debates, this study focuses on the role of states, non-state actors and intergovernmental organisations such as international United Nations and ASEAN, in developing legal frameworks and norms to counter cyber attacks. The measures to counter cyber attacks under international law might include: countermeasures; the satisfaction of the principle of state responsibility; the development of international legal and non-legal framework; and the imposition of criminal liability for cyber attacks under international criminal law. These measures will be discussed in the following sections.

6.4.1 Countermeasures

Countermeasure may be invoked against a state which is responsible for perpetrating cyber attacks. Countermeasures are defined as the derogation from an obligation under international law, which is perceived as a justifiable

---

[295] Herr T and Rosenzweig P, 'Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model' (n 229)

[296] Mcquade SC, *Understanding and Managing Cybercrime* (Pearson 2006) 282

[297] James Andre Lewis GN, 'The Cyber Index: International Security Trends and Realities' (*Center for Strategic and International Studies*, 2013) <http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf> accessed 7 March 2014

[298] Brown D, 'A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict' (n 74)

[299] Eichensehr KE, 'The Cyber-Law of Nations' (n 290) 365

response against an internationally wrongful act committed by a state.[300] For instance, the US imposed a ban on French civil air flights due to France's refusal to allow passengers to disembark in Paris following disagreement between both countries over the 1946 Air Services Agreement. [301] Countermeasures cease when state stops the wrongful conduct and resume its obligation under international law. Constraints over the application of countermeasure are necessary as states have a tendency to misuse them. [302] This self-help remedy may be taken upon fulfilment of several conditions. Firstly, the existence of an internationally wrongful act is necessary before countermeasures can be taken. Secondly, the purpose of countermeasures is to induce the wrongdoing state to comply with its international obligation. Accordingly, the reactions must be as far as possible reversible.[303] Thirdly, countermeasures must be proportionate to the injury suffered by the victim state. [304] In the light of all these conditions, it is necessary to discuss issues pertaining to the application of countermeasures to cyber attacks under international law.

To begin with, countermeasures can be taken in response to unlawful cyber operations under international law. However, sometimes states have difficulty discerning the legality of cyber operations. For instance, there may be an act of espionage, which is not outlawed under international law.[305] Next, countermeasures for cyber attacks must be reversible and appropriate for the purpose of stopping on-going and future attacks. The infliction of irreparable damage on the responsible state amounts to punishment for non-

---

[300] *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (Yearbook of the International Law Commission, 2001)

[301] *Air Services Agreement of 27 March 1946 (United States v France)*, R.I.A.A, Vol. XVIII, p.416 (1979)

[302] *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (n 300)

[303] Article 22 and 49 of the International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Act

[304] Article 49-53 of the ILC Draft Articles on Responsibility of States for Internationally Wrongful Acts*; Gabčíkovo-Nagymaros Project (Hungary /Slovakia)* ICJ Reports 1997

[305] Tsagourias N, 'The Tallinn Manual on the International Law Applicable to CyberWarfare: A Commentary on Chapter II—The Use of Force' (n 102)

compliance rather than a countermeasure.[306] Accordingly, the victim state is prohibited from using its cyber capabilities to conduct cyber operations to retaliate cyber attacks. Finally, the countermeasures to a large extent should be equivalent to the damage suffered by the victim state due to the cyber attacks. Proportionality is measured by taking into account the quantitative element of the injury and qualitative factors including the seriousness of the breach.[307] On the whole, states may encounter difficulties when they consider whether to apply countermeasures in response to cyber attacks due to these restrictions. Besides countermeasures, states may consider invoking the principle of state responsibility to redress the consequences of cyber attacks.

6.4.2 The Satisfaction of the Principle of State Responsibility

This study so far suggests that cyber attacks may amount to use of force under international law. Apart from the responsive mechanisms provided in the Charter of the United Nations, states must consider the principle of state responsibility when countering cyber attacks. The international responsibility of a state ensues upon the fulfilment of two conditions: (1) a breach of an international obligation; and (2) the breach is attributable to the state under international law.[308] Consequently, a state can be held accountable under international law for commissioning its organs or agents to commit cyber attacks against another state. In addition, the principle of state responsibility can be invoked against states that fail to exercise due diligence to prevent the commission of cyber attacks from their territory.

States may be held accountable for their failure to prevent the commission of trans-jurisdictional crimes. Particularly salient is to identify the appropriate standards and burden imposed on states to prevent harm from cyber attacks perpetrated by non-state actors on their territory.[309] Quentin Baxter, Special

---

[306] *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries* (n 300)

[307] ibid

[308] Article 2 ILC Draft Article on Responsibility of States for Internationally Wrongful Act 2001

[309] Brunnee J and Meshel T, 'Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance' (2015) 58 German Yearbook of International Law, 2015

Rapporteur appointed by the International Law Commission on international liability for injurious consequences arising out of act not prohibited by international law, specifies four criteria for acts that cause trans-jurisdictional harm: (1) the activity in question must be human activity; (2) it must be within the territory or control of a state; (3) it must give rise to harm; and (4) that harm must be to persons or thing within the territory or control of another state.[310] Ortner argues that the exercise of due diligence is based on the adequacy of the measures implemented by states in preventing trans-boundary crimes. [311] These include preventive measures such as disseminating international humanitarian law, the duty to prosecute grave breaches of the Geneva Conventions and the duty to ensure respect laid down in common Article 1 of the Geneva Conventions.[312] States have the obligation under customary international law to ensure their cyber infrastructures are not used to cause trans-boundary harm.[313] There is a need for international consensus on the application of due diligence to cyberspace including the invocation of state responsibility for the failure to prevent acts committed by non-state actors.[314]

Cyber attacks must be attributable to a state under international law in order to satisfy the principle of state responsibility. According to Donnellan and Kersley, there is a lack of legal clarity in the area of cyber attacks especially in determining the relationship between state and non-state actors.[315] Berton

---

[310] Magraw DB, 'Transboundary Harm: The International Law Commission's Study of "International Liability"' (1986) 80 The American Journal of International Law 305, 310

[311] Ortner D, 'Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-boundary Cybercrime' [2015] Brigham Young University Law Review

[312] Sassoli M, 'State Responsibility for Violations of International Humanitarian' (n 167)

[313] Ortner D, 'Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-boundary Cybercrime' (n 311)

[314] Brunnee J and Meshel T, 'Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance' (n 309)

[315] Donnellan C and Kersley E, 'New Ways of War: Is Remote Control Warfare Effective? Executive Summary' (2014) <http://oxfordresearchgroup.org.uk/sites/default/files/Remote%20Control%20Digest.pdf> accessed 7 March 2015

and Denning assert that numerous issues related to the conduct of states and cyber warfare arise with regard to the usage of hackers or cyber militia by governments.[316] It was reported that Chinese hackers known as the Red Hacker Alliance or the Honker Union of China were responsible for various cyber attacks due to patriotic reasons. Similarly, Russian hackers were suspected to be involved in cyber attacks against Israel, the Ukraine, Lithuania and others.[317] The relationships between states and these groups need to be determined for the purpose of ascertaining whether their conduct can be attributed to states and hence produces state responsibility.

A state is accountable for instructing, directing or controlling the conduct of a person under international law.[318] The conduct complained of must be an integral part of a specific operation directed or controlled by the state.[319] Non-state actors must have acted according to the instructions provided by the state. The instructions may be inserted into the contract between states and non-state actors such as private military or Security Corporation or in the field.[320] In the *Application of the Convention on the Prevention and Punishment of the Crime of Genocide,* the ICJ held that instructions must be given in each operation in which the alleged violations occurred.[321] However, Crawford argues that a general instruction that leaves it open as method of fulfilling the directive is sufficient in determining the attribution of conduct.[322] Thus, instructions also include 'acts which are considered incidental to the task in question or conceivable within its expressed ambit'.[323] As such, states may be held accountable for cyber attacks committed by non-state actors who acted pursuant to state instructions or directions. The

---

[316] Berton TA and Denning DE, 'Cyberwarfare' [2011] IEEE Security & Privacy September/October 2011

[317] ibid

[318] Article 8 ILC Draft Article on Responsibility of States for Internationally Wrongful Act 2001

[319] Harris D, *Cases and Materials on International Law* (n 103) 429

[320] Crawford J, *State Responsibility* (Cambridge University Press 2013) 145

[321] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* ICJ Reports 1996

[322] Crawford J, *State Responsibility* (n 320) 145

[323] ibid

accountability includes providing instruction to cyber militia or hackers to launch cyber attacks against other states. Mere encouragement does not amount to effective control unless the state acknowledges and adopts the attacks as its own.[324]

Apart from countermeasures, state responsibility can be implemented through formal claims. States can initiate action at the international tribunals such as International Court of Justice (ICJ) against the wrongdoing state, which has breached its international obligation. However, the ICJ lacks sufficient jurisdiction in dealing with cyber attacks.[325] The effectiveness of the ICJ depends on the degree of cooperation among interested parties.[326] This issue will be discussed in the following section.

6.4.3 The Development of International Legal and Non-Legal Framework to Counter Cyber Attacks

At the international level, cooperation between states in dealing with cyber attacks is essential. Ahead of the London Conference on Cyberspace in 2011, former Britain's Foreign Secretary William Hague stated that 'the internet was revolutionising people's lives but required a global co-ordinated response to ensure its transformative power was fully exploited and channelled in the right direction'.[327] Despite limited resources and power, international organisations can enhance the global cyber security strategies by promoting the creation of appropriate structures and norms to prevent the malicious use of cyber technologies.[328] Organisations such as United Nations, International Telecommunications Union (ITU), Organisation for Economic Cooperation and Development (OECD) and the Council of Europe

---

[324] Article 11 ILC Draft Article on Responsibility of States for Internationally Wrongful Act 2001

[325] Stevens SR, 'Internet War Crimes Tribunals and Security in an Interconnected World' (n 6)

[326] Griffin JB, 'A Predictive Framework for the Effectiveness of International Criminal Tribunals' 34 Vand J Transnatl L 405 2001

[327] Stamp G, 'UK Seeks 'Consensus' at Cyberspace Conference' (*BBC News Politics*, 18 October 2011) <http://www.bbc.co.uk/news/uk-politics-15355739> accessed 14 January 2014

[328] James A, Lewis GN, 'The Cyber Index: International Security Trends and Realities' (*Center for Strategic and International Studies*, 2013) <http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf> accessed 7 March 2014

have undertaken measures to address cyber attacks. United Nations has adopted several resolutions relating to the ICTs and cyber security. Resolution A/RES/57/239 of 2003 acknowledges the importance of international cooperation for achieving cyber security through the support of national efforts and calls member states to develop a culture of cyber security in using the information technologies.[329] Resolution A/58/481 of 2004 recognises the vulnerability of the critical national infrastructure due to variety of threats to information network. However, any efforts to protect critical national infrastructure must be undertaken with due regard to the national laws that protect privacy and other relevant legislation. This resolution reiterates the significant of international cooperation in securing critical information infrastructures by coordinating emergency warning systems and sharing of information.[330] Resolution A/65/405 of 2010 acknowledges the adverse effects of technologies which can be used for the purposes inconsistent with the objectives of maintaining peace and security and can be detrimental to the states in both civil and military fields. In this resolution, member states of the United Nations express their concern about the usage of information technologies by criminals and terrorists.[331] A group of experts has been given the mandate to investigate the potential threats in the realm of information security and the measures to address them.[332] Besides that, ITU has founded the High-Level Expert Group on Cybersecurity in 2007 to provide consultation for information security experts from various fields and regions.[333]

---

[329] Resolution 57/239 Creation of a Global Culture of Cybersecurity, <http://www.itu.int/ITUD/cyb/cybersecurity/docs/UN_Resolution_57_239> accessed 10 July 2014

[330] Resolution 58/199 Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures, <http://www.itu.int/int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199> accessed 10 July 2014

[331] Resolution 65/41 Developments in the Field of Information and Telecommunications in the Context of International Security, <http://www.un.org/en/ga/search/view_doc.asp?symbol+AA/Res?65/41> accessed 10 July 2014

[332] ibid

[333] James A, Lewis GN, 'The Cyber Index: International Security Trends and Realities' (n 328)

The OECD and the Council of Europe have also initiated efforts to harmonise the law and formulate legally binding norms on computer crimes by organising a convention on cybercrime in Budapest, Hungary in September 2001. Forty-eight articles were proposed on cybercrime which cover areas including the computer related definition, the development of criminal and procedural law, clarification with respect to jurisdiction and the principles of international cooperation between nations for investigation and prosecution.[334] The Convention entered into force on 1.07.2004 and is the only binding international instrument on cybercrime.[335] The convention is open for signature by the member states of the Council of Europe and non-member states. As at 3.06.2014, forty-two countries had ratified or acceded the convention including US. Malaysia has not signed this convention so far.

Due to the degree of support, the Convention has been considered as the de facto standard for cybercrime.[336] Nevertheless, the Convention does not regulate cyber operations commissioned by states. The convention is not applicable to states due to the principle of sovereign immunity in which government officials are conferred with immunity in respect of international crimes before national courts.[337] The exclusion of states activity from the purview of the Council of Europe Convention on Cybercrime provides the impetus for the adoption of an instrument to regulate the activities of states on cyberspace. This study examines the establishment of a cyber weapon convention and the function of transnational institutions to counter cyber attacks.

6.4.3.1 Cyber Weapons Convention

This section assesses the fairness and effectiveness of the formulation of a cyber weapon convention. The purpose of the formulation of arms control and disarmaments agreements is to control 'the production, testing,

---

[334] Mcquade SC, *Understanding and Managing Cybercrime* (n 296) 285

[335] Council of Europe 'Action Against Cybercrime' <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Default_en.asp> assessed 25 February 2017

[336] James A, Lewis GN, 'The Cyber Index: International Security Trends and Realities' (n 328)

[337] *Case Concerning the Arrest Warrant of 11 April 2000 (Democratic Republic of Congo v Belgium)* 2002 ICJ Reports 3

stockpiling, transfer, or deployment of the weapons by which armed conflict might be conducted'. [338] For instance, the 1980 Certain Conventional Weapons Convention forbids the use of incendiary weapons, blinding laser weapons, non-detectable fragments, mines and booby traps.[339] The 1972 Biological Weapons Convention prohibits the development, production and stockpiling of chemical and biological weapons.[340] Another example is the 1993 Chemical Weapons Convention that prohibits the development, produce, acquire, stockpile or retain of chemical weapons.[341]

Several scholars suggest that the 1993 Chemical Weapons Convention and the 1972 Biological Weapons Convention may be used as a model for a cyber weapon convention.[342] Biological, chemical and cyber weapons are similar as they can be used for defensive and civilian purposes. Biological and cyber weapons can be manufactured by using commercial and off the shelf technology. [343] In addition, these weapons are more appealing to weaker states and non-state actors as potential asymmetric weapons. [344]

Cogent evidence is required in order to demonstrate the necessity of an agreement to outlaw certain weapons under international law. [345] The adoption of an agreement depends on several factors: (1) 'the military

---

[338] Boothby WH, *Weapons and the Law of Armed Conflict* (n 146) 3

[339] 1980 UN Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which may be Deemed to be Excessively Injurious or to have Indiscriminate Effects, Protocol I on Non-Detectable Fragment, Protocol II on prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices, Protocol III on Prohibitions or Restrictions on the Use of Incendiary Weapons and Protocol IV on Blinding Laser Weapons

[340] Malaysia ratified the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction on 10.04.1972

[341] Malaysia acceded the Convention on the prohibition of the Development, Production, Stockpiling and the use of the Chemical Weapons and on Their Destruction on 20.04.2000

[342] Geers K, 'Cyber Weapons Convention' Computer Law and Security Review 26 (2010) 547-551

[343] Koblentz GD and Mazanec BM, 'Viral Warfare: The Security Implications of Cyber and Biological Weapons' Comparative Strategy, 32:5, 418-434, DOI: 101080/014959332013821845

[344] ibid

[345] Boothby WH, *Weapons and the Law of Armed Conflict* (n 146) 363

purpose or utility that the weapon fulfils and the consequences both satisfactory and otherwise of its actual use; (2) the evidence to show the claimed consequences actually occurred or would occur; (3) the evidence to prove the causal link between the challenged weapon and those alleged consequences; (4) the nature and extent of the military utility of the weapon and alternative available methods of achieving this; (5) the alternative methods, including technical methods of addressing the proven adverse consequences of the use of the particular weapon; (6) the humanitarian, military, technological and financial implications of the various possible methods of addressing the observed problems'.[346] This section evaluates the possibility of a cyber weapons convention in the light of the second and third factors. These factors are particularly salient in determining the necessity for a cyber weapons convention.

As stated above, arms control and disarmaments agreements are concerned primarily with the effect of the weapons during armed conflicts. States are prohibited from using means and methods of warfare that may inflict superfluous injury and unnecessary sufferings on combatants. In addition, the weapons must not trigger pervasive, prolonged and serious damage to the natural environment. Therefore, arms control and disarmaments agreement is necessary if it is shown that cyber attacks may lead to similar consequences. According to Blount, the likelihood of cyber capabilities to inflict unnecessary suffering is improbable as they are designed to affect computer related materials in order to cause real world effects.[347] Cyber attacks do not generally cause any direct personal injury or damage to health. Aside from damaging the military and civilian computer system, computer viruses and worms do not pose a direct threat to the natural environment. Nevertheless, the manipulation of the computer systems that control infrastructure, including electric power transmission, distribution of water and oil or gas pipelines, may indirectly harm people and environment. The adoption of a cyber weapon convention depends on reaching consensus on the effects of cyber attacks to be suppressed.

---

[346] ibid 364

[347] Blount PJ, 'The Preoperational Legal Review of Cyber Capabilities: Ensuring the Legality of Cyber Weapons' (2012) 39 N Ky L Rev 211

However, it is difficult to prove the causal link between cyber weapon and superfluous or pervasive consequences. In addition, the production of cyber weaponry is a worldwide cottage industry compared to other weapons such as tanks and ballistic missiles.[348] Malware can be downloaded from websites and written by any computer programmer. Moreover, cyber weaponry is extremely difficult to delineate.[349] A precise definition of weapon is necessary for the purpose of policy and legal responses including the formulation of arms limitations treaties.[350]

Despite these arguments, this study considers the advantages of the establishment of an international instrument on cyber attacks. This instrument may obligate states to provide assistance and protection to any state party that experience cyber attacks by a state or non-state actor. Furthermore, an institution may be created to assist member states to improve their cyber defences and responses to cyber attacks.[351] Institutional capacity is needed to facilitate the implementation of strategies for early detection and preparedness against attacks and to coordinate cooperation with public and private sectors.[352] This institution may assist the establishment of an assistance, coordination and assessment team similar to the one formed by the Organisation for the Prohibition of Chemical Weapons (OPCW).[353]

However, the adoption of such instrument is not feasible currently due to several constraints, such as the uncertainty surrounding states' cyber

---

[348] Johnson PA, 'Is It Time for a Treaty on Information Warfare? ' in Schmitt MN and O'Donnell BT (eds), *Computer Network Attack and International Law* (Naval War College Newport Rhode Island 2002) 448

[349] Blount PJ, 'The Preoperational Legal Review of Cyber Capabilities: Ensuring the Legality of Cyber Weapons' (n 347)

[350] Herr T and Rosenzweig P, 'Cyber Weapons and Export Control: Incorporating Dual Use with the PrEP Model' (n 229)

[351] Blount PJ, 'The Preoperational Legal Review of Cyber Capabilities: Ensuring the Legality of Cyber Weapons' (n 347)

[352] Kellman B, 'The Biological Weapons Convention and the Democratization of Mass Violence' Global Policy Volume 2 Issue 2 May 2011

[353] Tucker JB, 'The Role of the Chemical Weapons Convention in Countering Chemical Terrorism, Terrorism and Political Violence' Terrorism and Political Violence, 24:105–119, 2012, DOI: 101080/095465532011611839

capabilities and the refusal of states to restrict their capabilities.[354] Alternatively, the implementation and promotion of existing legal norms and the development of offences against dangers posed by certain technology are considered sufficient to address this problem.[355] This study shall return to the question of criminalisation of cyber attacks under international law in the later part of this chapter.

6.4.3.2 Transnational Networks

Apart from legal mechanism, non-legal framework such as transnational networks may be utilised in dealing with cyber attacks. Some states contend that international legal code is unnecessary especially in dealing with globalised crime due to the existence of cooperation among the police bureau, intergovernmental agencies and civil society.[356] Hurrell suggests that the present international legal system is moving towards global governance in which the societal, ecological and economic problems are addressed through collective action in the form of transnational institutions and networks.[357] Non-state actors are entrusted with wide range of function including the determination of the design of secondary rules of international law in relation to sources.[358] These agencies can facilitate cooperation and coordinate strategies during multilateral negotiations between states.[359] Simultaneously, they can contribute to the development and enforcement of norms in various areas such as banking and health policy.[360] Various scientific and technical expert bodies collectively formulate the regulatory strategies for the environment. A similar framework may be adopted to cater the constantly shifting needs of cyber security and to develop the due

---

[354] Eichensehr KE, 'The Cyber-Law of Nations' (n 290)

[355] Boothby WH, *Weapons and the Law of Armed Conflict* (n 146) 364

[356] Elfstrom G, *International Ethics: A Reference Handbook* (n 31) 49-50

[357] Hurrell A, *On Global Order: Power, Values and the Constitution of International Society* (n 1) 15

[358] D'Aspremont J, 'Non-State Actors and the Social Practice of International Law' in Noortmann M, Reinisch A and Ryngaert C (eds), *Non-State Actors in International Law* (Hart Publishing Oxford and Portland, Oregon 2015) 12

[359] Hurrell A, *On Global Order: Power, Values and the Constitution of International Society* (n 1) 68

[360] ibid 98

diligence standards to guard against or limit the use of cyber attacks.[361] Several transnational networks have been established for the purpose of examining the policies related to cyberspace. They provide the avenue for the governments and non-governmental actors to engage in discussion, exchange information and best practices in countering cyber attacks. This section analyses the fairness and effectiveness of these networks in countering cyber attacks.

The success of an intergovernmental network in dealing with cyber attacks depends on the values of its architects and participants. Slaughter defines government networks as 'a pattern of regular and purposive relations among like government units working across the borders that divide countries from one another'.[362] They are usually informal, scattered and not authorised to exercise centralised coercive authority.[363] Therefore, government officials are not entitled to specific rights and are not subjected to certain obligations under international law.[364] Sceptics raise questions concerning the lack of formality of the intergovernmental network. They perceive the networks as trying to promote 'global technocracy-secret governance by unelected regulators and judges'.[365] In addition, the networks deliberately circumvent the rule-making process imposed on international organisations such as voting procedures. Consequently, powerful states tend to exclude weaker states from influential intergovernmental networks.[366] For example, the Internet Corporation for Assigned Names and Numbers (ICANN) has been criticised for lacking of democratic legitimacy due to its dependence on the US government.[367] Slaughter suggests the working relationship between the government officials should be based on the values of 'equality, tolerance,

---

[361] Brunnee J and Meshel T, 'Teaching an Old Law New Tricks: International Environmental Law Lessons for Cyberspace Governance' (n 309)

[362] Slaughter AM, *A New World Order* (Princeton University Press 2004) 14

[363] ibid 11

[364] ibid 33

[365] ibid 27-28

[366] ibid

[367] Etzioni A, *From Empire to Community: A New Approach to International Relations* (n 40) 162-163

autonomy, interdependence, liberty and self-government'.[368] The adoption of these values may encourage participation from other governments, international organisations and civil society. The involvement of powerful and weaker states may strengthen the legitimacy of the networks pursuant to the equitable principles. This may be deduced from the work done by networks affiliated to the United Nations such as the Groups of Governmental Experts on Information Technology and International Telecommunication Union.

The United Nations Groups of Governmental Experts on Information Technology plays a part in the development of the framework to counter cyber attacks.[369] These groups comprise policymakers from 20 countries, including the US, UK, Israel, Pakistan, Japan, Malaysia, China and Egypt. They contribute to the general understanding on the law applicable to cyber attacks and facilitate collaboration among government officials in addressing this problem. Another example is the International Telecommunication Union (ITU), a specialised agency of the United Nations, which has membership of 193 countries and close to 800 private sector entities and academic institutions.[370] ITU provides assistance to member states to mitigate the consequences of cyber crimes and to ensure the security of information and communication technologies.[371] This includes facilitating the implementation of policies, strategies and legislation related to cyber security.

The success of such intergovernmental networks depends on the willingness of the governments to permit continuous consultation and to adopt the strategies proposed by the networks at the domestic level. States are not obliged to implement the strategies, as the networks are merely informal arrangements. This undermines the credibility of the networks in responding to the rapidness of change in cyberspace. Accordingly, intergovernmental

---

[368] Slaughter AM, *A New World Order* (n 362) 31

[369] UNODA 'Developments in the Field of Information and Telecommunications in the Context of International Security <https://www.un.org/disarmament/topics/informationsecurity> accessed 15 January 2017

[370] ITU, 'About ITU <http://www.itu.int/en/about/Pages/default.aspx> accessed 15 January 2017

[371] ITU, 'Legislation'<http://www.itu.int/en/ITU-D/Cybersecurity/Pages/Legal-Measures.aspx> accessed 15 January 2017

networks, especially the ITU, may be equipped with the power to regulate non-technical areas of cyberspace including criminal law.[372] Formalising the networks through a treaty may enhance their role in countering cyber attacks.

Besides the government officials, non-governmental networks play a part in developing the framework to counter cyber attacks at the international level. A coherent strategy in dealing with cyber attacks entails cooperation with multi stakeholders particularly the architectures of cyberspace. This is necessary, as private parties have predominantly run the Internet since its inception.[373] Internet companies and operators are usually the first line of defence against cyber attacks.[374] In addition, the architecture of cyberspace may influence people's behaviour on cyberspace through its code.[375] For instance, the Internet Engineering Task Force (IETF) is an open international network of Internet architecture community. It comprises designers, operators, vendors and researchers who are concerned with the operation of the Internet.[376]

The Internet Architecture Board (IAB) is one of the working groups established by IETF. The members of IAB are selected from experts on Internet architecture, engineers, researchers and consultants in Internet operations and policy.[377] IAB provides a forum to develop and promote security and privacy guidance within the Internet Technical Community.[378] Another example is the Internet Society which consists of 80 000 members

---

[372] Etzioni A, *From Empire to Community: A New Approach to International Relations* (n 40) 162-163

[373] Eichensehr KE, 'The Cyber-Law of Nations' (n 290)

[374] Palovirta M, 'The State of Cybersecurity in Europe - Should We Reboot?' Internet Society <https://www.internetsociety.org/blog/europe-bureau/2016/06/state-cybersecurity-europe-should-we-reboot> accessed 27 July 2016

[375] Lessig L, *Code Version 2.0* (n 289) 24

[376] IETF, 'About the IETF' <https://www.ietf.org/about/> accessed 27 July 2016

[377] Internet Architecture Board <https://www.iab.org/about/iab-members/> accessed 27 July 2016

[378] IAB, 'Privacy and Security Programme' <https://www.iab.org/activities/programs/privacy-and-security-program/> accessed 27 July 2016

from 110 chapters around the world.[379] The purpose of the Internet Society is to provide a forum in promoting an open development, evolution and the use of the Internet.[380] The Internet Governance Forum (IGF) is another international network that provide the platform to discuss public policy in relation to the Internet.[381] It gathers people from various groups to discuss, exchange information and shared good practices on the maximization of the Internet opportunities and challenges.[382]

These networks strive to improve the usage of the Internet based on the notion of fairness and the rule of law. This may be observed from the process and resolutions adopted by these networks. The IGF Code of Conduct emphasises that the discussions must be done based on equality, respect and in good faith.[383] Participants may be removed from the activities conducted by the IGF for their failure to adhere to the code of conduct.

The government led cyber security platforms are not open to all, tend to be fragmented and publicised only within trusted communities.[384] In contrast, non-governmental networks promote governance of Internet based on the notions of openness and transparency. They champion the value of privacy and reject special controls that may hinder trust in the network.[385] Therefore, the ability of the non-governmental networks in using technical means to stop cyber attacks such as DDOS may be restricted due to the nature of the Internet including flexibility and open network. Moreover, their views are apt to discord with the governments. Surveillance and some degree of control

---

[379] Internet Society <https://www.internetsociety.org/who-we-are/our-members> accessed 27 July 2016

[380] Internet Society, 'Mission and Vision' <https://www.internetsociety.org/who-we-are/mission> accessed 27 July 2016

[381] Internet Governance Forum <https://www.intgovforum.org/cms/> accessed 27 July 2016

[382] ibid

[383] IGF 'Code of Conduct' <https://www.intgovforum.org/cms/aboutigf/igf-code-of-conduct> accessed 27 July 2016

[384] Palovirta M, 'The State of Cybersecurity in Europe - Should We Reboot?' Internet Society (n 374)

[385] IAB, 'Overview' <https://www.iab.org/about/iab-overview/> accessed 27 July 2016

are seen as necessary by governments in order to maintain national security.

6.4.3.3 Regional Cooperation: ASEAN

This section examines the cooperation within the framework of ASEAN in countering cyber attacks. Regional organisations were established with the primary aim of maintaining peace and resolving conflicts or containing conflicts to avoid further escalation'.[386] They are pivotal in dealing with cross regional issues and global security concerns including cyber attacks. Regional organisations are effectively positioned and politically able to enforce legal rules due to closer geographic proximity.[387] The likelihood of establishing instruments at the regional level is higher than at the global level. Shared regional sensitivity, values and common security concerns also allow for concerted effort in dealing with globalised problem such as terrorism and cyber attacks. Regional resilience may facilitate national resilience by creating a peaceful and stable environment.[388] The significance of the role of regional organisations in maintaining international peace and security is acknowledged by the United Nations. Article 52 of the Charter of the United Nations affirmed the role of regional agencies in settling dispute between states before a referral is made to the Security Council.

The Association of South East Asian Nations (ASEAN) can facilitate cooperation between its member states in countering cyber attacks. According to Mely Caballero-Anthony:

> A region's approach to security is often reflected in how member states structure their relations among other states within and outside the grouping in pursuing the goal of regional security. Factors such as shared systems, mutual flow of ideas,

---

[386] Caballero-Anthony M, *Regional Security in Southeast Asia: Beyond the ASEAN Way* (The Institute of Southeast Asian Studies 2005) 15

[387] Burke-White WW, 'Regionalization of International Criminal Law Enforcement: A Preliminary Exploration' (2003) 38 ex Int'l LJ 729

[388] Anwar DF, 'Indonesia: National vs Regional Resilience*?'* in Cunha DD (ed), *Southeast Asian Perspectives on Security* (Institute of Southeast Asian Studies 2000) 82

> and level of social communication all become important in shaping security policy orientations of states.[389]

Thus, understanding the background of ASEAN is essential in order to examine its approach to security. ASEAN was established on 8 August 1967 by its founding members, which consist of Indonesia, Malaysia, the Philippines, Singapore and Thailand. The purpose of the establishment of ASEAN is to foster 'cooperation in the economic, social, cultural, technical, educational and other fields, and in the promotion of regional peace and stability'. [390] According to Hung: 'The numerous Southeast Asian States represent a full spectrum of political, legal and ideological diversity that veers away from the typical homogeneity of most regional groupings'.[391] Despite this, ASEAN has moved forward by fostering a greater regional integration through the conclusion of the ASEAN Charter in 2007. This signifies that 'ASEAN is not an informal family grouping of Southeast Asian nation-states but one that has status under international law as well as domestic laws within member states, and can make agreements in its own right'.[392] Other features of ASEAN included non-interference in each other's domestic affairs and decision-making by consensus.[393] Daljit Singh examined the rationale behind the ASEAN way:

> In the ASEAN model of confidence-building and development of a limited security regime, the emphasis has been on improving the political climate of relations through frequent dialogue and interaction between political leaders and official elites of member countries; shelving disputes which cannot be settled in the belief that the change of circumstances or attitudes would

---

[389] Caballero-Anthony M, *Regional Security in Southeast Asia: Beyond the ASEAN Way* (n 386) 23

[390] ASEAN, 'History' <http://www.asean.org/asean/about-asean/history> accessed 20 January 2017

[391] Hung LC, 'ASEAN Charter: Deeper Regional Integration under International Law?' (2010) 9 Chinese J Int'l L 821 2010, 821

[392] Tan EKB, 'The ASEAN Charter as "Legs to Go Places": Ideational Norms and Pragmatic Legalism in Community Building in Southeast Asia' 12 SYBIL 171 2008, 178

[393] Singh D, 'Evolution of the Security Dialogue Process Asia-Pacific Region' in Cunha DD (ed), *Southeast Asian Perspectives on Security* (Institute of Southeast Asian Studies 2000)

> make a solution easier sometime in the future; refraining from interference in each other's internal affairs and, generally, from debating differences between members in public; and making decisions through consensus.[394]

Accordingly, ASEAN lacks power to implement cross-border security operation including military action compared to EU. Article 222 of the Treaty on the Functioning of the European Union allows EU to mobilise instruments including military resources to prevent and protect member states from terrorist attack and man-made disaster. In contrast, ASEAN Convention on Counter Terrorism emphasises the adherence to the principles of state sovereignty, territorial integrity and non-interference. It provides for areas of cooperation and mutual legal assistance in countering cyber attacks. Cross-border operations such as military force are excluded from this convention.

National security is of utmost concern among the member states of ASEAN. Article 2 (b) of the ASEAN Charter provides that member states share the commitment and are collectively responsible for 'enhancing regional peace, security and prosperity'.[395] The focus of ASEAN is on the development of instruments to address transnational crimes in the region which 'include eight priority areas, namely terrorism, illicit drug trafficking, trafficking in persons, arms smuggling, sea piracy, money laundering, international economic crime and cybercrime'.[396]

The ASEAN ICT Masterplan 2015 (ICT Masterplan) was established in order to foster cooperation between the member states of ASEAN in developing the region's ICT landscape.[397] The aim of the ICT Masterplan is to provide affordable ICT access especially to the rural population of ASEAN as part of the project to establish a single ASEAN Community. The ASEAN

---

[394] ibid 47

[395] ASEAN, 'ASEAN Charter' <http://www.asean.org/archive/publications/ASEAN-Charter.pdf> accessed 16 February 2014

[396] ASEAN, 'ASEAN Security Outlook' (*ASEAN*, 2013) <http://www.asean.org/images/2013/resources/publication/asean%20security%20outlook%202013.pdf> accessed 16 February 2014

[397] ASEAN, 'ICT Masterplan' <http://www.asean.org/images/2012/publications/ASEAN%20ICT%20Masterplan%20(AIM2015).pdf> accessed 16 February 2014

Telecommunications and IT Minister (TELMIN) leads the effort to realise the objectives of the ICT Masterplan. Among the objectives of the ICT Masterplan is to promote network integrity and information security, data protection and CERT cooperation. Common standards and framework for information security among member states will be developed. Besides that, ASEAN Network Security Council Action will be established to promote CERT cooperation and sharing of expertise.

Yet, no definite cyber defence policy has been adopted by ASEAN. The proposed establishment of the ASEAN Network Security Council Action is not sufficient for protecting the region's critical infrastructures and information system from cyber attacks. ASEAN should adopt the measures implemented by the EU in protecting the critical national infrastructure. The EU is the most developed example of regional initiatives to develop policies and guidelines on cyber attacks. It proposes the creation of rules and standards on cyber security due to the concerns over cyber attacks targeting critical infrastructure such as airports or power stations.[398] In a press release on 7 December 2015, Andreas Schwab, EU Parliament's rapporteur said that the MEPs close a deal on the first EU rules on cyber security.[399] The rules impose obligations on companies in critical service including energy, transport, banking, heath and water supply to report serious security breaches. The rules are perceived as necessary to strengthen the consumer's trust in cross border Internet services.[400]

To summarise, regional organisations may foster cooperation between member states and coordinate the measures against cyber attacks. However, this mechanism has not been fully utilised by states in South East

---

[398] 'Europe Agrees Response to Cyber-Attacks' *BBC News Technology* (8 December 2015) <http://www.bbc.co.uk/news/technology-35038424> accessed 1 January 2016

[399] European Parliament, 'MEPs Close Deal with Council on First Ever EU Rules on Cybersecurity' (*European Parliament*, 7 December 2015) <http://www.europarl.europa.eu/news/en/news-room/20151207IPR06449/MEPs-close-deal-with-Council-on-first-ever-EU-rules-on-cybersecurity> accessed 16 May 2016

[400] 'EU Lawmakers, Countries Agree on Bloc's First Cybersecurity Law' *The Star Online Tech News* (8 December 2015) <http://www.thestar.com.my/tech/tech-news/2015/12/08/eu-lawmakers-countries-agree-on-blocs-first-cyber-security-law/> accessed 1 January 2016

Asia due to political barriers and the limitation of the power conferred for the regional organisation. It is difficult to establish a binding regulation at the regional level as the decision making process by ASEAN is based on consensus. Thus, any measures to counter cyber attacks will be in the form of directives and guidelines. Member states have the leeway to adopt the directives according to their own needs. Accordingly, ASEAN is using the soft law approach in dealing with cyber attacks.

The development of non-binding norms on state behaviour may prevent conflict and contribute to the peaceful use of ICTs.[401] Soft law instruments can be used in dealing with cyber attacks at the international level. Soft law refers to any international instruments containing principles, norms, standards or statements of expected behaviour.[402] Soft law instruments can be distinguish from hard law instruments by analysing the intention of the maker of the instruments. Treaties are usually regarded as hard law as they are endowed with legally binding effects. Whereas, soft law consists of rules of conduct that are not intended to be legally binding and cannot be enforced in court.[403] Positivists do not consider soft law instruments such as the resolutions of the General Assembly as law proper.[404] Nonetheless, soft law instruments are significant on international relations and may crystallise into customary law. They are frequently used as a device to overcome a deadlock in relations between state pursuing different ideological or aims.[405]

6.4.4 The Imposition of Criminal Liability for Cyber Attacks Under International Law

The focus of this section is to analyse the imposition of criminal liability for cyber attacks under international criminal law. International criminal law is

---

[401] 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (2015) <http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174> accessed 14 April 2016

[402] Shelton D, 'International law and Relative Normativity' in Evans MD (ed), *International Law* (4th edn, Oxford University Press 2014) 141-169

[403] Harris D, *Cases and Materials on International Law* (n 103) 57

[404] Boyle A and Chinkin C, *The Making of International Law* (Oxford University Press 2007) 12

[405] Harris D, *Cases and Materials on International Law* (n 103) 57

designed to outlaw certain types of conduct including war crimes, genocide and international terrorism. It imposes obligation or authorises states to prosecute and punish those who engage in such conduct.[406] A state is held responsible for the violation of international humanitarian law committed by individuals whose acts are attributable to the state under international law.[407] Consequently, it is imposed with the obligation to pay compensation and to initiate disciplinary or penal action against the violators.[408] The international humanitarian law does not directly address individuals in comparison to international criminal law. Thus, the latter may be used as the mechanism to punish the perpetrator of cyber attacks. However, cyber attacks must be classified as crimes under international law to enable the international criminal tribunals such as the International Criminal Court (ICC) and national courts to exercise their jurisdiction.

The Cybercrime Convention does not address cyber attacks committed by individuals whose acts are attributable to states.[409] The Convention may be used as a basis to convict non-state actors such as Al-Qaida. The preamble to the Convention does not specify that the offences must be committed for personal purposes such as private gain or revenge. The explanatory report of the Convention stipulates that the exact meaning of intentionality should be left to national interpretation.[410] Member states are obliged to prosecute cyber attacks committed in their territory or by one of their nationals.[411] Therefore, states may initiate action against cyber attacks perpetrated by non-states actors in their territory or if the members of the armed groups are their nationals. Apart from territoriality and nationality principle, member states are not precluded from exercising universal jurisdiction.

---

[406] Cassese A and others, *Cassese's International Criminal Law* (3rd edn, Oxford University Press 2013)

[407] Article 91 1977 Geneva Protocol 1

[408] Article 87 (3) 1977 Geneva Protocol 1

[409] Section 6.4.3 p.285

[410] Council of Europe, Explanatory Report on 2001 Convention on Cybercrime, ETS No 185

[411] Article 22 of 2001 Cybercrime Convention

There is a gap in the position of cyber attacks as crimes under international law. The Tallinn Manual does not delve into the issue of individual criminal liability under either domestic or international law.[412] The existing jurisdiction of international criminal tribunals is limited compared to the national courts. For instance, the ICC can only exercise jurisdiction with respect to the commission of the crime of genocide, crimes against humanity, war crimes and the crime of aggression.[413] This demonstrates the need to analyse cyber attacks' position under international criminal law.

6.4.4.1 Rome Statue of International Criminal Court

This section analyses the inclusion of cyber attacks within the jurisdiction of the ICC. The prosecution of crimes under international law has been delegated to the international criminal tribunals such as the ICC. Article 25 of the Rome Statute provides for individual criminal responsibility, as crime against international law are committed by men, not abstract entities. The attribution of conduct to a state is necessary as actions by non-state actors that cause loss of life or serious interference with vital operations are classified as terrorism.[414] The ICC does not have the jurisdiction to hear cases involving terrorism per se unless it is committed during an armed conflict.

The ICC plays a significant role to end impunity. However, the system is not without its flaws. The ICC sometimes is incapable to investigate or to serve its indictments due to factors such as geography, history, domestic politics, traditional alliances and conflict of interests.[415] The ICC can only exercise jurisdiction to prosecute individuals for 'committing international crimes in the territory of state parties to the Rome Statute of the International Criminal Court or when the perpetrators are the nationals of the state parties'.[416] The ICC is unable to prosecute cyber attacks launched outside of the territory of a state party by a national of non-state party such as US and China. The

---

[412] Schmitt MN, *Tallinn Manual* (n 49)

[413] Article 5 of the Rome Statute of the International Criminal Court

[414] Wedgewood RG, 'Proportionality, Cyber War and the Law of War' (n 45)

[415] Griffin JB, 'A Predictive Framework for the Effectiveness of International Criminal Tribunals' (n 326)

[416] Article 12 of the Rome Statute

inability to prosecute individuals from these states weakens enforcement by the ICC.

As indicated above, the ICC may only exercise jurisdiction with respect to the crime of genocide, crimes against humanity, war crimes and the crime of aggression. The Rome Statute of International Criminal Court and the Elements of War Crimes under the Rome Statute of the International Criminal Court do not expressly provide for the offence of the interference to data and computer system. However, cyber attacks that violate the norms of international humanitarian law constitute war crimes punishable under the international criminal law. The perpetrator of cyber attacks may be prosecuted for these offences during armed conflict: (1) cyber attacks against a civilian population; (2) cyber attacks against non-military objects; and (3) cyber attacks that cause excessive collateral damage to civilians.[417]

However, some scholars argue that the ICC lacks jurisdiction to prosecute the perpetrators of information war crimes.[418] Orphardt contends that since Article 8 of the Rome Statute contains an extensive list of specific acts considered war crimes, those occurring in the cyberspace would not be included in the ICC jurisdiction.[419] The listed acts are based on the provisions of the Four Geneva Conventions, Additional Protocols to the Geneva Conventions and the Hague Regulations. Furthermore, information warfare does not fit neatly under the elements of crimes of the Rome Statute of International Criminal Court.[420] Stevens contend that the ICC may be forced to rely on the general principles stipulated in domestic law to define the elements of crimes for cyber attacks.[421] This gives a good reason for the

[417] Stevens SR, 'Internet War Crimes Tribunals and Security in an Interconnected World' (n 6)

[418] Brown D, 'A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict' (n 74)

[419] Ophardt JA, 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield' (2010) 3 Duke L & Tech Rev 1

[420] Brown D, 'A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict' (n 74)

[421] Stevens SR, 'Internet War Crimes Tribunals and Security in an Interconnected World' (n 6)

creation of an international agreement to clarify the elements of crimes for cyber attacks.[422]

6.4.4.2 The Prosecution of Cyber Attacks as Crimes Under International Law In Malaysia

This section analyses the jurisdiction of the courts in Malaysia to prosecute the perpetrator of cyber attacks under international criminal law. The prosecution of international crimes at the domestic level is done through the exercise of universal jurisdiction by national courts and the establishment of specialised international criminal tribunal usually within the domestic judiciary of post-conflict states.[423] The enforcement of international criminal law through the domestic criminal justice processes is based on the principle of aut dedere aut judicare or the duty to prosecute or extradite.[424] The exercise of these obligations depends on the standard adopted by the national criminal justice system.[425]

In Malaysia, the prosecution of the perpetrators of crimes under international law depends on two factors; firstly, a treaty ratified by Malaysia and secondly, legislation promulgated pursuant to the ratification of the treaty. Customary international law is only persuasive and can only be applied if it is not inconsistent with the provisions of the Federal Constitution.[426] Malaysia has not ratified the Rome Statute. This is perhaps due to several issues including the position of the ruler of Malaysia, Yang Di-Pertuan Agong (YDPA), the head of the armed forces of Malaysia. Yang Di Pertuan Agong is conferred with immunity under the law of Malaysia whereas the Statute of the ICC clearly negates immunity for state leaders. The ICC cannot exercise its jurisdiction with regard to the commission of crimes under international law in Malaysia unless the Security Council makes a referral.[427] Despite not

---

[422] ibid

[423] Burke-White WW, 'Regionalization of International Criminal Law Enforcement: A Preliminary Exploration' 38 Tex Int'l LJ 729 2003

[424] Bassiouni MC, 'Policy Considerations On Interstate Cooperation in Criminal Matters' 4 Pace YB Int'l L 123 1992

[425] ibid

[426] *Mohamad Ezam Bin Mohd Noor v Ketua Polis Negara & Other Appeal* [2002] 4 MLJ 449

[427] Article 13 (b) of the 1998 Rome Statute of the International Criminal Court

ratifying the Rome Statute of International Criminal Court, Malaysia has acceded the Geneva Conventions 1949.[428] The Parliament enacted the Geneva Conventions Act 1962 to transform the provisions of the conventions into the law of Malaysia. Thus, the courts in Malaysia can prosecute the perpetrators of cyber attacks by relying on the provisions of the Geneva Conventions Act 1962.

The legal issues of cybercrime and its prosecution by national courts especially in the context of armed conflict require more examination. Fleck contends that further discussion is needed to determine whether the jurisdiction of the state can be extended to objects used by the foreign government for non-commercial or official purpose and whether it entails exclusive or concurrent jurisdiction.[429] In addition, even if cyber attacks constitutes a crime under customary international law, the duty to prosecute the perpetrators can only arise based on a treaty. In the case of *Questions Relating to the Obligation to Prosecute or Extradite (Belgium v Senegal)*, the ICJ held that even though prohibition on torture is a crime under customary international law, however, the obligation to prosecute the alleged perpetrators of acts of torture under the Torture Convention applies only to facts having occurred after its entry into force for the state concerned.[430] Consequently, states are not obliged to prosecute the perpetrators of cyber attacks unless they have ratified the Rome statute of International Criminal Court or the Geneva Conventions.[431] Thus, issues may arise with regard to the willingness of the national courts to prosecute the perpetrators of cyber attacks.

6.5 Conclusion

The objective of this chapter is to ascertain the position of cyber attacks under international law and the measures used to address this problem at

[428] Geneva Conventions Act 1962

[429] Fleck D, 'Searching for International Rules Applicable to Cyber Warfare-A Critical First Assessment of the New Tallinn Manual' (2013) 18 J Conflict and Security Law 331

[430] *Questions Relating to the Obligation to Prosecute or Extradite (Belgium v Senegal)* ICJ Reports 2012

[431] Article 87 (3) of the 1977 Geneva Protocol 1

the international level. This study suggests that international law is instrumental in legitimising states' effort, establishing norms and fostering cooperation among states in dealing with cyber attacks. International law may ensure the fairness of the measures to counter cyber attacks as it champions humanitarian values and peaceful coexistence among states. The findings of the study showed that international law regulates the activities of states and non-state actors in cyberspace including use of force, cyber warfare and cyber espionage.

However, the implementation of the measures under international law in countering cyber attacks is difficult compared to other measures discussed in the previous chapters due to several reasons. The principle of state sovereignty entails that states are not obliged to abide with rules that they have not consented to. In addition, the Security Council is not a general enforcer of international law as it is subjected to the veto power. Furthermore, the jurisdiction of the international tribunals such as the ICC is limited. Malaysia's rights and obligations under international law are restricted as it is not a party to international instruments related to cyber attacks such as the Cybercrime Convention and the Rome Statute of International Criminal Court. Moreover, it lacks of capability to influence concerted action at the international level. Thus, Malaysia relies on international law by working in a cooperative way with its allies and the United Nations. Therefore, this study provides suggestions to enhance the measures to counter cyber attacks at the international level.

Firstly, international legal and non-legal frameworks should be strengthened to increase the effectiveness of the efforts to counter cyber attacks. This includes the formulation of an instrument to govern cyber weaponry and the establishment of an institution to provide assistance, coordination and assessment similar to the OPCW. Apart from international legal instrument, intergovernmental and non-governmental networks play important roles in fostering cooperation with multi stakeholders particularly the architectures of cyberspace.

Secondly, regional organisations such as ASEAN should actively engage in formulating policies and strategies to counter cyber attacks at the regional

level. The likelihood of establishing instruments at the regional level is higher due to factors such as closer geographic proximity. Moreover, soft law instruments should be fully utilised to persuade state and non-state actors including Internet and social media companies such as Google or Facebook in dealing with cyber attacks.

Thirdly, the perpetrator of cyber attacks should be imposed with criminal liability under international criminal law. Cyber attacks may constitute war crimes punishable under the Rome Statute of the International Criminal Law. However, this study suggests the creation of an international agreement to clarify the position of cyber operations conducted by states outside of armed conflict. This includes ascertaining the elements of crimes for cyber attacks under international criminal law, the jurisdiction of national courts and immunity from jurisdiction.

Finally, countermeasure should be taken against a state which is responsible for perpetrating cyber attacks. States are required to ensure that the countermeasure is proportionate, reversible and taken in response to unlawful cyber operations. They are also entitled to reparation such as compensation and restitution for wrongful acts upon satisfying the conditions to invoke the principle of state responsibility. The conduct complained of must be directed or controlled by the state that has committed the wrongful acts.

Chapter 7

Conclusion

7.1 Introduction

This chapter is structured as follows. To begin with, it gives an overview of the findings of the study. It also provides the policy implications derived from the study. Next, this chapter provides the responses to the thesis statement and research objectives. Finally, it specifies the key recommendations and suggestions for future fieldwork research and doctrinal analysis. The chapter will end with the overall conclusion of the study.

7.2 Summary of the Findings

In the beginning, this study investigated the nature of cyber attacks in order to understand its conceptual framework. This is necessary for the purpose of examining the policy and the application of the law in relation to cyber attacks in Malaysia. The doctrinal analyses showed that there has not been a consensus on the definition of cyber attacks and describing the phenomenon of cyber attacks is not straightforward.[1] Ontological enquiry was conducted in order to identify the classifications of cyber attacks. Empirical study was used in understanding cyber attacks as a phenomenon. Therefore, several variables had been identified for the enquiry.

Firstly, this study examined the identity of the perpetrator of cyber attacks. The findings suggested that the threats of cyber attacks might originate from outside or inside of Malaysia.[2] State and non-state actors may commit cyber attacks. They include foreign intelligence services, criminals, industrial competitors, hackers, hactivists and ex-employees. However, many of the participants argued that it is difficult to distinguish attacks committed by states or non-state actors.[3] Furthermore, tracing the perpetrator is

[1] Section 3.1, p.33

[2] Section 3.2.1, p.37

[3] ibid

challenging especially if the attack originates from outside of Malaysia. This may affect the investigation and apprehension of the perpetrators.

Secondly, this study assessed the victims and targets of cyber attacks. They may include specific individuals, public or private organisations. The doctrinal analysis shows that the perpetrators may target critical national infrastructure such as energy, banking, finance, transportation and telecommunications.[4] They have become increasingly integrated with the computer system. The findings also showed that attacks on critical national infrastructure might cause severe impact to the society.[5]

Thirdly, this study investigated the method and impact of cyber attacks. The findings suggested that the range of cyber attacks comprises two broad categories.[6] The first category is the attacks on the computer system and server. As indicated in chapter 3, the Tallinn Manual described cyber attacks as offensive or defensive cyber operation during international or non-international armed conflict. The purpose of the operation is to cause injury, death or destruction to military objects. It is however, noted from this study that cyber attacks are not confined to the situation of armed conflict. They may be committed during peacetime. The majority of the participants from all categories agreed that cyber attacks refer to the attacks on the computer system and server using tools including malware.[7] Furthermore, some of them argued that the attacks must cause serious impact to the victims. Consequently, an attempt to penetrate the computer system or server is classified as a threat or potential cyber attack. The second category is the disruption of national security and harmony through online seditious and defamatory statements. Most of the law enforcement officers categorised these activities as cyber attacks.[8] The maintenance of racial harmony is perceived as a matter of utmost importance in Malaysia. It is however, noted

[4] Section 3.2.2, p.45-47

[5] ibid

[6] Section 3.2.3

[7] ibid p.49-50

[8] ibid p.55-56

from this study that the measures to regulate these activities may jeopardise fundamental human rights.

The last variable is the motives of the attack. The findings indicated that the motives are divided into private and public realms.[9] The former includes acquisitive purposes such as commercial advantage and malice, while the latter comprises military strategy, political, racial and religious ideologies. Based on the variables above, this study suggested that cyber attacks could be classified into four categories of cyber wrongdoing: cybercrimes; cyberterrorism; cyber warfare and use of force under international law; and cyber espionage. This study adopted a broad approach in formulating the concept of cyber attacks. The classification of cyber attacks into different categories of cyber wrongdoing is important for the purpose of identifying the appropriate countermeasures.

After investigating the concept of cyber attacks, this study examined the strategy to counter cyber attacks in Malaysia. This includes situating the position of non-criminal and criminal law measures within the ambit of the strategy. The measures taken against the perpetrators must be real and meaningful. Therefore, an effective strategy is necessary in dealing with this problem. Results of the study have revealed that Malaysia does not have an extensive plan for cyber security at the national level.[10] Thus, this study proposed that Malaysia's National Cyber Security Policy may be strengthened by including four objectives: defend, deter, develop and international action.[11] This is based on the UK's National Cyber Security Strategy 2016-2021. The danger of cyber attacks requires responses at the domestic and international level. Therefore, non-criminal measures including social and situational crime prevention and criminal law are possible solutions to this problem. The former should be used to defend the computer networks and data system, while the latter may deter the occurrence of cyber attacks. Technological measures should be developed in order to enhance Malaysia's cyber security. Finally, action at the international level is

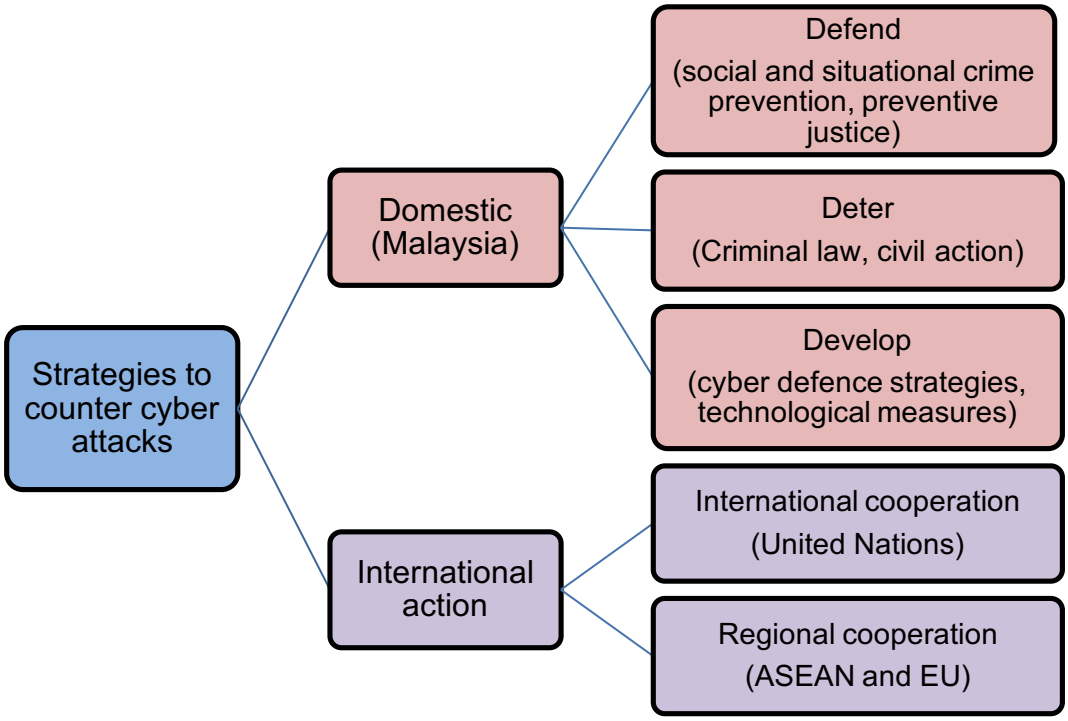
[9] Section 3.2.4, p.58

[10] Section 4.2, p.65

[11] ibid

necessary to overcome transnational issues related to cyber attacks. The strategies to counter cyber attacks in Malaysia can be summarized based on the following diagram.

Figure 7.1: Strategies to counter cyber attacks in Malaysia



As indicated in the above diagram, the strategies to counter cyber attacks in Malaysia are implemented through non-criminal measures, technological measures and criminal law. This study analysed their effectiveness and fairness in dealing with this problem. The latter is especially important for situational crime prevention such as encryption and surveillance and criminal law measures. This is to ensure that these measures conform to fundamental human rights. However, this study highlighted that the values upheld by the Malaysian society differ from the Western society.[12] Doctrinal analysis and empirical fieldwork study show that communitarianism is prevalent in Malaysian society. In addition, the effectiveness of the measures depends on factors such as good governance.

Non-criminal measures are divided into several categories. The first category is preventive measures. It comprises social prevention policy, situational crime prevention, and the role of the architecture of the Internet,

[12] Section 4.2, p.67

national CERT and private sector. Social prevention policy may be used to deter the commission of cyber attacks. This includes educating the potential victims and wrongdoers. The majority of the participants from all categories felt that education is pertinent in order to increase awareness among the public especially the youths. The findings showed that they are vulnerable to computer misuse.[13] They need to know the repercussion of being involved in organised crime and to avoid from becoming a victim. Some of the participants argued that the public should assume the responsibility for their own failure in taking adequate preventive measures such as using appropriate password for their computer. Results of the study have revealed that the Malaysian Communications and Multimedia Commission and Cybersecurity Malaysia have been actively involved in education campaigns. [14] However, some of the participants contended that the campaigns should be stepped up. Consequent, this study suggested that institutions such as the National Youth Consultative Council should take active role in developing cyber security courses especially for youth.

The data also revealed that situational crime prevention is perceived as an effective tool in dealing with cyber attacks. Doctrinal analysis showed that intervention strategies and devices could be used to decrease the opportunities to commit crimes.[15] Consequently, they play a role in reducing the crime rate. The findings have indicated a number of strategies that may be used to prevent the commission of cyber attacks. [16] Firstly, risk assessment may be used to enhance the reliability of the information system. Secondly, target hardening may be used to deter cyber attacks. This includes controlling the access to computer system and the usage of anti virus software, anti spyware and firewall.

In addition, encryption may reduce the opportunities to commit cyber attacks. However, the results showed that many people do not possess the

[13] Section 4.3.1.1, p.81-82

[14] ibid, p.83-84

[15] Section 4.3.1.2, p.88-90

[16] ibid, p.90

knowledge to use this programme.[17] Moreover, some of the law enforcement officers contended that encryption might impede the process of investigation. Criminals may use encryption to evade the law. Therefore, the enforcement officers in Malaysia are allowed to access computerised data including encryption and decryption codes. Nevertheless, they should be cautious in exercising this power in order to avoid infringing the right of privacy.

This study found that some of the organisations in Malaysia use surveillance to enhance their security especially against their own employees.[18] In addition, the law enforcement officers in Malaysia are vested with the power to conduct interception of communications. This study showed that surveillance in Malaysia is difficult due to the decentralisation of the Internet.[19] In addition, disparity of laws between states especially on the regulation of the content of the Internet may render this measure ineffective. Furthermore, the perpetrators may use masking tools to evade this measure. Apart from the effectiveness, some of the participants perceived this measure as unfair as it can be used to infringe their privacy. Accordingly, surveillance should be done in accordance with due process of law.

Besides situational crime prevention, this study examined the role of the architecture of the Internet in dealing with cyber attacks in Malaysia. Some of the participants in this study asserted that architects such as the Internet Service Providers prefer self-regulation. Furthermore, they argued that the intervention by the government should be done sparingly. The imposition of regulatory measures such as the storage of data on the architects may affect their profits and financial capability. Therefore, this measure is difficult to be implemented in Malaysia.

The study revealed that the Computer Emergency Response Team and the private sector might take a more active role in dealing with cyber attacks.[20] MyCERT provides technical advice and assistance especially to small companies and individuals who cannot afford to hire security professionals.

---

[17] Section 4.3.1.2.4, p.97

[18] Section 4.3.1.2.5, p.100

[19] ibid, p.101-102

[20] Section 4.3.1.4, p. 111-118

In addition, the law enforcement officers seek Mycert's assistance to identify and apprehend the perpetrator of cyber attacks. The findings also suggested that cooperation among CERTs at the domestic and international level should be strengthened in addressing cross boundaries attacks.[21]

For their part, private entities play a significant role in developing Malaysia's cyber security policy through the establishment of groups such as Mysecurity Community. In addition, the rise of cyber attacks and concern with cyber security has caused a rapid proliferation of private security companies. They offer solutions and services including intelligence and the investigation of cybercrime cases.

Civil action and remedy could be used against the perpetrators of cyber attacks. However, the empirical findings showed that most of the participants especially the law enforcement officers taught that this measure is not effectiveness in dealing with cyber attacks.[22] Nevertheless, doctrinal analysis suggests that civil action and remedy have been used to recover losses suffered as a result of breach of data caused by cyber attacks in countries such as the US. Therefore, this study suggests that the victims may consider initiating civil action to seek for damages as an alternative to criminal law especially in situation involving the theft of confidential data. This remedy may be included in the Personal Data Protection Act 2010 or the Criminal Procedure Code. Apart from damages, the Malaysian lawmakers may consider the application of civil remedy such as injunction against the perpetrators of cyber attacks.

After examining the effectiveness and fairness of non-criminal measures, this study reviewed the application of criminal law in dealing with cyber attacks. The empirical findings revealed that the law enforcement officers in Malaysia do not officially use the term 'cyber attacks'. Furthermore, this term is not expressly provided in any legislation in Malaysia. Accordingly, there is no specific offence for cyber attacks in Malaysia. Thus, the categories of cyber wrongdoing stipulated in chapter 1 are used to identify the law governing cyber attacks in Malaysia. The first category is cyber attacks in

[21] ibid

[22] Section 4.3.2, p.119

the guise of cybercrime. This category comprises: computer integrity crimes; computer related crimes; and computer content crimes.

Cyber attacks on the computer system using tools such as malware are classified as computer integrity crimes. The empirical findings showed that they fall within the ambit of the Computer Crimes Act 1997.[23] The perpetrators may be charged for committing unauthorised access to the computer system, unauthorised modification of the computer programme and data or illegal interception. It is however, noted from this study that cyber attacks should be differentiated from mere trespassing or modification of data without the usage of tools such as malware.[24] Most of the law enforcement officers and deputy public prosecutors contended that the Act focuses on the means of attacks instead of dishonest intention. Thus, the Act usually is read together with other legislation such as the Penal Code. Therefore, some of the police officers and deputy public prosecutors argued that the Act is sufficient in dealing with cyber attacks in this category. However, they also acknowledged that a large-scale cyber attacks including the attacks on the critical national infrastructure may not fall within the ambit of the Act due to the inadequacy of sentencing. Thus, they argued that the perpetrator should be charged under the Penal Code for murder, destruction to property or causing bodily injury.

As discussed in chapter 3, cyber attacks include online sedition and defamation in Malaysia. They are categorised as computer content crime. Theoretical analysis and empirical findings showed that the law enforcement officers and criminal agencies have extensive powers in this area. This includes blocking and removing the online content. Furthermore, the Sedition Act 1948 and the Evidence Act 1950 have been amended in order to deal with computer content crime especially seditious offences more effectively. On the other hand, some of the participants argued that the government should not use this power to suppress dissenting opinions and political views. They applauded the recent Federal Court's decision to declare that s 3 (3) of the Sedition Act 1948 as unconstitutional. Accordingly,

[23] Section 5.2.1.1, p.141-145

[24] ibid, p.144

the law enforcement officers especially the Malaysian Communications and Multimedia Commission must be seen as being fair and impartial.

Cyber attacks may be committed for the purpose of stealing confidential information and espionage. They are classified as computer related crime. The empirical findings showed that these attacks are perceived as severe and do not fall within the ambit of the Computer Crimes Act 1997.[25] They fall within the ambit of the Officials Secret Act 1972 and the Penal Code. These laws provide harsh penalty for spying and espionage. However, doctrinal analysis revealed that the government could invoke the Officials Secret Act 1972 to restrict the access to information on matters of public interest.[26]

Next, the Personal Data Protection Act 2010 protects personal information from cyber attacks. The Act criminalises the unlawful collection, disclosure and procurement of personal data. However, the empirical findings suggested that the effectiveness of the Act depends on the awareness of the data subjects of their rights. Thus, this study recommended several measures to enhance the effectiveness of the Act including strict enforcement and regular advisory visits and audit by the Department of the Personal Data Protection.

The next category of cyber wrongdoing is cyberterrorism. Doctrinal analysis and empirical findings indicated that terrorist groups use the computer technology and cyberspace for various purposes such as recruitment and to disseminate their propaganda.[27] They may even use the cyberspace to commit cyber attacks. Terrorism is perceived as a serious threat in Malaysia. Accordingly, the law enforcement officers and criminal agencies are vested with extensive powers in dealing with terrorism. Apart from the Penal Code, the Security Offences (Special Measures) Act 2012 and Prevention of Terrorism Act 2015 were enacted to deal with this problem. So far, these laws have been used significantly to arrest and detain suspected members of terrorist organisations such as ISIS. In addition, a special tribunal has been established to hear cases involving extremism and militancy. The

[25] Section 5.2.1.3, p.160-161

[26] ibid, p.162

[27] Section 5.2.2, p.167-168

usage of executive order especially the Prevention of Terrorism Act 2015 may infringe fundamental liberties. Accordingly, this study suggested several safeguards including the establishment of an independent body to review any detention.

After analysing the laws governing cyber attacks, this study considered the introduction of new offences for cyber attacks in Malaysia.[28] The EU Directive 2013/40/EU recommended the imposition of harsh punishment for attacks against computer system in order to protect the critical national infrastructure. Consequently, a new offence was created in UK to cater for the most serious cyber attacks. This study has used empirical findings to show that similar offence should be introduced in Malaysia. Some of the participants in this study highlighted the inadequacy of the Computer Crimes Act 1997 in dealing with a large scale cyber attacks. In addition, the proposed offence provides clarity with regards to the elements of crimes and the appropriate sentencing.

Preventive justice should be used as a tool to dissuade the potential perpetrators from committing the attacks. It comprises precursor offences, executive orders and the power of the enforcement and criminal justice agencies. The Cybercrime Convention criminalises the possession of computer programme and code for the purpose of conducting a cyber attack. This study has used empirical findings to determine the need for such measures to be implemented in Malaysia. Half of the participants from all categories consider that the creation of this offence may deter the commission of cyber attacks and enhance the power of the enforcement officers.

Besides possessing the materials to commit cyber attacks, precursor offences also include criminalising the creation, distribution and procurement of materials to commit cyber attacks. Directive 2013/40/EU and the Cybercrime Convention provide for the criminalisation of production, sale, procurement for use, import and distribution of devices to commit cyber attacks. Doctrinal analysis suggested that these offences are created for the purpose of disrupting the availability of tools to commit cyber attacks in black

[28] Section 5.3, p.171-203

market. The empirical findings showed that the law in Malaysia is vague in relation to these offences. Some of the participants acknowledged the absence of the law in Malaysia with respect to the creation and distribution of malware. More than half of the participants from all categories agreed that this measure might be effective in dealing with cyber attacks. The Malaysian lawmakers should consider the inclusion of these offences in the Communications and Multimedia Act 1998 or the Computer Crimes Act 1997.

This study analysed the usage of executive orders against the perpetrator of cyber attacks in Malaysia. The empirical analysis showed that executive orders are prevalent Malaysia.[29] As indicated above, the device has been used as countermeasure against actions that may jeopardise national security including terrorism. The findings also revealed that this measure is perceived as necessary in order to circumvent the rigidity of criminal process.[30] Some of the participants from all category felt that the potential perpetrators of cyber attacks should be denied access to computers and the Internet. Therefore, the Prevention of Crime Act may be invoked to register and detain the potential wrongdoers. It is noted, however from this study that human rights implication must be considered before denying or restricting a person's access to computer and Internet. This is pertinent as the government may abuse executive order in order to suppress political views. Accordingly, this study suggested that the executive order in Malaysia should be reviewed to include procedural safeguards including declaring the gist of the case, consultation with the Chief Officer of the Police and conferring the power of review on the High Court.

Lastly, this study examined the implementation of criminal law measures against cyber attacks in Malaysia. This includes the obstacles and possible reforms. To begin with, this study observed that cyber attacks are underreported in Malaysia.[31] The public are reluctant to report cyber attacks to the authorities due to several reasons. Some of the participants

[29] Section 5.3.3, p.202

[30] ibid, p.201

[31] Section 5.4.1, p.205

suggested that individuals and corporations might be reluctant to report the attacks in order to maintain their reputation and public confidence. In addition, their business may be disrupted due to the investigations. However, the refusal of the victims to report cyber attacks may hamper the criminal justice process in dealing with this problem. Thus, this study suggested that the government should encourage the public to report the occurrence of cyber attacks through education and awareness campaigns.

Next, this study assessed the technical expertise among law enforcement officers, prosecutors and judges in Malaysia. The empirical findings showed that the law enforcement officers especially from the Cybercrime and Multimedia Investigation Division of the Royal Malaysia Police are performing several tasks including forensic analysis and surveillance.[32] In addition, they are handling not only cybercrimes but also other crimes that have computer element such as online cheating and gambling. Apart from multitasking and a broad scope of cases, some of the participants argued that the police lack the expertise especially in handling forensic investigations. However, this assessment is perceived as inaccurate as the police are not trained to become cyber security specialists.[33] This task is performed by other agencies such as Cybersecurity Malaysia, Mycert and the Malaysian Communications and Multimedia Commission. Therefore, this study suggested that Malaysia should consider the establishment of a specialised law enforcement agency to deal with cybercrimes especially a large-scale cyber attacks. The agency should be based on the UK's National Crime Agency. Alternatively, the Malaysian Communications and Multimedia Commission should be vested with the power to investigate and prosecute a large-scale cyber attacks due to their technical capability.

Apart from the technical expertise, the empirical findings suggested that the investigation and prosecution of the perpetrators of cyber attacks might be hampered by extra-territoriality.[34] This is due to the lack of cooperation among nation states in areas such as the request for mutual legal

[32] Section 5.4.2, p.210

[33] ibid, p.212

[34] Section 5.4.3, p.216-220

assistance. Moreover, some of the law enforcement officers argued that the principle of dual criminality might impede the apprehension of the wrongdoers outside of Malaysia especially in relation to computer content crimes. The regulations of the Internet are not the same for every country. Thus, this study examined the ways to foster cooperation among states in chapter six.

Finally, this study analysed the role of sentencing in countering cyber attacks in Malaysia. The empirical findings showed that severe punishment is perceived as necessary for symbolic reasons such as to denounce the commission of cyber attacks.[35] Furthermore, the empirical findings revealed that sentencing might be designed to allow the authorities to utilise the perpetrators' technical expertise. [36] Accordingly, the formulation of an appropriate rehabilitation programme should be conducted for the perpetrator of cyber attacks.

Alternatively, this study suggested that the establishment of a sentencing guideline for cyber attacks. The Sentencing Guidelines Council of UK has issued the Overarching Principles: Seriousness Guideline. It provides the standard of culpability and harm for the purpose of sentencing. So far, the empirical findings suggested that there is no sentencing guideline in Malaysia.[37] Some of the participants in this study argued that this guideline might ensure the uniformity and certainty of the punishment. Therefore, this study proposed that the sentencing guideline should be used to determine the seriousness of cyber attacks for the purpose of sentencing. It should be read together with other legislation such as the Computer Crimes Act 1997 and the Penal Code.

In summary, the measures to deal with cyber attacks in Malaysia could be divided into several levels. Ayres and Braithwaite formulated the 'Pyramid of Strategies of Responsive Regulation', which prescribe the phase of enforcement actions for occupational health and safety, environment or nursing home regulation. At the base of the pyramid is persuasion. This

---

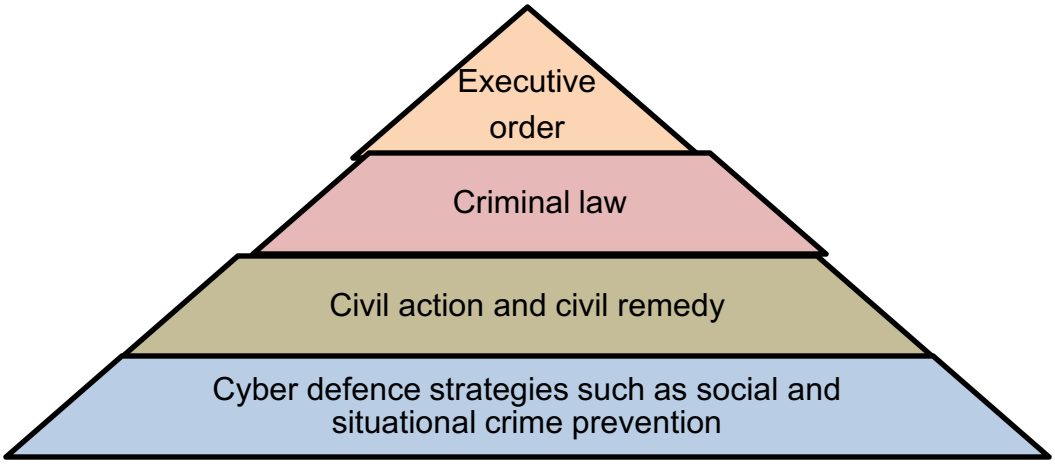
[35] Section 5.4.4, p.221

[36] ibid, p.224

[37] ibid, p.225

measure should be used especially in 'industries where technological and environmental realities change so quickly that give detailed content to the law cannot keep up to date'.[38] If the wrongful acts persist, the next layer provides for a warning letter. After that is the imposition of civil monetary penalties. If this fails, criminal prosecution should be used.[39] At the top layer is a plant shutdown or temporary suspension of license to operate and permanent revocation of license'.[40] The focus of the pyramid is in its form rather than the content. This is because different sanctions apply to different regulatory arenas.[41] Thus, the same structure with modification is applicable to the measures in dealing with cyber attacks. The width of each layer of the pyramid represents the frequency in which these responses are used and the severity of the responses in dealing with cyber attacks.

Figure 7.2: Pyramid of the measures to counter cyber attacks at the domestic level



As indicated in Figure 1, at the base of the pyramid are cyber defence strategies such as social and situational crime prevention. Education, campaigns and situational crime prevention may be used to persuade and prevent the public from committing cyber attacks. The next layer is civil action and remedy such as injunction. After that, criminal law should be

[38] Ayres I and Braithwaite J, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992) 26

[39] ibid 35

[40] ibid 36

[41] ibid

invoked against the perpetrator of cyber attacks. At the uppermost of the pyramid is executive order. This measure should only be used to defend the computer systems of critical national infrastructure against a large-scale cyber attacks when all other responses have failed or are more than likely to fail. It should be used to protect the critical national infrastructure instead of a vague concept like national security. The executive order should be used as the last resort in order to avoid potential abuse by the government.

Apart from the measures to counter cyber attacks in Malaysia, the next strategy is international action. This strategy is used especially in dealing with use of force; cyber attacks in the guise of cyber warfare; and cyber espionage. Doctrinal analysis suggested that international law is necessary in countering cyber attacks due to several reasons. Firstly, it symbolises solidarity among states in dealing with this problem. Secondly, it legitimises the efforts to counter cyber attacks at the international level. International instruments such as the international humanitarian law emphasises humanitarian values.[42] Apart from fairness, the findings showed that international law is perceived as an effective measure to counter cyber attacks due to their trans-jurisdictional character.[43] It may facilitate the standardisation of the laws and the legal processes in dealing with this problem. Furthermore, international law is instrumental in dealing with threats to international peace and security including cyber attacks.

This study investigated the position and the regime governing cyber attacks under international law. To begin with, it examines the prohibition of the threat or use of force involving cyber attacks. Doctrinal analysis showed that scale and effect are important for the purpose of categorising cyber attacks as a use of force amounting to armed attack within the purview of Article 2(4) of the Charter of the United Nations.[44] The attacks must cause direct destructive effects on the victims and property. It is however, noted from this study that the direct effect approach excludes economic violence caused by

[42] Section 6.2, p.229

[43] Section 6.2.2, p.232-235

[44] Section 6.3.1.1, p.242

cyber attacks. This study suggested that they might be classified as unlawful intervention under international law.

Next, this study examined the application of the law of armed conflict in relation to cyber attacks guise as cyber warfare. The doctrinal analysis revealed that the Geneva and Hague Conventions as well as customary international humanitarian law might be invoked against cyber attacks committed during international and non-international armed conflict. [45] Accordingly, states are obliged to adhere to the principles of international humanitarian law in conducting cyber attacks during armed conflict. However, doctrinal analysis revealed that the implementation of the rules might be challenging due to the nature of cyber attacks.[46] For instance, the principle of distinction is difficult to implement as most instruments of communication and information are categorised as dual- purpose objects.

After examining cyber attacks in the guise of cyber warfare, this study assessed the position of cyber espionage under international law. As stated chapter 3, cyber espionage may be classified as cyber attacks as it may cause serious harm to national security. Doctrinal analysis showed that cyber espionage might be committed during armed conflict or peacetime. The law of armed conflict does not expressly prohibit cyber espionage. Nevertheless, states have to ensure that cyber operations including surveillance during armed conflict are done in conformity with the human rights laws. During peacetime, states may conduct intelligence gathering in order to counter external and internal threats such as organised crime and terrorism. It is however, noted from this study that the public are sceptical about the need for extensive surveillance and data collection by the authorities and intelligence services. They are worried that these activities may interfere with their right to privacy. Therefore, surveillance should be done in accordance to the due process of law.

Finally this study assessed the measures to counter cyber attacks under international law. Doctrinal analysis suggested that the regulation of cyberspace at the international level is difficult due to disagreement over the

[45] Section 6.3.2

[46] Section 6.3.2.1.3, p.257-265

form of governance. Moreover, states may have different views on key issues such as the classification of cyber attacks. In the absence of international agreement to regulate cyber attacks, states may resort to remedies under customary international law such as countermeasures and the principle of state responsibility. Apart from that, other mechanisms may be used including soft law instruments, transnational networks and international criminal law. The findings of this thesis also suggested that regional organisations including ASEAN might play an active role to facilitate cooperation among member states in dealing with cyber attacks.[47]

7.3 Thesis Responses

The primary purpose of this thesis is to examine the current roles, values and potential of non-criminal and criminal law in dealing with cyber attacks in Malaysian law. Accordingly, this thesis used doctrinal study, empirical method and policy transfer to analyse the implementation of non-criminal and criminal law measures to counter cyber attacks in Malaysia. The findings showed that criminal law is a necessary reaction to counter cyber attacks alongside non-criminal measures on the basis of effectiveness and fairness.

7.4 Research Objectives Responses

This study was designed to answer the objectives of the research. Firstly, it identified the concept of cyber attacks by investigating the nature and attributes of cyber attacks as a phenomenon. There has not been a consensus on the definition of cyber attacks. Accordingly, this study adopted a broad approach in formulating a concept of cyber attacks. Cyber attacks maybe committed by states and non-state actors for private and public purposes. The perpetrators may target individuals, private or public organisations and critical national infrastructure. The attacks may be committed during situation of armed conflict or outside of armed conflict. The attacks must cause serious impact to the victims. This includes the destruction or incapacitation of the computer system and server. In addition,

[47] Section 6.4.3.3, p. 298-299

the disruption of national security and harmony through online seditious and defamatory statements is classified as cyber attacks in Malaysia. Therefore, cyber attacks are divided into four categories: cybercrimes; cyberterrorism; cyber warfare and use of force under international law; and cyber espionage.

Secondly, this study assessed the approaches to counter cyber attacks and to situate non-criminal and criminal measures within the strategy to counter cyber attacks. Malaysia does not have an extensive plan for cyber security at the national level. This study proposed that Malaysia should strengthen its cyber security policy by adopting these strategies: defend, deter, develop and international action. Social and situational crime prevention should be used to defend Malaysia against the threat of cyber attacks. Criminal law should be utilised to deter the perpetrator of cyber attacks. Technological measures should be developed in dealing with cyber attacks. International action including cooperation between regional and international organisations is necessary due to the trans-jurisdictional characteristics of cyber attacks.

Thirdly, this study examined the effectiveness and fairness of non-criminal law and criminal law measures in dealing with cyber attacks in Malaysia. This study suggested that education; campaigns; and situational crime prevention should be used as the primary mechanisms in countering cyber attacks in Malaysia. In addition, the victims may initiate civil action to claim damages and civil remedy such as injunction against the perpetrators of cyber attacks. Regulatory measures such as financial penalty should be used against serious cyber attacks including data breach. The application of criminal law depends on the gravity of cyber attacks. Severe punishment should be imposed on a large-scale cyber attacks including attacks against critical national infrastructure. Finally, executive measures should be used as the last resort to protect critical national infrastructure from cyber attacks.

Finally, this study ascertained the position of cyber attacks under international law and the measures used to address this problem at the international level. This study suggested that international law is instrumental in dealing with cyber attacks due to their trans-jurisdictional character. The prohibition against use of force is applicable to cyber attacks that amount to

an armed attack. In addition states are obliged to conduct their cyber operations during armed conflict in accordance with the provisions of international humanitarian law. International law does not prohibit cyber espionage during armed conflict and peacetime. Nevertheless, states have to ensure that their intelligence gathering activities are conducted in conformity with the human rights law. The function of international law in countering cyber attacks may be enhanced through the development of legal and non-legal framework including the formulation of a cyber weapon convention, transnational networks, regional cooperation and international criminal law.

7.5 Key Recommendations

This study recommends several measures based on the notion of fairness and effectiveness to improve the laws and responses to counter cyber attacks in Malaysia. First, Malaysia should make cyber security education and campaigns a focus of attention. The National Youth Consultative Council and the Malaysian Institute for Research in Youth Development should conduct studies to develop cyber security courses and syllabus for youth. Second, Malaysia should fully exploit and explore the usage of technological measures and situational crime prevention such as encryption in dealing with cyber attacks. Third, the PDPA should be extended to the government officials in order to ensure that they are accountable for data breach. In addition, the Personal Data Protection Commissioner should be conferred with the power to impose financial penalties. Fourth, Malaysia should promulgate an offence similar to s 3ZA (1) of the Computer Misuse Act 1990. Fifth, Malaysia should criminalise precursor offences including the possession of materials and the creation, distribution and procurement of materials to commit cyber attacks. Sixth, Malaysia should establish a sentencing guideline for cyber attacks to ensure the certainty, uniformity and fairness of the punishment. Seventh, the government should play an active role to persuade the public to report cyber attacks through awareness campaigns. Eight, Malaysia should establish a specialist unit similar to the NCA to increase the effectiveness of criminal law in dealing with cyber attacks.

Besides the domestic level, Malaysia should exercise several actions at the international level. First, Malaysia should support the adoption of an international instrument to govern cyber weaponry and establish an institution similar to OPCW. Second, Malaysia should intensify its effort to persuade the members of ASEAN to formulate stronger policy and legal instrument in dealing with cyber attacks at the regional level. Third, Malaysia should actively engage in supporting intergovernmental networks in order to foster cooperation with multi stakeholders. Lastly, Malaysia should invoke countermeasures and state responsibility against unlawful cyber operations perpetrated by another state.

7.6 Recommendations for Future Fieldwork Research

This study provided an evaluative perspective on the concept, strategy and the measures to counter cyber attacks in Malaysia through doctrinal analysis, policy transfer and empirical fieldwork study. It encountered several limitations during the process of gathering information and collection of data in Malaysia. Interviewing more information security officers from different national infrastructure sectors would have strengthened the study. However, the researcher's application to interview officers from health and energy sectors was declined due to reasons such as security and administrative obstacles. In addition, the researcher could have drawn information about the formulation of cyber security policy and strategy at the regional and international level by interviewing officials from organisations such as ASEAN. Besides that, this study has not offered an evaluative perspective on the power of the police, court processes, prosecution and the law of evidence, as the scale of the debate in these areas is extensive. Future research will involve interviews with the law enforcement officers, legal practitioners and judges in order to improve these areas in dealing with cyber attacks in Malaysia.

Moreover, the researcher would wish to discover more information about the phenomenon of cyber attacks in Malaysia by interviewing individuals such as hackers, hacktivists and the victims of cyber attacks. Some of the participants were willing to introduce the researcher to the victims and hackers. However, the researcher was unable to arrange the meeting due to

time constraint and ethical concerns. Future research should involve interviews with hackers and the victims in order to understand the phenomenon of cyber attacks in Malaysia.

7.7 Future Doctrinal Analysis

Doctrinal analysis suggested that there is a gap in the position of cyber attacks that are committed outside of armed conflict as a crime under international law. Accordingly, future research is necessary in order to clarify issues such as the elements of crimes and the prosecution of states' officials for orchestrating cyber attacks. Besides that, the researcher could explore other alternative in countering cyber attack in Malaysia including mandatory cyber security education at schools. There is also a need to further investigate the usage of civil remedy and situational crime prevention in dealing with crimes including cyber attacks in Malaysia.

7.8 Conclusion

Cyber attacks have been designated a prime threat to national security in Malaysia, the UK, and elsewhere. Within this intensifying and highly topical policy field, the study argues for an integrated approach, combining legal and non-legal, criminal and non-criminal responses. To date, cyber security policies have emphasised proactive mechanisms, such as technical tools and standards. Reactive measures, including criminal offences, have not been fully utilised. Accordingly, this study assesses the extent to which Malaysia domestic measures and International laws have tackled cyber attacks and the potential reforms. Proposed ideas include social education, cyber architecture, preventive justice, civil liability, new criminal offences, and new institutions. Effectiveness is a key performance indicator, but, especially following revelations by Edward Snowden, a fair balance must be struck between individual rights, such as privacy, and the collective interest in state security.

Bibliography

Abdullah MDH, 'A Practical Approach to Criminal Procedure' (2002) 4 [2002] 4 MLJ i

Abdullah KB, 'Emerging Threats to Malaysia's National Security' (2010) 5 Journal of Policing, Intelligence and Counter Terrorism 55

Ablon L and Libicki M, 'Hackers' Bazaar: The Markets for Cybercrime Tools and Stolen Data' Defense Counsel Journal; Apr 2015; 82,2; ABI/INFORM Collection 143

Ahmad R, Yunos Z, 'The Application of Mixed Method in Developing a Cyber Terrorism Framework' (2012) 3 Journal of Information Security 209

Ahmad R, Yunos Z, Sahib S, Yusof M, 'Perception on Cyber Terrorism: A Focus Group Discussion Approach' (2012) 3 Journal of Information Security 231

Ahmad SSS, *Malaysian Legal System* (2nd edn, LexisNexis 2007)

Akdeniz Y, Walker C, Wall D (eds), *The Internet, Law and Society* (Longman 2000)

Alexander L and Kessler KD, 'Mens Rea and Inchoate Crimes' The Journal of Criminal Law and Criminology (1973-), Vol 87, No 4 (Summer,1997), 1138-1193

Annual Report 2015 Human Rights Commission of Malaysia' (*Human Rights Commission of Malaysia*) <https://drive.google.com/file/d/0B_iu0JnQlclBQW5OZTRhTF9XTnc/view?pref=2&pli=1> accessed 7 February 2017

Anwar DF, 'Indonesia: National vs Regional Resilience?' in Cunha DD (ed), *Southeast Asian Perspectives on Security* (Institute of Southeast Asian Studies 2000)

Arquilla J, 'Rebuttal Cyberwar is Already Upon Us' (2012) 192 Foreign Policy; Mar/Apr 2012; 192 84

Aruna P and Inn TK, 'Fewer Political Appointees on GLCs' *The Star* (22.07.2016) Business News

Ashworth A, 'Criminal Justice Act 2003: Part 2: Criminal Justice Reform - Principles, Human Rights and Public Protection' [2004] Criminal Law Review

Ashworth A and Zedner L, 'Prevention and Criminalization: Justifications and Limits' (2012) 15 New Crim L Rev 542

Ashworth A and Zedner L, *Preventive Justice* (Oxford University Press 2014)

Ashworth A, *Sentencing and Criminal Justice* (5th edn Cambridge University Press, 2010)

Awang ZH, *Research Methodology for Business and Social Science* (UPENA UiTM 2011)

Ayres I and Braithwaite J, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992)

Azmil S, 'Crimes on the Electronic Frontier-Some Thoughts on the Computer Crimes Act 1997' [1997] 3 MLJ lix

Aziz SA, 'The Malaysian Legal System: The Roots, The Influence and The Future' (2009) 3 [2009] 3 MLJ xcii

Bachman R, Schutt RK, *The Practice of Research in Criminology and Criminal Justice* (5th edn, Sage 2014) 119

Baker DJ, *The Right Not to be Criminalized* (Ashgate, 2011) 92

Bassiouni MC, 'Policy Considerations On Interstate Cooperation in Criminal Matters' 4 Pace YB Int'l L 123 1992

Bauman Z, *Globalization. The Human Consequences* (Polity Press 1998)

Barak G, 'Towards an Integrative Study of International Crimes and State-Corporate Criminality: A Reciprocal to Gross HUman Rights Violations' in Smeulers A and Haveman R (eds), *Supranational Criminology: Towards a Criminology of International Crimes* (intersentia 2008) 5

BBC, 'Researchers Warn of New Stuxnet Worm' (*BBC News Technology*, 19 October 2011) <http://www.bbc.co.uk/news/technology-15367816> accessed 14 January 2014; Taddeo M, 'Information Warfare: A Philosophical Perspective' (2012) 25 Philos Technol (2012) 25:105–120

Beck U, *Risk Society: Towards a New Modernity* (SAGE Publications Ltd 1992) 4

Beck U, Giddens A and Lash S, *Reflexive Modernization: Politics, Tradition and Aesthetics in the Modern Social Order* (Polity Press 1994)

Bejtlich R, 'To hack, or not to hack?' (*The Brookings Institution*, 28 September 2015) <http://www.brookings.edu/blogs/up-front/posts/2015/09/28-us-china-hacking-agreement-bejtlich> accessed 16 May 2016

Bell D, *The Coming of-Post-Industrial Society* (Basic Books 1999)

Bell J, 'Legal Research and Comparative Law' in Hoecke MV (ed), *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline* (Hart Publishing 2013)

Bentham J, *An Introduction to the Principles of Morals and Legislation* (Burns JH and Hart HLA eds, Clarendon Press Oxford 1996)

Berman G and Gold E, 'Procedural Justice from the Bench: How Judges Can Improve the Effectiveness of Criminal Courts' (2012) 51 Judges J 20

Bernama, 'Lebih 2 Juta Sertai Program Klik Dengan Bijak SKMM' <http://www.skmm.gov.my/Media/Press-Clippings/Lebih-2-Juta-Sertai-Program-Klik-Dengan-Bijak-SKMM.aspx> accessed 9.09.2016

BERNAMA, 'Tackling Daish More Difficult Than Tackling Communists - DPM' *Astro Awani* (1.11.2016) <http://english.astroawani.com/malaysia-news/tackling-daish-more-difficult-tackling-communists-dpm-121160> accessed 2.11.2016

Berton TA and Denning DE, 'Cyberwarfare' [2011] IEEE Security & Privacy September/October 2011

Bevir M and Rhodes R.A.W, *Interpreting British Governance* (Routledge 2003)

Bishop P, 'Criminal Law as a Preventative Tool of Environmental Regulation: Compliance Versus Deterrence' (2009) 60 N Ir Legal Q 279

Black R, 'A Brief History of Climate Change' (*BBC News Science and Environment*, 20 September 2013) <http://www.bbc.co.uk/news/science-environment-15874560> accessed 14 January 2014

Blank LR, 'After "Top Gun": How Drone Strikes Impact the Law of War' (2011-2012) 33 U Pa J Int'l L 675

Blount PJ, 'The Preoperational Legal Review of Cyber Capabilities: Ensuring the Legality of Cyber Weapons' (2012) 39 N Ky L Rev 211

Bowles R, Faure M and Garoupa N, 'The Scope of Criminal Law and Criminal Sanctions: An Economic View and Policy Implications' (2008) 35 JL & Soc'y 389

Brenner SW, 'Cybercrime: Rethinking Crime Control Strategies' in Jewkes Y (ed), *Crime Online* (Willan Publishing 2007) 24

Brenner SW and Clarke LL, 'Distributed Security: Preventing Cybercrime' 23 J Marshall J Computer & Info L 659 2004-2005

Bright J, 'Crime Prevention: the British Experience' in Stenson K and Cowell D (eds), *The Politics of Crime Control* (SAGE Publications, 1991)

Broomhall B, *International Justice and the International Criminal Court: Between Sovereignty and the Rule of Law* (Oxford University Press 2004)

Brown D, 'A Proposal for an International Convention To Regulate the Use of Information Systems in Armed Conflict' (2006) 47 Harv Int'l LJ 179

Brown DK, 'Criminal Law Theory and Criminal Justice Practice' (2012) 49 Am Crim L Rev 73

Brown G, 'Spying and Fighting in Cyberspace: What is Which?' 8 J NAT'L SECURITY L &POL'Y ___ (forthcoming 2016)

Buchan R, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 J Conflict Security Law 211.

Burke-White WW, 'Regionalization of International Criminal Law Enforcement: A Preliminary Exploration' (2003) 38 ex Int'l LJ 729

Buchan R, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?' (2012) 17 J Conflict Security Law 211

Byman D, 'Why Drones Work: The Case for Washington's Weapon of Choice' (2013) 92 Foreign Aff 32

Caballero-Anthony M, *Regional Security in Southeast Asia: Beyond the ASEAN Way* (The Institute of Southeast Asian Studies 2005)

Parker G (ed), *Cambridge Illustrated History. Warfare* (Cambridge University Press 1995)

Cane P and Kritzered HM (eds), *The Oxford Handbook of Empirical Legal Research* (Oxford University Press 2010)

Carozza PG, 'Uses and Misuses of Comparative Law In International Human Rights: Some Reflections on the Jurisprudence of the European Court of Human Rights ' (1997-1998) 73 Notre Dame L Rev 1217

Cassese A and others, *Cassese's International Criminal Law* (3rd edn, Oxford University Press 2013)

Castells M, *The Rise of the Network Society*, vol 1 (2nd edn, Blackwell Publishing 2000)

Castro RCD, *Managing Strategic Unipolarity* in Cunha DD (ed), *Southeast Asian Perspectives on Security* (Institute of Southeast Asian Studies 2000)

Caton JL, *Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations, And Response Implications* (United States Army War College Press, 2014)

Cavadino M and Dignan J, *Penal Systems: A Comparative Approach* (SAGE Publications 2006)

Cavelty MD, 'Cyber Threats' in Cavelty MD and Mauer V (eds), *The Routledge Handbook of Securities Studies* (Routledge 2010)

Chandler D and Munday R, *A Dictionary of Media and Communication* (Oxford University Press 2011)

Charney JI, 'Universal International Law' (1993) 87 A.J.I.L 529

Chesterman S, 'The Spy Who Came in From the Cold War: Intelligence and International Law ' 27 Mich J Int'l L 1071 2005-2006

Childers J and Hentzi G (eds), *The Columbia Dictionary of Modern Literary and Cultural Criticism* (Columbia University Press 1995)

Chimni B.S, 'Sovereignty, Rights and Armed Intervention' in Charlesworth H and Coicaud J-M (eds), *Fault Lines of International Legitimacy* (Cambridge University Press 2010)

Chokkattu J, 'A New Bill Will Force Companies to Place a Backdoor in Their Devices to Undermine Their Own Encryption' (*Digital Trends*, 24.04.2016) <http://www.digitaltrends.com/mobile/compliance-with-court-orders-act-of-2016-news/> accessed 12.09.2016

Chong PK, 'Bloated Malaysia Civil Service Presents Headache for Najib' *Bloomberg* (10.08.2016) Bloomberg Markets <http://www.bloomberg.com/news/articles/2016-08-10/jobs-for-life-malaysians-hard-to-budge-as-najib-eyes-voter-risk> accessed 20.08.2016

Chu B, Holt TJ and Ahn GJ, 'Examining the Creation, Distribution, and Function of Malware On-Line: Executive Summary' NCJRS <https://www.ncjrs.gov/pdffiles1/nij/grants/230112.pdf>

Coicaud J-M, 'Deconstructing International Legitimacy' in Charlesworth H and Coicaud J-M (eds), *Fault Lines of International Legitimacy* (Cambridge University Press 2010)

Coicaud J-M, 'The Evolution of International Order and Fault Line of International Legitimacy' in Charlesworth H and Coicaud J-M (eds), *Fault Lines of International Legitimacy* (Cambridge University Press 2010)

Clarke RV, 'Introduction' in Clarke RV (ed), *Situational Crime Prevention: Successful Case Studies* (2nd edn, Harrow and Heston 1997)

Code of Ethics for Researchers in the Field of Criminology *(British Society of Criminology)* <http://britsoccrim.org/docs/CodeofEthics.pdf> accessed 12 July 2014

Committee of the Ministers of the Council of Europe, 'Convention on Cybercrime: Explanatory Report' ((ETS No 185), 2001)

Commission of the European Communities, Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF accessed 23.04.2015

Commission, 'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union' COM (2013) 48 final

Council of Europe, 'International Co-operation Under the Convention on Cybercrime'<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304352> accessed 3 January 2016

Cornwell R, 'US Declares Cyber War on China: Chinese Military Hackers Charged with Trying to Steal Secrets from Companies including Nuclear Energy Firm' *Independent* (19 May 2014) <http://www.independent.co.uk/life-style/gadgets-and-tech/us-charges-chinese-military-hackers-with-cyber-espionage-bid-to-gain-

advantage-in-nuclear-power-9397661.html> accessed 13 May 2014

Crawford J, 'Sovereignty as Legal Value' in Crawford J and Koskenniemi M (eds), *The Cambridge Companion to International Law* (Cambridge University Press 2012)

Crawford J, *State Responsibility* (Cambridge University Press 2013)

Cryer R, Harvey T, Sokhi-Bulley B, *Research Methodologies in EU and International Law* (Hart Publishing 2011)

Csonka P, 'The Council of Europe's Convention on Cyber Crime and Other European Initiatives' <http://www.cairn-int.info/article.php?ID_ARTICLE=E_RIDP_773_0473> accessed 22.06.2016

Cybersecurity: A Global Issue Demanding a Global Approach' <http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html> accessed 11 April 2016

'Cyber-security: Problems Outpace Solutions' (*Security & Defence Agenda*, 2013) <www.securitydefenceagenda.org> accessed 13 March 2014

Daddow O and Gaskarth Jamie, 'From Value Protection to Value Promotion' in Bevir M, Daddow O and Hall I (eds), *Interpreting Global Security* (Routledge 2014)

D'Aspremont J, 'Non-State Actors and the Social Practice of International Law' in Noortmann M, Reinisch A and Ryngaert C (eds), *Non-State Actors in International Law* (Hart Publishing Oxford and Portland, Oregon 2015) 12

Dawson C, *Introduction to Research Methods: A Practical Guide for Anyone Undertaking a Research Project* (4th edn, howtobooks 2009)

Dearth DH, 'Critical Infrastructures and the Human Target in Information Operations' in Campen AD and Dearth DH (eds), *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict* (AFCEA International Press, 2000) 204

Denning DE, 'Activism, Hacktivism and Cyberterrorism: The Internet As A Tool For Influencing Foreign Policy' in Arquilla J and Ronfeldt D eds, *Networks and Netwars* (RAND 2001)

Denning DE, 'The Future of Cryptography' in Loader BD (ed) *The Governance of Cyberspace* (Routledge 1997)

Denning DE, 'Cyberterrorism: The Logic Bomb versus the Truck Bomb' Global Dialogue; Autumn 2000; 2, 4, 29

Dev PR, '"Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Needs for Formal U.N Response' 50 Tex Int'l L J 381 2015

Dhanapal S and Sabaruddin JS, 'Rule of Law: An Initial Analysis of Security Offences (Special Measures) Act (SOSMA) 2012' (2015) 23 IIUMLJ 1

Diffie W and Landau S, *Privacy on the Line: The Politics of Wiretapping and Encryption* (The MIT Press 2007)

Dijk JV, *The World of Crime. Breaking the Silence on Problems of Security, Justice, and Development Across the World* (Sage Publications 2008)

Doig A, *State Crime* (Willan Publishing 2011) 77

Dörmann K, *Elements of War Crimes Under the Rome Statute of the International Criminal Court: Sources and Commentary* (Cambridge University Press 2003)

Droege C, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2013) 94 International Review of the Red Cross 533

Duff RA and Marshall SE, 'Benefits, Burdens and Responsibilities: Some Ethical Dimensions of Situational Crime Prevention' in Hirsch Av, Garland D and Wakefield A (eds)*, Ethical and Social Perspectives on Situational Crime Prevention* (Hart Publishing 2000)

Dugard J, *International Law: A South African Perspective* (3rd edn, Juta & Co Ltd 2005)

Dunlap CJ, 'Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors' 87 Neb L Rev 712

Dunlap JC Jr, 'The Law and the Human target in Information Warfare: Cautions and Opportunities' in Campen AD and Dearth DH (eds), *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict* (AFCEA International Press, 2000)

Dupont B, 'Hacking the Panopticon' in Deflem M (ed), *Surveillance and Governance: Crime Control and Beyond* (Emerald JAI Press 2008)

Dworkin R, *Taking Rights Seriously* (Duckworth 1997) 184

Eck JE and Clarke RV, 'Classifying Common Police Problems: A Routine Activity Approach' in Smith MJ and Cornish DB (eds), *Theory For Practice in Situational Crime Prevention* vol 16 (Willan Publishing 2003) 8

Elfstrom G, *International Ethics: A Reference Handbook* (ABC-CLIO 1998)

Eijkelhof HMC and others, 'Weapons' (1982) 2 Bulletin of Science Technology & Society 1982 2: 59

Etzioni A, 'Communitarian Revisited' Journal of Political Ideologies, 19:3, 241-260

Etzioni A, *The Spirit of the Community* (Fontana Press London 1995)

Etzioni A, 'Cybersecurity in the Private Sector' (2011) 28 Issues in Science and Technology 58

Etzioni A, *From Empire to Community: A New Approach to International Relations* (Palgrave Macmillan 2004)

European Parliament and the Council Directive 2013/40/EU of 12 August 2013 on attacks against information systems and replacing council framework decision 2005/222/JHA

European Union Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU Mapping Member States' Legal Frameworks* (Publications Office of the European Union, 2015)

Fafinski S, *Computer Misuse. Responses, Regulation and the Law* (Willan Publishing 2009)

Farrell G and others, 'The Crime Drop and the Security Hypothesis' Journal of Research in Crime and Delinquency 48 (2) 147-175

Faulkner D, *Crime, State and Citizen: A Field Full of Folk* (2nd edn Waterside Press, 2006)

Feinberg J, *Harm to Others. The Moral Limits of the Criminal Law*, vol one (Oxford University Press 1984)

Ferzan KK, 'Preventive Justice and the Presumption of Innocence ' Crim Law and Philos (2014) 8: 505-525

Finch BE and Spiegel LH, 'Litigation Following a Cyber attack: Possible Outcomes and Mitigation Strategies Utilising the Safety Act' 30 Santa Clara Computer & High Tech LJ 350

Fleck D, ‘Searching for International Rules applicable to Cyber Warfare-A Critical First Assessment of the New Tallinn Manual’ (2013) 18 J Conflict and Security Law 331

Flick U, *An Introduction to Qualitative Research* (Metzler K ed, 5 edn, Sage 2014)

Fook LC, Hassan CA and Bajury MSHM, *Introduction to Principles and Liabilities in Criminal Law* (2nd edn, LexisNexis 2012)

Forcese C, ‘Spies Without Borders: International Law and Intelligence Collection’ Journal of National Security Law & Policy 01/2011, Volume 5, Issue 1

Foreign Involvement In the Critical National Infrastructure: The Implications for National Security (*Intelligence and Security Committee*, 2013), Cm 8629

Franck TM, *Fairness In International Law and Institutions* (Oxford University Press New York 1995)

Friesen TL, ‘Resolving Tomorrow's Conflicts Today: How New Developments Within The U.N. Security Council Can Be Used To Combat Cvberwarfare’ (2009) 58 Naval L Rev 89

Fritz N and Flaherty M, ‘Unjust Order: Malaysia's Internal Security Act’ (2002) 26 Fordham International Law Journal

Fu C and others, ‘Study on the Contract Characteristics of Internet Architecture’ Enterprise Information Systems, 5:4, 495-513, DOI: 101080/175175752011570457

Fuller LL, *The Morality of Law* (New Haven and London, Yale University Press 1964)

Galletta A, *Mastering the Semi-structured Interview and Beyond* (New York University Press 2013)

Gallie WB, *Understanding War* (Routledge 1991)

Garland D, ‘Ideas, Institutions and Situational Crime Prevention’ in Hirsch Av, Garland D and Wakefield A (eds), *Ethical and Social Perspectives on Situational Crime Prevention* (Hart Publishing 2000)

GCHQ, ‘Common Cyber Attacks: Reducing the Impact’ <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/400106/Common_Cyber_Attacks-Reducing_The_Impact.pdf> accessed 23.02.2015

Gibbs JP, ‘Towards Theories About Criminal Justice’ Journal of Contemporary Criminal Justice, 02/1998, Volume 4, Issue 1

Giddens A, ‘The Nation State and Violence: Volume Two of a Contemporary Critique of Historical Materialism’ in Webster F (ed), *Theories of the Information Society* (Routledge 1995)

Graham DE, 'Cyber Threats and the Law of War' (2010) 4 J. Nat'l Sec L. & Pol'y 2010 87

Grant J, Will There Be Cybersecurity Legislation? 4 J. Nat’l Sec. L.& Policy 103 2010

Gray C, ‘The Use of Force and International Legal Order’ in Evans MD (ed), *International Law* (4th edn, Oxford University Press 2010)

Greenfield VA and Paoli L, ‘A Framework to Access the Harms of Crimes’ (2013) Br J Criminal (2013) 53 (5): 864-885 doi: 101093/bjc/azt018

Greenwald G, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (Penguin Books 2014)

Gurule J, ‘Holding Banks Liable Under the anti-Terrorism Act for Providing Financial Services to Terrorists: An Ineffective Legal Remedy in Need of Reform’ 41 J Legis 184 2014-2015

Handler SG, ‘The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare’ (2012) 48 Stan J Int'l L 209

Haley HJ, ‘Correctional Effectiveness: An Elusive Concept’ (1982) 24 Canadian J Criminology 205

Harding C, ‘Member State Enforcement of European Community Measures: The Chimera of 'Effective' Enforcement’ (1997) 4 Maastricht J Eur & Comp L 5

Harris D, *Cases and Materials on International Law* (7th edn, Sweet and Maxwell 2010)

Hart HLA, *The Concept of Law* (2nd edn, Oxford University Press 1997)

Henckaerts J-M and Doswald-Beck L, *Customary International Humanitarian Law Volume 1: Rules* (Cambridge University Press 2005)

Hickling RH, *Malaysian Law. An Introduction to the Concept of Law in Malaysia* (2nd edn, Pelanduk Publications 2001)

Hiller JS, ‘Civil Cyberconflict: Microsoft, Cybercrime, and Botnets’ 31 Santa Clara Computer & High Tech LJ 163

Hollis DB, ‘Why States Need An International Law For Information Operations’ 11 Lewis & Clark L Rev 1023 2007

Holt TJ, ‘Examining the Forces Shaping Cybercrime Markets Online’ Social Science Computer Review 31(2) 165-177

Holt TJ, Burrus GW and Bossler AM, *Policing Cybercrime and Cyberterror* (Carolina Academic Press 2015)

Home Affairs Committee, *Radicalisation: the Counter-narrative and Identifying the Tipping Point (*HC 2016-17, 135)

Home Office UK, A Strong Britain in an Age of Uncertainty: The National Security Strategy, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf accessed 23.04.2015

Home Office and Ministry of Justice, ‘Impact Assessment. Serious Crime Bill: Amendments to Computer Misuse Act 1990’, 2014, S 42 of the UK’s Serious Crimes Act 2015

Home Office, *Home Office Circular Serious Crime Act 2015* (Home Office, 2015)

Honderich T, *The Oxford Companion to Philosophy* (2nd edn, Oxford University Press 2006)

House of Lords and House of Common Joint Committee on Human Rights, *The Government’s Policy on the Use of Drones for Targeted Killing. Second Report of Session 2015–16* (House of Lords and House of Commons, 2016)

House of Representatives Deb 17 April 2012, 3

House of Representatives Deb 18 April 2012, 9

House of Representatives Deb 6 April 2016, 18

House TW, ‘Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"’ (*The White House*, i April 2015) <https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m> accessed 16 May 2016

Hudson A, 'Is Cyber-Warfare a Genuine Threat?' (*BBC Click*, 1 February 2011) <http://news.bbc.co.uk/1/hi/programmes/click_online/9393589.stm> accessed 15 January 2014

Hung LC, 'ASEAN Charter: Deeper Regional Integration under International Law?' (2010) 9 Chinese J Int'l L 821 2010

Hurrell A, *On Global Order: Power, Values and the Constitution of International Society* (Oxford University Press New York 2007)

Ince D, *A Dictionary of the Internet* (3rd edn, Oxford University Press 2013)

'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (*The Red Cross and The Red Crescent* 2011)

Institute for Economics and Peace, 'Global Terrorism Index 2015: Measuring and Understanding the Impact of Terrorism' START <http://economicsandpeace.org/wp-content/uploads/2015/11/2015-Global-Terrorism-Index-Report.pdf> accessed 1.11.2016

Jacquette D, *Ontology* (Shand J ed, Acumen 2002)

Jewkes Y and Yar M, 'Policing Cybercrime: Emerging Trends and Future Challenges' in Newburn T (ed), *Handbook of Policing* (2nd edn, Willan Publishing 2008

Jones T and Newburn T, *Policy Transfer and Criminal Justice: Exploring US Influence Over British Crime Control Policy* (Open University Press 2007) 3

Jones T and Newburn T, 'Comparative Criminal Justice Policy Making in the United States and the United Kingdom: The Case of Private Prisons' (2005) 45 Brit J Criminal 58

Jougleux P and Synodinou T-E, 'Prevention of Cyber Attacks' in Iglezakis I (ed), *The Legal Regulation of Cyber Attacks* (Kluewer Law International BV, The Netherlands 2016) 104

Josiane Cauquelin PL, Birgit Mayer-Konig ed, *Asian Values: An Encounter with Diversity* Curzon (Press 1998)

Jupp V, *Methods of Criminalogical Research* (Routledge 1989)

Kamarudin ARB, 'The Relevancy of Preventive Detention in Malaysia' (2005) 6 MLJ xcvii

Kartha T, 'Trans-national Crime and Light Weapons Proliferation: Security Implications for the State' <https://www.idsa-india.org/an-dec9-3.html> accessed 7.04.2016

Katzenstein PJ, 'Introduction: Alternatives Perspectives on National Security' in Katzenstein PJ (ed), *The Culture of National Security*: *Norms and Identity in World Politics* (Columbia University Press New York 1996)

Kaye D, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, General Assembly A/71/373

Kennedy J and Weimann G, 'The Strength of Weak Terrorist Ties' (2011) Terrorism and Political Violence, 23:2, 201-212, DOI: 101080/095465532010521087

Kessler O and Werner W, 'Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare' (2013) 26 Leiden Journal of International Law 793

King M, 'The Political Construction of Crime Prevention: A Contrast between the French and British Experience' in Stenson K and Cowell D (eds), *The Politics of Crime Control* (Sage Publications 1991)

King N and Horrocks C, *Interviews in Qualitative Research* (Sage Publications 2010)

Koblentz GD and Mazanec BM, 'Viral Warfare: The Security Implications of Cyber and Biological Weapons' Comparative Strategy, 32:5, 418-434, DOI: 101080/014959332013821845

Kodar E, 'Computer Network Attacks in the Grey Areas of Jus Ad Bellum and Jus In Bello' (2009) 9 Baltic YB Int'l L 133

Koepsell DR, *The Ontology of Cyberspace. Philosophy, Law and the Future of Intellectual Property* (Open Court 2000)

Koops BJ and Brenner SW (ed), *Cybercrime and Jurisdiction: A Global Survey* (T.M.C. Asser Press 2006)

Koskenniemi M, 'What Is International Law For' in Evans MD (ed), *International Law* (4th edn, Oxford University Press 2010)

Kowert P and Legro J, 'Norms, Identity and Their Limits: A Theoretical Reprise' in Katzenstein PJ (ed), *The Culture of National Security: Norms and Identity in World Politics* (Columbia University Press New York 1996)

Kravets D, 'Guilty Plea in Anonymous' DDoS Scientology Attack' (*wired.com*, 26.01.2010) <http://www.wired.com/2010/01/guilty-plea-in-scientology-ddos-attack/> accessed 1.03.2015

Kvale S, *Interviews. An Introduction to Qualitative Research Interviewing* (Sage Publications 1996)

Lea J, *Crime & Modernity* (Sage Publications 2002)

Lebow RN, *Why Nations Fight. Past and Future Motives for War* (Cambridge University Press 2010)

Lefkowitz D, 'The Principle of Fairness and States' Duty to Obey International Law' 24 Can J L & Jurisprudence 327 2011

Leng OTS, Khan S, Hossein RM, *Cybercrime and Cyber Terrorism: The Security Measures In Malaysia* (Lamber Academic Publishing 2012)

Leong C, 'Speech by Christopher Leong, President of the Malaysian Bar at the Openinng of the Legal Year 2014' (2014) 1 [2014] 1 MLJ

Lepage H, 'Study On Measures Other Than Criminal Ones In Cases Where Environmental Community Law Has Not Been Respected in the EU Member States' (*Milieu Ltd. and Huglo Lepage Associates*, 2004) <http://ec.europa.eu/environment/legal/crime/pdf/ms_summary_report.pdf> accessed 16 February 2014

Lipton JD, 'Combating Cyber-Victimization' 26 Berkeley Tech LJ 1103 2011

Loader BD (ed), *The Governance of Cyberspace* (Routledge 1997)

Marra WC, McNeil SK, 'Understanding "The Loop": Regulating the Next Generation of War Machines' (2013) 36 Harv J L & Pub Pol'y 1139

Masum A, 'The Rule of Law Under the Malaysian Federal Constitution' (2009) 6 MLJ c

Marcus J, 'Are We Really Facing Cyberwar?' (*BBC News Technology*, 5 March 2013) <http://www.bbc.co.uk/news/technology-21653361> accessed 13 January 2014

May T, *Social Research. Issues, Methods and Process* (2nd edn, Open University Press 1997)

Mccahill M, 'Plural Policing and CCTV Surveillance' in Deflem M (ed), *Surveillance and Governance: Crime Control and Beyond* (Emerald JAI Press 2008) 215

McNamara MR, 'Dysfunction in Cyberspace: The Insider Threat' in Campen AD and Dearth DH (eds), *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict* (AFCEA International Press, 2000)

Mcquade SC, *Understanding and Managing Cybercrime* (Pearson 2006)

Melzer N, 'Cyberwarfare and International Law' (*UNIDIR*, 2011) <http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf> accessed 7 March 2014

Michalowski RJ and Pfuhl EH, 'Technology, Property and Law: The Case of Computer Crime' (1991) 15 Crime, Law and Social Change

Mill JS, *Utilitarianism and the 1868 Speech on Capital Punishment* (Sher G ed, 2nd edn, Hackett Publishing Company 2001)

Moir L, *The Law of Internal Armed Conflict* (Cambridge University Press 2002)

Morris C, Murphy C, *Getting a PhD in Law* (Hart Publishing 2011)

Mushkat R, *International Environmental Law and Asian Values: Legal Norms and Cultural Influences* (UBC Press 2004)

Muti A, Tajer K and Macfaul L, 'Cyberspace: An Assessment of Current Threats, Real Consequences and Potential solutions in New Ways of War: Is Remote Control Warfare Effective' [2014] The Remote Control Digest

National Security Council, *Arahan No. 24 (Directive No. 24)* (National Security Council, Prime Minister's Department Malaysia, 2011)

Nelken D, *Comparative Criminal Justice* (Sage Publications 2010)

Noor NM, *Writing Research and Thesis Proposals: Guidelines and Examples* (UPENA UiTM 2011)

Nor MWH, 'Hate Speech on the Rise: Lacunae in Malaysian Law' [2016] 1 LNS(A) lxvii 1

Office of the Press Secretary, 'Launch of the Cybersecurity Framework' (*The White House*, 12 February 2014) <http://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework> accessed 13 August 2014

Oona A. Hathaway RC, Levitz P, Nix H, Nowlan A, Perdue W, Spiegel J, 'The Law of Cyber-Attack' (2012) 100 Calif L Rev 817

Ophardt JA, 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield' (2010) 3 Duke L & Tech Rev 1

Ortner D, 'Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-boundary Cybercrime' [2015] Brigham Young University Law Review

Osborne D and Gaebler T, *Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector* (Addison-Wesley Publishing Company 1992)

Partington M, 'Empirical Legal Research and Policy Making' in Cane P and Herbert M. Kritzered (eds), *The Oxford Handbook of Empirical Legal Research* (Oxford University Press 2010)

Patail AG, 'Speech by the Attorney General of Malaysia, At the Opening of the Legal Year 2012' (2012) 1 MLJ cxiii

Patail AG, 'Speech by the Attorney General of Malaysia at the Opening of the Legal Year 2013' (2013) 1 MLJ ccxi

Pearton M, *Diplomacy, War and Technology Since 1830* (University Press of Kansas 1984)

Perry AE, Mcdougall C and Parrington DP (eds)*, Reducing Crime. The Effectiveness of Criminal Justice Intervention* (John Wiley & Sons 2006)

Peters M, 'Section 114A...A Presumption of Guilt?' [2012] 6 MLJ ciii

Adams M and Bomhoff J (eds), *Practice and Theory in Comparative Law* (Cambridge University Press 2012)

Prime Minister, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and prosperous United Kingdom* (Cm 9161, 2015)

Rainsford S, 'Hackers for Hire' (BBC World Service Assignment 14 March 2010) <http://www.bbc.co.uk/programmes/p006j7qf> accessed 14 January 2014

Reid G, Kamarulzaman A and Sran SK, 'Malaysia and Harm Reduction: The Challenges and Responses' The International Journal on Drug Policy April 2007

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (2015) <http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174> accessed 14 April 2016

"Report on Developments in the Field of Information and Telecommunications in the Context of International Security" (RES 69/28) https://unoda-web.s3.amazonaws.com/wp-content/uploads/2015/08/GermanyISinfull.pdf accessed 11.04.2016;

Banakar R and Travers M (eds), *Theory and Method in Socio-Legal Research* (Hart Publishing 2005) 279

Rhodes RAW, 'The Hollowing Out of the State: The Changing Nature of the Public Service in Britain ' The Political Quarterly Publishing Co Ltd 1994

Riesta I, 'Global Accounts of the Wrongfulness of Criminal Behaviour' (2011) 3 Contemp Readings L & Soc Just 110

Rid T and Mcburney P, 'Cyber-Weapons' (2012) 157 The RUSI Journal, 157:1, 6-13

Riccio LJ, 'Direct Deterrence-An Analysis of the Effectiveness of Police Patrol and Other Crime Prevention Technologies' (1974) Journal of Criminal Justice, Vol 2 pp 207-217

Riesta I, 'Global Accounts of the Wrongfulness of Criminal Behaviour' (2011) 3 Contemp Readings L & Soc Just 110

Rosenbaum DP, Lurigio AJ and Davis RC, *The Prevention of Crime: Social and Situational Strategies* (Wadsworth Publishing Company 1998)

Roscini M, *Cyber Operations and the Use of Force in International Law* (Oxford Univerity Press 2014)

Rubin AP, *Ethics and Authority in International Law* (Cambridge University Press 1997)

Rubin HJ and Rubin IS, *Qualitative Interviewing. The Art of Hearing Data* (2nd edn, Sage 2005)

Rutherford A, *Transforming Criminal Policy* (Waterside Press, 1996)

Sahamid B, *Jurisprudens dan Teori Undang-undang dalam Konteks Malaysia (Jurisprudence and Legal Theories in Malaysia)* (Sweet & Maxwell Asia 2005)

Sani MAM, 'Balancing Freedom of Speech and National Security in Malaysia' Asian Politics & Policy Volume 5, Number 4 Pages 585–607

Saul B, *Defining Terrorism In International law* (Oxford University Press 2006)

MC Bassiouni, 'A Policy-Oriented Inquiry into the Different Forms and Manifestations of International Terrorism' in MC Bassiouni (ed), Legal Responses to International Terrorism (Martinus Nijhoff 1988) 1

Salman A, Er AC, Wan MWA, Abdul Latif R, 'Tracing the Diffusion of Internet in Malaysia: Then and Now' (2013) 9 Asian Social Science 9

Sands P and Klein P, *Bowett's Law of International Institutions* (5th edn, Sweet & Maxwell London 2001)

Scheppele KL, 'Comparative Law: Problems and Prospects ' (2011) 26 Am U Int'l l 935

Schmitt MN (ed), *Tallinn Manual on the International law Applicable to Cyber Warfare* (Cambridge University Press 2013)

Schmitt MN, '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law' [2014] Virginia Journal of International Law 54

Schmitt MN, 'Classification of Cyber Conflict' (2012) 17 J Conflict Security Law 245

Schmitt MN, 'Wired Warfare: Computer Network Attack and Jus In Bello' (2002) 84 IRRC 365

Schwartz KD, 'Industrial Automation Enters the Internet Era' [2002] Electronic Business Oct 2002, 28, 10

Schaap AJ, 'Cyber Law Edition: Cyber Warfare Operations: Development and User Under International Law' (2009) 64 AF L Rev 121

Schewick BV, *Internet Architecture and Innovation* (MIT Press 2010) 19-20

Sentencing Guidelines Council, *Overarching Principles: Seriousness Guideline*, http://www.sentencingcouncil.org.uk/wp-content/uploads/web_seriousness_guideline.pdf, accessed 15 December 2016

Faruqi SS, 'Free Speech and the Constitution' [1992] 4 CLJ 1xiv

Faruqi SS, *Document of Destiny: the Constitution of the Federation Of Malaysia* (Star Publications (Malaysia) Berhad 2008)

Shiels M, 'Cyber War Threat Exaggerated Claims Security Expert' (*BBC News Technology*, 16 February 2011) <http://www.bbc.co.uk/news/technology-12473809> accessed 14 January 2014

Silver DB, 'Computer Network Attack as a Use of Force under Article 2(4)' in Schmitt MN and O'Donnell BT (eds), *Computer Network Attack and International Law* (Naval War College Newport, Rhode Island 2002) 83

Singh D, "Evolution of the Security Dialogue Process Asia-Pacific Region" in Cunha DD (ed), *Southeast Asian Perspectives on Security* (Institute of Southeast Asian Studies 2000)

Singh P, Chan YF, Sidhu GK, *A Comprehensive Guide to Writing A Research proposal* (Venton Publishing 2006)

Simma B and others (eds), *The Charter of the United Nations. A Commentary*, vol III (3rd edn, Oxford University Press 2012)

Sivalingam J, 'Bar Begins Campaign to Repeal Anti-Terror Law' (*The Malaysian Bar*, 16.05.2015)

<http://www.malaysianbar.org.my/legal/general_news/bar_begins_campaign_to_repeal_anti_terror_law.html> accessed 19.05.2015

Sivanandram H, Keng YM and Carvalho M, 'Prevention of Terrorism, Special Measures Against Terrorism Bills tabled for First Reading' *The Star Online* (30.03.2015) <http://www.thestar.com.my/News/Nation/2015/03/30/POTA-Bill-tabled-first-reading/> accessed 19.06.2015

Smith DJ, 'Less Crime Without More Punishment' [1999] Edinburgh Law Review

Solce N, 'The Battlefield of Cyberspace: The Inevitable New Military Branch-the Cyber Force' 18 Alb LJ Sci & Tech 293

Stevens SR, 'Internet War Crimes Tribunals and Security in an Interconnected World' (2009) 18 Transnat'l L & Contemp Probs 657

Strachan H, *European Armies and the Conduct of War* (Routledge 1983)

Stamp G, 'UK Seeks 'Consensus' at Cyberspace Conference' (*BBC News Politics*, 18 October 2011) <http://www.bbc.co.uk/news/uk-politics-15355739> accessed 14 January 2014

Stohl M, 'Cyber Terrorism: a Clear and Present Danger, the Sum of All Fears, Breaking Point or Patriot Games?' Crime Law Soc Change (2006) 46:223–238, DOI 101007/s10611-007-9061-94

Sulmasy G and Yoo J, 'Counterintuitive: Intelligence Operations and International Law' 28 Mich J Int'l L 625 2006-2007

Sutton A, Cherney A and White R, *Crime Prevention: Principles, Perspectives and Practices* (Cambridge University Press 2008)

Taddeo M, 'Information Warfare: A Philosophical Perspective' (2012) 25 Philos Technol (2012) 25:105–120

Tan EKB, 'The ASEAN Charter as "Legs to Go Places": Ideational Norms and Pragmatic Legalism in Community Building in Southeast Asia' 12 SYBIL 171 2008

Tasioulas J, 'International Law and the Limits of Fairness' EJIL (2002), Vol 13 No 4, 993–1023

Taylor C, 'Disclosure of Foreign Intelligence Material: CPIA, Norwich Pharmacal and the War on Terror' (2011) 15 Int'l J Evidence & Proof

Taylor PA, *Hackers* (Routledge 1999)

The Concise Oxford English Dictionary (11th edn, Oxford University Press 2008)

Thomson JE, *Mercenaries, Pirates and Sovereigns* (Princeton University Press 1994)

Thorp A, 'Drone Attacks and the Killing of Anwar al- Awlaqi: Legal Issues' (*International Affairs and Defence Section, House of Commons Library*, 20 December 2011) <http://www.parliament.uk/business/publications/research/briefing-papers/SN06165/drone-attacks-and-the-killing-of-anwar-alawlaqi-legal-issues> accessed 9 February 2014

Thiru S, 'Speech by Steven Thiru, President, Malaysian Bar at the Opening of the Legal Year 2016' [2016] MLJ xxiv

Tranter K, 'The speculative Jurisdiction. The Science Fictionality of Law and Technology' 20 Griffith L Rev 817

Trapp KN, 'Back to Basics: Necessity, Proportionality, and the Right of Self-Defence against Non-State Terrorist Actors' The International and Comparative

Law Quarterly, Vol 56, No 1 (Jan, 2007)

Tsagourias N, 'The Tallinn Manual on the International Law Applicable to CyberWarfare: A Commentary on Chapter II—The Use of Force' in Gill TD (ed), *Year Book of International Humanitarian Law 2012* (15th edn, T.M.C. Asser Press)

Tubbs D, Luzwick PG and Sharp WGS, 'Technology and Law: The Evolution of Digital Warfare' in Schmitt MN and O'Donnell BT (eds), *Computer Network Attack and International Law* (Naval War College Newport, Rhode Island 2002)

Tyrell PJ, 'Protecting the National Critical Infrastructure: The Human Dimension From a Government Perspective' in Campen AD and Dearth DH (eds), *Cyberwar 3.0: Human Factors in Information Operations and Future Conflict* (AFCEA International Press, 2000) 212

United Nations Office on Drugs and Crime, 'Comprehensive Study on Cybercrime' (*United Nations* 2013) <http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf> accessed 20.10.2016

US Department of Homeland Security, NIPP 2013 Partnering for Critical Infrastructure Security and Resilience, http://www.dhs.gov/sites/default/files/publications/National-Infrastructure-Protection-Plan-2013-508.pdf accessed 23.04.2015

Waheed AH, 'Offences of the New World: Understanding E-Crime' [2010] 1 LNS(A) lii

Walden I, *Computer Crimes and Digital Investigations* (2nd edn, Oxford University Press 2015) 12

Walker C, *Blackstone's Guide to the Anti-Terrorism Legislation* (Oxford University Press 2009)

Walker C (ed), *The Criminal Law Review. Special Edition: Crime, Criminal Justice and the Internet* (Sweet & Maxwell 1998)

Walker C and Rehman J, ''Prevent' Responses to Jihadi Extremism' in *Global Anti-Terrorism Law and Policy* (2nd edn, Cambridge University Press 2012)

Walker C, 'The Impact of Contemporary Security Agendas against Terrorism on the Substantive Criminal Law' in Masferrer A (ed), *Post 9/11 and the State of Permanent Legal Emergency Security and Human Rights in Countering Terrorism* (Springer 2012)

Wall DS, *Cybercrime. The Transformation of Crime in the Informative Age* (Polity Press 2007)

Wall DS, 'Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace' Police Practice and Research, Vol 8, No 2, May 2007, pp 183–205

Wall DS, 'The Internet as a Conduit for Criminal Activity' in Pattavina A (ed), *Information Technology and the Criminal Justice System* (SAGE Publications 2005) 79-80

Wasik M, *Crime and the Computer* (Clarendon Press 1991)

Waxman MC, 'Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)' (2011) 36 Yale J Int'l L 421

Weber R, 'Inside Cybersecurity' Inside Washington Publishers <http://0-search.proquest.com.wam.leeds.ac.uk/docview/1492017089?accountid=14664> accessed 6.10.2016

Wedgwood RG, 'Proportionality, Cyberwar, and the Law of War' (2002) 76 Int'l L Stud Ser US Naval War Col 219

Weimann G, 'Cyberterrorism: How Real is the Threat?' (2004) The United States Institute of Peace Special Report 119

Weimann G, 'Cyberterrorism: The Sum of All Fears?' Studies in Conflict & Terrorism 28:2, 129-149, DOI: 101080/10576100590905110

Werle G, *Principles of International Criminal Law*, (2nd edn, T.M.C. Asser Press 2005)

Williams PD (ed), *Security Studies: An Introduction* (2nd edn, Routledge 2013) 187

Wilson JQ and Kelling GL, 'Making Neighbourhood Safe' The Atlantic; Feb 1989; 263, 2: ABI/ INFORM Collection

Wilson W, *Central Issues in Criminal Theory* (Hart Publishing 2002)

Wuschka S, 'The Use of Combat Drones in Current Conflicts - A Legal Issue or a Political Problem?' (2011) 3 Goettingen J Int'l L 891

Yar M, 'Computer Hacking: Just Another Case of Juvenile Delinquency?' The Howard Journal Vol 44 No 4 September 2005

Yar M, *Cybercrime and Society* (SAGE Publications 2006)

Yar M, 'E-Crime 2.0: the Criminological Landscape of New Social Media' Information & Communications Technology Law Vol 21, No 3, October 2012, 207–219

Yar M, 'Sociological and Criminological Theories in the Information Era' in Leukfeldt R and Stol W (eds), *Cyber Safety: An Introduction* (Eleven International Publishing 2012) 52-53

Yeo S, Morgan N and Cheong CW, *Criminal Law in Malaysia and Singapore* (2nd edn, LexisNexis 2012)

Young J, 'Left Realism and the Priorities of Crime Control' in Stenson K and Cowell D eds, *The Politics of Crime Control* (Sage Publications 1991)

Yunos Z, Ahmad R, Mat Ali S, Shamsuddin S, 'Illicit Activities and Terrorism in Cyberspace: An Exploratory Study in the Southeast Asian Region' [2012] PAISI 2012, LNCS 27

Yunos Z, Ahmad R, Abd Aziz NA, 'Definition and Framework of Cyber Terrorism' (2013) 1 SEARCCT Selection of Articles 67

Yunos Z, Ahmad R, Suid SH, Ismail Z, 'Safeguarding Malaysia's Critical National Information Infrastructure (CNII) Against Cyber Terrorism: Towards Development of a Policy Framework' (Sixth International Conference on Information Assurance and Security, 2010)

Zedner L, *Security* (Routledge 2009)

Zelle AR and Whitehead SM, 'Cyber Liability: It's Just a Click Away' Journal of Insurance Regulation, 01/2014, Volume 33

Zakaria TAB, 'Speech by YAA Tun Ariffin Bin Zakaria, Chief Justice of Malaysia at the Opening of the Legal Year 2016' [2016] MLJ i

Zolkepli F, 'Long Wait to Extradite Hacker' *The Star Online* (18 October 2015) http://www.thestar.com.my/news/nation/2015/10/18/long-wait-to-extradite-hacker/ accessed 1 January 2016

Table of Cases

Malaysia

Basheer Ahmad Maula Sahul Hameed & Ors v PP [2016] 9 MLJ 549

Malaysian Trade Union Congress & Ors v Menteri Tenaga, Air dan Komunikasi & Anor [2014] 2 CLJ 525

*Mat Shuhaimi Shafiei v Government of Mala*ysia [2016] 1 LNS 1119

Mohamad Ezam Bin Mohd Noor v Ketua Polis Negara & Other Appeal [2002] 4 MLJ 449

PP v Azmi Sharom [2015] 8 CLJ 921

PP v Muslim Ahmad [2013] 5 CLJ

PP v Param Cumaraswamy [1986] CLJ Rep 606

PP v Rutinin Suhaimin [2013] 2 CLJ 427

PP lwn Abdul Halim Ishak & Satu Lagi [2013] 9 CLJ 559

Public Prosecutor v Yazid Bin Sufaat & Ors [2015] 1 MLJ 571

Takong Tabari v Government of Sarawak (1995) 1 CLJ 405 *citing B.A. Rao & Others v. Sapuran Kaur & Anor* [1978] 2 MLJ 146

Tong Seak Kan & Anor v Loke Ah Kin & Anor [2014] 6 CLJ 904

Yap Sing Hock v PP [1992] 2 MLJ 714

United Kingdom

Astraneca UK Ltd. V Vincent & Ors [2014] EWHC 1637 (QB)

Breslin v McKevitt [2011] NICA 33

Eli Lilly & Company Limited & Others and Stop Huntingdon Animal Cruelty & Others (2011) EWHC 3527 (QB)

Halan Laboratories UK Ltd v SHAC [2012] EWHC 3408 QB

Human Rights Watch Inc v Secretary of State for the Foreign & Commonwealth Office & Ors [2016] UKIPTrib 15_165-CH

Huntingdon Life Sciences Group Plc and others v Stop Huntingdon Animal Cruelty & others [2004] EWHC 1231 (QB)

In *R (Khan) v Secretary of State for Foreign and Commonwealth Affairs* [2014] EWCA Civ 24

Jones (Respondent) v. Ministry of Interior Al-Mamlaka Al-Arabiya AS Saudiya (the Kingdom of Saudi Arabia) (Appellants) [2006] UKHL 26

Liberty (National Council of Civil Liberties) v Government Communications Headquarters and Others [2015] UKIPTrib 13 77-H

Mohamed v. Secretary of State for Foreign & Commonwealth Affairs, [2009] EWHC (Admin) 152, [14] (Eng.)

Mohamed v. Secretary of State for Foreign & Commonwealth Affairs [2011] Q.B. 218 (Eng)

Greennet Ltd & Others v Secretary of State for foreign & Commonwealth Affairs & Another [2016] UKIPTrib 14_85-CH

Regina (Miranda) v Secretary of State for the Home Department and another (Liberty and Others intervening) [2016] 1 W.L.R. 1505

United States

Lone Star Bank, et. al v. Heartland Payment Systems, Case: 12-20648

*Microsoft Corporation v. John Does 1-27, et. a*l. Civil action number 1:10CV156

Order Compelling Apple, Inc to Assist Agents in Search, No. ED 15-0451M, United States District Court for the Central District of California

Israel

The Public Committee against Torture in Israel v Government of Israel HCJ 769/02

European Court of Human Rights

A and Others v United Kingdom (App no 3455/05, ECtHR, 19 February 2009)

Al-Skeini and Others v United Kingdom, (Application no 55721/07)

Armani Da Silva v United Kingdom (Application no 5878/08)

Bankovic and Others v Belgium and Others, (Application no 52207/99, ECHR 2001-XII)

Case of Halford v United Kingdom (Application no 20605/92, ECtHR, 25 June 2004)

Del Río Prada v Spain (Application No.42750/09, ECtHR, 21 October 2013)

McCann & Ors v United Kingdom (Application no 18984/91)

International Court of Justice

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) ICJ Reports 1996

Congo v Uganda ICJ Reports 2005

Gabčíkovo-Nagymaros Project (Hungary /Slovakia) ICJ Reports 1997

Jurisdictional Immunities of the State (Germany v. Italy: Greece intervening) ICJ Reports 2012

Legality of the Threat or Use of Nuclear Weapons ICJ Reports 1996

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory ICJ Reports 2004

Nicaragua v United States ICJ Reports 1986

Questions Relating to the Obligation to Prosecute or Extradite (Belgium v Senegal) ICJ Reports 2012

International Criminal Tribunal for the Former Yugoslavia

Prosecutor v Tadic, Case No. IT-94-1-AR72

Table of Statutes

Protocol Additional to the Geneva Conventions of 1 August 1949: article 1(4), article 44(3), article 43, article 51(1), article 51(3), article 50 (7), article 51 (4), article 51 (5), article 52(2), article 52(3)

Regulation of Investigatory Powers Act 2000: s 49(3), s 49 (4)

Security Offences (Special Measures) Act 2012: s 11

Resolution 57/239 Creation of a Global Culture of Cybersecurity,

Resolution 58/199 Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures

Resolution 65/41 Developments in the Field of Information and Telecommunications in the Context of International Security

Rome Statute of International Criminal Court 1998: article 5, article 8(2)(d), article 12, article 13(b)

Sedition Act 1958: s 4

Sedition (Amendment) Act 2015: s 3, s10

Serious Crimes Act 2015: s1, s 5, s 43, paragraph 11A, Schedule 1

Specific Relief Act 1950: s 4 (c) of the Specific Relief Act 1950, s 6, s 51, s 52 (3), s 53, illustration e s 53

Strategic Trade Act 2010: s 32

Terrorism Act 2006: s 1, s 2

Terrorism Prevention and Investigation Measures Act 2011: s 4, s 6(3), s 6(4), s 6(6), schedule 1

Third Geneva Conventions 1949: article 4, article 4(A)(2)

United Nations Charter: article 2(4), article 2(7), article 51

Appendix A

Interview schedules for policing

Note: The italicised notes will be mentioned to the interviewees as an introduction to each section and to help guide the conversation.

I should like to start by asking biographical questions about your background, job description and working experience. The purpose of this exercise is to correlate your later answers with your professional profile.

A1. Professional profile

A1.1. What is the title of your current job?

A1.2. Can you please describe your duties?

A1.3. How long have you been working with this organisation?

A1.4. How long have you been dealing with the issues related to cyber attacks?

A1.4.1. Have you been required to undertake training courses relating to cyber attacks for your current role?

The purpose of this section is to clarify the context of cyber attacks. I should now like to seek your opinion about the definition of cyber attacks by asking the following questions.

A2. The definition of cyber attacks

A2.1. Do you use the term 'cyber attack'?

A2.2. What do you understand by the term cyber attack?

A2.3. Do you consider the following scenarios as cyber attacks?

I	Several animal rights activists embarked on a campaign against a pharmaceutical company for conducting experiment on animals. They hacked the company's computer system and illegally obtained confidential information including the personal record of the employees of the company. They send spam messages containing virus through emails to the employees of the company. The website of the company was crippled for several weeks due to the Distributed Denial of Service (DDOS) attack by this group. The company lost

	profits due to this incident
II	A computer virus disabling computer networks across Malaysia was discovered. The origin of the attack is unknown and still being investigated by the Police. The virus spread through emails. John did not create the virus; however he thought that the attacks were necessary in order to eliminate capitalism. He discovered the link to the virus and decided to post it on several websites.

A2.4. What do you understand by the term cybercrime? What is the difference, if any, between cyber attacks and cyber crime?

A2.5. Do you agree with the following definition of cyber attacks: 'The use of malicious software and malware by states and non-state actors to penetrate, disrupt and destroy the computer and telecommunication system of their enemy. The purpose of the attack is to incapacitate the enemy during armed conflict by targeting their military objectives and/or to cause serious and widespread harm to victims, which include mental and bodily injury, damage to critical national infrastructure and damage to objects which are critical to the economy and national security'.

A3. The attributes of cyber attacks

Source of the attacks

A3.1. If the sources of the threats are from outside of Malaysia, who is responsible? Can they be attributed to a state or non-state actors?

A3.2. If the sources of the threats are from inside of Malaysia, who is responsible? Can you give some typical profiles of the attackers?

The scale of the attacks

A3.3. How do you measure the seriousness of the attack? What is the extent of harm or damaged cause by cyber attacks?

Method of the attacks

A3.4. How are cyber attacks committed? How is malware created? Can cyber attacks be done by other means?

The targets

A3.5. What are the common targets of cyber attacks?

A3.6. Do you think the following acts tantamount to cyber attacks?

A3.6.1. Attack on a single computer system?

A3.6.2. Attack on critical infrastructure? Are they confined to the computer system of the government, military and corporate entities?

A3.6.3. Attack on economic target such as stock market and banking institutions?

A3.7. Why are the victims of cyber attacks being targeted? What separates them from organisations or individuals that are not attacked?

A3.7.1. Is it because they are more vulnerable in comparison to other objects?

A3.7.2. Is it because they are more valuable?

A3.7.3. Are they being targeted for symbolic reasons?

A3.7.4. How often they are being targeted?

Motives and objectives

A3.8. What is the motive behind the threats or attacks? Is it done in furtherance of political agenda or for any other reasons? What evidence do you have to support your contention?

The following questions explore whether cyber attacks should be dealt with by social crime prevention policy, situational crime prevention, prevention legislation, executive orders or criminal law.

A4. Criminal justice measures to counter cyber attacks

Policy

A4.1. Do you know any initiatives taken by the government for dealing with cyber attacks? How do you rate the effectiveness of the

initiatives? Do you think the measures are fair or effective having regard to the gravity of the attacks?

A4.2. Has Malaysia developed an effective strategy against cyber attacks? Does it have the capacity to do so?

A4.3. Are there any difficulties faced by the government? If so, what are the difficulties?

Measures

A4.4. I would like to seek your opinion on the responses in dealing with this problem. The measures are stated on these blocks. Which measure is the most effective? Can you arrange these blocks according to their rank?

The next questions depend on the rank of the blocks. The interviewer has to adjust and adapt the questions based on the arrangement made by the interviewee. The description of the blocks is attached in the thesis. The following approaches will be stated on the blocks:

- *Education and campaigns*
- *Activities for the young people such as sports to divert their attention from engaging in bad behaviours*
- *Installation of anti virus software on computers*
- *Encryption*
- *Surveillance by the police or state agencies*
- *Regulating the creation and distribution of malware*
- *Preventive legislation to criminalise acts such as the possession of materials to commit cyber attacks*
- *Executive orders against potential perpetrators of cyber attacks such as house arrest with no access to computer and Internet*
- *Civil action*
- *Criminal law*

After arranging the blocks, the interviewee will be asked the following questions. The objective is to analyse their preferences.

A4.5. Why do you think _____ are more effective in countering cyber attacks in comparison to _____ ?

A4.6. What is your opinion on the appropriateness of using surveillance (electronic or visual) as a preventive measure against cyber attacks?

A4.7. What would be the advantage and disadvantage of using criminal law against the perpetrator of cyber attacks

A4.8. Why do you say that _____ is more effective than _____?

A4.9. Why _____ is ranked last?

A4.10. Do you think imposing legal obligations on the Internet service providers, telecommunication and software companies to ensure the security of computer system could help to prevent cyber attacks?

A4.11. Do you think it is necessary for the government to establish a specialist institution to conduct surveillance or to counter illegal activities on cyber space especially those that are harmful to national security?

A4.12. Does preventive legislation such as Security Offences (Special Measures) Act 2012, Prevention of Terrorism Act 2015 and the Special Measures Against Terrorism in Foreign Countries Act 2015 have a role to counter cyber attacks? [Security Offences (Special Measures) Act 2015 provides for special measures relating to security offences such as terrorism. The police are vested with special powers including the power to intercept communication and surveillance for the purpose of maintaining public order; Prevention of Terrorism Act 2015 provides for an inquiry proceeding of any person who is suspected of engaging in the commission or supporting terrorist acts. The Inquiry Officer submits the report of the inquiry to the Board established under the Act. The Board is vested with the power to order detention for not exceeding two years and to restrict freedom of movement, places of residence or employment; Special Measures Against Terrorism in Foreign Countries Act 2015

provides for the power of the Director General of Immigration to suspend or revoke the travel documents of a person who is suspected to leave Malaysia in order to engage in the commission or support terrorists acts in a foreign country].

The following questions are designed to elucidate the position of cyber attacks under the domestic criminal law of Malaysia.

A5. The position of cyber attacks under the domestic law of Malaysia

A5.1. Can cyber attacks fall within the ambit of the Computer Crimes Act 1997? (Computer Crimes Act 1997 provides for the offence of unauthorised access to computer material and unauthorised modification of the contents of any computer).

A5.1.1. Is the Computer Crimes Act 1997 effective in dealing with cyber attacks?

A5.1.2. How about the punishment provided under the Computer Crimes Act 1997? Do you think the punishment is fair or effective? (A fine not exceeding RM50 000 or imprisonment for a term not exceeding 5 years or both for unauthorised access to computer material; a fine not exceeding RM100 000 or to imprisonment for a term not exceeding 7 years or to both for unauthorised modification of the contents of any computer)

A5.2. Can other provisions of the Penal Code be invoked as a basis for prosecuting the perpetrators of cyber attacks? For instance, offences against property.

A5.3. Do you think more laws are needed in order to deal with cyber attacks more fairly and effectively?

A5.3.1. Should cyber attacks be considered always as a crime? If not, how else should they be dealt with?

The following questions seek to understand the usage of criminal justice for cyber attacks in Malaysia.

A6. Policing, investigation, prosecution and punishment

<u>Policing/investigation</u>

A6.1. Do you think the police have sufficient capabilities and expertise in dealing with cyber attacks?

A6.2. Do you think the police should play active roles in preventing the occurrence of cyber attacks? What has been done so far? Do you think the preventive measures carried out so far are effective?

A6.3. Is investigating cyber attacks straightforward or difficult for the police?

A6.4. Is it difficult to trace and arrest the perpetrators of cyber attacks? What are the obstacles and challenges in apprehending the offenders?

A6.5. What is the method that you use in tracing the origin of an attack?

A6.6. Are the attacks discovered through reports made by the public or detected by your organisation?

A6.7. Do the people under attack cooperate with the investigation?

Prosecution

A6.8. How effective are the prosecutors when involved in the investigation of cyber attacks?

A6.9. How well do the prosecutors and police coordinate their efforts during the investigation?

A6.10. Are there any typical obstacles in the prosecution of the perpetrators of cyber attacks?

A6.11. How feasible would it be for the courts in Malaysia to exercise jurisdiction over cyber attacks committed outside of Malaysia?

A6.12. How feasible would it be to extradite perpetrators who committed cyber attacks outside of Malaysia?

A6.13. Are you aware of any prosecution with respect to cyber attacks? If so, what was the outcome?

Sentencing

A6.14. Do you think the punishment in the form of imprisonment should be applied to cyber attacks?

A6.15. Would it be appropriate for the perpetrators of cyber attacks to serve their sentences on community service or probation?

A6.16. What is the most appropriate form of punishment for cyber attacks?

The following questions seek to understand the role of government agencies and private institutions in countering cyber attacks in Malaysia.

A7. The role of Cybersecurity Malaysia, CERT and private institutions

Government agencies

A7.1. Do you know any government agencies responsible for dealing with cyber security in Malaysia? Have you herd of the CERT?

A7.2. What is their role in dealing with cyber attacks? Do you think they are more effective in comparison to policing?

Private institutions

A7.3. Compared to the state agencies, do you think there is a role for private companies in countering cyber attacks? If so, what role?

A7.4. Would you like them to be more involved?

A7.5. Should there be more cooperation between the private sectors, policy makers, military and the police?

A7.6. Do you think the private sectors report cyber attacks to the police?

A7.7. Do you think that they are underreported?

A7.8. What should happen? How can the situation be reformed?

The following questions seek to understand the effort to counter cyber attacks at the regional (ASEAN) and international level.

A8. ASEAN and international organisations

International law

A8.1. Are you aware of any international obligations regarding cyber crime and cyber attacks? What are they? Does Malaysia comply with these obligations? Do you foresee the possibility of Malaysia acceding to the Cybercrime Convention?

ASEAN

A8.2. Are you aware of any efforts at the ASEAN level in dealing with cyber attacks or cyber threats?

A8.3. What is your opinion of the measures adopted by ASEAN so far pertaining to this issue?

A8.4. Do you think ASEAN has adopted a sound policy in countering cyber attacks?

A8.5. Should ASEAN have a role in this matter?

A8.6. Should ASEAN be more or less proactive in facilitating regional effort to counter cyber attacks?

A9. Miscellaneous

A9.1. Is there anything else you would like to add? Thank you.

A9.2. Are there any additional documents or materials related to this research that you would suggest to me?

Appendix B

An Analysis of Criminal Liability and Enforcement for Cyber Attacks Under International Law and the Law of Malaysia

Information Sheet

You are being invited to take part in this research project. It is pertinent for you to understand the aim of this research and what it will involve before you decide. Please take time to read the following information carefully and discuss it with others if you wish. Please do not hesitate to ask me for further clarification or information. I am grateful if you would notify me within three weeks of your intention to participate or not in this study.

My name is Ummi Hani Binti Masood. I am a doctoral student at the School of Law, University of Leeds in the United Kingdom under the supervision of Professor Clive Walker and Dr. Henry Yeomans. I am sponsored by the Ministry of Higher Education of Malaysia. The rise of cyber attacks has triggered responses from states. In the light of recent developments, this study evaluates the imposition of criminal liability and enforcement in relation to cyber attacks: under international law; the domestic law specifically in Malaysia with some comparison to the UK; and regional organisations in particular ASEAN and EU. This study examines other alternatives besides criminal law that can be used to counter cyber attacks. The primary purpose of this study, therefore, is to examine the nature of cyber attacks and the regime governing cyber attacks under international law and the domestic criminal law especially in Malaysia and the current roles, values and potential of criminal law as a countermeasure. At the completion of this study, the outcomes will contribute to the enhancement of the body of knowledge on the area of international law and domestic law pertaining to cyber attacks. This study offers some guidance on the enforcement of criminal measure in countering cyber attacks at the international and domestic level. As part of the research, I would like to ask you questions concerning your experiences in dealing with cyber attacks. I am interviewing a total of 25 participants from areas related to cyber security. You have been chosen to take part in the research due to your expertise and experience in this area.

Taking part in the interview is entirely voluntary and you can stop the interview at any time, for any reason, without any negative consequences. You can also withdraw your consent for your interview to be used in my study within two weeks from the date of the interview by contacting me at

lwuhm@leeds.ac.uk. The information gathered during the interview will be destroyed pursuant to your withdrawal within the specified period. The interview should last no more than an hour. I would like to tape – record the interview so that I can make sure your views and experiences are correctly recorded. Please let me know if you prefer the interview not to be recorded; I will take notes instead. The audio recording made during this research will be used only for analysis and for illustration in conference presentations and lectures. No other use will be made of them without your written permission, and no one outside the project will be allowed access to the original recording. If you decide to take part, you can stop the interview at any time or refuse to answer any questions. You can also raise new subjects that you think maybe useful for this research. Please let me know if you need a break at any time during the interview.

This interview is confidential and only my supervisors and myself will see your interview. The important exception to this is if you say anything, in the opinion of me or my supervisors, might cause an unacceptable risk to you or others such as instances of criminal remarks and serious harm or wrongdoing. The data gathered in this research is utilised for lawful purposes and handled in accordance to the provisions of the data protection legislation. The data is made available to others through conferences, seminars and publications arising from the thesis in academic journals and books. I will stop the interview if such information begins to be mentioned and reiterate the limits to confidentiality during the interview if instances of malpractice are discussed. In addition, if this is the case, the information will be reported to the relevant authorities. Any published record of statements from the interviews and quotations will be anonymised so that any material used in the research report will not be attributable to any individual. The data will be stored and used according to the University of Leeds Code of Practice on Data Protection and the data protection legislation. The findings of the research will be applied in my PhD thesis and published as academic papers. People who take part in the research will not be named in the thesis or in any publications. Whilst there are no immediate benefits for those participating in the project, it is hoped that this work will contribute to the body of knowledge on cyber security and criminal law.

If you require further information, please contact me via email at lwuhm@leeds.ac.uk or my supervisors, Professor Clive Walker at C.P.Walker@leeds.ac.uk or Dr Henry Yeomans at H.P.Yeomans@leeds.ac.uk . You can also send your enquiry to the following address: School Of Law, University of Leeds, LS2 9JT, UK. Thank you very much for your kind consideration to participate in this research.

Consent to take part in 'An Analysis of Criminal Liability and Enforcement for Cyber Attacks Under International Law and the Law of Malaysia'

	Add your initials next to the statements you agree with
I confirm that I have read and understand the information sheet dated ……. explaining the above research project and I have had the opportunity to ask questions about the project.	
I agree for the data collected from me to be stored and used in relevant future research in an anonymised form.	
I understand that relevant sections of the data collected during the study, may be looked at by individuals from the University of Leeds or from regulatory authorities where it is relevant to my taking part in this research. I give permission for these individuals to have access to my records.	
I agree to take part in the above research project and will inform the researcher should my contact details change.	

Name of participant	
Participant's signature	
Date	
Name of researcher	Ummi Hani Binti Masood
Signature	
Date*	

*To be signed and dated in the presence of the participant.

Once this has been signed by all parties the participant should receive a copy of the signed and dated participant consent form, the letter/ pre-written script/ information sheet and any other written information provided to the participants. A copy of the signed and dated consent form should be kept with the project's main documents which must be kept in a secure location.

Appendix C

Performance, Governance and Operations
Research & Innovation Service
Charles Thackrah Building
101 Clarendon Road
Leeds LS2 9LJ Tel: 0113 343 4873
Email: ResearchEthics@leeds.ac.uk

UNIVERSITY OF LEEDS

Ummi Hani Binti Masood
School of Law
University of Leeds
Leeds, LS2 9JT

ESSL, Environment and LUBS (AREA) Faculty Research Ethics Committee
University of Leeds

12 June 2017

Dear Ummi

Title of study: **An Analysis of Criminal Liability and Enforcement for Cyber Attacks Under International Law and the Law of Malaysia**
Ethics reference: **AREA 15-029**

I am pleased to inform you that the above research application has been reviewed by the ESSL, Environment and LUBS (AREA) Faculty Research Ethics Committee and following receipt of your response to the Committee's initial comments, I can confirm a favourable ethical opinion as of the date of this letter. The following documentation was considered:

Document	Version	Date
AREA 15-029 Amended Ethics Application Ummi Hani.doc	1	29/10/15
AREA 15-029 Amended Information Sheet Ummi Hani.docx	1	29/10/15
AREA 15-029 Confidentiality Form Ummi Hani.doc	1	29/10/15
AREA 15-029 Ethics Application Ummi Hani.doc	1	02/10/15
AREA 15-029 Information Sheet Ummi Hani.docx	1	02/10/15
AREA 15-029 Consent Form Ummi Hani.doc	1	02/10/15
AREA 15-029 fieldwork-assessment-form-low-risk- Ummi Hani.doc	1	02/10/15

Please notify the committee if you intend to make any amendments to the original research as submitted at date of this approval, including changes to recruitment methodology. All changes must receive ethical approval prior to implementation. The amendment form is available at http://ris.leeds.ac.uk/EthicsAmendment.

Please note: You are expected to keep a record of all your approved documentation, as well as documents such as sample consent forms, and other documents relating to the study. This should be kept in your study file, which should be readily available for audit purposes. You will be given a two week notice period if your project is to be audited. There is a checklist listing examples of documents to be kept which is available at http://ris.leeds.ac.uk/EthicsAudits.

We welcome feedback on your experience of the ethical review process and suggestions for improvement. Please email any comments to ResearchEthics@leeds.ac.uk.

Yours sincerely

Jennifer Blaikie
Senior Research Ethics Administrator, Research & Innovation Service
On behalf of Dr Andrew Evans, Chair, AREA Faculty Research Ethics Committee

CC: Student's supervisor(s)