Cybercrime in Vietnam:
A critical analysis of its regulatory framework

Hai Van Nguyen

This thesis is submitted in partial fulfillment of the requirements for award of the degree of Doctor of Philosophy of the University of Portsmouth

April 2019
ABSTRACT

This research is a critical analysis of cybercrime and its regulatory framework in Vietnam. Starting in October 2013, it was the first research study, on cybercrime, funded by the Vietnamese Ministry of Public Security. It explores critically i) how cybercrime is defined by high-level professionals from key regulatory institutions in Vietnam; ii) the extent to which the current Vietnamese Cybercrime Regulation Policies (VCRPs) are fit for its intended purposes. It also examines the key factors that make cybercrime difficult and challenging for Vietnamese authorities to regulate; and possible preventative measures that can be put in place to reduce the occurrence and growth of cybercrime in Vietnam.

Based on document analysis and 35 semi-structured interviews of high-level professionals from key regulatory institutions in Vietnam, this research presents two sets of findings in Chapter 4 (document analysis) and Chapter 5 (semi-structured interviews). The findings show that there are several characteristics of cybercrime in Vietnam that have posed significant difficulties and challenges for Vietnamese authorities to regulate. These include: i) the presence of multiple opportunities to commit cybercrime; ii) the transnational nature of the crimes; and iii) the anonymity of cybercriminals, and in cyberspace in general. In addition, the research also points out some limitations of the current VCRPs, including problems over jurisdiction, the lack of legal coverage of cybercriminal activities, and the present state of the legal language used. These limitations make the current VCRPs less effective in fulfilling their intended purposes. This thesis concludes by stressing the important roles of computer users, Internet Service Providers (ISPs), and the Police play in regulating cybercrime. It also stresses the importance of education and increasing awareness in tackling cybercrime in the Vietnamese context.
First of all, I would like to express my sincere appreciation and thanks to Dr. Victoria Wang for her untiring guidance and supervision over the five-year duration of my doctoral studies. She has encouraged me to explore new ideas and knowledge, and supported me through the many difficult times that inevitably arise when undertaking and writing-up such a large project. Her expertise, experience and patience have helped to build my confidence, not just so that I could complete one of the most important tasks in my life, but in terms of going forward into my future career. Without her guidance, the completion of this thesis would have not been possible.

I would also like to thank Professor Steve Savage for his detailed feedback on my work that guided me in the direction of many chapters. My utmost gratitude to all research participants who made this research possible.

Lastly, I would like to thank my family: my wife and my two lovely sons for their endless patience and encouragement during my studies. I would like to dedicate this thesis to my family. Every bit of support from my parents, my sisters and my parents-in-law are also greatly appreciated.

This work is supported by the Vietnamese Government - Project 165.
DECLARATION

Whilst registered as a candidate for the above degree, I have not registered for any other research award. The results and conclusions embodied in this thesis are the work of the named candidate and have not been submitted for any other academic award.

HAI VAN NGUYEN

Total word count (whole document): **81,845** words, of which:

- Word count excluding appendices: **70,980**
- Word count of appendices: **1,204**
- Abstract, Contents, References: **9,649**
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASEAN</td>
<td>The Association of Southeast Asian Nations</td>
</tr>
<tr>
<td>FPT</td>
<td>The Corporate for Financing and Promoting Technology</td>
</tr>
<tr>
<td>ICTs</td>
<td>Information Communication Technologies</td>
</tr>
<tr>
<td>IRMs</td>
<td>Institutional Regulatory Mechanisms</td>
</tr>
<tr>
<td>ISPs</td>
<td>Internet Service Providers</td>
</tr>
<tr>
<td>MIC</td>
<td>The Ministry of Information and Communications</td>
</tr>
<tr>
<td>MOPS</td>
<td>The Ministry of Public Security</td>
</tr>
<tr>
<td>RAT</td>
<td>Routine Activity Theory</td>
</tr>
<tr>
<td>VCP</td>
<td>The Vietnamese Communist Party</td>
</tr>
<tr>
<td>VCRPs</td>
<td>Vietnamese Cybercrime Regulation Policies</td>
</tr>
<tr>
<td>VNCERT</td>
<td>The Vietnamese Computer Emergency Response Team</td>
</tr>
<tr>
<td>VNPT</td>
<td>The Vietnamese post and telecommunication</td>
</tr>
<tr>
<td>WTO</td>
<td>The World Trade Organisation</td>
</tr>
</tbody>
</table>
Chapter 1. Introduction and scope of the research .............................................. 1
  1.1. Background ................................................................................................. 2
  1.2. Aims and scope of the research .................................................................. 5
  1.3. Significance of the research ........................................................................ 6
  1.4. The organisation of the thesis ..................................................................... 8

Chapter 2. Cybercrime and its regulation – A general overview ..................... 11
  2.1. Introduction .................................................................................................. 11
  2.2. Cybercrime definitions and typology ......................................................... 11
    2.2.1. Definition ............................................................................................... 11
    2.2.2. Typology ............................................................................................... 15
  2.3. The unique characteristics of cybercrime ............................................... 19
    2.3.1. Multiple opportunities .......................................................................... 19
    2.3.2 Transnational in nature ........................................................................... 23
    2.3.3. Anonymity ............................................................................................. 25
  2.4. The current state of the art of cybercrime regulation ............................. 27
    2.4.1. The ‘Peelian paradigm’ – A modern regulatory framework ............... 27
    2.4.2. National efforts to regulate cybercrime ............................................... 30
    2.4.3. International measures .......................................................................... 33
    2.4.4. The measurement of cybercrime reduction .......................................... 38
  2.5. Conclusion .................................................................................................. 47

Chapter 3. Research methodology and methods .......................................... 49
  3.1. Introduction ................................................................................................ 49
  3.2. A piece of qualitative research ................................................................... 49
  3.3. Two research methods .............................................................................. 51
    3.3.1. Document analysis .............................................................................. 52
3.3.2. Qualitative interview ........................................... 55

3.4. Data analysis .......................................................... 63

3.5. Ethical considerations ............................................... 67
  3.5.1. Informed consent ............................................... 68
  3.5.2. Confidentiality and anonymity .......................... 68
  3.5.3. Code of ethics .................................................. 69

3.6. Limitations of the chosen methodology and methods ............. 69
  3.6.1. Disadvantages of thematic analysis ....................... 69
  3.6.2. Validity and reliability ....................................... 70
  3.6.3. Generalisability ................................................ 71

3.7. Conclusion .................................................................. 72

Chapter 4: Cybercrime and its regulation in Vietnam .................... 73
  4.1. Introduction .......................................................... 73

  4.2. The Vietnamese context: Society and technology ............... 74
    4.2.1. The socio-economic background ................................ 74
    4.2.2. The growth of the Internet in Vietnam .................... 78

  4.3. Cybercrime in Vietnam ............................................. 82

  4.4. The state of cybercrime regulation in Vietnam .................. 86
    4.4.1. The lack of a legal definition of cybercrime in Vietnam ... 86
    4.4.2. Policy measures ................................................ 89
    4.4.3. Institutional regulatory mechanisms (IRMs) ................ 91
    4.4.4. Other legislations with cybercriminal activities implication ... 95
    4.4.5. The Vietnamese Penal Code .................................. 98

  4.5. Cybercrime regulation in Vietnam – key challenges .......... 105
    4.5.1. The challenges for the police .................................. 105
    4.5.2. The challenges for prosecutors .............................. 111
4.5.3. The challenges for judges.................................................................114
4.5.4. The challenges for ISPs.....................................................................117
4.6. Conclusion.............................................................................................121

Chapter 5. Findings ..................................................................................123
5.1. Introduction............................................................................................123
5.2. Descriptive overview of the research sample ........................................124
5.3. Attitude and perception toward definitions of cybercrime...................128
5.4. Attitude and perception toward the policies of cybercrime regulation......138
5.5. Attitude and perception toward the current Vietnamese cybercrime
    regulation mechanism .............................................................................146
      5.5.1. The Police - Role and challenges..................................................146
      5.5.2. The Prosecutor – Role and challenges..........................................152
      5.5.3. The Judge – Role and challenges..................................................153
      5.5.4. The Internet service providers (ISPs) – Role and challenges........153
5.6. Reducing the growth of cybercrime in Vietnam – some possible
    approaches ...............................................................................................156
5.7. Conclusion.............................................................................................162

Chapter 6. Discussions ..............................................................................163
6.1. Research question 1: How is cybercrime perceived by high-level
    professionals from key regulatory institutions in Vietnam? .........................164
      6.1.1. Defining cybercrime - perceptions of high-level professionals from
            key regulatory institutions in Vietnam.............................................164
      6.1.2. Unique characteristics of cybercrime - perceptions of high-level
            professionals from key regulatory institutions in Vietnam.................166
6.2. Research question 2: How adequate are the current policies responding to
    cybercrime in Vietnam? ............................................................................171
      6.2.1. The natural limitations of the VCRPs - Jurisdictional/Transnational
            issues – a major factor that reduces the effectiveness of VCRPs............171
6.2.2. The inadequacy of the Vietnamese cybercrime regulation policies (VCRPs)...................................................................................174

6.3. Research question 3: Who should be the key players in the regulation of cybercrime in Vietnam? ........................................................................177

6.3.1. Internet users ...............................................................................178

6.3.2. Internet services providers (ISPs)..................................................180

6.3.3. The police..................................................................................182

6.4. Research question 4: What possible responses can be put in place in terms of cybercrime regulation in Vietnam? ..................................................185

6.4.1. Technical solutions: To apply advanced technologies..................185

6.4.2. Education: To increase awareness .............................................188

Chapter 7. Conclusion and the implications........................................191

7.1. Summary of key findings ..............................................................191

7.2. Implications ..............................................................................196

7.3. Directions for future research .....................................................197

Appendix 1: Interview schedule for Police Officer/Prosecutor/ Judge ..........199

Appendix 2: Interview schedule for policy maker ...................................202

Appendix 3: Interview schedule for internet provider services ................205

Appendix 4: Information sheet to accompany consent form ....................208

Appendix 5: The letter of introduction for assessing to the five institutions in Vietnam.................................................................212

Appendix 6: Ethical review confirmation................................................213

Appendix 7: Research ethics review checklist........................................215

References..........................................................................................216
Chapter 1. Introduction and scope of the research

This research is an empirical research project, which explores the phenomenon of cybercrime and its regulation in Vietnam. In doing so, it also proposes some of the possible measures in mitigating cybercrime that can be applied in the context of Vietnam.

The growth of cybercrime is a significant phenomenon in both international and national levels including Vietnam. Over the past two decades, Vietnam has been host to an increasing number of cybercriminal activities (Lee, 2016). The main reasons for this include but are not necessarily limited to: i) the development of computer technologies; ii) an increase in the usage of the Internet; and iii) a lack of understanding of various types of activities that are often placed under the umbrella term of ‘cybercrime’. More importantly, there is a lack of appreciation of legislation and regulatory framework concerning cybercrime. Consequently, dealing with cybercrime will be increasingly difficult and challenging for authorities.

In relation to these issues, research projects have been conducted to explore the phenomenon of cybercrime from different perspectives. For example, scholars have explored the role of the Internet in the trafficking of human beings (Latonero, 2011), cyberstalking (Reyns et al., 2011), cyber bullying (Kraft and Wang, 2009) and, online harassment (Moore et al., 2010). Others have been interested in understanding the role of computer networks in relation to extortion (Polatsek, 2014), identity theft (Wang & Huang, 2011a), online fraud (Kerr et al., 2012) and, digital piracy (Moore & McMullan, 2009). Furthermore, other research projects have been conducted to highlight how Information Communication Technologies (ICTs) can possibly create new types of crime, such as spamming, identity theft, malicious software and cyber piracy (Wall, 2007; Holt & Graves, 2007; Yar, 2013). Particularly, Wall (2015) has explored how cybercrimes are organised by networked technologies, and has suggested that “the very nature of cybercrimes being informational, global and networked (and increasingly automated) has encouraged different, flatter, forms of organisation than the hierarchies of control found in more traditional forms of offending” (p. 85).

Some scholars have used traditional theories of crime to explain newly emerged crimes in cyberspace. For example, some research projects have proved that Routine Activity
Theory (RAT) (Cohen & Felson, 1979) can be applied to analyse online harassment (e.g., Holt & Bossler, 2009), malware victimisation (e.g., Bossler & Holt, 2009, 2012, 2013) and, phishing victimisation (e.g., Hutchings, 2014). The general theory of crime (e.g., Gottfredon & Hirschi, 1990) and aspects of social learning theory (e.g., Akers, 1998) have both been applied to analyse digital and software piracy (Donner et al., 2014; Higgins & Marcum, 2011; Holt et al., 2010, 2012; Holt & Copes, 2010). However, cyberspace not only creates a new environment for committing new types of crimes, but it also facilitates traditional conventional crimes that are perpetrated in the real world (Basu, 2012; Newman, 2009).

Despite various research studies that have examined the phenomenon of cybercrime in different perspectives, and in different regions and, countries, there has been no academic research on the phenomenon of cybercrime and its regulation conducted in Vietnam. At least, not at the inception of this research. This is, therefore, the first time the phenomenon of cybercrime and its regulation has been studied in Vietnam.

This first chapter introduces the thesis and is divided into four sections. The first section provides background on this area of research. The second section sets out the aims and the scope of this research. The third section explains the necessity and importance of this research. The final section explains the organisation of this thesis.

1.1. Background

The growth of the Internet and its associated technologies, and its impact on existing political, social, economic and cultural life, both locally and globally, is astonishing. These developments have penetrated all aspects of human lives by enabling new forms of communication, interaction and social structure. These developments have also underpinned both state and commercial enterprises; and have transformed many of the routine daily activities of individuals (Holt & Schell, 2011).

Along with the radical changes and benefits brought about by the Internet and its associated technology, serious problems have also emerged. Amongst these problems, the exploitation of Internet technologies for criminal purposes is the most prominent (Fafinski, 2009). Indeed, computers and the Internet, like other less advanced tools that came before them, can be used for good or evil. With various advanced developments in

The Internet and its associated technologies have created a vital environment, known as ‘cyberspace’. ‘Cyberspace’ offers criminals a space in which to pursue criminal activities with little possibility of being detected (Smith & Jorna, 2011; Wang & Huang, 2011). These activities range from petty crimes to professional high-tech crimes (Wall, 2015). Cybercrime is unique in that it provides the opportunity to “commit many crimes simultaneously in ways not previously imagined and previously beyond their financial and organisational means, and on a global scale” (Wall, 2015, p. 74). For example, malicious software can be released with ease and go on to infect millions of computers through emails or social network sites (McEwan, 2013). By a single click, child pornography and sexual exploitation of online images of children can be made available in every country in the world connected to the Internet (Beech et al., 2008; McGuire & Dowling, 2013). Personal or commercial bank account details can be stolen and turned into illegal commercial products very cheaply and easily (Cornish et al., 2009).

Legislation both nationally and globally are theoretically supposed to be effective in dealing with most aspects of criminal activities. However, dealing effectively with these criminal activities in cyberspace is more complex than dealing with more traditional crimes. Criminals can take advantage of the development of Internet technologies to be anonymous via specific software, such as TOR\(^1\). These advanced technologies also open up opportunities for criminal activities across national boundaries (Holt, 2013). Even where and when cybercrime is identifiable, criminal activities, and any evidence of such could be scattered across numerous territories, and/or be volatile in nature (Brenner, 2012, 2014).

These difficulties can be further complicated where those suspected of engaging in cybercrime are physically located in jurisdictions with weak or non-existent legislations against cybercrime. For example, many forms of pornography are legal in the United State of America, but such material is clearly not allowed in other nations (Marion, 2012).

\(^1\) TOR is free software and an open network that helps users defend against traffic analysis, a form of network surveillance, confidential business activities and relationships, and state security. See: https://www.torproject.org/ (accessed 06/10/2016).
The Internet and its associated technologies have transformed criminal behaviour, (Wall, 2015/2007), created automated crime (Wall, 2015, p. 73), and enabled the committing of thousands of crimes at multiple locations simultaneously (Brenner, 2010). Therefore, cybercrime is difficult and challenging for authorities, and even nations, to deal with (Brenner, 2010; Wall, 2015), since power of the legal authorities of nations is restricted by national and international laws (Giraldo & Trinkunas, 2009). Additionally, national legal authorities, for example, law enforcement authorities, have never faced a form of criminality where the suspects, evidence, and victims are so globally dispersed. Dealing with this type of criminal demands highly technical experts that legal authorities often do not have (Wall, 2011; Brown, 2015; Stol et al., 2011).

In particular, the Internet allows for real time connections between criminals and victims regardless of their locations. Hence, some restricting factors, such as time, distance and borders are less important than in traditional societies. In addition, no longer is the evidence of perpetrators visible to their victims, nor to legal authorities. Cybercrimes can be carried out very quickly, even with a click of a mouse. At the same time, investigative procedures for these crimes tend to be very slow and time-consuming (McGuire & Dowling, 2013). The Internet and its associated technologies are viewed not only as technical tools but also as a part of contemporary culture (Maltzahn, 2005; Furedi, 2014). In the global context, the Internet and its associated advanced technologies have been a part of the globalisation process that is supposedly changing old realities and certainties, offering new opportunities and challenges for global society (Yar, 2013).

In fact, a new avenue for criminality has been opened. In other words, the Internet and its associated technologies have created great opportunities for criminal activities, previously operating on a national level, to become global. These criminal opportunities arise mainly from a very large number of software vulnerabilities (Bambauer, 2014) and evolving threats. Furthermore, cybercrime is said to be more profitable than the combined global trade in marijuana, cocaine and heroin (Shaik & Shailk, 2014). The constant development of new criminal opportunities and approaches in cyberspace has made cybercriminal activities increasingly sophisticated (ENISA, 2013). Moreover, cybercrime can be committed in minutes, while the investigation of such crime can
often take months, if not years (see: the case of the Red October\(^2\) (2007 – 2012) – the largest bot net attack). As a consequence, traditional mechanisms of policing and protection of assets have been reduced in terms of effectiveness in cyberspace. Furthermore, old methods of regulating crime are considered as obsolete or irrelevant in the context of the Internet (Balkin et al., 2007). Thus, new thinking on appropriate forms of regulation is necessary in order to manage cyberspace and reduce the growth of cybercrime.

In short, cybercrime reflects a peculiar type of technologically sophisticated criminality, having different features from traditional types of criminal activity. The inherent characteristics of cybercrime, including: i) multiplicity of opportunities, ii) transnational locations, iii) anonymity, and iv) advancement of technology are not only used to explain how cybercrime can be different from traditional crime, but can also be used to explain how difficult and challenging cybercrime can be for national authorities, in the case of this research, the Vietnamese authorities, to regulate. Unsurprisingly, cybercrime deserves special attention owing to these key characteristics.

Based on its empirical findings, this research argues that a simple and fixed regulation approach cannot effectively regulate cyberspace or reduce cybercrime due to these special characteristics. Thus, it is necessary to have a multi-agency approach towards the regulation of cybercrime.

1.2. Aims and scope of the research

The overachieving aim of the research is to obtain a better understanding of the phenomenon of cybercrime and its regulation in Vietnam. In doing so, this thesis has four specific objectives:

i) To critically assess the extent to which the regulatory framework of cybercrime in Vietnam is fit for its intended purposes.

ii) To explore how cybercrime is defined by high-level professionals from key regulatory institutions in Vietnam;

---

iii) To explore the key factors that make cybercrime difficult and challenging for Vietnamese authorities to regulate; and,

iv) To explore possible measures that can be put in place to reduce the growth of cybercrime in Vietnam.

In order to achieve these four objectives above, the research will answer the following four research questions:

1. How is cybercrime perceived by high-level professionals from key regulatory institutions in Vietnam?

2. How adequate are the current policies in responding to cybercrime in Vietnam?

3. Who should be the key players in the regulation of cybercrime in Vietnam?

4. What possible responses can be put in place in terms of the regulation of cybercrime in Vietnam?

1.3. Significance of the research

This research is the very first research project on cybercrime and its regulation in Vietnam. It can be argued that cybercrime is new compared to various forms of traditional crime. Some members of the Association of Southeast Asian Nations (ASEAN) are among the world’s leading economies (Lee, 2016). Member states, including Vietnam, have become attractive places for commercial activities (Lee, 2016). Consequently, this success has also made the ASEAN countries, including Vietnam, more attractive to criminals, including cyber criminals (Heinl, 2013; Lee, 2016). Thus, it is absolutely necessary, and important, to carry out such a study to discover the key characteristics of cybercrime in Vietnam, and subsequently, to discover the appropriate measures that could be put in place to protect individuals, businesses, critical infrastructures and government institutions in Vietnam.

Cybercrime frequently hits the headlines of most newspapers and social media sites in Vietnam. For some examples, Vietnamese authorities and its citizens have paid more attention to cyber-attacks because of significant attacks on two major airports in Vietnam in July 2016. This event hit the headlines of most newspapers and social media sites in Vietnam and internationally with headlines such as: ‘Cyber-terrorists attack
flight info screens at Vietnam’s 2 major airports’; ‘Passengers stuck at Vietnam’s major airports after cyber-attack’ (Vnexpress, 29 July 2016); ‘More than 100 flight delayed due to cyber-attacks at Vietnam’s airports’ (Thanh Nien News, 30 July 2016); and, ‘Flight information screens in two Vietnam airports hacked’ (the Guardian, 29 July 2016). ‘Hacking dominates Vietnam’s list of noteworthy Internet security news items in 2014’ (tuoitrenews, 01 February 2015). ‘Microsoft names Vietnam among world’s biggest cybercrime victims’ (Thanh Nien News, 26 May 2014); and ‘Cybercrimes causes million in damage in Vietnam’ (tuoitrenews, 20 June 2013); ‘Police arrested 43 foreign hi-tech fraudsters’ (Vietnambreakingnews, 7 April 2012); ‘Experts urge greater IT security awareness’ (Vietnamese breaking new, dated 06 April, 2011); ‘Information insecurity danger for Vietnam’ (The Saigon Times daily, 25 October 2010); ‘Hi-tech criminals target Vietnam’ (dantri, 27 October 2010); and ‘Vigilance needed against rising high-tech crime in banking sector’ (Vietnam news, 07 April 2009).

However, little attention is paid to the nature, prevalence, manifestation and regulation of cybercrime in Vietnam. In fact, cybercrime itself is a rather new subject of academic enquiry, and thus many individuals, including relevant professionals in Vietnam, know very little about it. The result of knowing very little about cybercrime has not only had a significant negative impact on drafting regulatory framework to deal with cybercrime, but also on developing and deploying cybercrime prevention strategies. Furthermore, since incidents of cybercrime and its victimisation are increasing, it becomes necessary to study cybercrime and identify some key potential difficulties and challenges which the Vietnamese authorities need to confront when dealing with the regulation of cybercrime.

There is an absence of previous research on the topic of cybercrime and its regulation in a Vietnamese context. Although there have been a number of books and high-profile articles about Information and Communications Technologies (ICTs) and laws in Vietnam, they are more descriptive than critical in their analysis (Loi, 2007). Moreover, there is a lack of focus on cybercrime or criminal activity related to the Internet. As the Vietnamese literature on the regulation of cybercrime is very limited, documented analysis is a key part of the methodology of this research.

In particular, this thesis will be the first study using in-depth face-to-face semi-structured interviews to reveal information on the regulation of cybercrime in Vietnam. In-depth information and knowledge from high-level professionals from key regulatory
institutions who are responsible for, and are directly dealing with, cybercrime will be presented. The methodology used in this research is qualitative. Through the use of qualitative research methods – document analysis and face-to-face semi-structured interviews this study offers a critical analysis of cybercrime and its regulation in Vietnam. It also provides Vietnamese policymakers and researchers with a better direction in cybercrime research and policy-making.

1.4. The organisation of the thesis

This thesis will be structured as follows:

Chapter 1 is divided into four sections. The first section provides a brief background of the research topic. The second section provides the aim and scope of this research study. The third section explains the necessity and importance of this research. The final section ends with the organisation of the thesis.

Chapter 2 is focused on cybercrime and its regulation; and it consists of four main sections. After the introductory section, the second section presents current academic debates over the definition and typology of cybercrime. The third section discusses some key characteristics of cybercrime. The fourth section considers the current state of the art of cybercrime regulation.

Chapter 3 details the research methodology and the two research methods used in this study. It explains the rationale behind using a qualitative methodology to collect data and the two-specific research qualitative methods used in this research – (document analysis and face-to-face semi–structured interviews). Aside from the introductory and concluding sections, the chapter consists of five parts. The first part explains why this research adopts the qualitative methodology. The second part explains why document analysis and face-to-face semi-structured interviews are adopted in this research. This part of the chapter also explains how data is collected from semi-structured face-to-face interviews. The third part describes the methods used in the analysis of research data. In the fourth part, the ethical protocols observed by the researcher in this study are discussed. The final part of the chapter considers the limitations of the chosen methodology and methods.
Chapter 4 presents the current state of the art concerning cybercrime and its regulation in Vietnam as part of the thesis findings. This chapter contains three main parts. First, it briefly presents an overview of the socio-economic and technological context of Vietnam. It discusses the background of Vietnam in relation to Information Communications Technologies (ICTs). Then, it sets out the growth of the Internet in Vietnam, as it has been given top priority in terms of the country’s policies, strategies, and masterplans. The second part starts with a brief snapshot of cybercrime in Vietnam. The meaning of the term ‘cybercrime’ in the Vietnamese legal system is fully considered. The research indicates that the Vietnamese government has tried to establish its own definition of ‘cybercrime’ to be used in its legal system. However, the term ‘cybercrime’ and its relationships with other forms of crime are still unclear, this is due to the many unique features and nature of cybercrime. The challenges associated with the emergency of cybercrime are not only faced by Vietnam; there are global challenges. This section also addresses the establishment of institutional regulatory mechanisms in relation to the regulation of cybercrime. This section explores two major issues in the regulation of cybercrime in Vietnam: i) how the initial Vietnamese legal framework responds to cybercrime; and, ii) the key challenges facing for Vietnamese law enforcement agencies in responding to cybercrime. In addition, this part also introduces the challenges facing Vietnam’s Internet Service Providers (ISPs).

Chapter 5 presents findings of this research. It presents the data collected and themes identified in a series of face-to-face interviews from high-level professionals from key regulatory institutions in Vietnam, between July and November 2015. The chapter first presents an overview of the research sample. Next, it provides details of the perceptions of relevant Vietnamese high-level professionals concerning the definition and nature of cybercrime, and its impacts. The chapter then focuses on presenting the viewpoints of high-profile Vietnamese government officials on the current policies concerning the regulation of cybercrime. In doing so, the research illustrates the key limitations of the regulation of cybercrime in Vietnam and existing policies tackling cybercrime. Finally, the chapter explains some possible approaches to reducing the growth of cybercrime in Vietnam.

Chapter 6 discusses the key research findings in light of relevant literature and theory. The research questions will be used to guide the discussion of key research findings. The chapter is divided into five sections. The first section discusses research findings in
relation to perceptions of the definition of cybercrime and its impact in Vietnam. The chapter then discusses the research findings in regard to the current regulation in response to cybercrime in Vietnam, identifying some limitations of Vietnamese policies. Thirdly, the chapter moves on to discuss the role of three key players in regulating cybercrime in Vietnam: i) the role of users; ii) the role of ISPs; and iii) the role of the Police. Finally, two possible approaches are discussed that could reduce the growth of cybercrime in Vietnam.

Chapter 7 concludes this thesis; it outlines a summary of the research findings and conclusions. Key implications are provided. In addition, directions for possible future research are identified in view of the current research findings.
Chapter 2. Cybercrime and its regulation – A general overview

2.1. Introduction

Arguably, the exponential growth in advanced technology has transformed human societies, with consequent and dramatic changes in every aspect of the daily lives of individuals, private businesses and governments. These changes include: communication, interaction, the emergence of new types of economic activity, new social behaviours, and even new social structures. Along with these, advanced technology has also created a new criminological phenomenon – cybercrime. However, understanding what cybercrimes actually are, and what make these activities difficult for authorities to regulate, is not easy. However, a better understanding of these challenges is needed to frame law and policy, and thus to better respond to cybercrime.

Cybercrime is an umbrella term that covers a wide range of illegal activities related to computers and networked technologies (Wall, 2015). Moreover, the term cybercrime has neither origin nor reference point in law, science or social action (Wall, 2012/2008; Chhabra & Chhabra, 2014). Nevertheless, the term cybercrime is widely used by both the general public and in academic circles. In fact, cybercrimes are of such theoretical and empirical complexity that the root of a standard definition and typology is very difficult to find. Thus, cybercrime deserves specific attention from a criminological perspective (Koop, 2010). For this reason, this chapter, firstly, introduces current academic debates over the definition and typology of cybercrime. Secondly, this chapter will discuss some key characteristics of cybercrime. Thirdly and finally, the chapter concludes with a discussion of the current state of the art of cybercrime regulation.

2.2. Cybercrime definitions and typology

2.2.1. Definition

The term cybercrime has been used to describe a wide range of criminal activities that are Internet-related. Cybercrime is defined differently by different individuals, such as technical experts, Police, criminologists, national security experts, and lay persons
The definition of cybercrime is hardly a settled one because it can be defined more broadly or narrowly (Hathaway, 2012). Simply put, the definition of cybercrime should not be constricting, because “the advancement of technology will almost certainly lead to a transformation of cybercrime which is why, some prefer to think of cybercrime as an ever-changing set of behaviours” (Gillespie, 2016, p. 13). Therefore, there is no consistent definition of the term cybercrime, and there is no national or international consensus on what cybercrime actually is (Brenner, 2012, 2010; Yar, 2013; Wall, 2015/2007). As a result, a universal definition of cybercrime remains elusive (Kshetri, 2010). Here are some examples of definitions:

- “computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks” (Thomas & Loader, 2013, p. 3);
- “a criminal act that is committed using a computer that occurs over the Internet” (Vito & Maahs, 2015, p. 296);
- “Any crime that can be committed by means of a computer system or network, in a computer system or network or against a computer system or network. In principle, it encompasses any crime capable of being committed in an electronic environment” (United Nation, 2010);
- “can be either cyber-dependent crime - committed only through the use of Information and Communication Technology devices, where the devices are both the tool for committing the crime, and the target of the crime; or cyber-enabled crimes that are traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT” (HM. Government, 2016, p. 17); and
- “refers to methods by which computers or other electronic devices are used to carry out criminal activity and cause harm to others” (Hill & Marion, 2016, p. 5).

Although some individuals define cybercrime differently, they all agree on the significant role that networked technologies play in relation to this type of criminal activity (Wall, 2012). In fact, many activities that have been classified under the umbrella of cybercrime are Internet-related. Many of these activities (e.g., cyber-violence, cyber-vandalism and cyber-rape) might be more appropriately classified as
deviant behaviours occurring in cyberspace rather than classified as cybercrime because they do not have clear legal status (Chhabra & Chhabra, 2014).

Not having a clear view of what cybercrime is makes it particularly difficult to classify and to distinguish from traditional crimes. More importantly, it makes it more difficult and challenging for authorities to handle. Furthermore, “we cannot hope to adequately combat it” (Hill & Marion, 2016, p. 155). Therefore, it is useful to make some distinctions, since the motivations and modus operandi of perpetrators may differ for various types of cybercrime (Koops, 2011).

In fact, many scholars (e.g., Yar, 2006, 2013; Brenner, 2001, 2010, 2012; Wall, 2015/2012/2007) have questioned whether behaviours that have been categorised under the umbrella of cybercrime are new forms of criminal activities; and if so, whether a new theory is needed or if cybercrime should be regarded as simply the same as traditional crimes. Some scholars (e.g., Payne, 2016; Harknett & Stever, 2009) argue that cybercrime is no different to traditional crime – it is simply a new way of committing conventional crime. Others, particularly Wall (2015, 2012, 2007), have argued that cybercrime differs from traditional criminal activities in a number of distinctive ways:

i) cybercrimes are mostly free of physical time frames, are trans-jurisdiction, and instantaneous (Johnson & Post, 1996; Koops, 2010, Yar, 2013);

ii) there are contentious values to inform a general opinion regarding the legal enforcement of cybercrime (Davies et al., 2017);

iii) they require considerable technical knowledge to perform – hacking, for example (Davies et al., 2017);

iv) there is no one set of consensual values about what does, or what does not, constitute a cybercrime (Davies et al., 2017); and

v) discussions on cybercrimes tend to be offender-based, not victim-based (Davies et al., 2017; Wall, 2007).

Furthermore, other scholars (e.g., Brenner, 2012, 2010, 2007, 2001; Moitra, 2005; Wall, 2015/2012/2010/2007) argue that computer and network technologies have not only provided novel ways of committing traditional crimes, those technologies have also
created new forms of criminal activities which would disappear if the Internet were eliminated.

Particularly, addressing this argument, Wall (2007) has identified three different generations of cybercrime, each generation is distinctive, and the conceptual differences between them can be used to explain the current differences in the scope of criminal opportunity. The first generation of cybercrimes consists of traditional crimes, where computers are merely a tool, these are ‘low end’ cybercrime (Wall, 2007, p. 45). It can be seen that the first generation of cybercrime involves the use of a computer, sometimes, even networked technologies. However, these technologies are used to support traditional criminal activities and these activities would persist by other means if the technologies were removed. A good example is trafficking in human beings – traffickers will use whatever forms of communications and information technologies that are available, convenient and less risky.

The second generation of cybercrimes are committed across networks (Wall, 2007). These crimes are named as ‘hybrid’ due to the fact that Internet has provided new opportunities for traditional forms of criminal activities to span global networks. Their global nature requires trans-jurisdictional procedures, which seem difficult to achieve.

The third generation of cybercrimes are ‘true crimes wholly mediated by technology’ (Wall, 2007, p. 47). Because these crime types are the sole product of opportunities created by the Internet, they would not exist if the Internet were taken away, for instance, spamming3, phishing4 and ransomware5 (Wall, 2015/2014/2007). As they are the product of the Internet, they embody all of its transformative characteristics. Particularly, these types of crimes make the physical distance between crime and its victims irrelevant. Cyber-criminals can break the relationship between crime and space – being able to commit the crime at any place where the technology exists, and at any time and– not requiring the physical presence of a victim. As a consequence, online activities can be vulnerable to criminals instantaneously and unconstrainedly outside

---

3 Spamming is defined as “the distribution of unsolicited bulk emails that contain invitations to participate in ways to earn money; obtain free products and services; win prizes; spy upon others (Wall, 2005; HM. Government, 2016).
4 Phishing is a kind of cyber-attack in which perpetrators use spoofed emails and fraudulent web sites to lure unsuspecting online users into giving up personal information (Akanbi et al., 2015; HM. Government, 2016).
5 Ransomware is a malware that renders a victim's computer or data unusable and is increasingly being used by criminals to generate revenue through extortion (Philip et al., 2018).
normal barriers of physical distance (Yar, 2013). Simply put, the victims of cybercrime can be anywhere in the world.

In addition, with the advent of the ‘internet of things’\(^6\), there are many different Internet technology-related activities that can still emerge as cybercrimes. However, not all of them have, or would have, clear criminal status because some are still subjects of ongoing legal debates, and many of them are simply viewed as ‘deviant’. Spamming is a good example of an Internet related activity which can be classified as illegal behaviour under the United Kingdom and the United States law and that of many other jurisdictions such as Australia, Canada and European countries (Mueller, 2010).

2.2.2. Typology

The term ‘cybercrime’ is defined by a variety of approaches depending on the creator’s point of view. Differences in viewpoint provide alternative ways of categorising cybercrime or creating appropriate typologies. The creation of a suitable typology of cybercrime is in itself complicated.

For example, one approach to categorising cybercrime can be found in the Convention on Cybercrime (2001), which provides four different types of offence as listed below (Council of Europe, 2001):

- Offences against the confidentiality, integrity and availability of computers and systems including illegal access, illegal interception, data interference, system interference, and misuse of devices,
- Computer-related offences: forgery and fraud,
- Content-related offences: child pornography,
- Copyright-related offences.

These four categories are further subdivided into subgroups. Indeed, the Convention serves as a general model by which to understand what constitutes cybercrime. It can be used to educate people about appropriate behaviour on the Internet, and also acts as a

\(^6\) The Internet of things is a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies (International Telecommunication Union, 2012, Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks).
general legal framework for European and other countries in the development of countermeasures against cybercrime. This approach, indeed, does not include some types of crime which have been committed or facilitated using the computer, such as money laundering or identity theft. Nevertheless, this approach is said to be a useful basis for discussing the phenomena of cybercrime.

A different approach suggests that there are three categories of cybercrime, Sandywell (2010) points out as: (1) Traditional criminal activities that are expanded or enhanced by the Internet; (2) Traditional criminal activities which are generalised and radicalised by the Internet; and (3) Criminal activities which are created by the Internet (p. 46).

This approach provides a useful understanding of cybercrime because it does not only indicate new criminal behaviour, it also shows new ways of committing existing criminal acts (Gillespie, 2016). The first two categories demonstrate how old crimes can now be carried out via the new tool of the Internet, such as, credit card fraud which has been transformed by the internet and growth of e-commerce. However, some forms of crime did not exist before the intervention of the Internet, such as phishing and hacking⁷.

Brenner (2012, 2010, 2004, 2002, 2001) provides a typology of cybercrime based on the role of the computer in relation to criminal behaviours, such as: (1) the computer as the target of the offence; (2) the computer as the tool with which to commit the offence; and (3) the computer as an incidental aspect in committing a traditional offence (p. 14).

The first category of cybercrimes, where computers are the target of an unlawful activity (Brenner, 2012, 2004), means that the computer plays an essential role in relation to criminal activity, and, without a computer, it would be impossible for this type of crime to occur. Brenner (2012) describes cybercrimes under the category as ‘the perpetrator attacks the computer by breaking into it, introducing a code that damages it, or bombarding it with data’ (p. 14). Examples of such crimes range from simple hacking (unauthorised access to a computer system or part of it) and aggravated hacking (unauthorised access with the purpose of committing a crime such as copying or altering

⁷ Hacking generally describes deliberate unauthorised access to spaces over which rights of ownership or access have already been established (Wall, 2007; HM. Government, 2016).
the information in the system) to denial of service attacks\textsuperscript{8} and the dissemination of viruses\textsuperscript{9}, worms\textsuperscript{10} and various malware\textsuperscript{11} (Brenner, 2012, 2010).

The second category of cybercrime includes those crimes in which computers are used as a tool to commit crimes (Brenner, 2012). Based on this category, all forms of traditional crimes are classified as cybercrime when a computer network is involved, such as fraud, theft, stalking, harassment, forgery, obstruction of justice, the creation and dissemination of child pornography, and copyright infringements. In this approach, instead of being the target of a cybercrime, the computer is just a tool which is used to commit a criminal act. For Brenner (2012), the role the computer plays in these forms of criminal activity is lesser but still far from insignificant. This second category of cybercrimes can be prosecuted under traditional criminal law, because the use of advanced technology only facilitates committing the crime and does not alter the nature of the offence (Brenner, 2012). However, when traditional crimes are committed online, it becomes difficult to prosecute them under traditional criminal law.

Brenner (2012) defines the third category of cybercrime as crimes where “a computer can play an incidental role in the commission of a crime” (p. 14). This category encompasses a variety of activities, such as the use of computer by a blackmailer to write extortion letters to victims, or the use of a computer by a drug dealer to perform criminal activities. Thus, Brenner suggests that the role of the computer in relation to these criminal activities is a source of evidence and the computer’s role can be important, in effect, becoming the crime scene (Brenner, 2012, 2004).

Interestingly, from Brenner’s approach, it might be argued that the second category of cybercrime can include the first category of cybercrime, that is where computers are both the target of a crime and can be used as a tool to commit crime. For example, all kinds of unauthorised access, denial of service attacks, dissemination of viruses, etc. require the use of computers to perpetrate such acts. However, crimes are identified as cybercrime under the first category which are not considered as cybercrime under the second category. Nevertheless, the key principle that can be used to distinguish the first category from the second category is to consider whether a computer, or a computer

---

\textsuperscript{8} Denial of service attack is any type of attack performed on a networking structure to disable a server from servicing its clients (Rao, 2018).

\textsuperscript{9} Virus is a program that can copy itself and infect computers (Brenner, 2012).

\textsuperscript{10} Worm is a self-replicating computer program (Brenner, 2012).

\textsuperscript{11} Malware is designed to infiltrate or damage a computer without the owner’s knowledge and consent (Brenner, 2012).
system, is the target of any attack. Another way of distinguishing between these first
two categories of cybercrime is to think whether crime would have occurred in the
absence of a computer.

David Wall (2001), one of the earliest authors to study cybercrime, identified and put
forward a four-category typology, combining both offender behaviour and technology.
Although it was created some time ago Wall’s earliest typology of cybercrime is widely
recognised as the main reference point when studying cybercrime. Wall (2001)
suggested that cybercrimes could be categorised as follows:

i) The first typology is cyber-trespass;

ii) The second cybercrime typology is cyber-deception/theft;

iii) The third cybercrime typology is cyber-porn and obscenity; and

iv) The fourth is cyber-violence (p. 6).

These categories of cybercrime vary according to the object, or target, of the illicit
activity in which cyber-trespass and cyber-deception/theft refer to ‘crime against
property’; cyber-pornography/obscenity represents ‘crime against morality’; and cyber-
violence relates to ‘crime against the person’ (Wall, 2011). Extending Wall’s categories,
Although Wall’s category of cybercrime is said to be preferable to use when studying
cybercrime (Holt et al, 2016), this approach is also criticised. For example, Gillespie
(2016) argues that the approach borrows much of the offender-focus model by looking
at aspects of what the person is trying to do rather than considering why the offender
acted in the way that he/she did. Therefore, Gillespie (2016) concludes that this
approach does not allow or assist in identification of which crimes are genuinely new
and which are merely new forms of existing offences. Moreover, Wall’s categorisation
does stress some aspects of cybercrime that are continuous with traditional crime and
“does little in the way of isolating what might be qualitatively different or new about
such offences and their commission” (Yar, 2013, p. 11).

The discussion of definitions and typologies of cybercrime indicates a common feature
that, regardless of the different ways of defining or categorising cybercrime, cyberspace
provides unique characteristics for cybercriminals. These characteristics present
challenges not only to individuals and businesses, but also to governments and criminal
justice systems throughout the world, in keeping pace with, and enjoying the many
benefits of, advanced technology. Several scholars (e.g., Wall, Brenner, Yar, Smith, Holt, Bossler) who specialise in cybercrime suggest that to understand why cybercrime is a complex topic to study, the unique characteristics of cybercrime should be considered. For this reason, the section below will look at these characteristics.

2.3. The unique characteristics of cybercrime

There is no doubt that the introduction of computer and network technology, especially the emergence of the Internet and its associated advanced technology, brings many benefits to individuals, businesses and society. Especially, in communication, the way in which information can easily be accessed, distributed and proliferated, has accelerated and contributed to the development of cyberspace (Grabosky & Smith, 2001; Nasheri, 2005; Wall, 2007; Yar, 2006, 2013). In addition, the growth in computer and Internet usage has colonised and changed every aspect of the daily lives of individuals, organisations, and governments, creating more efficiency, especially in personal and business interactions and transactions. Those technologies have, in fact, not only changed daily life, but they have also provided new opportunities for traditional crime and created new crimes which cannot exist without the existence of those technologies (Furnell, 2002; Wall, 2015/2012/2007/2001). Thus, the question which should be asked here is: in what ways have these advanced technologies created opportunities for cybercriminals (Geer, 2007; Wall, 2015/2012/2007/2001)? The following subsections will discuss in detail some major categories of characteristics which lead to cybercrime becoming a special phenomenon and hamper legal authorities in dealing with it.

2.3.1. Multiple opportunities

The evolution of the Internet and its associated advanced technologies have created fresh opportunities for criminals. In other words, advanced technologies can provide fertile ground for criminals (Clough, 2015, 2010). As technologies develop increasingly, criminals are also adopting or developing new ways to commit crimes by using such technologies. In fact, in criminological studies, there are an increasing number of studies which have investigated complex criminal activities by looking at opportunity as the
‘root cause’ of all crime (Felson & Clarke, 1998). Thus, it can be argued that random opportunities play a fundamental role in shaping behaviours; and that the reduction of opportunities is the best way to combat crime. In doing so, it is necessary to look at how advanced technologies create opportunities for criminal activity. In respect of cybercrime, Clough (2015, 2010) believes that there are five features of digital technology which are creating opportunities for criminal activity. On the other hand, these five aspects of digital technology are also seen as creating more challenges for law enforcement. For Clough, the features of digital technology are: scale, accessibility, anonymity, portability and transferability, global reach, and the absence of capable guardians (pp. 5-7). Gillespie (2016) agrees with Clough’s (2015, 2010) opinion and adds technological advancement to be among other features which are believed to provide more opportunities for criminal activity.

Specifically, Wall (2015, 2010, 2007) argues that advanced technologies have transformed criminal behaviour into three main ways, which are considered to provide multiple opportunities for cybercriminal activity as follows.

Firstly, cybercrime is an aspect of globalisation; this means that the scope of criminal acts can be expanded. In other words, the scope of opportunity for cybercrime can provide a world of opportunity for offenders (Clough, 2015, 2010). This can be easily seen by comparing cybercrime with traditional crimes. Traditional crimes can be limited by a specific physical location. It is difficult, though not impossible, for criminals to take their criminal acts into other countries. In contrast, cybercriminals do not have to physically enter the territory of the sovereign entity to commit their crimes there (Brenner, 2010). In other words, cybercriminal acts are not confined by borders or other physical constraints because the relatively clear borders and turf lines within the physical world are not replicated in the virtual world (Finklea, 2013). As Finklea states: “high-speed Internet communication has not only facilitated the growth of legitimate business, but it has bolstered criminals’ abilities to operate in an environment where they can broaden their pool of potential targets and rapidly exploit their victims” (p. 4).

Moreover, since the birth of smart phones, it becomes essentially a powerful hand-held computer, capable of performing a wide range of computing functions and enjoying connectivity to the Internet and other networked services. In other words, accessibility to the Internet and its services are increasingly open for all to use. Similarly, cybercriminals employ all the features that are best designed to carry out their activities.
(Dean et al., 2012). As a consequence, cybercrime can now be easy to carry out remotely from across countries, even across the world (Finklea, 2013). This has been proven by the fact that since the introduction of digital cameras there has, and continues to be, a growth in child pornography, or through the development of social media and electronic messaging, such sites are increasingly used to stalk, harass and intimidate (Clough, 2015, 2010).

Furthermore, in cyberspace everything is in digital format and the flow of digital information transmission is not limited by any physical means. It can go to every corner of the world. Moreover, at present, with the advent of ‘the internet of things’ there are ever-increasing opportunities for cybercriminals to commit crime.

More importantly, cybercriminals can operate at a very low risk of being apprehended or punished for their criminal acts, because of the fact that it is difficult to trace the actual location from which they operate (Brenner, 2010, 2012; Brown, 2015). In other words, cybercrime presents enormous challenges to law enforcement.

Secondly, advanced technology allows users to communicate/make contact with a vast number of people worldwide, at any time of the day, simply and in a cost-efficient manner (Clough, 2015, 2010). In fact, individuals, businesses, organisations and governments are increasingly conducting their day-to-day business with the assistance of advanced technologies. So are criminals, and they are able to reach millions of potential victims virtually and without cost (Clough, 2015, 2010). Therefore, it can be said that advanced technologies create an unprecedented pool of potential offenders and victims which in turn allows “offending to be committed on a scale that could not be achieved in the offline environment” (Clough, 2015, p. 6). Similarly, Wall (2015) asserts that advanced technologies can create the potential for ‘asymmetric relationships’ that means a cybercriminal can victimise many easily, and cheaply, at the same time.

Thirdly, advanced technology has created new forms of networked social relationships, such as Facebook, Twitter, Instagram, Bebo, Myspace, and Second life, and these can be the source of new criminal opportunities (Wall, 2013/2007). This is because they take the forms of Internet-based applications which allow users to present themselves and share details of their lives, activities, interests and even to display their identities for others to view, comment upon and interact with (Miller, 2011). On the other hand, they
have attracted the attention of many businesses, individuals, organisation and governments applying these advanced technologies in their daily businesses, management and services. Furthermore, these social networks are not only integrated with computer networks, they are increasingly integrated with a range of technological devices, such as smartphones, which allow users to instantaneously capture and share images, video and text with others. Facebook is a good example of a social network site which was first launched in February 2004 by Mark Zuckerberg and co-founders Dustin Moskovitz, Chris Hughes and Eduardo Saverin from their Harvard University dorm room (Carlson, 2010; Facebook, 2011). Since Facebook allows all individuals to join the site, it has fast become the largest social network site with over 1.8 billion active users.\(^\text{12}\) Although, Facebook allows only individuals over a certain age to create an account with them, there are, in fact, no robust checks in place for this requirement. Thus, young children can engage in online interactions and make themselves available for contact with unknown persons.

Alongside the many benefits then, social network sites have become a platform for criminals. In other words, social network sites contribute to the creation of new forms of vulnerability to criminals (Yar, 2012) and increasingly become a hub of criminal activity (Schneider, 2016). The main reason for this is that social networks are characterised by a ‘few too many’ model of communication and they are organised into unidirectional channels of communication that flow ‘one-way’ (McQuail, 2010), whilst at the same time enabling ‘many to many’ and ‘two-way’ interactions (Miller, 2011). Therefore, there have been many headlines in the media warning of the dangers to individual users when engaging in various activities on social network sites. For example, The Independent had a headline ‘Crime risk warning to users of social networking sites’ (Barrett, 2007), and the Daily Mail had ‘The Facebook crime-wave hits 100,000 in the last five years’ (Gill, 2010). An array of criminal activities related to social network sites are often featured in newspaper articles, for instance, privacy issues, fraud (Mail Online, 2007; Finkle, 2009), identity theft (BBC, 2011a), hacking (Williams, 2012; Holden, 2012), and hate crimes (Channel 4 News, 2012). In addition, social network sites provide an avenue for various other criminal activities such as

stalking\textsuperscript{13}, hate speech, and cyber-bullying\textsuperscript{14} (BBC, 2011b), and more serious offences, for instance, sexting\textsuperscript{15} (Mail Online, 2011), and grooming\textsuperscript{16} (BBC, 2012). Therefore, in relation to social network sites, Yar (2012) draws the conclusion that “participation in social media, with the extension of personal lives into quasi-public spaces that it necessarily entails, brings as its inescapable counterpart a vulnerability to a wide range of criminal victimisations than previously seen” (p. 217).

2.3.2 Transnational in nature

As mentioned above, advanced technologies have contributed to the acceleration of globalisation by collapsing traditional physical geographies of nations. The global nature of cyberspace allows criminals sitting on one side of the world to conduct illegal activity on the other side. There is no need for criminals and victims to be in the same jurisdiction. This means that cybercriminals can easily enter the physical boundaries of the sovereign entity where they commit their crimes because every nation is now connected to the Internet. Cybercriminals can commit their criminal acts from anywhere and can quickly impact on victims in multiple states and national jurisdictions (Clough, 2015, 2013). Simply put, cybercrimes are borderless crimes (Hill & Marion, 2016).

The borderless nature of cybercrime can be understood by the way that any nation can be targeted, and its citizens victimised from anywhere in the world (Hill & Marion, 2016). In contrast, law enforcement officers cannot work in this way, as the exercise of their power is often constrained by physical boundaries (Finkle, 2009). Additionally, not all nations have their own laws to regulate cybercrime, and the lack of cybercrime legislation in one country can influence directly, or indirectly, the rest of the world, by creating, for instance, jurisdictional havens. The transnational feature of cybercrime poses a number of challenges for legal authorities to deal with:

\textsuperscript{13} Stalking is defined as using the internet, email, and other electronic communication devices to stalk another person (Reyns et al., 2012).
\textsuperscript{14} Cyber-bullying involves the use of modern communication technologies to torment, embarrass, humiliate or intimidate an individual (Altobelli, 2010).
\textsuperscript{15} Sexting is defined as the act of sending and receiving nude or semi-nude pictures of another via text messages (Ostrager, 2010)).
\textsuperscript{16} Grooming is defined as establishing a trust-based relationship between minors and usually adults using ICTs to systematically solicit and exploit the minors for sexual purposes (Wachs et al., 2012)).
(1) The transnational aspect of cybercrime is also viewed as the most distinctive feature with which to distinguish cybercrime from traditional crimes, and it is also considered to create a significant challenge for legal authorities to deal with, in terms of jurisdictional problems (Brown, 2015; Yar, 2013, 2006; Clough, 2015, 2010). Cyberspace is a distinct place, beyond traditional rules, based on geographical location (Clough, 2015, 2010).

(2) Another challenge is to obtain sufficient evidence because of the fact that evidence in cybercrime cases can be located in one or more foreign countries, and access to these may be difficult or impossible. In terms of collecting evidence, the take-up of advanced technology has changed the landscape of the crime scene, increasing the need for cross-jurisdictional investigation. This is because with respect to cyberspace, identifying cybercrime crime scenes can be a daunting task. The key reason for this is that cybercriminals can attack victims through computer networks in three or four or many countries, with obscure networks that are inaccessible to investigators.

(3) Identifying the perpetrator and determining where the perpetrator is physically located is a further challenge. This is because advanced technologies offer valuable opportunities to disguise both cybercrime and the identity of perpetrators (Yar, 2013). Cybercriminals can present themselves under false aliases or steal the identity of some other unsuspecting and innocent person for the purposes of committing their offences (Smith, 2010). In this respect, Yar (2013) asserts that regulating cybercrime will be more difficult in terms of identifying, and bringing criminal sanctions against, cybercrime and cybercriminals. This is because cyberspace is a distinct phenomenon that is either beyond traditional rules or beyond geographical location (Clough, 2010). The exercise of jurisdictional power becomes problematic. As cybercriminals can act remotely, the law enforcement response to cybercriminal conduct must rely significantly on trans-border mechanisms such as mutual legal assistance and extradition (Weber, 2003). Thus, Yar (2013) argues that in doing so, the cooperation of law enforcement agencies with other countries is required. This not easy as it is time-consuming and costly for law enforcement agencies, in part because of conflicts between legal regulations in different countries. These mechanisms are not always readily available, or practicable, because of the different legal qualifications and definitions of online conduct in various jurisdictions (Urbas, 2012).
2.3.3. Anonymity

The anonymity which is created by advanced technology is an incentive and advantage for cybercriminal activity. In fact, in cyberspace, users are not required to provide a real identity. They can present themselves under false aliases or steal the identity of others, including innocent persons, for the purposes of committing their offences. In this respect, Thomas and Loader (2013) argue that determining the identity of cybercrime can be far more difficult and complex, for three main reasons: i) advanced technologies facilitate cybercrime at a distance; ii) cybercrime can be committed without providing any physical identification; iii) cybercrime is committed in a special environment – cyberspace – where everything can be in digital format. Thus, with these special characteristics, cybercrime is distinct from traditional crimes. This provides a further challenge to legal authorities in identifying and imposing criminal sanctions to it (Wall, 2015; Yar, 2013). This will be even more difficult and complicated when cybercriminals use advanced technologies and encryption techniques which allow a high level of anonymity or the assumption of a false identity.

As illustrated above, the prevention and protection of users from cybercrime attacks has become one of the major challenges of the 21st century. The increasing use of Information Communication Technologies (ICTs) and especially computer networks is seen as fundamental to various key functions of our society, including economics, government, society, and culture (Deibert & Rohozinski, 2010b). The growing influence of cyberspace and the Internet in everyday life has created multiple opportunities for some individuals to exploit weaknesses in the virtual world. Therefore, securing cyberspace is becoming a major challenge both nationally and internationally.

Cybercrime has distinctive characteristics such as multiplicity of opportunities, transnationality and anonymity which make cybercrime a separate phenomenon requiring special attention. These features also make cybercrime difficult to regulate. Cybercrime impacts not only on individuals, but also upon businesses, organisations and governments both nationally and internationally. Many cybercriminals may commit or live in different countries from their victims and, even if they were in the same country, the victim may have no idea where the offender actually resides (Holt et al., 2015). This creates significant confusion for individuals, businesses, organisations and even law enforcement to know which appropriate agency or authority to contact.
Increasingly, technologies are readily available in assisting connectivity, providing cybercriminals with widespread access to resources. Moreover, the increased numbers of users and social network sites, also creates a resource for cybercriminals. Networked technologies create an environment allowing criminals to commit a large crime, or many small crimes, with lesser risk to themselves (Wall, 2015).

Furthermore, advanced technology affords, and also offers, cybercriminals the ability to hide their actual identity in a number of ways, such as the use of false names and locations, making it difficult for authorities to determine who is responsible for criminal acts. This rapid technological development will continue posing new challenges as it grows.

As a matter of fact, the full consequences of cybercrime are unforeseen. Moreover, law enforcement agencies have traditionally exercised their legal powers based on physical boundaries. Thus, in regulating cybercrime effectively, traditional mechanisms of enforcement may be difficult, even to the extent of being impossible in some cases. Simply put, cybercrime cannot be effectively regulated by national or international policies alone. In addition, the scope and complexity of cybercrime shows that no single actor can manage cybercrime effectively. It requires individuals, businesses, organisations and governments to work together, at both national and international levels.

Despite numerous initiatives to reduce cybercriminal activities, destroying one network often results in the establishment of another, re-shaping criminal activity and methods, and in turn, allowing a new type of cyberattack to develop. Nonetheless, the rapid increase in cyberattacks calls for the use of flexible measures, which demands high levels of cooperation from individuals, businesses, organisations with governments. Without the involvement of all of these actors, the effective regulation of cybercrime will remain impossible (Jakobi, 2016). Simply put, a successful response to cybercrime will depend on the requirement of a high degree of cooperation across and between multiple actors and agencies.
2.4. The current state of the art of cybercrime regulation

The previous section has shown that the current existing literature indicates that advanced technologies do not only provide new opportunities for traditional criminals, but also create new criminal activities, so-called cybercrime. Cybercrime is a complicated problem due to the fact that it is far beyond the physical borders of any nation, it becomes an international issue. Dealing with this typical and complicated cybercrime problem does, therefore, require both national and international involvement. Cybercrime issues have been addressed by a number of steps, from both national and international actors, in order to protect the interests of individuals, organisations, governments, and society at whole (Clough, 2010). The following subsections below will examine and describe the current state of the art of cybercrime regulation by exploring: i) some of the clear contradictions between the fundamental characteristics of the widely used classic regulatory framework – the Peel’s model of policing (Peel, 1829) – and the nature of cybercrime; ii) what nations such as the UK, Australia, Canada and US have done to combat cybercrime at the national level; iii) what efforts have been taken at an international level to regulate cybercriminal activities; and iv) what cybercrime prevention initiative measures have been taken in order to reduce the growth of cybercriminal activities.

2.4.1. The ‘Peelian paradigm’ – A modern regulatory framework

To deal with the rising of crime and deviance brought about urbanisation, the ‘Peelian model’ was introduced by Sir Robert Peel in 1829 as he was founding the London Metropolitan Police (Reiner, 2010, Peel, Glensor & Peak, 1999). This professional policing model was implemented throughout England and its Colonies, including Canada (de Lint, 2004), Australia (Goldsmith, 2001), and New Zealand (Buttle, 2013), and then spread around the world to incorporate other nations, such as the USA (Brenner, 2010; Egger & O’Leary, 1995). In fact, this model is considered as the regulatory approach that all modern societies use to control crime. The ‘Peelian paradigm’ is, of course, territorial in nature. Thus, it embodies the following key characteristics of traditional crime (Brenner, 2010):
1. Both victim and perpetrator occupy the same geographic place, even to the extent of being proximate to each other.

2. Crimes often spread rather slowly, on a one-to-one basis. The perpetrator usually needs to focus his/her attention on perpetrating a crime prior on to moving the next. Usually, a murderer can only kill one person at one time.

3. Crimes are subject to physical constrains, thus demanding certain degrees of planning to succeed.

4. The ease to track crimes insofar as victimisation is concerned tends to fall into geographic or demographic patterns, resulting in large amount of crimes in concentrated areas.

Taking for granted the persistence of this specific crime ecosystem as constructed by the above four key characteristics, the ‘Peelian model’ accepts that the task of law enforcement is to deploy force to respond to a threat in a specific territorial area (Brenner, 2014). The Metropolitan Police was, indeed, created alongside this model under this perception. It was, at that time, a new creation – an independent, quasi-military agency staffed by full-service, uniformed professionals whose task was to react to crimes and apprehend the perpetrators, who would then be appropriately punished (Brenner, 2004). Almost two hundred years later, current police forces still have a leading role in crime investigation, being responsible for victim interviews and suspect arrests (Hodgson, 2010). More importantly, these police forces are still responsive to local crimes, which are identifiable from the public and accountable to territorial law (Wall, 2011/2007).

This professional policing model was implemented throughout England and its Colonies, and then eventually spread around the world (Brenner, 2010). This professional policing model is viewed as the approach all modern societies use to control crime. This model was created to apply for real-world crime. Although, it has been a long time, many original principles remain firmly intact. Police today still adopt a leading role in the investigation of crimes, holding responsibility for interviewing victims and arresting suspects (Hodgson, 2010). Moreover, modern policing continues to be ordained within bureaucratic hierarchical structures that are responsive to local crime, identifiable from the public and accountable to law (Wall, 2007/2011).
However, the Internet has changed the landscape of human communications and activities, creating new forms of technically enabled opportunities, including new forms of crimes. Actually, cybercrimes cannot be limited to specific geolocations as traditional crimes (Brenner, 2013; Europol, 2018). Multiple opportunities created by technologies have enabled cybercrimes to have much larger scales than that of their traditional counterparts since these crimes could easily be automated, e.g., Phishing (Nurse, 2018; McGuire & Dowling, 2013). Furthermore, often occurring in anonymous digital environments, cybercrimes escape the physical constraints that govern traditional crimes. Thus, by the time cybercrime is detected, it may become immediately untraceable. In short, key characteristics of cybercrime, including multiple opportunities, transnational and anonymity have altered traditional modes of crime and delinquency, thus creating new and difficult challenges to the maintenance of social order (Wall, 2015/2011/2017). In fact, the rapid growth and spread of cyber-related offences confront the essences of the ‘Peelian model’ – its territorial nature – thus presents challenges to the prevention and detection of crime (Brenner, 2013). For Stenning and Shearing (2015), cybercrime “will present some of the biggest policing challenges in the immediately foreseeable future” (p. 7).

For Wall (2011/2007), the limitations of the ‘Peelian model’ have long been dealt with, at least, at a procedural level, by the establishing of international harmonisation/police organisations (e.g., Interpol, Europol) and police coordination treaties (e.g., Council of Europe’s Convention on Cybercrime, 2001\(^7\)). These treaties and police organisations would enable the investigating of crime across jurisdictions. Nevertheless, despite these efforts, cybercrimes still present a range of challenges to the police. Wall (2011/2007) has summarised these into several key points:

i) **De Minimism** – The law does not deal with trifles (de minimis non curat lex). Many cybercrimes are small-impact bulk victimisations with a large amassed loss, spreading out globally across a range of jurisdictions (e.g., salami attacks on bank accounts).

ii) **Nullum Crimen Disparities** – Although more recent protocols (e.g., the cybercrime convention and the establishment of multi-agency partnerships)

could facilitate inter-force cooperation, effectiveness depends on the offences in question having similar priority in each jurisdiction.

iii) Jurisdictional Disparities – “Faced with a jurisdictional or evidential disparity, police or prosecutors use their resourcefulness to forum-shop (Braithwaite & Drahos, 2000) to increase the prospect of obtaining a conviction (Wall, 2002b, p. 103).” Unfortunately, inter-jurisdictional cooperation is less likely to work with cases of cybercrime due to their contentious nature of non-routine offending.

iv) Non-routine Activity and Police Culture – Since most police forces are defined by their specific occupational cultures etc. (Reiner, 2000), non-routine events (such as cross-border investigations and trivial deviant behaviours) created by the Internet would be difficult for police officers to handle.

v) Under-reporting – The problem of under-reporting to the police. This is especially true in cases of bulk victimisation – victims sometimes do not realise the fact that they have been victimised.

vi) Policing using Non-traditional Methods (e.g., technological interventions) – As technologies have created more opportunities for crime and more sophisticated ways of conducting crime, they also have created more sophisticated methods of policing (e.g., advanced surveillance technologies; The Investigatory Powers (Codes of Practice) Regulations 2018). Potentially, we will be facing a situation, where ‘code is law’ (Lessig, 1999, 2001), and where ‘ubiquitous law enforcement’ (Vinge, 2000) is upon us.

With all these in mind, it is important for policy makers to review the effectiveness of current regulatory arrangements, and to reflect on future improvements.

2.4.2. National efforts to regulate cybercrime

At the national level, every nation should have responsibility for taking action to regulate cybercrime. To date, nations such as the UK, Australia, Canada and US have put combating cybercrime on the national agenda by addressing cybercriminal activities

---

in their cybercrime regulation policy or cyber-security strategies. The purpose of this section is to review how cybercriminal activities have been addressed at a national level.

The criminal law/penal code is viewed as an instrument or a technique which may serve several ends (Holt et al., 2015). As previously mentioned, there are two distinct approaches to the issue of cybercrime. At first glance, cybercrime is treated the same as other crimes which are regulated according to the criminal law/penal code. Therefore, there should not be a need to create new laws to deal with this kind of threat. The other approach is that cybercrime is distinct, and needs to be treated as a new, special crime. Thus, it is argued, it will be necessary to have new laws to treat this kind of threat.

Support for creating a new law came for the US Senate Governmental Affairs Committee, which debated the need for computer crime legislation in 1976 (Kutz, 1986). This was promoted by Senator Abraham Ribicoff who introduced the first proposed federal computer crime legislation at this time, which was the Federal Computer Systems Protection Act in 1977 (Olivenbaum, 1997). This legislation was revised and reintroduced two years later (Ibid). The revised bill then failed at the committee stage in 1979, but nonetheless played an important role in promoting the subsequent enactment of federal computer crime legislation and encouraged the adoption of such legislation at state level, in Florida and Arizona (Bloom-Becker, 1985; Kutz, 1986).

Both developed and developing countries have increasingly recognised the emerging information society and its values and risks. These new values could not be protected from the new risks by traditional mechanisms. They require new legal regulations and mechanisms (Ibid). The first development in new legislation to serve the issue regarding cybercrime was the protection of privacy as a response to the vast emerging capabilities of ICT for collecting, storing and transmitting data (Ibid). ‘Data protection legislation’ was born and has since been constantly revised and updated, protecting the rights of privacy of citizens with administrative, civil, and criminal law in many countries such as Australia (The Privacy Act 1988), the United States of America (The Privacy Act 1974; The Electronic Communications Privacy Act 1986), and the United Kingdom (The Data Protection Act 1984). Following that, the legislation has turned to preventing computer-related economic crime such as fraud, computer software and legislation directed toward protecting intellectual property, and against harmful content. For
example, in the UK, several laws dealing with these issues have been enacted, such as the Forgery and Counterfeit Act 1981, and the Computer Misuse Act 1990. However, the use of legislation to combat cybercrime still faces many challenges, because advanced technology, particularly the Internet, is accessible from any physical geographical location throughout the world, while the impact of national legislation is comparatively narrow. National legislation is enacted to impact only within the national physical boundaries of the country (Furnell, 2002; Brenner, 2010, 2012). At the same time, it is difficult to trace the exact geographical location of any attack or crime, and hence to apply the correct jurisdiction (Brenner, 2010, 2012; Brown, 2015). Furthermore, the legal conflict between nations is an issue that might be unavoidable (Brenner, 2010, 2012; Brown, 2015). Besides, there needs to be sufficiently technically skilled law enforcement personnel to detect cybercrime and enforce the law.

The other aspects of national approaches for controlling or dealing with the issue of cybercrime is law enforcement. Several states have established a specialist agency; the UK is considered to be one of the first countries to have its own specialist squad of computer crime Police (Sommer, 2004). In 1985, the Metropolitan Police’s Computer Crime Unit was established within the Fraud Squad (Ibid). After that, several organisations and units were born such as the National Criminal Intelligence Service (NCIS), the Serious Fraud Office, and National Hi-tech Crime Unit (Ibid). However, the National Hi-tech Crime Unit was replaced by the Serious Organised Crime Agency (SOCA), which was established by the Serious Organised Crime and Police Bill 2005 (The Serious Organised Crime and Police Bill, 2005).

As illustrated above, cybercrime has some unique characteristics which create many problems for law enforcement agencies, including special cybercrime units. In fact, the special units are not only faced with problems, such as lack of cooperation, jurisdictional and technical difficulties, they are, in fact, confronted with a large number and variety of victims of cybercrimes from government, businesses and organisations to individuals.
2.4.3. International measures

Cybercriminal threats are viewed as posing increasingly serious risks to the economy, and to both national and international security. Since cybercrimes affect practically all nations, there is no question of the need to take action against cybercrime. Substantial evidence that criminals, including organised criminals, exploit new opportunities offered by advanced technologies to carry out their illegal acts, has been compiled and addressed over the last decade by several international bodies such as the International Narcotics Control Board (INCB) (2001, 2010), Interpol (Hui, 2011), and Europol (2011a). In particular, Europol has stressed how increasingly the Internet and its associated advanced technology facilitate all types of traditional criminals, including organised crime. As an international phenomenon, it is necessary for the international community to take action to manage this issue, otherwise, it will encourage cybercriminals, and more serious cybercriminal behaviour will result. Therefore, the purpose of this part of the chapter is to review how the international community has addressed cybercriminal issues, particularly, some major international organisations, such as United Nations (UN), the Council of Europe (CoE) and The International Criminal Police Organisation (Interpol).

2.4.3.1. United Nations

The United Nation (UN) is an international and worldwide organisation comprising 193 Member States in total.\(^{19}\) It has broad purposes in relation to the arena of international relations. The most relevant purpose regarding cybercrime is to be ‘a centre for harmonising the actions of nations’. Like the European Union and the Council of Europe, the UN has the capability to bind its members by Treaty and could achieve an almost global reach in the approximation of law.

In respect of cybercrime issues, the UN General Assembly addressed and provided a general resolution on computer-related crimes at the Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders in September 1990 (UN Doc E/91/IV/2, 1990). This general solution is viewed as a foundation for Member States to

intensify their efforts to combat computer-related crime by modernising their national legislation, improving security measures and promoting the development of a comprehensive international framework of guidelines and standards for prosecuting these criminals the future. Following that in 1994, the UN published a manual on the prevention and control of computer-related crime to re-affirm the issue of computer-related crime as a global problem identifying the need for global action in this respect (United Nations, 1994). The manual indicated that global action was required through international cooperation in areas of substantive and procedural law, and in data security as a preventative measure (ibid). Furthermore, this manual also recommended the criminalisation of ‘the alteration of computer data or computer programs without right, computer espionage, and the unauthorised use of a computer and the unauthorised copy of a protected computer program’ into legislation (United Nations, 1994, p. 122). Moreover, it was suggested that states should consider criminalisation of other computer abuses such as trafficking in wrongfully obtained computer passwords and other information as a means of obtaining unauthorized access to computer systems, and the distribution or viruses or similar programs. The manual warned that states should give special attention to ‘the use of criminal norms that penalise recklessness or the creation of dangerous risks’ and to practical problems of enforcement (Ibid, p. 125).

In 2001, the General Assembly adopted a second resolution on ‘Combating the Criminal Misuse of Information Technologies’ (A/RES/55/63, 2001). This resolution provided a series of very general recommendations concerned with the elimination of safe havens, cooperation between states, investigation and prosecution and adequate training of law enforcement personnel before inviting states to take its measures into account in their efforts to combat the criminal misuse of information technology. Following that, a report called ‘Conclusions of the Study on Effective Measures to Prevent and Control High Technology and Computer-Related Crimes’ was produced to recommend setting strategies and enhancing international cooperation to counter and prevent computer crime (E/CN.15/2001/4, 2001).

Furthermore, at the Eleventh UN Congress on Crime Prevention and Criminal Justice in 2005, there was some discussion in relation to the creation of a UN Convention on Cybercrime (A/CONF/203/PM/1, 2005). However, finally, the Congress concluded: ‘While there was a wide consensus on the need for a combined approach, and better mechanisms of international cooperation, participants felt that a United Nations
Convention on Cybercrime would be premature at this stage, and it was more critical to provide technical assistance to Member States, in order to provide a level playing field’ (BKK/CP/22, 2005, p. 2)

Moreover, the UN established the International Telecommunication Union as a specialised agency for telecommunications. It coordinates the global use of telecommunications and improves the telecommunications infrastructure in the developing world. As a specialised agency, the ITU took the lead in ‘Combating criminal misuse of information technology’ by ‘Building confidence and security in the use of information and communication technologies’. In doing so, the ITU created and provided the ‘ITU Toolkit for Cybercrime Legislation’ with the aim of providing countries with sample legislative language and reference materials to assist in the establishment of harmonised cybercrime laws and procedural rules.

2.4.3.2. The Council of Europe

The Council of Europe (CoE) was established in 1949 and now has 47 member countries. In addition, there are six countries which are observer States including the United States, Canada, Mexico, Japan, the Holy See and Israel. The CoE was among the first international bodies to address the rising threats created by computer-related crime since the late 1980s (CoE, 1989). The CoE made a first attempt to harmonise substantive computer crime laws in 1989 by providing guidelines to national lawmakers in its member states (CoE, 1990). Particularly, the CoE recommended its member states should criminalise unlawful acts using computer networks by giving a minimum list of computer-specific offences including the definition of each offence such as computer-related fraud; computer forgery; damage to computer data or computer programs; computer sabotage; unauthorised access; unauthorised interception; unauthorised reproduction of a protected computer program; and unauthorised reproduction of a topography (CoE, 1990). In addition, the CoE also provided an optional list which contained four additional offences; for instance, alteration of computer data or computer programs; computer espionage; unauthorised use of a computer; unauthorised use of a protected computer program.

---

The CoE took further action by establishing a Committee of Experts on Crime in Cyberspace in order to begin preparing a draft Convention on Cybercrime as a considered solution to the problems posed by cybercrime in 1997. Indeed, the Convention on Cybercrime (the Convention) was approved in 2001 and it is currently the only global document on this issue (CoE, 2001). The Convention is viewed as a very important step towards defining cybercrimes and harmonising domestic criminal laws in order to prevent cybercrimes (Clough, 2012). The Convention also sets out a framework for international cooperation between countries in investigating and prosecuting possible cybercrime. More importantly, the Convention addresses the important points that it is not only important to provide the necessary domestic criminal procedures and legal powers for the investigation and prosecution of cybercrime, it also provides for any type of criminal investigation that requires collecting evidence in electronic form. One reason for this is that most countries do not have adequate procedural rules applicable for cybercriminal investigation such as how to compile evidence, locate the source and identify the perpetrator of an offence. Instead, conventional investigative powers are still used. However, whilst the provisions of the Convention enable computer data to be obtained or generated for ongoing criminal investigations, it does not, in fact, offer a proactive measure to deal with cybercrime (Cangemi, 2004).

Although the Convention appears to be a genuine attempt at addressing cybercriminal activities, the Convention is also viewed as a largely symbolic piece of legislation (Marion, 2010). Thus, the Convention is said to have had a limited effect on cybercrime in the long term. However, Marion (2010) indicates that the Convention has clear elements of the four functions of symbolic regulation as follows: i) The Convention serves to reassure the public that action is being taken against cybercrime; ii) the treaty is serving to educate people in all countries with regard to what is right, or wrong, behaviour when using the Internet; iii) the treaty is acting as a model for the states (Gillespie, 2016); and iv) the treaty is to serve as a deterrent to future criminal behaviour (pp. 702 – 707).

Clough (2012) argues that the Convention is outdated and has failed to keep up with the rapid technological development for two main reasons including: i) the language of the Convention has not kept pace with technological change; and, ii) the Convention does not address new forms of offending which have appeared since it was drafted (p. 375).
Furthermore, the Convention has also been criticised by civil liberties groups for undermining individual privacy and expanding surveillance powers far beyond the current state (Huey & Rosenberg, 2004).

2.4.3.3. The International Criminal Police Organisation

Interpol is an international law enforcement organisation which aims to ensure and promote the widest possible mutual assistance between all criminal Police authorities, within the limits of the law existing in the different countries, in order to combat crime (The ICP)-Interpol General Secretariat, 1956). Interpol has recognised the issue of cybercrime since early 1990 and considered cybercrime as having one of the greatest increases in scale and quantity among other crimes. Since cybercrime is viewed as a serious problem, Interpol has taken its own actions to deal with this problem, for instance, creating its own international conference on cybercrime, and creating several regional working parties on information technology crime.

In seeking to address cybercrime, Interpol developed and implemented an international police communication system called 1-24/7 to enable and facilitate the exchange of information among member Police forces (Interpol.int, 2016). Interpol has facilitated a secure communications system for collecting, storing, analysing, sharing and requesting information (Ibid). Members can access Interpol’s databases to look for and verify data in regard to cybercrime. Members are supported 24 hours a day, seven days a week in a variety of ways:

- Assistance and cooperation between the member countries is facilitated by a list of contact officers available for cybercrime investigation
- The exchange of information on cybercrime between the member countries has been enhanced
- Member countries are supported in the event of cybercrime investigations or attacks
- Partnerships with other international and private organisations have been built up (Interpol.int, 2016).

Furthermore, Interpol has established collaborative work with the private sector in
countering the spread of cybercrime. For instance, in 2004, Interpol and Microsoft had a meeting to discuss efforts to tackle and address the issue of the growing threats posed by ‘Botnets’ (Interpol, 2006). In addition, Interpol incorporated with the G8 High Tech Crime Group to support the recommendations provided by the USA and the UK law enforcement agencies for changes to the Internet Corporation for Assigned Names and Numbers (ICANN) (Kirk, 2010).

2.4.4. The measurement of cybercrime reduction

The previous sections reviewed key characteristics of cybercrime and possible difficulties in regulating it. It also reviewed practical initiatives to address cybercrime at national and international levels. All of the literature indicates that cybercrime involves a multiplicity of national and transnational actors, due to its nature and characteristics, making it difficult to deal with. This in turn suggests a more comprehensive and flexible approach including cybercrime prevention. This section reviews the practical implementation of prevention initiatives to date.

In attempting to address cybercrime prevention measures, three main theories, that are known as crime opportunity theories, have been used in different contexts to explain different types of cybercriminal activities (Thomas et al., 2015). These theories are: Routine Activity Theory (RAT), Rational Choice Theory (RTC), and Crime Pattern Theory (CPT). The theories provide a framework to help shape and orientate policing strategies (Clarke & Eck, 2007). These have been applied through various empirical research studies to both cybercrimes generally (e.g. Hinduja, 2003; Higgins & Makin, 2004) and cybercriminal victimisation (e.g. Holt & Bossler, 2009). The majority of these studies have agreed that opportunity ‘plays a role in all crime’ (Felson & Clarke, 1998).

The Crime Pattern Theory (Brantingham & Brantingham, 1993) stresses the importance of the location of criminal opportunities by looking at the interactions between targets and offenders in their daily routines. The Rational Choice Theory (Cornish & Clarke, 1986) is concerned with the idea that criminals make very specific and, in their own mind, rational and logical choices when deciding to commit a crime. The Routine Activity Theory (RAT) developed by Cohen and Felson (1979), aims to explain that, for
a criminal act to happen, there has to be the convergence in space and time of a likely or motivated offender, a suitable target, and the absence of a capable guardian (Cohen & Felson, 1979). Traditionally, RAT has been used in explaining wide ranging forms of criminal behaviour, such as burglary (Cohen & Felson, 1979; Coupe & Blake, 2006), larceny (Mustaine & Tewksbury, 1998), vandalism (Tewksbury & Mustaine, 2000), physical assault (Stewart et al., 2004), robbery (Spano & Nagy, 2005), and fraud (Holtfreter et al., 2008).

In relation to cybercrime prevention, the Routine Activities Theory has been explored by several empirical research studies (e.g., Fratt et al., 2010; Leukfeldt, 2014; Williams, 2016; Choi, 2008; Holt & Bossler, 2008; Bossler et al., 2012; van Wilsem, 2011; Ngo & Paternoster, 2011; Marcum et al., 2010). Most research studies focused on one specific case of cybercrime. Other studies have shown mixed results when RAT is applied. In other words, outcomes regarding the usability of RAT differ from one study to another.

For example, Choi (2008) undertook a virus victimisation research among students and found that online lifestyle and physical guardianship were both related to victimisation. Meanwhile, Bossler and Holt (2009) identified that neither personal nor physical guardianship were related. Ngo and Paternoster (2011) applied RAT into seven forms of cybercrime victimization (computer viruses, harassment by a stranger, harassment by a non-stranger, unwanted pornography, sexual solicitation, phishing, and defamation) among college students. They concluded that “the results indicate that neither individual nor situational characteristics consistently impacted the likelihood of being victimized in cyberspace. … although five of the coefficients in the routine activity models were significant, all but one of these significant effects were in the opposite direction to that expected from the theory” (p. 773).

Marcum et al., (2010) examined three types of cybercrime, such as unwanted sexually explicit material, unwanted non-sexual harassment and unwanted sexual solicitation by looking at three specific factors including visibility, accessibility and guardianship. Marcum et al. (2010) confirmed that “participating in behaviours that increased exposure to motivated offenders and target suitability in turn increased the likelihood of the three types of victimisation measured” (p. 382) and protective measures such as a capable guardian did not decrease the likelihood of victimisation.

For example, Fratt et al. (2010) showed how the RAT can be applied to online identify
theft and found that changing consumer behaviour, especially in the use of online shopping, was significantly related to the crime and more important than attributes of age and education in predicting victimisation. Leukfeldt (2014) conducted a similar study on phishing and concluded that different elements of RAT such as personal and financial characteristics, online activities and online accessibility do not appear to increase risk of victimisation.

Recently, Van Wilsem (2011, 2013a) conducted research studies in relation to online harassment victimisation by using data from a national sample of Dutch citizens and found that online harassment victimisation was related to using webcams, social networking sites, forums, and intensive purchasing. Routine activities in one setting, either physical or virtual, are asserted to influence the risks of threat victimisation in the other (van Wilsem, 2011). Similarity, Navarro & Jasinski (2013) used RAT to explain another aspect of cybercrime, that of cyber-bullying or harassment and showed how RAT could explain incidences of cyber-bullying victimization when there was a lack of capable guardianship – one of the three conditions for crime to occur.

Situational crime prevention is viewed as a primary prevention measure that aims to change the situational elements surrounding a crime, in order to prevent it (LaFree & Freilich, 2016). Situational Crime Prevention (SCP) is a technique that has emerged from the Crime Opportunity Theory co-developed by Clark (1983). Clark (1997) asserted that to reduce crime, there must be changes to the environment of a crime to reduce the opportunities for a crime to occur. In doing so, there are five main elements designed to impact upon both offenders and potential victims by identifying strategies that directly influence opportunities to offend by (1) making it more challenging to engage in crime; (2) increasing the risk of detection; (3) reducing the rewards that may result from offending; (4) reducing provocations to offend; and (5) removing excuses for offending (Clarke, 1997, Cornish & Clarke, 2003). In relation to each strategy above, five techniques have been added to increase a total of 25 techniques that can be applied to influence the likelihood of crime, such as target-hardening to increase the effort offenders must exert, using place managers to increase the risk of detection, concealing targets to reduce the potential rewards of offending, and posting clear rules for behaviours to remove excuses for criminality (Cornish & Clarke, 2003).

There has generally been little empirical research on the application of Situational Crime Prevention in different forms of cybercrime. Most of the existing studies utilize
aspects of SCP to examine a specific crime type (e.g., Collins et al., 2011; Khey & Sainato, 2013) or provide summary overviews of existing knowledge within an SCP framework (e.g. Hinduja & Kooi, 2013). Hinduja and Kooi (2013) suggested that technological solutions are not enough to address vulnerabilities in information systems, but that SCP can be used to combat the more opportunistic elements of cybercrime. Hinduja and Kooi (2013) only considered using Clarke’s original 16 opportunity reducing techniques instead of the latter 25, primarily because of some of the newer techniques were not relevant to information security, such as a reduction of provocations due to drugs and alcohol.

In short, it is difficult to either confirm or refute, the application of Routine Activity Theory and Situational Crime Prevention to cybercrime. However, these theories can be applied to the reduction of some specifics of cybercriminal activities, such as fraud, identity theft, malware, cyber bullying and cyber harassment. Most studies focus only on one specific cybercrime, while a range of cybercriminal activities remain to be examined.

The application of multi-agency crime reduction partnerships is argued to be an effective cybercrime prevention mechanism by many scholars (e.g., Williams, 2006; Wall, 2015/2007; 2010; Sulek and Doscher, 2011; Levi and William, 2013, 2012; William and Levi, 2015; Levi et al., 2015). Cybercrime is said to be complicated, sophisticated and distinct from traditional crimes such that it cannot be solved by law enforcement (Wall, 2005/15, 2010, 2007; Sulek & Doscher, 2011; Levi & Williams, 2013, 2012; Williams & Levi, 2015; Levi et al., 2015; Jamie, 2017) or by government alone (HM. Government, 2011, 2016). This is illustrated by a number of studies in different countries which show that policing cybercrime requires effort involving a number of sectors including law enforcement, the public sector, the business community, academia and the public as whole (Wall, 2015/ 2010; and Levi & Williams, 2013). Each of these sectors, it is argued, contribute different abilities that enable the creation of effective policies (Wall, 2015/ 2010; and Williams, 2015).

The application of a multi-agency approach to cybercrime can be seen through the UK national cyber-security strategy. The UK adopted a cyber-security strategy in 2009 and released a new strategy in November 2011. The main reason for adopting a cybersecurity strategy in 2009 was the identification of the increasing importance of cyberspace in the UK life (Cabinet Office, 2009) and that the argument that cyberspace
drives economic growth and supports open and strong societies (Cabinet Office, 2011a). At the same time, the UK found that the cost of cyber incidents for business and the potential reduction in trust towards online communications “can now cause serious economic and social harm to the UK” (Cabinet Office, 2011a, p. 17), and that securing cyberspace is one of the highest priorities for action in relation to national security (Cabinet Office, 2009). Therefore, it was argued that a coherent approach for cybersecurity was required in which the Government, organisations across all sectors, including public, and international partners all had a part to play due to the diverse nature of cyber-criminality, actors and motivations (Cornish et al, 2009). In doing so, the UK government has created a national cybersecurity strategy referring to the existing government strategy, particularly, its Counter Terrorism Strategy, by deploying four components (so called the four Ps Model) to tackle cybercrime as ‘Pursue’, ‘Prevent’, ‘Protect’ and ‘Prepare’ (Levi et al., 2015). The four components focus on as the following:

1. Cyberattacks targeting UK victims: increasing the reporting of cybercrime, supporting victims, and increasing the take-up of protective security;

2. UK-based cyber criminals: making the UK a high-risk country for criminals to host and perpetrate cybercrime;

3. International cyber criminals and groups: identifying, prosecuting, and disrupting the most significant cyber criminals worldwide; and

4. The enabling international cybercrime marketplace: degrading the criminal marketplace, undermining the profitability of the cybercriminal business model, and raising the barrier to entry and operating for cyber criminals (NCA, 2016a).

To achieve the objectives above, the UK established a multi-agency unit –the Cyber Security Operations Centre (CSOC) to i) actively monitor the health of cyberspace, provide collective situation awareness, ii) enable better understanding of attacks against UK networks and users, iii) co-ordinate incident response, iv) and provide better advice and information about the risks to business and the public (Cabinet Office, 2009). The Office of Cyber Security (OCS) was then renamed as the ‘Office of Cyber Security and Information Assurance’ in the Cabinet Office to provide strategic leadership for and coherence across the government. Its missions were set out clearly to include the provision of strategic direction, supporting education, awareness and training, working
with the private sector and working with the Office of the Government Chief Information Office in order to ensure the resilience and security of government infrastructure, engaging with international partners.

The UK is one of the leading digital nations and it also makes industry, the country and the public a big target to cybercriminals (National Crime Agency, 2015). In 2016, the UK created its National Cyber Security Strategy 2016-2021 with the aim of improving the country’s resilience to existing and emerging threats (HM Government, 2016). This new strategy was built on the achievements, objectives and judgments of the National Cyber Security Strategy, 2011. The new Strategy drew up an implementation plan for 2021 with three elements ‘Defend’, ‘Deter’ and ‘Develop’ that seek to respond to the breadth of the challenge facing the UK (National Cyber Security Strategy 2016, 2016). This Strategy (HM Government, 2016) sets out to: (1) conduct the strategy in accordance with a range of different principles, and (2) commit to push forward with the strategy in collaboration with other actors and institutions.

This strategy is aiming to make the UK ‘secure and resilient to cyber threats’ by 2021 (HM Government, 2016, p. 25). The first aspect of this is defence, accepting that while ‘it will never be possible to stop every cyber-attack’ (p. 33), it is nevertheless possible to develop layers of defence that significantly reduce the UK’s exposure to cyberattacks. The UK should be far more difficult to attack because its networks, data and systems are resilient. Deterrence is about increasing the cost and reducing the benefits of any attack on the UK. The UK should be a ‘hard target’ and the nation will have the means to respond effectively to attacks be it via international law, the criminal justice system or offensive cyber means of its own. Finally, development refers to the drive to expand the cybersecurity industry and cultivate the necessary skills within our society to ensure the UK keeps pace with cyber-threats.

2.4.4.1. Raising public awareness

As illustrated above cybercrime cannot easily be combated by applying either policy measures or law enforcement alone because of its unique characteristics. In fact, cybercrime is not simply about advanced technologies, it is also associated with human activity. However, the complexity of cybercrime goes beyond the understanding of most
people. Raising public awareness is viewed as a key preventative factor which has a significant impact on cyber criminals. As mentioned above, the majority of Internet users are unaware of how harmful the online world in which they participate can be. They lack a basic understanding of how the system works. Indeed, many of them may feel that they do not need to have a deep understanding of the technology as they simply want to use it.

Recognising the crucial, and vital, vehicle of raising awareness regarding cybersecurity in general and preventing users becoming victims of cybercrime, many countries, such as the UK, Australia and Canada have created several awareness campaigns. In the UK, for example, the government has several campaigns in relation to increasing awareness of Internet users, such as Get Safe Online\(^{22}\), the ‘Cyber Streetwise’\(^{23}\), Webwise Campaign\(^{24}\), Good to know Google’\(’s\)\(^{25}\), Behind the Screen\(^{26}\), the Devil’s In Your Details\(^{27}\), Cyber Security Challenge UK\(^{28}\), and Visualisation and Other Methods of Expression (VOME)\(^{29}\). The purpose of these campaigns is to provide basic knowledge on various cyber risks and basic protection measures including using strong, memorable passwords, installing antivirus software on all work devices, checking privacy setting on social media, checking the security of online retailers before loading card details and patching systems as soon as updates are available.

Education is seen as the most useful method to increase the awareness of users. The main reason for this is that education can provide basic information of understanding, and advice to users to be aware of computers, computer networks, and associated risks (Wall, 2005). This will help users to make up their own minds and express their own choices in order to deal with their own problems. In doing so, it could not only save huge numbers of people from the hassle of having their data stolen but also from becoming a direct physical victim of cybercrime (Buono, 2014).

Educating users may take one of several forms. Moore (2014) asserts that the best education for users comes through training seminars and publications. There are several

---

\(^{24}\) See: http://www.bbc.co.uk/webwise/0/ (accessed: 22/02/2017).
\(^{25}\) See: https://www.google.co.uk/goodtoknow/ (accessed: 22/02/2017).
\(^{27}\) See: http://www.actionfraud.police.uk/thedevilsinyourdetails (accessed: 22/02/2017).
\(^{29}\) See: http://www.vome.org.uk (accessed 22/02/2017).
ways to do this, such as via private organisations or government agencies, including ISPs. In the UK and European countries, education is one of the functions of both Computer Emergency Response Teams (CERTs) and Warning, Advice and Reporting Points\(^\text{30}\) (WARPs) who provide advisory services to their constituents (Fafinski, 2009).

Furthermore, education can change social norms (Lessig, 1998). As Thurgood Marshall stated ‘Education is not the teaching of the three R’s. Education is the teaching of overall citizenship, to learn to live together with fellow citizens and above all to learn to obey the law’ (Cooper & Aaron, 1958, p. 358). Thus, education can be understood to be a means by which certain social norms may be supported whose content is regulated by law (Lessig, 2006). Moreover, the law can conceivably intervene to compel a certain level of education regarding the issues surrounding protection from computer crime (ibid). As a result, education is considered as a vehicle to transmit information, knowledge, skills, and laws to people, in order to make them more confident to deal with the issues they face in life.

2.4.4.2. Technical responses

The use of advanced technologies is considered as one measure of preventing cybercrime. Lessig (1999) asserted the use of technologies in preventing crime and has claimed that technologies can be an invisible hand that constructs an architecture that makes possible highly efficient regulation. He argues that ‘Some architectures of cyberspace are more regulatable than others; some architectures enable better control than others. Thus, whether a part of cyberspace generally can be regulated turns on the nature of its code’ (p. 20). It can be said that if ability to regulate is the aim of the state and some architectures are more amenable to regulation than other, the state will be then likely to use some technical architectures more than others (Fafinski, 2009).

Supporting a similar point of view, Katyal (2003) stated that digital architecture can be used as a regulator to control cybercrime. It can be viewed far more efficiently in response to cybercrimes than law as a regulator of digital environments (Hale et al., 2013). The key reason is that advanced technologies cannot just control its architecture; it can also shape the behaviour that takes place within its environment.

\(^{30}\) See: http://www.warp.gov.uk/about.html (accesses 25/02/2017).
Wall (2007) argues that ‘the networked technologies which cause crime can also be utilized to regulate, police, and prevent it’ (p. 186). He also indicates that the characteristics of networked technology can be used to generate ‘a range of automated active policing tools that seek to identify wrongdoing’ (p. 190). The honeynets, for example, consist of a wide range of honeyposts; their aim is to improve security of the Internet by detecting attempts at illegal activity of attackers, analysing these attacks, and sharing the findings in order to provide support for users to defend against cybercrime. These honeyposts include a computer, data, a site to appear as a part of a legitimate network and they seem to comprise rich and valuable information for attracting attackers. These honeyposts socially engineer users who are able to access the site and pass through various levels of security, indicating their intention and willingness to process at each stage that they are aware of the content. Their details, at the end, will be recorded and will be used for investigating if appropriate.

There are several reasons that support the suggestion of using technology to control cybercrime is easier and more effective than legal regulation. Firstly, technology can disrupt criminal activity, forcing criminals back to negotiate paths and goals (Latour, 2000). For instance, some websites require users to give information, requiring a password before gaining access to that website; in others, a user’s identification might be required in order to access it. Some websites allow users to choose a certain kind of language that only their users can understand. These features are the production of the code or software or architecture that are created by code writers. Secondly, technology, code or architecture is malleable; it is easily shaped by users that have access to its control (Wall & William, 2007). Thirdly, the way in which technology imposes constraints on how users can behave is more pervasive and immediate than laws (Wall & William, 2007). Fourthly, users seem to be more readily and rapidly adaptable to technology than laws, technology then can control criminal and sub-criminal behaviours (Wall, 2007). Technology is also claimed as a native form of regulation making it less debatable than legal instruction (Wall, 2007).

However, using technology to respond to cybercrime cannot avoid all problems. It is very hard to ensure how effective an intervention has been at the first stage of technology creation, especially, what functionality is primarily determined by software and its accompanying procedures rather than by hardware itself (Wall, 2007).

Therefore, the un-expectation of negative effects from technology design cannot ignore this, and it should be taken into consideration when they interfere with the free flow of information (Ibid). Using technology to control cybercrime is claimed to conflict with the level of security provided and the functionality of the product, and it is even argued to conflict with the public interest (Ibid). Indeed, responding to cybercrime through the use of technology can trigger issues of infringement of individual rights of privacy and freedom of speech (Yar & Walker, 2000; Fafinski, 2009). As Yar & Walker (2000) comment “there is no compelling state interest in such an invasion of privacy, as perpetrators have been detected and evidence gathered without any new powers to survey or research” (p. 319). Encryption technology is even claimed to circumvent the legal powers of interception afforded to the state (Fafinski, 2009). As Yar & Walker (2000) have argued, that ‘technology can be so effective against oversight that law enforcement agencies have begun to voice concerns about the viability of future crime detection in cyberspace’ (p. 319).

Overall, it is clear to see that the application of technologies to control cybercrime does provide advantages and, at the same time, creates some new problems. For instance, ‘Cryptography surely is the best of technologies and the worst of technologies. It will stop crimes, and it will create new crime. It will undermine dictatorships, and it will drive them to new excesses. It will make us all anonymous, and will track our every transaction’ (Baker & Hurt, 1998, xv). As a result, it can be concluded that cybercrime cannot be entirely controlled using technology alone. This requires a cost-effectiveness approach to using technology to counter cybercrime. It also has the benefit of being portable throughout the world. Put differently, using technology to response to cybercrime cannot be without considerations of complexity and cost.

2.5. Conclusion

Cybercrime is a global phenomenon. National and international authorities face many challenges in order to control it. The Internet and its associated advanced technology provide new ways for traditional crime to take place and create new types of criminal activity. The emergence of the Internet makes the definition of this kind of crime less clear. Legal definitions of cybercrime are claimed to have remained static even as
technology has advanced and will continue to develop further. This does not mean that if an offence cannot be easily defined, it should not be an offence. However, in relation to cybercrime, the difficulty of definition is said to render its boundaries uncertain.

In particular, cybercrime has made it difficult for national and international bodies to identify who commits the crime, and where it has been committed and for legal authorities to respond to this kind of threat. The Internet and its associated advanced technologies have posed many challenges for law and law enforcement. There are several steps or actions that should be taken to deal with this kind of threat, at national and international levels, such as the establishment of new laws, amendment of old laws, the development of technology, creation of support teams, and greater cooperation between organisations and nations. However, responses to this crime seem to be of limited effect because of the specific characteristics of this kind of crime and the technological advances creating it. It is clearly necessary to improve existing approaches to enhance the applicability of laws and their enforcement.
3.1. Introduction

This chapter aims to present the methodology and methods employed in this research study. It is divided into seven sections. The first section is the introduction. The second section is the explanation of the rationale behind the use of a qualitative methodology. The third section describes the two research methods that are adopted in this research as follows: i) document analysis; and ii) qualitative face-to-face semi-structured interviews. Other issues involved in the interviews are also discussed, such as interview schedules, purposive sampling and interviewees by institutions. The fourth section discusses the process of data analysis. The fifth section deals with the ethical issues involved in this research study in Vietnam are also considered. The sixth section is the consideration of some of the limitations of the chosen research methodology and methods in this research study. This chapter ends with the conclusion.

3.2. A piece of qualitative research

Qualitative research is identified as one of the two primary approaches for the conduct of social science research (Tewksbury, 2009). It is also identified as a superior means for conducting meaningful research in criminal justice studies as it focuses on the meanings, traits and defining characteristics of events, people, interactions, and experience (Tewksbury, 2009; Morgan, 2012). For instance, Berg (2007) has explained qualitative research as “Quality refers to the what, how, when and where of a thing - its essence and ambience. Qualitative research thus refers to the meanings, concepts, definitions, characteristics, metaphors, symbols, and descriptions of things” (p. 3). The qualitative approach focuses on the naturalistic environment of social phenomenon and the personal interpretation of the participants. For example, Hagan (2000) notes, interpretive-oriented researchers “hope to immerse themselves in the subject matter and develop ‘sensitising concepts’ that enhance their understanding and explanation of reality” (p. 19). In addition, qualitative methods offer a unique way to address some of
these more complicated phenomena as it naturally occurs, thus allowing researchers to organize and describe phenomena with depth and richness (John Dumay, 2011).

There are three main reasons for choosing a qualitative approach in this thesis. These are:

i) Firstly, as mentioned in Chapter 1, this research is the very first study on cybercrime and its regulation in Vietnam and there is little existing knowledge relating to this research study area. Qualitative interviews are, therefore, the most appropriate approach to gain valuable knowledge, views and understanding the phenomenon of cybercrime, and its regulation in Vietnam, from participants who are currently working across key regulatory institutional bodies. In fact, the participants who are selected to be interviewed in this research are high-level professionals from key regulatory institutions. They are hard to connect with and have significant knowledge in relation to this research study.

The data produced by interviewing such individuals is regarded as being obtained from a direct data source. A face-to-face interview approach has advantages since it is open, flexible and reflective, and also gives priority to the respondents (Saratakos, 2005). In other terms, research questions in qualitative approaches are designed in an open way in which participants can freely describe or interpret their experience. Anderson (2010) concludes that this qualitative approach is more appropriate and powerful to gather more in-depth and detailed information in revealing human being’s perceptions and interactions.

ii) Secondly, the research is concerned with the timely issues of cybercrime regulation policies and the regulation of cybercrime mechanisms in Vietnam. It is, therefore, necessary to acquire data by interacting with people who are experienced in dealing with this type of issue. The interaction with people in the sample, by the way of conversation, will be a valid means to generate data (Robson, 2011). Additionally, qualitative research data is created by conversation (Kvale, 2007), asking questions, listening and reflecting, and the participants responding (Tewksbury, 2009). They are structured by a relatively informal style, a thematic approach and the assumption that the data will be taken via interaction (Mason, 1996). The positive results of qualitative research include explaining and creating generalisations, providing insights about changing behaviour, refining knowledge, identifying issues, verifying theories and
generalisations, and evaluating policies and practices (Pushkin, 1993). These issues cannot, therefore, be explored through a statistical approach or by closed questionnaires.

iii) Thirdly, the qualitative approach is employed to help comprehend the regulating of cybercrime and its related issues in terms of how people think, feel, believe and even apply the regulations and policies, not just what they do. Without understanding how people think, the research would be severely limited (Sarat, 1996). Thus, this research tries to explore the viewpoint of people from various government agencies through the meaning of data obtainable from their daily life experience, their perspectives rather than by the analysis of statistics and questionnaires.

Qualitative research is recognized for the value and unique contributions that it can make (Tewksbury, 2009). By contrast, a quantitative approach has limitations which make it unsuitable for this study because the meanings of the detected relations cannot be explored by the quantitative approach. Typically, a quantitative approach is based on obtaining numbers regarding a large sample size in a highly structured manner. Because of the very limited number of reported cybercrimes in Vietnam, the meanings of this social phenomena cannot be recognized through this approach. Furthermore, an understanding of the meaning of the social phenomena can be better obtained through narrated perceptions and experiences. As a result, qualitative methods are the approach which centralizes and places primary value on a complete understanding of how people understand, experience and operate within their milieu (ibid).

3.3. Two research methods

There is, in fact, a range of data collection methods in qualitative research, including interviews with individuals, focus groups, and participant/non-participant observation of people, places and actions/interactions, immersion. This research could have used a survey and focus group as a data collection method. However, it would be challenging when conducting this research in Vietnam. The main reason for this is that Vietnamese people, in particular people that work for the government or regulatory institutions, they are defined not by who they are, but their viewpoint would be influenced by their supervisors or high ranked colleagues if they would be invited to a focus group
interview. They might not even express their clearer views on their daily work as they would be afraid for their position and even future work.

In addition, as mentioned in Chapter 1, this thesis will explore three specific objectives:

i) To critically assess the extent to which the regulatory framework of cybercrime in Vietnam is fit for its intended purpose.

ii) To explore how cybercrime is defined by high-level professionals from key regulatory institutions in Vietnam;

iii) To explore the key factors that make cybercrime difficult and challenging for Vietnamese authorities to regulate; and,

iii) To explore possible measures that can be put in place to reduce the growth of cybercrime in Vietnam.

In order to do so, it is necessary to obtain the viewpoints of experts on the definition of cybercrime, the value of various forms of policies on cybercrime regulation, and the current practical responses to the needs of cybercrime regulation in Vietnam. In addition, this research study would appear to be the first study on cybercrime and its regulation in Vietnam, thus, it is necessary to get as much information and policies in relation to cybercrime as possible in order to provide a holistic picture of the subject area. To do so, qualitative face-to-face semi-structured interviews are adopted after document analysis to collect data from key regulatory institutions, including:

i) investigation body,

ii) prosecution body,

iii) judicial body,

iv) information communication and technology firms, and

v) Internet Service Providers (ISPs).

3.3.1. Document analysis

A document is defined as “any written material” which is produced by individuals and groups in the course of their everyday practises and which is geared exclusively for their own immediate practical needs (Scott, 1990; Guba & Lincoln, 1994). In addition, documents can be written with a specific purpose, based on particular assumptions, and presented for certain audiences and contexts (Cohen et al., 2007). However, documents
can have an independent existence beyond the writer and beyond the context of its production (Jary & Jary, 1991).

Documents can take a variety of forms such as Acts, policy statements, Census reports, statistical bulletins, reports of Commissions of Inquiry, Ministerial or department annual reports, minutes of meetings, manuals, background papers, books, brochures, diaries and journals, even programs, letters and memoranda, maps and charts, newspaper, organisational or institutional reports (Mogalakwe, 2006). These types of documents can be found in ministry and departmental libraries, newspaper archives, historical society office, organisational or institutional files. However, using documents, a researcher must take the authenticity, credibility, representativeness, and meaning of the document into account (Hartas, 2010).

Document analysis has been used in various ways in social research since its earliest inception (Punch, 2013). It is an important product that provides access to, and can facilitate insights into, areas of knowledge about social activities (Cohen et al., 2013). More importantly, this research is the first research on this topic in Vietnam, thus, there is little understanding in this area. It is therefore necessary to have document analysis which not only helps the researcher get a better picture of cybercrime and its regulation in Vietnam, but also to guide the researcher to know what questions to ask at interview. The use of document analysis is carried out in a number of ways, including the analysis of documents that contain information relevant to the phenomenon under study (Walsh, 2014). Similar to other analytical methods in qualitative research, document analysis requires that data be examined and interpreted in order to elicit meaning, gain understanding, and develop empirical knowledge (Corbin & Trauss, 2008; Bowen, 2009). Such an approach can even be used to identify the limitations of physical sources (Payne & Payne, 2004).

Document analysis is often used in combination with other qualitative research techniques as a method of providing ‘triangulation’ of data from multiple sources, which are combined to form a more complete and representative understanding of phenomena (French & Gordon, 2015). The combination of document analysis with other qualitative research methods will not only draw upon multiple sources and methods, but also ensure that evidence can be supported by other sources (Bowen, 2009). Furthermore, the researcher can corroborate findings across data sets, and thus can limit the impact of potential biases that can occur in a single study (Bowen, 2009).
Document analysis is particularly considered to provide rich descriptions of a single phenomenon, event, organisation, or programme (Stake, 1995; Yin, 1995). Moreover, it will help the researcher uncover meaning, develop an understanding, and discover insights relevant to the research problem (Merriam & Tisdell, 2015).

The document research was concerned with the selection of available literature that was based on the research questions examined within this study. The sources used in this research study originate from data that has been collected within existing resources such as books, peer-reviewed journal articles, academic journals, articles, legislations, reports, conference papers, statistics, news cutting and webpages. The findings of document have been embedded throughout the main body of the study rather than being summarised in a separate section. However, there is the question of how many documents the researcher should collect. In this regard, Bowen suggested that a wide array of documents is better, although the question should be more about quality of the document rather than the quantity (Bowen, 2009). In addition, Bowen also added that the researcher must evaluate the original purpose of the document and consider whether the author was a first-hand witness or used second-hand sources in order to determine whether the document was solicited, edited and anonymous (Bowen, 2009).

In doing so, the researcher used sources contained in the University’s library and on Internet databases such as Google Scholar, Westlaw, Web of Science, Nexis Library, Jstor, IEEE Explore, ScienceDirect, and Wiley, web pages, and news cuttings.

The research covers academic publications, public policies, international conventions, legislation, frameworks and action plans. In order to focus on the aims of the thesis, and obtain relevant information, the research terms used were “cybercrime”, “regulation of cybercrime”, “Regulation of cybersecurity”, “regulation of the Internet”, “regulation of cyberspace”, “cybercrime and law”, “high tech crime and its policy”, “Internet crime”, “Internet regulation policy”, and “crime in the information age”, “online crime”; “crime in the digital age”, and “cybersecurity”, “information security”.

Using document analysis, as Corbetta (2003) indicated, has a number of advantages over other research methods, as follows: i) it is a non-reactive technique where the information given in a document is not subject to possible distortion as a result of the interaction between the researcher and the respondent; ii) it helps the researcher to study
the past; iii) it is an efficient, cost-effective and productive method as the information has already been produced (Wellington & Szczerbinski, 2007, p. 109).

Alongside several advantages, document research has some limitations such as: i) insufficient detail as documents might be produced for purposes other than research, thus, they might not provide sufficient details to answer a research question (Bowen, 2009; Cohen et al., 2007); ii) not all documents are easily accessible (Mogalakwe, 2009; Barlow, 2016); and iii) the selection process of documents to be analysed may be highly biased (Cohen et al., 2007).

3.3.2. Qualitative interview

The qualitative interview is viewed as a powerful tool for getting information, gathering knowledge of the participants by means of conversations within the purpose of the research and the phenomena which it is designed to explore (Robson, 2011; Pasian, 2015). As mentioned above, interviews are generally used to explore participant’s understanding, experiences, and perspectives of their social world (Rubin & Rubin, 2012). In addition, the researcher, as an interviewer, can be allowed to have personal contact with the participants, in which misunderstandings or confusions of the participants can be solved (Hagan, 2010). On the other hand, the researcher can use their discretion to ask more sensitive or additional questions (Hagan, 2010).

Having emphasised that the qualitative interview is an appropriate and valid research method for this thesis, it is also necessary to describe the form of interview that will be used in order to collect data. Interviews can take various forms. In principle, there are three types of interview: the scheduled standardised interview; the non-scheduled standardised interview; and, the non-standardised interview (Gill et al., 2008; Fontana & Frey, 2005; Berg & Lune, 2014).

Scheduled or structured interviews are essentially administered by a structured sequence of questions to be asked in the same way to all interviewees (Gill et al., 2008). In other words, the interviewer follows scripted questions and there is no deviation from question order. Furthermore, the wording of each question is exactly as written (Berg & Lune, 2014). Thus, no additional questions may be added to clarify the answers of participants. Accordingly, the respondents may interpret or understand the question in
an unwanted manner (David & Sutton, 2004; Cohen et al., 2007). Moreover, the researcher’s verbal comments and non-verbal cues can cause bias and have an influence upon respondents’ answers (David & Sutton, 2004; Cohen et al., 2003).

Conversely, unstructured interviews allow free-flowing conversation between interviewers and participants. There is no set order to any questions or discussion topics and it is useful when little or no knowledge exists about a topic (Cohen et al., 2007). Additionally, although using open-ended questions allows participants to describe or explain their views, it is usually very time consuming as well as difficult to manage, and hard to participate in, because of the lack of predetermined interview questions and therefore there is little guidance on what to talk about (Gill et al., 2008). Furthermore, the interviewer may be biased and ask inappropriate questions or more importantly, respondents may reply by talking about irrelevant subjects and inconsequential issues (Cohen et al., 2007).

In contrast, semi-structured interviews are used in the research where depth of study is one of the foremost concerns and in situations which explore the ways complex phenomena have developed over time (Crow & Semmer, 2008; Judith & Kathleen, 2004). This approach not only allows the researcher to freely follow up ideas, probe and ask for clarification or further elaboration if needed (David & Sutton, 2004; Lawrence, 2007; Berg & Lune, 2014). It also allows informants to express themselves freely and openly (Hancock et al., 2009). This is very important in Vietnam, because it is a Communist country: people in a position of authority rarely talk openly about their work. At the same time, the interviewer and participants are also allowed freedom to wander; ‘interviews are permitted to probe far beyond the answers to their prepared and standardised questions’ (Berg, 2007, p. 95). In addition, the semi-structured in-depth interviews are the most widely used approach. It can be used either with an individual or in groups. Therefore, instead of either selecting the fully structured interview method or the unstructured version, this research chose to use semi-structured interviews with a list of questions so that the researcher can easily focus on specific topics with the interviewees (Robson, 2016). As mentioned above, the primary purpose of the interviews is to elicit the viewpoints of knowledgeable individuals who are directly involved in some way with one or more cybercrime regulation policies, and the current practice responses to cybercrime regulation mechanism systems in Vietnam, therefore
the fieldwork can be considered as a form of elite study. Thus, the body of data they provide is of a very high quality and an authoritative voice.

As mentioned above, the purpose of the qualitative research interview is to gather descriptions of the life-world of the interviewee with respect to interpretation of the meaning of the described phenomena. Collecting these descriptions can be done in several ways such as focus groups interviews, observations, action research and individual interviews. As the overreaching aim of research is to obtain a better understanding the phenomenon of cybercrime and its regulation in Vietnam via opinions from people who, in various Vietnamese government agency and directly relate to cybercrime in some way, thus, either focus groups or individual interview can be used in this research study. However, individual face-to-face semi-structured interviews were considered to be the most appropriate within this study. The reason for this is that face-to-face semi-structured interviews are principally structured by conversations between the researcher and the respondent (Robson, 2011). It is said to provide contact between the researcher and the respondent. This contact can make positive reinforcement for participating in the research. It seems to be one of the most productive ways to learn about a person, place, and so on, by asking questions on what the researcher wants to explore, allowing the research to probe such issues in greater depth.

In addition, as a conversation between the researcher and the respondent, any confusion or misunderstanding can be resolved. This means that the researcher can adjust or further explain the questions for the respondent should the respondent become confused or misunderstand questions the researcher has asked. Furthermore, face-to-face semi-structured interviews also allow the researcher to act as an observer, giving the interviewer the opportunity to focus on non-verbal cues (Robson, 2016). Moreover, the interviewer is able to use audio-visual aids, schedule additional interviews, make use of language the respondent can relate to, and also utilise discretion. In return, it can make it easier for the researcher to transcribe these details for data analysis.

As mentioned above, face-to-face semi-structured interviews have a number of advantages. However, there are also disadvantages, the biggest disadvantages of using the face-to-face semi-structured interviews are time consumption and cost. In fact, each interview will take at least an hour, if not far more. Thus, time consumption makes demands on both the researcher and the participant. In addition, the participant needs to
travel to the location where the interviews are being conducted. So time spent travelling should be included. Furthermore, in this case, participants had to cover their own travel expenses. Thus, the two factors above can become a challenge to be managed by the researcher which depends on each research participant situation. However, for this research, the two negative affects above will be limited due to the research sites which are located in one area - Hanoi, Vietnam, thus, interviews will be timely and travel expenditure limited.

3.3.2.1. Interview schedules

There are four parts to the interview schedules. The first part of the interview is to obtain participants’ background information. It contained closed questions relating to the demographic information of the interviewees. Then the interviewer formulated questions on the current regulating of cybercrime policy as well as the current practise response of cybercrime regulation mechanisms and systems in Vietnam. In order to obtain participants’ views on the definition of cybercrime, cybercrime in general, the regulation of cybercrime, and Vietnamese mechanisms and systems of regulating cybercrime, it was necessary to ask in-depth questions. It also included their own perception on the role that they play. The final part is the general view of the interviewees on the application of the Vietnamese cybercrime regulation structure and policies. The next section considers the selection of interview participants.

3.3.2.2. Purposive Sampling

Choosing a research sample is an important process for any research study (Robson, 2016). It is considered to be rarely practical, efficient or ethical to study the whole community and sampling also provides a way of getting the best information (Denscombe, 2014). At the same time, the people being sampled should have good knowledge and experience in order to provide quality information and valuable insights on the research study (Denscombe, 2014).

There are two types of sampling methods in qualitative interviews: probability samples (random samples) and purposive samples (non-probability samples) (Robson, 2016).
These samples are suitable for studies aiming to evaluate particular characteristics of the population or testing empirical hypotheses (Arber, 2001). It is suited to reveal and develop theory within which probability statements are not required (Crow and Semmens, 2008).

The researcher has decided to use purposive sample in this study for a number of reasons as set out below:

i) Firstly, purposive sampling is highlighted as useful for in-depth interviews to provide rich information from selected people that are especially knowledgeable about, or experienced with, a phenomenon of the interest (Palinkas et al., 2015). It is viewed to be the best sample strategy where the aim of the study is to consider a wider understanding of social processes and actions (Arber, 2001). This is suitable for this thesis because the objective of this research is to gather a wide range of views from a sample of knowledgeable individuals in order to explore, and critically analyse, whether current Vietnamese regulation policies as well as regulation mechanism approaches are effective in responses to cybercrime rather than to produce meaningful statistical data.

ii) Secondly, the limitations of time, budget and other resources are major reasons for the researcher choosing a non-probability sample for his research in order to collect data from the interview that is credible. Meanwhile, probability sampling requires large populations and large samples (Firestone, 1993) in order to predict or describe, and then generalise accurately back to the large population from which a sample is drawn (ibid.). Therefore, probability sampling takes more time to complete and thus increases the costs of research.

Using a purposive sample in this research to gain the viewpoint of knowledgeable individuals about the issues of the current cybercrime regulation policies and practise response of cybercrime regulation systems will supplement and enhance the findings of the document research. The interviewees were selected because they are experts in this field and they will provide valuable information. In order to do that, this research will select a number of people in the different institutions listed in Table 1 below.

The interviews need to be conducted in the mother tongue of the interviewer and interviewees - Vietnamese. The main reason for this is that Vietnamese, in most cases, is the only language that participants speak. Some might understand another language, such as English, but this is unlikely that a significant proportion will, and those who do
understand English are, because of their age and generation especially, unlikely to be able to speak English very well. Particularly, in relation to this research study, using Vietnamese was the most appropriate for the interviewees. Therefore, they could choose their own way to answer questions, and even, in some cases, the interviewer had a chance to encourage them to clarify their own viewpoints by follow up questions.

The seven institutions operate under the management of different Ministries. These seven institutions are regionally located in the capital of Vietnam – Hanoi. Thus, the researcher could access the research sites easier and limit travel expenditure. Furthermore, there is no connection between the researcher and these institutions, even in the case of the Department of Cybercrime Prevention which operates under the management of the Ministry of Public Security.

The researcher is an Investigative Officer of the Bureau of Security and Investigative Services – Ministry of Public Security. Therefore, in order to access the research sites to obtain the viewpoint of interviewees, as a member of the Ministry of Public Security, the researcher requested his office to issue the formal letter of introduction concerning his research to the participants who might, or might not, be a member of the Ministry of Public Security (see Document dated January 22, 2015, Appendix: The letter of introduction). By using the letter of introduction, the researcher would meet with gatekeepers employed in this research to gather some initial information and advice in order to make sure that selected participants were suitable for the purpose of this research. Gatekeepers (Davies et al., 2011) control the researcher’s access to information in a study. They will be managers of each institution listed in Table 3.1 below. Moreover, the research is a PhD project under the supervision of the University of Portsmouth, and adheres to the institution’s research ethical procedures as well as the Guidelines of the British Sociological Association. The research was granted ethical approval on 19th June 2015 (see appendix: Ethical approval). Consequently, the researcher is unlikely to be the subject of any conflict of interest with these institutions.
Table 3.1: Types of participation

<table>
<thead>
<tr>
<th>Institution</th>
<th>Number of people</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Ministry of Public Security</td>
<td>5</td>
</tr>
<tr>
<td>The Supreme People’s Procuracy</td>
<td>5</td>
</tr>
<tr>
<td>The Supreme People’s Courts</td>
<td>5</td>
</tr>
<tr>
<td>The Ministry of Information and Communications</td>
<td>5</td>
</tr>
<tr>
<td>The Ministry of Justice</td>
<td>5</td>
</tr>
<tr>
<td>The Vietnamese post and telecommunication (VNPT)</td>
<td>5</td>
</tr>
<tr>
<td>The corporate for financing and promoting technology (FPT)</td>
<td>5</td>
</tr>
</tbody>
</table>

3.3.2.3. Interviewees by institutions

The interviewees are those with some responsibility for aspects of cybercrime regulation policies in general, as well as Criminal Law in particular, and the current practice response of cybercrime regulation in Vietnam. As professionals, the participants should be able to understand abstract questions and to contribute valuable and coherent information in relation to cybercrime regulation policies as well as the issue of current practise response of cybercrime regulation mechanism systems in Vietnam with which they are most familiar, particularly within their own work.

As mentioned above, the aim of the qualitative interview is to obtain the viewpoints of experts on the definition of cybercrime, the value of various forms of cybercrime regulation policies, and the current regulation of cybercrime mechanism system in Vietnam. In doing so, this research intended to interview people in those institutions who had worked directly with policies and law enforcement.

The interview schedule used with the Police/Prosecutor/Judge officers was designed to collect information on three aspects of the issue and consisted of 28 questions. Some of these are ‘prompt’ questions, in case officers do not know what kind of information the researcher wanted to collect. The first part includes seven questions which were designed to collect information on an interviewee’s background. This includes matters
of gender, age, education level, experience in policing, level of understanding of computers and networks, and any relevant training they had received. This generates a profile of the Police officers, which the researcher is able to use to understand the critical role they play in regulating cybercrime. The second part was designed with seven ‘open’ and ‘closed’ questions to collect general views on cybercrime, including the definition of cybercrime, characteristics, and their opinions on the impact of cybercrime on society. The third and final part was divided into two perspectives. One perspective was on the regulation of cybercrime policy, on which there were eight questions about their views and an assessment on the efficiency and effectiveness of the regulation of cybercrime in Vietnam. Particularly, questions were designed to gain an in-depth understanding of the coverage of cybercriminal activity in regulation policy. Indeed, this included obtaining their views on improving/amending the regulation of cybercrime policies. The other perspective is on the regulation of cybercrime in practise. Seven questions were designed to obtain information on the role, function, and accountability of the Police/Prosecutor/Judge officers in regulating cybercriminal activity in Vietnam. Typically, one opening question aimed to understand the role the interviewee played in regulating cybercrime. The final question was an open-ended question to let the interviewee add their own views on both cybercriminal issues and its regulation.

Five staff members from Ministry of Information Communication Technology, Ministry of Justice, and five staff members from each ISP (VNPT, FPT) were invited to participate in this research study. The interviews gathered their views in general of cybercrime, and the regulation of cybercrime policies and practise in Vietnam. Questions were used to explore their perceptions on the definition of cybercrime, regulation policy and practise of cybercrime, and their responsibilities for regulating cybercrime. Thus, the questions were designed to gain information on the three aspects and consisted of 28 questions, divided into three sections. The first section comprises seven questions to collect the general information of participants such as their age, years of working experience, educational level, understanding computer and networks level, and participated training. The second section aims to gather participants’ views on the general of cybercrime, including seven questions. Questions were created to ask about the definition of cybercrime, characteristics, consequences and the impact of cybercrime on society. This section provides an open-ended question to let participants give their
views freely on who is responsible for cybercrime. The third section is about regulation policy and its practice in relation to cybercrime. This comprises 14 questions. Questions one to seven were designed to elicit views and assessments on the effectiveness and coverage of regulation policies in regulating cybercrime. Questions eight to 14 were designed to collect the point of view of participants on the regulation of cybercrime in practise. Particularly, these focused on the role of ISPs and users in reducing the growth of cybercrime in Vietnam. The end of this section is an ‘open’ question for participants to give freely their recommendation on both the regulation of cybercrime policies and its practical.

3.4. Data analysis

There are various methods of data analysis, such as: content analysis, discourse analysis, interpretative phenomenological analysis (IPA) and grounded theory. In the case of this research, thematic analysis is the most appropriate to be used to analyse the data collected. Thematic analysis, a type of qualitative research, is used to analyse the interview transcripts. The reasons for choosing a thematic analysis approach for this research are outlined below:

i) Thematic analysis was chosen as it provides a “useful and flexible method for qualitative research” (Braun and Clarke, 2006, p. 77), enabling the data from qualitative interviews to be subjected to the same analysis. It is also arguably the most common approach to qualitative analysis of data in the social sciences (Holstein & Gubrium, 1994).

ii) Thematic analysis has been criticised for being poorly defined yet widely utilised, with little information available regarding its implementation (Boyatzis, 1998; Roulston, 2001). Rather than being a specific approach in its own right, such as grounded theory, it is also considered to be a process that is performed within an analytical approach, aiding the researcher to search for meaning and insight (Boyatzis, 1998; Ryan & Benard, 2000). In addition, Holloway and Todres (2003) assert ‘thematizing themes’ is a common feature of all qualitative approaches and thematic analysis can be considered to be the foundation on which other qualitative methods are founded (Roulston, 2001).
Thematic analysis offers an accessible and theoretically flexible approach to analyse qualitative data (Braun and Clarke, 2006). As a flexible approach, thematic analysis is considered as the most appropriate for this study. Additionally, the flexible method can be used within existing criminological theories, unlike other approaches, for instance, grounded theory and interpretative phenomenological analysis, which are theoretically bound (Braun & Clarke, 2006). Thematic analysis also often goes further and interprets various aspects of the research topic (Boyatzis, 1998). In this, the approach is particularly suited to the analysis of a range of qualitative data when the researcher seeks to allow for key themes from the entire body of data to emerge (Caulfield & Hill, 2014). It allows the researcher to associate an analysis of the frequency of a theme with one of the whole content. This will confer accuracy and intricacy and enhance the research’s whole meaning. Thematic analysis is said to give an opportunity to understand the potential of any issues more widely (Marks and Yardley, 2004). Namey et al., (2008) assert: “Thematic [analysis] moves beyond counting explicit words or phrases and focuses on identifying and describing both implicit and explicit ideas. Codes developed for ideas or themes are then applied or linked to raw data as summary markers for later analysis, which may include comparing the relative frequencies of themes or topics within a data set, looking for code co-occurrence, or graphically displaying code relationships (p. 138)”.

As mentioned above, unlike IPA (interpretative phenomenological analysis) and grounded theory, thematic analysis is not theoretically bound; therefore, it provides an opportunity for flexibility. Although grounded theory and IPA both seek patterns in the data, they are theoretically bounded. Grounded theory is theoretically bounded and seeks to impose theory upon the interpreted data, the role of the researcher as being to “organise, select and construct explanation” (Daly, 1997, p. 350). Simply put, grounded theory directly requires data analysis to be oriented towards theory development (Holloway & Todres, 2003). As a consequence, the research will be pressured by the use of grounded theory to develop a model to explain phenomena (Robson, 2011; Willig, 2001). Thus, in this research, thematic analysis is used because it is a flexible method seeking to describe patterns across qualitative data rather than from within.

Braun and Clarke (2006) have provided an evidence-based argument for the use of thematic analysis and have also produced a useful step-by-step guide on how to conduct
thematic analysis. As a useful guide, this research adopts Braun and Clarke’s guide for the research data analysis.

In regard to identifying themes or patterns, there are two primary ways of identifying themes. The first one is an inductive approach (Frith and Gleeson, 2004) and the other is a theoretical deductive approach (Braun and Clarke, 2006). The themes identified through an inductive approach are not coded into pre-existing categories and are strongly linked to the data themselves. In this method, thematic analysis allows researchers to provide a rich description of the data set related to a broad research question, enabling the specific research question to evolve through the coding process (Braun and Clarke, 2006). The second approach is more explicitly analysis-driven. In other words, it is driven by the researcher’s theoretical interest in the area. This form of thematic analysis tends to provide a less rich description of the data overall and instead focuses on a more detailed analysis of some aspect of the data, coding for a specific research question (Braun and Clarke, 2006). As Braun and Clarke (2006) have illustrated, thematic analysis, in general, seeks to provide a description and interpretation of themes, often in relation to previous studies.

In qualitative research, researchers need to be clear about what they are doing and why, including how the data analysis will be presented (Attride-Stirling, 2001). In order to analyse transcribed interview data, this research applies the six guided steps of thematic analysis that Braun and Clarke (2006) have outlined. The sequential process of thematic analysis will be as follows:

i) Becoming familiar with data

Becoming familiar with the data involves immersion in the data. As mentioned above, the interviews will be conducted in the mother tongue of both the interviewer and the interviewees – Vietnamese. Thus, familiarisation with data in this research will be internalised through translation and transcription of the interviews. All data collected through face-to-face interviews with participants will be read and reread a number of times in order to make sure that it will be accurate when the interview transcripts are translated into English. All interviews will be directly translated into English, verbatim, by the researcher. However, before doing that the pre-translated transcription will take place. The main reason for this is that helps the researcher to communicate with the researcher’s supervisors and get advice and guidelines on coding and theme
development. This also makes sure that all original meaning of information will be accurate when translated into English. Most of the translated transcriptions will be carried out immediately after the interview for clarification.

ii) Generating initial codes

Following familiarisation with the data, the next phase in thematic analysis will involve generating initial codes from the data. At this stage, the researcher carefully reads the transcript line by line, applying a paraphrase that describes what the researcher has interpreted in the passage as important. To assist in the manual coding, the researcher will use highlighter pens to highlight the relevant text.

iii) Searching for patterns/themes

This stage starts after all data has been initially coded. This is an important aspect of the data in relation to the research question. At this stage, the researcher needs to read and re-read coded data in order to identify significant patterns of meaning. A theme often represents a patterned response or meaning within the dataset. Therefore, Braun and Clarke (2006) advise the researcher not to relate the importance of a theme to quantifiable measures, but to how it relates to the research question.

iv) Reviewing themes

According to Braun and Clarke (2006), there are two levels of reviewing and refining themes. Level one aims to ensure that each theme contains coherent supporting evidence clearly distinguishable from each other. In case a theme does not contain enough evidence, it collapses into other themes.

At level two, the researcher needs to re-read the entire data set and consider whether the themes reflect the data. This also enables the researcher to avoid data missing from existing themes.

v) Defining and naming themes

At this stage, the researcher needs to define and further refine the themes that will be presented for the research data analysis in relation to the story that was told as well as its relationship to the research question and to the other identified themes. The researcher should consider what is interesting about the themes and why they are of relevance.
vi) Producing the report

The research findings section will be written up in a way which aims to provide a coherent description of the story told by the data, considering information from within and across themes. This will be shown in the next chapter.

3.5. Ethical considerations

Ethical issues arise in all type of research and criminological research is not an exception, that indeed, ‘ethical predicaments cannot be avoided’ (Liebling & Stanko, 2001). The meaning of ethical dimensions is “both to safeguard the proper interests of those involved in or affected by their work and to report their findings accurately and truthfully” (British Sociological Association, 2002, Para. 6) in carrying out qualitative research in criminology. Furthermore, the research is not designed to treat, help or harm individuals. This research is designed to discover the point of view of the participants to gain further the viewpoints of experts on the definition of cybercrime, the value of various forms of cybercrime regulation policies, and the current practise response of cybercrime regulation in Vietnam. Therefore, the researcher must take responsibility to protect all interviewees, especially when they are in Vietnam. Because most participants are working for a Vietnamese government institution, they are voicing opinions about the government, its policies and also about their employer.

The research has to be approved in relation to the requirements of the Research Ethics Review process by the Faculty of Humanities, Social Sciences and Law within the University of Portsmouth. This significantly includes combining the University’s guidance on ethical considerations in research and practical procedures. In addition, this research follows the ethical guidelines of the British Society of Criminology and the Social Legal Studies Association.

Based on the primary aim of this research, this research is going to select interview participants who are all over the age of 18 years and engaged in a professional occupation. Accordingly, the research does not involve vulnerable participants or individuals who might find it difficult to decline a request for informed consent. The following ethical issues are fully taken into account: Informed consent, confidentiality and anonymity, and code of ethics guiding the study.
3.5.1. Informed consent

Ethical issues concerning informed consent refer to informing participants that they have rights to refuse or withdraw, thereby ensuring voluntary participation in the research. Participants need to be informed in advance by the researcher, so as to completely understand at all times what the research is about; the purpose of the research; the implications for themselves in being involved; how interview data will be used; and, how the research will be disseminated (Robson, 2011; Ritchie et al., 2013). A personalized letter of invitation should be sent to each interviewee. In addition, the participants should also be given a written consent paper to sign before each interview commences. All interviewees will be reminded that their participation in the interview is voluntary and they have rights to withdraw without giving a reason at any point during the interview or refuse to answer any individual question (Orb et al., 2001). It will be necessary to repeat the rights of participants individually before every interview (Bailey, 1996).

3.5.2. Confidentiality and anonymity

The identity of all respondents (anonymity) and confidentiality of the interviews must be considered to protect all participants in the research (Meyer, 2000; Orb et al., 2001), this is a common practise to be followed. In order to help all participants to understand clearly the concepts of anonymity and confidentiality, the researcher will need to explain this to them before each interview.

Using qualitative interviews in criminological research means that the researcher must take his or her responsibility seriously to all interviewees at the various stages of the research process, including the initial approach, during the interview, and in subsequent handling of information acquired (Noakes & Wincup, 2004). The researcher must always be aware of the responsibility of protecting confidentiality in this research (Kaiser, 2009). All interviewees are informed verbally that the information in the interviews will be treated as strictly confidential and will be used solely for study purposes (Qu & Dumay, 2011). The researcher needs to ensure that data, including
written notes, interview schedules and audiotapes, are adequately protected (Noakes & Wincup, 2004). All of these will be stored securely, and some will be further protected from disclosure by use of a password. Only authorized persons could therefore gain access to them.

3.5.3. Code of ethics

There is, currently, no ethical regulation of research available in Vietnam. The research is, therefore, guided by the Codes of Ethics for UK academic research, to ensure the validity and reliability of outcomes (Clause 4xi, British Society of Criminology, 2006) and ethical conduct in the research throughout. As the research is mainly based in the Vietnamese context, those ethical issues will be addressed by following similar studies that have been carried out in the UK. Although there will be differences between cultures and regulations between Vietnam and the UK, the academic approach for the issues of cybercrime regulation will be similar.

3.6. Limitations of the chosen methodology and methods

The chosen methodology and methods above were thought to be the best for this thesis although they are not perfect. In doing so, the following will discuss some limitation of the chosen methodology and methods in this thesis.

3.6.1. Disadvantages of Thematic Analysis

It could be agreed with some authors’ argument by saying that Thematic Analysis as a means of analysing qualitative data is not a specific ‘branded’ qualitative approach (Boyatzis, 1998; Ryan & Bernard, 2000). However, Braun and Clarke (2006) have illustrated that Thematic Analysis is a flexible approach which can produce insightful analysis. It is important for the method to be appropriate to the research questions (Holloway & Todres, 2003; Silverman, 2010) and for analysis to be driven by both the research questions and the epistemological position. Nonetheless, the methods and forms of analysis employed in this research were appropriate for the research questions.
Thematic Analysis can usefully summarise a large amount of data, and offers a rich
description across data sets. Similarities and differences can be highlighted, and
unanticipated insights can be generated (Braun & Clarke, 2006). These principles were
useful in generating the findings of this research.

As previously illustrated how the flexibility of thematic analysis was adapted to
maximise robust results for the purposes of this research study. This would have not
been possible with more prescriptive approaches such as Grounded Theory. The
flexibility of Thematic Analysis is viewed as both an advantage and disadvantage.
Thematic Analysis offers a number of advantages by providing the researcher is clear
and explicit about what he is doing. The research has attempted to make this research
study transparent, about the beliefs and approach adopted by the researcher, and on how
the outcomes were reached in order to make this research study valid and credible. At
the same time, the flexibility this approach offers can be offset by a lack of rigid
guidelines for data analysis. This can be challenging when deciding what aspects of the
research topic to focus on over the course of the research (Nowell et al., 2017).

3.6.2. Validity and reliability

It can be seen that qualitative research has been criticised for its lack of ‘scientific
rigour’, as it is compared to frameworks which are used to evaluate quantitative
methods, such as validity and reliability, which “were not devised for this purpose”
(Horsburgh, 2003, p. 307). Reliability refers to the possibility of the outcomes being
repeated and validity refers to the outcomes being correct.

The research has described in detail, particularly in Chapter 3, how the theoretical
framework, methodology and methods have been applied to the research topic.
Decisions taken to guide the research have been made explicit in addition to a detailed
account of data analysis. Data mainly gathered via semi-structured interviews was
appropriate for the purpose of this study and was analysed using techniques consistent
with a social science approach, thus achieving data consistency.

The validity of the present study could be considered to be threatened by the
subjectivity inherent in data analysis processes (Braun & Clarke, 2006). The researcher
is considered as an active participant within the research process and themes do not just
emerge from the data (Braun & Clarke, 2006). Meanings and themes were checked with participants during data collection in order to reduce researcher bias and to promote the views of participants as explicitly as possible. Furthermore, the research transparency regarding the methods and methodology was demonstrated that could be an allegation for the research validity. Data was collected from a total of 35 people working across seven institutions. Commonalities between views have been identified and have provided evidence regarding the key factors that make cybercrime difficult and challenging for Vietnamese authorities to regulate, and clear positions have emerged as to the role key players should take in reducing the growth of cybercrime in Vietnam. Extracts from the data provided evidence to answer the research questions.

3.6.3. Generalisability

This research study is a small-scale project, conducted in a specific location (Hanoi-Vietnam) and within a time limitation, therefore, the ability of the research study to make general statements regarding the key factors that make cybercrime a challenge for Vietnamese authorities to regulate it, and possible future cybercrime regulation approaches were developed by interviewing face-to-face people in only seven different institutions, that is limited. In this regard, Willig (2001) states: “… even though we do not know who or how many people share a particular experience, once we have identified it through qualitative research, we do know that it is available within a culture or society” (p. 17).

The themes and ideas presented as the perspectives of participants within the current research study, regarding the key factors make cybercrime challenges to regulate, and possible approaches for the future, suggest that they were available within a particular context, at a particular moment in time. This means that whilst the findings are specific to a particular time and situation, the findings may inform similar or related research. Although it is conceded that the findings of this study have limited generalisability, it is reinforced that achieving this was not the intention of this study.
3.7. Conclusion

This chapter has presented and discussed the methodological approach and research methods adopted to answer the research questions. To produce useful data about the challenges of cybercrime regulation in Vietnam, the study applied a qualitative interview design, using face-to-face interviews to research the selected population. As no previous study has been conducted in this way in Vietnam, this research will then be guided by the research ethics of UK institutions. By doing so, the research is credible, not only in terms of the current literature on cybercrime regulation in Vietnam, but also in relation to the literature which has been published about cybercrime regulation in other countries.
Chapter 4: Cybercrime and its regulation in Vietnam

4.1. Introduction

The purpose of this chapter is to provide some background information from existing literature concerning cybercrime and its regulation in the Vietnamese context. Social-technical information concerning the growth of information technologies in Vietnam is also introduced to provide more contextual material. This chapter contains five main parts, exclusive of the introduction. First, it briefly presents an overview of the socio-economic and technological conditions of the country. It begins with the socio-economic background of Vietnam in relation to Information Communication Technologies (ICTs). Then, it moves forward to show a picture of the growth of the Internet in Vietnam, as it has been given top policy priority, strategies, and master plans. The second part starts with a brief picture of cybercrime in Vietnam. The third part presents a picture of the current state of cybercrime regulation in Vietnam. It starts by discussing the meaning of the term ‘cybercrime’ in the Vietnamese legal system. In doing so, the research will indicate that the current Vietnamese approach has established its own working definition of ‘cybercrime’ to be used in its legal system. However, the term ‘cybercrime’ and its relation to other forms of crime remain unclear due to the nature and many unique features of cybercrime. This challenge is only not faced by Vietnam, but it is, indeed, a global challenge. This part gives a brief overview of how cybercrime regulation policy measures in Vietnam are working to date. Then, this part continues to provide the establishment of institutional regulatory mechanisms regarding the regulation of cybercrime. Furthermore, this part provides other legislations in relation to cybercriminal activities in Vietnam. The final part will give a brief overview of how the Vietnamese Penal Code has responded to cybercrime.

The fourth part of the chapter introduces some key challenges brought about by cybercrime by exploring how the initial Vietnamese legal framework responds to this new criminological phenomenon; and by exploring some of the main challenges that the Vietnamese law enforcement agencies have in response to cybercrime. At the same time, it also indicates how and what challenges Vietnam’s Internet Service Providers
face in regulating these issues. The final part of chapter will summarise the main contents of this chapter.

4.2. The Vietnamese context: Society and technology

This section presents some aspects of Vietnamese society in relation to the context of cybercrime and regulation of cybercrime in Vietnam. First, it provides a brief socio-economic background of Vietnam. It then presents a current assessment of the use of the Internet in Vietnam. It finally provides a picture of cybercrime in Vietnam.

4.2.1. The socio-economic background

After the reunification of Vietnam in 1975, the two parts of the country were united to become the Socialist Republic of Vietnam, which has since been led solely by the Communist Party. Vietnam began to find a suitable path of development and started focusing on its reconstruction due to the socio-economic status of the country, which had significant problems caused by many years of war, policy weakness and a difficult international environment. These difficulties were illustrated through the talk in 1981 between a French journalist - Stanley Karnov, and Mr Pham Van Dong, then the Prime Minister, who said that “Yes, we defeated the US, but now we are plagued by problems. We do not have enough to eat. We are a poor, undeveloped nation. Vous savez, waging a war is simple, but running a country is difficult” (Karnov, 1997, p. 36). To overcome these difficulties, a reform known as ‘Renovation’ was initiated at the Sixth Congress of the Communist Party of Vietnam, in December 1986. In its approach, the government implemented free market reforms, which carefully managed the transition from a planned economy to a socialist-oriented market economy.

---

32 Vietnam is located in the Southeast Asia region and shares borders with the People’s Republic of China in the North and, to the west, the Lao People’s Democratic Republic and the Kingdom of Cambodia. Over 86 million people from 54 different ethnic groups live on its narrow s-shaped 331,000 km2 and along its more than 3,000 km of coastline. Three-quarters of the country is hilly and mountainous, arable land accounts for only 28.4%.

33 Socialist-oriented market economy: a new economic model intended to be a transitional phase in the development of a full socialist economy, with the goal of improving productive forces and developing a firm material base for the foundation of socialism. The socialist-oriented market economy is a multi-
The Vietnamese society has gradually changed since the implementation of this renovation. Vietnam’s economy subsequently achieved rapid growth in agricultural and industrial production, construction, housing, exports and foreign investment. As a result, Vietnam was regarded as one of the most successful transition economies in the world (Godoy and Stiglitz, 2006).

However, at the Tenth Congress Communist Party in 2006, the requirement of integration into the international economy led the government to change the economic development to a new process called ‘industrialisation and modernisation’ (The report of the Party Central Committee, dated 10 April, 2006). Accordingly, Vietnam became a member of the World Trade Organisation (WTO), in 2007, which provided the legal framework for Vietnam to trade products with countries worldwide. Over the past decade, Vietnam was considered one of the best performing economies in the world (The World Bank, 2011), with fast-rising GDP and per capita income rates (Wilson, 2014). Although facing high inflation rates during the world economic crisis, the economic growth of Vietnam continued at a rate of 6.8% in 2010, 6.7% in 2015 (General Statistic Office of Vietnam, 2015).

The Vietnamese government has given the highest priority to the use and development of Information technology, in order to be integrated into the global economy. This is because the use and development of information communication technology is not only viewed as a key enabler, but is also considered as an independent economic sector, and it is a part of the infrastructure of the national economy (The Prime Minister’s Speech at the Vietnam ICT Summit 2013, date 20 June 2013). This issue was earlier identified in the 2000’s by the Communist Party of Vietnam – Directive No. 58/CT/TW, dated 17 October 2000. The Directive No 58-CT/TW does, in fact, seem to be old in comparison with the dramatic development of information technology, but it is still a significant and crucial policy in which other policies must comply with, especially in the use and development of ICTs in the Vietnamese context.

The use and development of IT was strongly emphasised by the Vietnamese government as follows:

sectors commodity economy regulated by the market, but under state management and largely under state ownership.
i) First, the use and development of IT is identified as one of the most important driving forces for economic development and social advancement. It is viewed as one of the quickest ways to achieve national industrialization and modernization goals, and provides an important contribution to national security (The Directive 58/CT-TW, 2000). Furthermore, the government’s strategy has viewed IT as a key element which “will quickly transform its socio-economic structure to become an advanced country in terms of a knowledge-based economy and information society”. The development of IT is also considered as making a significant contribution to “the success of country’s industrialization and modernization process” (Decision 246/2005/QD-TTg, dated 06 October, 2005, p. 1).

ii) Secondly, on the one hand the use and development of IT is not only seen as an economic sector making an important contribution to economic growth. On the other hand, it is also viewed as a factor that helps other sectors to develop, and enhances technology’s capacity in industrialization and modernization nationally (Decision No. 1755/QD-TTg, 22 September 2010). Thus, investment in IT infrastructure and communication will bring intensive, long-term benefits to the entire society (Decision No. 246/2005/DQ-TTg, 06 October 2005; Mitra, 2013).

Given the important role of IT in the country’s development, the Vietnamese government has made significant efforts to support the development of IT. It was illustrated via a wide range of legal regulations. For example, by 2015, Vietnam has made significant efforts to create a solid legal foundation for the use and development of IT, especially supporting the country’s economic development. According to the Law on the promulgation of Legal Documents, the legal documents that regulated the digital age of Vietnam can be classified as laws (passed by the National assembly); decrees, directive and decisions (made by the Prime Minister); and circulars (introduced by Ministerial level) (Law on the promulgation of legal documents, 2015).
Table 4: The key legal documents regulating Vietnam’s digital economy

<table>
<thead>
<tr>
<th>No.</th>
<th>Laws/document regulations</th>
<th>Year of introduction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Law on E-transaction</td>
<td>2005</td>
</tr>
<tr>
<td>2</td>
<td>Law on intellectual property and its amendment</td>
<td>2005, amended 2009</td>
</tr>
<tr>
<td>3</td>
<td>Law on information technology</td>
<td>2006</td>
</tr>
<tr>
<td>4</td>
<td>Law on Information Network Security</td>
<td>2015</td>
</tr>
<tr>
<td>5</td>
<td>Decision No.169/2006 on the investment and procurement of information technology products by agencies and organisations using state budget</td>
<td>2006</td>
</tr>
<tr>
<td>6</td>
<td>Directive No.04/2007 on enhancing the protection of copyright on software</td>
<td>2007</td>
</tr>
<tr>
<td>7</td>
<td>Decree No.26/2007 on digital signatures</td>
<td>2007</td>
</tr>
<tr>
<td>8</td>
<td>Decree No.27/2007 on e-transactions in financial activities</td>
<td>2007</td>
</tr>
<tr>
<td>9</td>
<td>Decree No.35/2007 on e-transaction in banking</td>
<td>2007</td>
</tr>
<tr>
<td>10</td>
<td>Directive No.03/2007 on enhancing information security over the Internet</td>
<td>2007</td>
</tr>
<tr>
<td>11</td>
<td>Decree No.90/2008 on anti-spam</td>
<td>2008</td>
</tr>
<tr>
<td>12</td>
<td>Decision No.50/2009 on management of the software industry development program and the digital content industry development program in Vietnam</td>
<td>2009</td>
</tr>
<tr>
<td>13</td>
<td>Decree No.102/2009 on the management of investment in information technology applications using state budget</td>
<td>2009</td>
</tr>
<tr>
<td>14</td>
<td>Decree No.43/2011 on the provision of information and online public services on websites or portals of state agencies</td>
<td>2011</td>
</tr>
<tr>
<td>15</td>
<td>Decree No.72/2013 on management, provision and use of the Internet service and online information</td>
<td>2013</td>
</tr>
</tbody>
</table>

Source: Compiled from Ministry of Information and Communications (2015)
As can be seen, under the Law on the promulgation of Legal Documents, the regulation of cybercrime policies is made at different levels or tiers. The intention is to strictly manage the problems related to the digital age of Vietnam. However, this research argues that these legal regulations just concentrate on how to support IT development and application, rather than regulate, criminal activity as it relates to information communication technology. This will be further illustrated in the following sections below.

4.2.2. The growth of the Internet in Vietnam

Despite the fact that Vietnam is a latecomer, even compared to many developing countries, ICT penetration and usage is steadily growing (Cimigo, 2010). Considering the potential of ICTs to increase economic growth and reduce poverty, Vietnam has to embrace use of ICTs in its entire social, economic and political structures. That is why the Vietnamese government envisions every aspect of Vietnamese life as ICT assisted, and has considered and made the development of ICT as one of its strategic plan priorities. At the initial stage, Vietnam has set out five guiding principles for promoting ICT and five strategic directions for policy formulation and implementation (The Directive 58/CT-TW, 2000). The details are provided below:

Five guiding principles

i) The use and development of ICT is a priority in the country’s socio-economic development strategy. It is a major engine for the country to catch up with, and even surpass, advanced nations;

ii) All sectors, be they economic, cultural, or defence-related, must embrace ICT in order to develop;

iii) The national information network is a strategic socio-economic infrastructure. It must be upgraded to create favourable conditions for the use and development of ICT, with high speeds, high quality, and low user costs;

iv) Development of ICT human resource is a vital factor, which determines the success of the use and development of ICT;
v) ICT industry, especially the software industry, should be developed into a strategic economic sector.

Five strategic directions for policy formulation and implementation

i) Promoting widespread and efficient usage of ICT across socio-economic sectors. In this direction, the state agencies should take a pioneering role;

ii) Creating a favourable environment for applications and development of ICT. Notable policy measures in this direction include:

- Encouraging investment in the ICT sector with highest possible levels of incentives, with the aim to be competitive compared to those offered by other countries in the region.

- Fostering foreign language proficiency of the population, especially the young people; while developing platforms that support the use of ICT in the Vietnamese language.

- Giving top priority to the application and development of ICT in socio-economic development plans and programs, especially in financial resource allocations.

- Providing incentives to businesses for investment in ICT to boost growth and competitiveness.

- Encouraging the use of ICT products and services produced locally. Domestic ICT products and services are exempted from value-added tax (VAT). ICT companies enjoy the highest possible preferences on corporate tax rates, access to bank credits, and land use.

- Developing export support programs for the ICT sector, firstly for the software industry.

- Providing favourable conditions for personnel working in the ICT sector to enable them to work abroad and return to the in their country.

- Developing major high-tech parks with special policies and measures; attracting foreign investment into these parks with stronger incentives compared to those offered by countries in the region.
- Enhancing legal documents and enforcement concerning intellectual property right protection, including the protection of copyright of software and other ICT products.

iii) Accelerating the training and utilisation of human resources for ICT application and development, with the target to reach the average rate of the countries in the region on the number of ICT specialists per 10,000 inhabitants;

iv) Speeding up the establishment of the national information network; creating a competitive environment, which enables companies of all types of ownership to participate in provision of telecom and Internet services;

v) Renovating and strengthening the state management of the ICT sector. Every state agency at the central and provincial levels needs to assign a senior leader to be in charge of ICT application (The Directive 58/CT-TW, 2000).

Applying these guiding principles and strategic directions, the Vietnamese government has issued a number of Decisions, Resolutions, and Plans. For example, there were four government policies issued from 2007 to 2010 in regarding plan on information technology application in state agency operation, such as Decree No. 64/2007/ND-CP dated 10 April 2007; Decision No.43/2008/DQ-TTg dated March 24th 2008, Decision No.48/2009/QD-TTg dated March 31st 2009 and Decision No. 1605/QD-TTg dated August 27th 2010.

It is because of this commitment that ICT penetration and usage is steadily growing in Vietnam. For example, the Ministry of Information Communication Technology has published Vietnam ICT White Book in 2014; and it showed that as of 2010, the total number of Internet users in Vietnam has reached 26.8 million and a rate of growth of 31% (Ministry of Information and Communications, 2014). The increase in the number of Internet users in Vietnam can be seen year after year – from 31.3 million in 2011, 35.6 million in 2012, 40.1 million 2013, 44.6 million in 2014, 47.5 million in 2015 and 49.06 million in 2016.\(^\text{34}\)

There is also a staggering increase in social networks such as Facebook, Zingme, Twitter, LinkedIn, Instagram and Pinterest. The younger generations of Vietnam are logging on every-day to the online environment. According to the Vietnam Digital Landscape 2015 report (Moore Corporation, 2015), there were 1.4 million Facebook users in Vietnam in 2015.

users in 2011 and the number of Facebook users has increased 22 times since 2011 (31.3 million Facebook users in March 2015). The number of Vietnam’s broadband Internet subscribers has also increased from 3.04 million in 2010 to 4.09 million in 2012 (Vietnam Internet Network Information Centre (VNNIC), 2012). The international connection bandwidth of Vietnam has dramatically increased from 96.320 billion in 2010 to 3006.176 billion in 2012 (VNNIC, 2012). Mobile subscription registered has dramatically increased from 1.29 in 2005 to 128.04 in 2016 for every 100 people. A report by the Vietnam Internet Network Information Centre (VNNIC, 2012, 2015) has shown that the Internet boom in Vietnam is the result of key developments in many areas including Internet resources (domain name, IP address, ASN) which are core factors to foster Internet development. As a result, Vietnam ranks 13rd in the world’s top 20 countries, at 7th place in Asia, and 3rd place in ASEAN in terms of Internet population.

In addition to the development of infrastructures, the Vietnamese government is also trying to promote and facilitate an extensive use of ICT and Internet supported services. To this effect, the Vietnamese government adopted a national strategy in 2010 on “Transforming Vietnam into an advanced ICT country” (Prime Minister’s Decision No.1755/QD-TTg dated Sep 22nd 2010); the national program on IT application in the operations of state agencies during period 2011-2015 (Decision No.1605/QD-TTg dated Aug 27th 2010). The Vietnamese government also created an action plan to promote the application and development of information technology of Vietnam to meet the requirements of sustainable development and international integration (Resolution No.26/NQ-CP dated Apr 15th 2015). Further, the government of Vietnam has adopted e-Government development (Decision No.714/QD-TTg dated May 22nd 2015). Recently, the Vietnamese government has issued the Resolution No.36a/NQ-CP dated Oct 14, 2015 to further accelerate IT application in management and provision of public services and development of e-government.

The use of ICT embraces almost every sector in Vietnamese society, including the banking and financial sector. Even though cash is still the most dominant medium of exchange in Vietnam, electronic-banking is becoming more popular. Electronic transactions were legally recognised for the first time in the Law on e-transection 2005;

electric commerce was also recognised in the Decree No.57/ND-CP, dated June 9th 2006, later it was replaced by Decree No.53/ND-CP, dated May 16th 2013. Almost all banks in Vietnam have now introduced a core banking system, mobile banking and ATM services.

The description of the dramatic growth of the Internet and a series of government policies and strategies for the use and development of ICTs in Vietnam above can suggest that the Vietnamese government seriously considers the importance of ICTs in driving the development of the country’s economy forward and integrating with international norms. However, the increasing dependence on computer systems and other digital technologies comes with vulnerability to cybercrime and cyber-attack. The dependence on computer systems and vulnerability to cybercrime are two sides of the same coin. Therefore, once Vietnam is connected to a global network, Vietnam becomes vulnerable to cybercriminals operating anywhere in the digital world. Vietnam becomes vulnerable to cybercriminals not only in theory, but in practical terms. The following section will show the current situation of cybercrime in Vietnam.

4.3. Cybercrime in Vietnam

As mentioned previously, the improved availability and increased accessibility of the Internet, its growth as a central part of people’s lives, and the consequent and rapid expansion of its use are considered the main causes of the occurrences of cybercrime, combined with an attendant lack of comprehensive regulations. The United Nations-led forum on cybersecurity (United Nations, 2011) has indicated that developing countries have become the most vulnerable to cyberattacks, with relatively weak protection systems. Asian countries, including Vietnam, have become places where cybercrime is becoming prevalent (Broadhurst & Chang, 2013). In other words, Asian countries are becoming a major source of cybercrime in cyberspace.

Vietnam is not an exception to this rule. On the one hand, there is a massive increase in Internet access and Internet user base is expanding. On the other hand, the regulation of cybercrime does seem to be in its early stages and much work still needs to be done. This is the reason why Vietnam has become an attractive place for cybercriminals. Simply put, Vietnam can be considered as a hot bed for cybercrimes.
As discussed above, the Vietnamese government is working on the use and development of ICT infrastructures and ICT based services. Greater bandwidth not only means faster and better Internet access, it also creates a faster and better Internet for illicit activities, and provides more opportunities for criminals to exploit Internet users. In addition, the pervasiveness of mobile phones throughout the country, the introduction of new services including Internet banking, mobile banking, financial service such as ATMs, will also create new opportunities for cybercriminals.

Despite the fact that Vietnam cannot be immune to the threat of cybercrime, there is no consolidated report that shows the exact prevalence and impact of cybercrime in Vietnam, and to what extent the Vietnamese information society is vulnerable. The reason for this can be, among others, that on the whole, neither organisations nor individual users seem prepared to report cybercrime incidents. This is for several reasons, for example they might be afraid of the impact of cybercrime on their business and their services, as well as their reputation, even where some of them are aware that they are targeted by cybercriminals. A further and significant problem is that records in the cybercrime prevention unit and the law enforcement are either not properly recorded or not accessible. Furthermore, literature on the extent of cybercriminal activities in Vietnam seems non-existent. It can, therefore, be argued that this inadequacy of cybercrime’s statistics could lead to over or under-estimating the threat of cybercrime in Vietnam. However, the researcher will endeavour to provide a better picture of cybercrime in Vietnam.

In fact, the use of the Internet in Vietnam is increasingly diffuse, due to the fact that the country relies more and more on data, electronic communications and information technology to drive innovation and efficiency, resulting in increased exposure to cyber security risks. As Dunn Cavelty (2012) has stated:

“The networked information environment – or cyberspace – is pervasively insecure, because it was never built with security in mind. The dynamic globalisation of information services in connection with technological innovation led to a steady increase of connectivity and complexity. The more complex an IT system is, the more problems it contains and the harder it is to control or manage its security” (p. 106).

Vietnam is facing the same challenges as other Asian countries in dealing with the most common forms of cybercrime, such as malware, spoofing, website defacement, high
yield investment programs, e-commerce fraud, phishing. For instance, in 2009 there were 1037 websites attacked, up from 461 in 2008 (Vietnam breaking news, 2010). The number of website attacks has increased dramatically, for instance only in the first three months of 2010, some 300 websites were attacked, and in 2013, in the first nine months, 2405 websites of Vietnamese government agencies and companies were attacked, up from 2203 in 2012.

Besides hacker attacks, computer viruses have become a big issue and increased rapidly as more types of computer viruses have appeared. For example, in 2009, there were 50128 new types of computer virus that infected 64.7 billion computers, up from 33137 in 2008 with more than 59 billion computers infected (Vietnamese Breaking news, 2009). Vietnam was identified as among the top five distributors of spam and malware in the world in 2013 (Brown, 2013).

According to the 2014 Internet security threat report (Symantec Corporation, 2014), Vietnam ranked in the top 10 in terms of malicious activities by source (Malicious code, Spam Zombies, Network attack origins). Similarly, in 2015, Vietnam was considered as the country where users face the greatest risk of online infection (Kaspersky, 2015). For example, as Kaspersky reported, Vietnam ranked among the top 20 countries facing the greatest risk of online infection. Vietnam also ranked in the top 20 countries with the highest risk of local infection.

In relation to the increase of cybercrimes, there are three main factors that are identified as the main causes. Firstly, there are the growing numbers of users who could then become the potential victims of cybercrime. In the past, a typical target of cybercrime was concentrated in the businesses sector, such as information brokers, manufacturers and distributors of digital media, and businesses which offered products or services through Internet services. At present, the typical targets of cybercrime are expanding in scope. As the report of the Internet Security Threat Report has shown, targeted threats are not limited to small and medium sized enterprises and executive levels all sizes of business are becoming targets of attack. In addition, non-business individuals are also being targeted because attackers can easily attack organisations through an individual. It can be said that no one is immune to these attacks.

Secondly, the number of people who are capable of committing, or directing others to commit, cybercrime is increasing. Theoretically, the scope of cybercriminals is limited
because of the requirement of technical knowledge; mastery of computer languages and programming, network architecture; and capability of orchestrating technically complicated systems. Therefore, to commit cybercrime, people need to accumulate knowledge, skills and understanding about the above mentioned aspects. However, this barrier is no longer effective since the increasing development and expansion of the Internet that allows for the operation of cybercriminals is expanding along two axes. On one axis, the number of people who have the ability to commit cybercrimes continues, as ICT is increasingly integrated into education, business culture and individual lives. On the other axis, some people may use their technical expertise and knowledge to create and sell their products to those who do not, as tools to engage in cybercrime, for example, software cracking is used to break passwords to access computer networks.

Thirdly, lower ‘perpetration cost’ is claimed as a factor to explain the increased numbers of cybercrimes (Anderson et al., 2012). There are two ways of understanding the meaning of ‘perpetration cost’: The first is the cost of crime commission. Cyberspace presents unique opportunities for criminals to reduce their perpetration cost by one click and many people, or organisations can become the victim of cybercrime without moving to attack a target (Finklea, 2013; Katyal, 2001). Simply by accessing the Internet, cybercrime can be committed anywhere with limited or no travel expense. In fact, the use of computers and other equipment is recognised as a cheap means to perpetrate crime such as by copying intellectual property to a CD. The second understanding of ‘perpetration cost’ relates to the cost of preventing this kind of crime. In terms of preventing cybercrime, there are several operations which need to be taken into account. For example, the cost of training for enforcement officers, the cost of research and prediction of the issue of cybercrime, the cost of making a new law to respond to cybercrime, and the cost of equipment in responding to cybercrime must all be considered.

Naturally, cybercrime is often transnational in nature, occurring across boundaries and impacting on users in different countries. It is, therefore, inevitable that Vietnam will become both victim of, and host to, cybercriminals. It can be argued that cybercrime is a real and growing threat to Vietnamese security, its citizens and economy. Thus, in order to protect the country from cyber-attacks, a comprehensive and systematic response is required for Vietnam.
The following sections will focus on the fact that the Vietnamese governments are currently taking policy measures on cyber-security in general, and cybercrime in particular. There are also some pieces of legislation, although scattered here and there, that can deal with some cybercrime issues. Therefore, to effectively protect users from cyber-attacks, organisations, and individual users are expected to fully appreciate the current cyber security situation and measures in Vietnam.

4.4. The state of cybercrime regulation in Vietnam

This section aims to explore the efforts and initiatives being made by the Vietnamese government to regulate cybercrime. This section contains five subsections. Firstly, it starts with how to define cybercrime. Secondly, it moves forward to explore cybercrime regulation related policies. Thirdly, it continues to provide a description of the establishment of institutional regulatory mechanisms in relation to cybersecurity in Vietnam. Fourthly, it further provides a brief overview of other legislation implications for cybercriminal activities in Vietnam. Fifthly, it ends with exploring how cybercriminal activities are regulated under the Vietnamese penal code.

4.4.1. The lack of a legal definition of cybercrime in Vietnam

This section aims to examine how cybercrime is understood in the Vietnamese legal context, whether Vietnam has its own definition for such threat, and if not, to explore what makes it hard to define for Vietnamese authorities.

There are various terms which are used to refer to computer and Internet related criminal activity in the Vietnamese context, some of which include cybercrime, computer crime, information technology crime, and high-tech crime (Loi, 2007). Even though the terms cybercrime or computer crime or high-tech crime are in general use, these terms are interchangeable in the sense that they refer to crimes that are committed by using a computer, networks, and other technological tools. The term ‘computer crime’ was used in the early stages of computer and network technology before the Internet came into existence in Vietnam. However, the term cybercrime is now the most popular and widely used term (Wall, 2015/2012/2007). It is clear that cybercrime is a
very common word which has appeared in the most relevant journals, media and newspapers as well as in government debates in the Vietnamese context.

According to Vietnamese criminal law, the term ‘computer crime’ is understood to include crimes where perpetrators utilise a computer or computers to commit crime, and the term cybercrime refers to crimes that not only involve computers, but also a computer network. However, the term cybercrime has become a widely used and accepted term with regard to the ‘transformation of criminal and harmful behaviour by networked technology’ (Wall, 2007).

Generally, studies of cybercrime have indicated that one of the major problems regarding cybercrime relates to its very definition. There is no consensus about cybercrime definition at a national or international level (Yar, 2013, 2005; Brenner, 2010, 2012, Wall, 2015/2012/2007). Vietnam is not exceptional. In addition, the term cybercrime is not a legal term contained in any law, but it has been identified as being used by politicians, academicians, media and the public to refer to computer and network mediated illicit activities (Wall, 2015/2007). Furthermore, cybercrime has been identified as a typical and controversial topic for debate among officials, scholars, reporters, and others (Finklea, 2015).

Cybercrime is identified as a new term. There is no consensus on what it means legally. It is therefore necessary to account for what cybercrime is and what makes it different from traditional crimes. Agreeing with international scholars, Vietnamese criminologists argue that cybercrime may not be different from conventional crime, and it is merely a new way of committing traditional crimes as dangerous acts to society. Indeed, cybercrime consists of the same element criminals as traditional crimes (Dung, 2009; Loi, 2007). Cybercrime can be therefore investigated, prosecuted and punished under the current law (Dung, 2009; Loi, 2007). This viewpoint seems to be a common view in many countries in the world. For instance, Grabosky (2001) uses the metaphor of ‘old wine in new bottles’, illustrating that crime in the virtual world is no different than that in the physical world.

However, cybercrime is said to be different from traditional crimes because of its decentralisation, interdependence, accessibility and anonymity (Balkin et al, 2007). Cybercrime can be committed anywhere, without the kinds of barriers experienced in the physical terrestrial world, and traditional geographies of distance and location are
destroyed. This means that there is an absence of territorial borders in cyberspace (Johnson & Post, 1996). In other words, the location of the occurrence of a crime is changed from the physical terrestrial world to the virtual world, in which there are no states or international geographic borders (Brenner, 2004a). In addition, cybercrime can be automated by multiplying the number of discrete offences, with the advances of technologies, so cybercrime can quickly and easily attack thousands of victims in remote locations in different timeframes (Brenner, 2004a, 2004b). In other words, cybercrime will never have a shortage of vulnerable targets due to a billion users and a billion-plus computers (Hallam-Baker, 2008). Thus, cybercrime, with little effort, can generate hugely harmful effects on multiple targets, which it is generally not possible to do within the real world’s physical constraints (Brenner, 2012; Wall, 2007; Yar, 2005). For example, cybercrime can attack thousands of people by sending thousands or millions of spam emails, that may contain malicious codes, or they can easily send spam or phishing emails to thousands of victims. As a result, Brenner (2004b) asserts that ‘one-to-many victimisation is ... the correct default assumption for cybercrime.’

Moreover, with its anonymity, cybercrime is identified to be different from traditional crimes. It can be seen that criminals have to use various techniques to conceal their identity in order to ensure that the crime is anonymous, such as covering their face, wearing gloves in order not to leave any traceable elements at a crime scene (Brenner, 2012, 2010). Meanwhile, cyberspace is considered as a special environment that provides efficient methods to secure anonymity without physically being at the crime scene. Arguably, using different tools and advanced technologies to disguise identity, such as encrypted communication, anonymous remailers or zombie computers, cybercrime makes it difficult to be identified and apprehended (Brown, 2015); thus increasing the challenges for criminal law enforcement to investigate (Wall, 2015).

Similar to other countries, the Vietnamese authority’s approaches to understanding cybercrime are based on two groups of criminal activity, instead of a practical working definition. Firstly, cybercrimes are understood as crimes that infringe on the normal operation of a computer’s operating system and computer network, which are determined in Articles 224, 225, 226 of the 1999 Vietnamese Penal Code, then further inserted into two more provisional legal Articles 226a, 226b of the 2009 Vietnamese Penal Code. Secondly, cybercrimes are defined as crimes committed with the use of computers and computer networks, including all traditional crimes as defined in the
2009 Vietnamese Penal Code. Although this approach is identified as having the advantage of specifying the charges to be processed, this approach makes it easy to miss some criminal acts identified as cybercrime such as identity theft, cyber threat, contribute denial of service attack and so on, due to the development of technology. As a result, a number of cybercriminal activities have not yet been criminalised in the 2009 Vietnamese Penal Code.

Actually, cybercrime has many unique features that are different from crime in the physical world. At the same time, more traditional criminals are increasingly using advanced technologies to support their criminal acts. Thus, policy makers are finding it difficult to combine both in one specific definition to describe all aspects of cybercrime. As a result, the definition of cybercrime remains unclear.

4.4.2. Policy measures

In fact, Vietnam has no national ICT policy in relation to cyber security at present. However, concerned with information security, in 2010, the Vietnamese government approved the National Planning on Development of Digital Information Security Through 2020 (Decision No.63/QD-TTg, dated 13 January 2010). This Decision indicated the need for the promotion and development of information security that denotes the protection of network and information infrastructure safety, computer and data safety and information technology application. In regard to information security, the Decision focuses on the following objectives

- Ensuring network and information structure safety
- Ensuring safety for data and information technology applications
- Developing human resources and raising awareness about information security
- Legal environment for information security

In order to achieve the objectives above, this decision identifies several tasks. These tasks include the adoption of appropriate legal and regulatory frameworks, building institutions and technical infrastructure for information security assurance, conducting communication to raise awareness and develop technological capacity in information
security; implementing information security projects and programs, and, promoting and strengthening international cooperation. Each task has specific objectives to be achieved and detailed in implementing the tasks. This shows that the Vietnamese government is ready and committed to responding to the threat of information security or cyber-attacks, at least at policy level.

Following the Decision above, the Vietnamese government has issued Decree No.25/2014/ND-CP dated 07 April 2014, on prescribing the prevention and combat of crimes and other legal violations involving high technology. This legal document is the most important document regarding the activities of preventing, detecting and handling crimes and other legal violations involving high technology, including information and telecommunication technologies. This Decree shows that the government is committed to ensuring the prevention, detection and handling of crimes that involve information and communication technology. This Decree clearly provides the way to prevent, detect and handle crime use of information communication technology. The Decree also outlines the responsibilities of eight government agencies, including the People’s Committees at all levels, in regard to these issues (Decree 25/2014/ND-CP, Articles 18, 19, 20, 21, 22, 23, 24, 25 and 26). It can be clearly seen that the Vietnamese government has put more effort in to ensure the effectives of preventing, detecting and handling crimes in relation to information communication technology, including generally how to report crimes involved in information technologies for individuals, and organisations. The government has given each agency responsibility to ensure they deal effectively with typical crimes. However, the Ministry of Public Security (MOPS) has been appointed to be the leader. Others take their responsibility in their management field and also coordinate with the MOPS implementation of measures to prevent, detect and handle crimes that use information communication technology.
According to this Decree, the Vietnamese government manages cybercrime regulation as illustrated below:

Although, the Decree shows how to report cybercrime, it is still too general due to criminal activities in relation to information technology that are also considered as other types of crime. Thus, it has the same reporting mechanism as for other more conventional crimes. Individuals, for example, “have responsibility to report criminal use of information technology to Police agencies, People’s Committees of communes, wards, towns or to any agency or organisation” (Decree 25/2014/ND-CP, Article 12). Organisations which receive reports of crime or other violations of other laws in regard to information technology are responsible for handling these, if they are authorised, or to immediately inform the investigating agency or other authority according to the provisions of law.

4.4.3. Institutional regulatory mechanisms (IRMs)

The adoption of a legal and policy framework is nothing unless they are effectively implemented. In doing so the establishment of robust and specialised institutions is necessary to manage cyber security. In the Vietnamese context the government has been working on the establishment of institutions dedicated to ensuring the ICTs development and security.

The Ministry of Public Security (MOPS) is responsible for the protection of national security and for the maintenance of order in security (The law on People’s Public
Security Force, 2005). The People’s Public Security Forces include the People’s Security Force and the People’s Police Force. However, in terms of cybercrime regulation, the Department of Cybercrime Prevention is a part of the People’s Police Force. This is the national cybercrime prevention organisation and operates under the Ministry of Public Security. It has been established recently and its duties include: advising the Director General in directing, inspecting and guiding the Police force, prevention and criminal use of high technology in the country; carrying out preventive measures; detection and investigation of crime and the prevention and regulation of cybercrime.

Alongside the MOPS, there are two government institutions such as the Supreme People’s Court and the Supreme People’s Procuracy of Vietnam that involve dealing with cybercrime issues. They are given the power to control and supervise compliance with the law. They are empowered to exercise the right to initiate the prosecution of members of the public, and to ensure effective and uniform implementation of the law. Both the Supreme People’s Court and Supreme Procuracy are in charge of all implementations of law, including criminal law, in Vietnam.

The Ministry of Information and Communications (MIC) was created in 2007 from its predecessor, the Ministry of Post and Telematics, along with several departments from the Ministry of Culture and Information (The MIC, 2014). The MIC is responsible for both policy and regulations, including telecommunication and the Internet, and information technology and management of public services on behalf of the government (Decree No.132/2013/ND-CP, dated 16 October 2013). As the policy maker, the MIC’s main functions include submitting drafts of laws, ordinances, regulation, strategies and development plans to the Vietnamese government. At the same time, the MIC provides guidance on the implementation of laws and its regulation policy in relation to the Internet, as well as the development of strategies and plans.

According to Decree No.22/2013/ND-CP dated 13 March 2013 of the Government, the Ministry of Justice is a government institution, which is, on behalf of the Vietnamese government to perform the state management on development and implementation of laws and regulations, post-review of legal normative documents, control of administrative procedures, and legal dissemination and education. As a major policy maker and a state manager in the field of laws and regulations, people from this
organisation will deeply understand the regulation of cybercrime policy and its related issues.

The Vietnamese post and telecommunication (VNPT) is the country’s main Internet Service Provider (ISP). VNPT operates the national backbone network that connects the provincial operating companies in 63 cities and provinces and indirectly controls the country’s two leading mobile operators, Vietnam Telecom Company (Vinaphone) and Vietnam Mobile Telecom Services (MobiFone) (The White Book, 2014). Therefore, VNPT is supposed to have a wide range of experts, including policymakers and technical experts. As they are experts in this field, their response will be crucially important and valuable to this research.

The Corporate for Financing and Promoting Technology (FPT) is viewed as the second largest ISP in Vietnam (The MIC, 2014). It was established in 1988 and was initially named the Food Processing Technology Company. FPT was then renamed as the Corporation for Financing and Promoting Technology in 1990. FPT started to become an ISP in 1997 at the same time the Internet came to exist in Vietnam. As its second largest ISP, FPT provides Internet services that cover 59 out of 63 provinces/cities in Vietnam. Thus, the FPT plays an important role in providing services to its users in Vietnam. FPT will therefore have significant experience in dealing with service problems, including cybercriminal issues. Thus, choosing people from FPT to be interviewed should provide an important viewpoint in relation to the regulation of cybercrime policies and the difficult aspects they have experienced to deal with cybercrime issues. Furthermore, these participants might be able to provide possible recommendations that could be used in order to limit the appearance of cybercrime issues.

The Vietnamese Computer Emergency Response Team (VNCERT) is an organisation which operates under the Ministry of Information Communications. VNCERT was established at national level in 2005 under Decision No.339/QD-TTg with its functions as:

- Coordinating the activities in computer’s incident response, and a nationwide early warning system,
- Building standards and conformity in network security,

---

• Facilitating the development of Computer Emergency Response Team (CERT) in Vietnam,

• Being a contact point with other countries’ CERTs.

Authority of Information Security (AIS) is the state organisation, and was established in 2014 (Decision No.1281/DQ-BTTTT, dated September 9th 2014) by the Ministry of Information Communications. The AIS is responsible for the following:

• To formulate laws, policies and other legislative documents related to information security,

• To implement technical and procedural measures, including critical information infrastructure protection and building nation-wide infrastructure to protect cyberspace in Vietnam,

• To guide and support governmental agencies and other organisations to enhance and protect their information system from information security risks,

• To giving out early warning in information security,

• To ordinate activities on preventing SPAM in Vietnam,

• To monitor and inspect the protection activities on information security,

• To evaluate the level of information security in organisations and critical information infrastructure,

• To raise awareness, improve capacity and cooperate with international organisations in information the security area.

Several cyber security agencies have been established to ensure protection of national security currently, in line with the policy of the Politburo on promoting the application and development of information technology of the country. However, it does not seem to be effective because the number of cyber-attacks in Vietnam continues to increase significantly.
4.4.4. Other legislations with cybercriminal activities implication

4.4.4.1. The Law on Information Technology

The establishment of the 2006 Law on information technology is evaluated as a significant step to regulate Internet activities in Vietnam. The law was enacted to “ensure information technology application and development, and rights and obligations of agencies, organisations and individuals (hereinafter collectively referred to as organisations and individuals) engaged in information technology application and development activities” (Article 1). From this legal text, it can be argued that the creation of this law is to provide a good and open policy condition for attracting and promoting economic development in Vietnam rather than being concerned with the issues of cybercriminal activities. The reason for this is that this law does not pay more attention to cyber security; it just provides some legal texts regarding cybercriminal activities. There are only three articles regarding illegal activities. In terms of criminalisation, this law only sets out some prohibited acts instead of criminalising them. Meanwhile, cybercriminal activities can take a wide range of forms, and are more sophisticated. They are not simply all computer viruses or hackers. For example, Article 72 (2) simply states:

(2). Organisations or individuals must not engage in any of the acts listed below:

a, Hacking into, modifying or deleting information of another organisations or individuals in the network environment,

b, Obstructing the provision of services by the information system,

c, Preventing access to information by other organisations and individuals in the network environment, unless the law so permits,

d, Cracking, stealing or using passwords, codes and information of another organisations or individuals in the network environment, and,

c, Other acts causing loss of safety or confidentiality of information of another organisations or individuals which is exchanged, transmitted or stored in the network environment.
Although, this law has taken further steps to explain several terms in relation to Internet activities, it is still limited in terms of technical and legal terminology, such as the precise definition of computer, computer networks, hacking, phishing and so on. The following section will further illustrate this.

4.4.4.2. The Law on Network Information Security

The Vietnamese Assembly has approved the Law on Network Information Security on 19th November 2015. It came into effect on the 1st of July 2016. This Law was created for a number of reasons, as stated in the government report to National Assembly (Report No. 509/TTr-CP, 24 May, 2014) as follows:

i) The Internet has become the centre of the economy and society of every nation, including Vietnam. Vietnamese authorities have found that the Internet is becoming an environment for new threats and Vietnam must find ways to overcome these, making Vietnam become an industrialised and modernisation country, to thrive in a competitive world and globally.

ii) The duality of advanced technology is a challenge for law enforcement due to the appearance of many acts of abusing the Internet to transmit, store, distribute false information, malicious, violate legitimate rights and interests of individuals and organisations, even governments.

iii) Many individuals, organisations and even governments are more frequently faced with increasingly various types of network attacks. Here are some examples: defacing of new sites, fraud, denial of service attacks, malware and computer viruses, spam, identity theft, data destruction, disrupting the operation of information systems, spyware, and attacks on the banking system, online sale network, phishing. Particularly, Vietnam and other countries in the world are facing many threats, from criminal behaviour in cyberspace due currently to many individuals, organisations at the national level using cyberspace as a platform to steal, compromise or destroy important information, data from other individuals, organisations and even other nations.

iv) There is still a lack of legal regulation in the field of information and communication technology needed to keep pace with the current state of social development and international integration. Particularly, there is no law to regulate all aspects of
information security. The previous legal regulations focused only on a single and particular field in each narrow range such as the Law on Electronic Transactions, the Law on Information Technology.

The establishment of the Law on information security was supposed to institutionalise all national regulation information protection policies in order to meet the requirement of sustainable development – economic society, protection of information and information systems on the one hand. On the other hand, it was also supposed to contribute to and ensure national security, sovereignty and national interests, in line with economic conditions, the society of the country in the current period and in the foreseeable future. Furthermore, it is a special foundation to meet the requirement of international economic integration, ensuring conformity with the provisions of the Constitution and legal system of Vietnam. Moreover, the creation of the Law on Information Security aimed to ensure information security safety proceeded in the direction of modern, integrated and long term stability, meeting the requirements of safety information for the development of economic, social and national security.

The establishment of this law is, generally, a significant step to expand Vietnam’s existing legal regulations in relation to information communication technology particularly, and to increase the focus on information security. This Law, to some extent, provides several clearer and broader concepts, especially, the concepts of personal information and data processing. For example, personal information is defined as ‘information associated with the identification of a specific person’ (Article 3(15)). This definition does seem to have a broader scope when making comparisons between this definition and the existing definition in Decree 72/2013/ND-CP on the Management of Internet use where ‘personal information’ is defined as ‘information which is attached to the identification of the identity and personal details of an individual including name, age, address, people’s identity card number, telephone number, email address and other information as stipulated by law’ (Decree 72/2013/ND-CP, Article 3(15)). Even when compared with the definition in Decree 52/2013/ND-CP on e-commerce where it is simply meant as ‘contributing to identifying a particular individual, including his/her name, age, home address, phone number, medical information, account number, information on personal payment transactions and other information that individual wishes to keep confidential’ (Decree 52/2013/ND-CP, Article 3).
Particularly, this is the first time the term ‘cyberspace’ is given clearly. It is defined as ‘an environment where information is provided, transmitted, collected, processed, stored and exchanged over telecommunications networks and computer networks’ (The Law on Information Network security, Article. 3(2)).

In relation to activity in cyberspace, this Law does not criminalise any activity in cyberspace, it merely provides a list of ‘prohibited acts’. This list of prohibited acts is broader in scope and encompasses illegal acts by third parties more comprehensively in comparison with the prohibited acts that were set out in the Law on Information and Technology. Indeed, the ‘prohibited acts’ in cyberspace outlined out in this Law includes not only the spreading of spam or malware but also ‘illegal collecting, utilising, spreading or trading in personal information of others; abusing weaknesses of information systems to collect or exploit personal information’ (Article 7(5)). Moreover, Article 7(6) of this Law describes that hacking ‘information on clients that lawfully use civil cryptographic products’ is prohibited.

Furthermore, and like the current Law on Information and Technology, this Law does not either define the term ‘cybercrime’ or what kind of activity in cyberspace can be considered as criminal. Moreover, this Law does not give clearer definitions of what sanctions should be applied for the violation of this law. It is defined too generally as ‘Individuals violating this law shall, depending on the nature and severity of their violations, be disciplined, administratively sanctioned or examined for penal liability and, if causing damage, pay compensation in accordance with the law’ (Article 8). Nevertheless, this Law is a significant development of legal regulation in relation to activities in cyberspace in Vietnam.

4.4.5. The Vietnamese Penal Code

The main aim of this section is to explore how the Vietnamese Penal Code has responded to cybercrime. The section is based on three main arguments. The first argument is that the Vietnamese Penal Code cannot effectively respond to cybercriminal activities due to several incompatibilities between the natural characteristics of cybercrime and the nature of the criminal law. Some criminological theories will be used to illustrate the nature of this issue. The second argument is that Vietnamese Penal
Code has less coverage of cybercrimes. The third argument is that Vietnamese criminal law suffers from legal linguistic problems compared with the nature of characteristics of cybercrime and cybercriminal activities and the recognition of international standards (particularly the convention of cybercrime).

The Vietnamese Penal Code plays a prominent role in the life of Vietnamese society and performs several functions. One of the main functions or tasks of the law is to ‘define crimes and the penalties for offenders’ (Article 1). It is viewed as an ‘effective instrument to prevent and combat crime’ (The Penal Code). The Vietnamese Penal Code cannot, however, simply be an instrument for crime prevention or deterrence. It also defines crime and punishment. From this point of view, it can suggest that without the criminal law there would be no crimes, no conduct could count as criminal. Put it in simple terms, the Penal code is the cause of crime. This seems to be at conflict with the purpose of the Penal Code itself. In other words, this is a circular argument (Fafinski, 2009). Similarity, as Michael and Adler (1933) have earlier asserted: ‘If crime is merely an instance of conduct that is proscribed by the criminal code, it follows that the criminal law is the cause of crime’ (p. 5).

From this viewpoint it can be seen that the traditional perception of criminal law as establishing prohibitive norms that forbid certain human conduct (Quinney, 1970) or creating disciplinary norms that bound acceptable behaviour (Foucault, 1977) is said to be unhelpful (Fafinski, 2009) to account for the nature of crime and the reasons for criminalisation. Thus, to have a clearer explanation of the nature of crime and reasons for criminalisation, the social setting in which the conduct occurs should be taken into consideration. For example, Packer (1968) contends: ‘Crime is a socio-political artefact, not a natural phenomenon. We can have as much or little as we please, depending on what we choose to count as criminal’ (p. 364).

Like other countries’ criminal law, the purpose of Vietnamese criminal law is said to be the protection of a particular set of ‘the interests of the state, the legitimate rights and interests of citizens and organisations’ and ‘the socialist law order’ (The Penal Code, Article 1). By giving a set of interests warranting protection from harmful behaviour, the criminal law should provide for the ‘smooth functioning of society and the preservation of order’ (Devlin, 1965, p. 5). However, it is worth asking here whether the harm resulting from cybercrime is as considerable as those harms traditionally recognised by Vietnamese criminal law. It can be seen that in the real world, criminal
acts are historically linked in social conscience as harmful, since they result in infringing personal interests widely recognised as legitimate and demanding respect from other individuals and from the state. In fact, the interests of the state, the legitimate rights and interests of citizens and organisations and the Vietnamese society order are clearly protected by the Vietnamese Penal Code. The creation of cybercriminal activities in Vietnamese Penal Code is confirmed in that the harm resulting from cybercrime can be the same as traditional crimes. However, the harm resulting from cybercrime may be viewed less than the harm resulting from traditional crime. There are a number of reasons to explain this argument including the nature and unique characteristics of cybercrime, and the virtual environment that has created cybercrime as latent and hidden, thus, the harm is not easily proved. In addition, the victim of cybercrime may not understand that they have been harmed due to the consequences of the invisible nature of cybercrimes. Even some types of cybercrime may not be considered harmful at all.

In addition, regarding the second natural incompatibility between the nature and characteristics of cybercrime and the nature and characteristics of the criminal law, is in relation to the effect of Vietnamese criminal law on criminal acts in general and cybercriminal acts in particular. In other words, is the nature of the problem one of jurisdiction? Cybercriminals have demonstrated that it cannot be easily limited to one or two countries. Cybercrimes can be committed anywhere, at any time or at the same time across multiple jurisdictions as its nature is transnational via the Internet (Cangemi, 2004). Although Vietnamese Penal Code states that the effect of the law is on criminal acts committed both inside and outside of the boundary of its country. However, with its transnational nature, cybercrime can create a significant challenge for Vietnamese authorities. Vietnamese authorities are confronted with a number of questions to be asked, for instance, whether Vietnamese Penal Code is compatible with others; if there is any conflict between Vietnam and others; whether Vietnam has signed any international treaty which relates to cybercrime, and, how Vietnamese authorities would process its legal procedures to find and collect evidences and so on. Even if Vietnam has signed international treaties or international laws, the challenges for Vietnamese authorities remain. The problem of multiple jurisdictions can be solved essentially by cooperation among various law enforcement agencies and countries (Moitra, 2005; Wall, 2007). However, it is not easy to establish cooperation between different
countries. Even if cooperation between countries can be established to deal with cybercrime, the definition of cybercrime or cybercrime laws in those countries it can be a problem to maintain that cooperation (Nasheri, 2005). Definitions of cybercrime and/or laws that define cybercrime can be different from one jurisdiction to another (Moitra, 2005). As the laws are not identical, it may become an obstacle to the establishment of cooperation and investigation of cybercrime. The nature of cybercrime as often transcending national boundaries is described as follows:

“A hacker, with or without dishonest intentions, may for instance sit in London, and, through an international telephone system, enter or try to enter a computer in New York or vice versa. More complex ‘chains’, involving computer systems in a number of countries before the ‘target’ computer is accessed are entirely possible” (The Law Commission, 1989).

Theoretically, the criminal law is said to be workable and viable within a state’s sovereignty (Fafinski, 2009). Hart (1961) has argued that the law is simply an aspect of sovereignty of a nation such that the necessary and sufficient conditions for the truth of a proposition of law are simple: that the law internally is logical and consistent and that state power is being exercised responsibly. The same argument can be found in Cangemi (2004), the author argues as follows:

“Under the traditional principles of international public law, States have jurisdiction only on the territory where they exercise their national sovereignty. There is thus a conflict between cybercrime, which is global in scale, and police activities that are confined to national borders” (p. 166).

The inherent problem with jurisdiction in relation to cybercrime is mentioned by Johnson and Post (1996) as follows:

“The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be regulated, satisfactorily, by any current territorially based sovereign” (p. 1375).

As mentioned above, the Vietnamese Penal Code is an important player in responding to cybercrime since it was recognised by this law. However, from its beginning and even since it was amended and supplied some provisional articles related to
cybercriminal activities, the law still suffers from defects, formulate problems, and even less coverage of cybercriminal activities.

Like other countries, the Vietnamese Penal Code is the main law dealing with cybercriminal activities. Although a number of legal regulations in relation to information communication technology have been created in Vietnam such as the Vietnamese Electronic Transaction Law 2005, Vietnam’s Information Communication Technology law 2006, Vietnam’s Intellectual Property law 2005 (amending and supplementing 2009), for example, these laws are recognised as legal regulations to focus on creating good and open conditions for attracting and promoting the economic development of Vietnam rather than regulating cybercriminal activities. They also concentrate mainly on the promotion of development and application of information communication technology in Vietnam. Nevertheless, they have come to play important roles to explain several terms that related to the Internet and Internet activities.

Cybercriminal activity was recognised in the Vietnamese Penal Code 1999 two years after the Internet was officially introduced in Vietnam. For the first time, the law has inserted the creation of three provisional articles in relation to cybercriminal activities. It included the offence of creating and spreading, scattering electronic virus programmes; the offence of breaching regulation on operating, exploiting and using computer networks; and, the offence of using illegal information in computer networks. This law has been further amended and has inserted two more legal provisional articles with regard to cybercriminal activities in 2009, this is because the Vietnamese government recognised ‘some socially dangerous offences which have emerged in the process of socioeconomic, scientific, and technological development, as well as international integration, as crime’ (Number 49/NQ/TW, 2005). Thus, a number of provisional articles with regard to cybercriminal activities in Vietnamese Penal Code have been increased from three to five in total in 2009.

However, in general, it could be said that the Vietnamese Penal Code has not covered all aspects of cybercriminal activities in comparison with other countries. Based on these provisional regulations of that law, cybercrime is identified in that law as illustrated in Table 4.1 below:
Table 4.1: Cybercrime as provided by the Vietnamese Penal Code 2009

<table>
<thead>
<tr>
<th>No</th>
<th>Offence</th>
<th>Article/Clause</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unauthorised Access to information system</td>
<td>Article 226a (1)</td>
</tr>
<tr>
<td>2</td>
<td>Unauthorised using credit card and banking information by insiders</td>
<td>Article 226b(1(b))</td>
</tr>
<tr>
<td>3</td>
<td>Impeding the information system</td>
<td>Article 225</td>
</tr>
<tr>
<td>4</td>
<td>Illegal access to data of state secrecy, information system in service of national defense and security</td>
<td>Article 226a (3(a))</td>
</tr>
<tr>
<td>5</td>
<td>Illegal access to National Information Infrastructure, National Grid Operation Information system, Banking and Financial Information System, Traffic Control System</td>
<td>Article 226a (3(b))</td>
</tr>
<tr>
<td>6</td>
<td>Unauthorised interference to information system</td>
<td>Article 224 (1)</td>
</tr>
<tr>
<td>7</td>
<td>Obstructing information system operation</td>
<td>Article 225 (1)</td>
</tr>
<tr>
<td>8</td>
<td>Computer related – fraud</td>
<td>Article 226b</td>
</tr>
</tbody>
</table>

From the provisional regulation of these five articles, it can be seen that the Vietnamese criminal law 2009 has neglected many significant issues related to cyber stalking or online abuse, harassment, cyber threat, spamming and moreover intellectual property rights, copyrighting and trade marking or patenting of electronic information, among other things that have not been addressed by this law.

The provisions of these articles have also missed some very important issues of cyberspace and electronic transactions which are related to the protection of trademarks and domain names against online illegal forgery, counterfeiting and copying, which are not criminalised.
There are no provisions for criminalising acts related to online gambling, prostitution and temptation, including child pornography, cyber terrorism, terrorist websites or the commission of organised crime by using information systems and information networks.

Furthermore, in relation to cybercrime, the Vietnamese Penal Code suffers from legal linguistic problems compared to the characteristics of cybercrime and international standards. This can be seen from the initial recognition of cybercrime in Vietnamese legal framework. Three groups of cybercriminal activities have been created in the Vietnamese Penal Code without any definition of such crime or clearer explanation of the term in use, such as what a computer virus means and so on. This problem remained until 2006 when the Vietnamese Information Communication Technology law was created and the general terms relating to information communication technology were explained, some of the features of cybercrime have also been explained but are very limited such as virus, spam. Furthermore, the explanation of the terms of legal linguistic definitions and specific types of cybercrime offenders were described in the Vietnamese Penal Code in 2012 under the Circular No10/2012 dated 10 September 2012. This Circular explains and guides application of the provision of the Criminal code offence in the field of information technology and telecommunications.

In summary, the 2006 Information Communication Technology law and the Circular No10/2012 have given a clearer picture of the problems of the 2009 Vietnamese criminal law in terms of legal linguistic issues. By giving a definition of the terms and guiding how these legal provisions can be used to apply to cybercrime in different legal documents, the 2009 Vietnamese criminal law has illustrated that the law itself is not good enough for Vietnamese authorities to apply it directly in response to cybercrime. Thus, a number of questions should be asked here as to how Vietnamese authorities understand such legal provisions related to cybercrime; how they make sure that they can apply these legal provisions for cybercrime the correct way to explain and guide later, and how effective these legal provisions can be. The next section will further explore what challenges cybercrime creates for Vietnamese authorities in responding to it.
4.5. Cybercrime regulation in Vietnam – key challenges

4.5.1. The challenges for the Police

As mentioned above, the growth of the Internet associated with the revolution of technology has significantly changed many aspects of society, including criminal activity. It has been shown to have changed the nature of criminal activities and created one of the most challenging areas for law enforcement officials (Toffler and Toffler, 1995; Byrne and Marx, 2011). It is plausible that changes to criminal activity will generally affect the role of law enforcement agencies, particularly the role of Police in regulating it, especially, regulating the cybercrime phenomenon, this has been shown by a number of scholars. For example, Walker (1997) asserted that the changing characteristics of offenders would also change the characteristics of Police officers, such as officers becoming more technologically proficient, and would therefore create a new breed of Police officer.

This sub-section considers the challenges Vietnamese Police face in dealing with cybercrime. Based on the nature of cybercrime, this research argues that Vietnamese Police officers will face a number of problems in regulating cybercrime. These problems include, but are not necessary limited to, the complexity of technology as well as the Vietnamese criminal law, and Vietnamese criminal procedure law, jurisdiction, collecting evidence, arresting suspects, level of victimisations, and supporting resources. However, due to the limitations of time, financial support, and purpose of this study, this research is not focusing on examining in detail each challenge set out above.

In the Vietnamese context, the role and function of the Police is defined as “the protection of national security and maintaining social order, social security” (The Law on the People’s Police, Article 4) of the State Socialist Republic of Vietnam. This means that the police’s tasks are territorially based: located in, and derived from its authority within Vietnam national territories. It is, therefore, understandable that Vietnamese Police have no legal authority to conduct an investigation in another country’s territory. This makes it difficult, or even impossible, for Vietnamese Police to investigate transnational crime in general, as well as cybercrime in particular, and to
apprehend cybercriminals who are located in another country. It is increasingly difficult for the Police to collect evidence, and to arrest a suspect in cybercrime cases.

Regarding challenges of collecting evidence, Vietnam has the separation of legal procedure for the operation of criminal investigation as well as criminal prosecution and criminal adjudication. The criminal procedure law of Vietnam determines “the order and procedure of instituting, investigating, prosecuting and adjudicating criminal cases” (The Vietnamese criminal procedure code, 2009). It means that every single operation of criminal investigation must be based on this code.

The evidence is, generally, the foundation of any criminal case, including those involving cybercriminal cases. Thus, the acts of searching, examining, collecting, and preserving the evidence in criminal cases, as well as cybercriminal cases, are strictly regulated by criminal procedure code and other legal documents in Vietnam. According to the Vietnamese criminal procedure code (Article 64), evidence is defined as: (1) exhibits; (2) testimonies of witnesses, victims, civil plaintiffs, civil defendants, persons who have interests and obligations related to the cases, the persons arrested, persons kept in custody, the accused or defendants; (3) Expertise conclusions; (4) Document records of investigating and adjudicating activities, and other documents and related evidence. As the foundation of any criminal case, evidence is a crucial factor that is collected “in accordance with the order and procedure prescribed by this code” and “can be used by the investigating bodies, procuracies and courts as grounds to determine whether or not criminal acts have been committed, who committed such acts as well as other necessary aspects related to the cases in order to get the proper settlement of the cases” (The criminal procedure code, Article 64). Therefore, errors in gathering, developing, or presenting evidence can have dire consequences in every single step of the criminal process in Vietnam. Especially, in the criminal investigation process, it could lead Police officers to go in the wrong direction, or misinterpret any action in support of their investigation. Furthermore, it will lead Police officers to come to the wrong conclusion at the end of their investigation. It will have serious affect on other steps in the process and might lead to a wrongful conviction after a criminal trial.

According to the Criminal Procedure Code (Article 65), evidence can be collected by: (1) summons of persons who know about the cases to ask and listen to their statements on the matters pertaining to the cases; (2) soliciting expertise; (3) conducting research;
The evidence in cybercriminal cases is increasingly important because the evidence of cybercriminal cases is not the same as physical evidence. Thus, collecting evidence in cybercriminal cases is increasingly challenging for Police officers, especially when evidence is located/existed in other countries.

Criminal evidence is a crucial factor from the beginning of an investigation, to the prosecution and adjudication of cases. The collection of evidence is a crucial part of a cybercrime investigation. Unlike obtaining physical evidence, obtaining appropriate evidence of cybercrime by investigation can be an extremely difficult and complex problem, a new form of evidence has been created – digital evidence (Kerr, 2005). This is a result of the intangible and often transient nature of data, particularly in a network environment (Walden, 2010). Digital evidence (also called digital forensic evidence) is the product of the digital forensics process (Cohen, 2008, 2010). The digital forensics process encompasses a wide range of activities such as investigating, collecting information, preserving the information from inadvertent changes, analysing the information, and reporting the results of the examination (Casey, 2011). Digital evidence combines computer science concepts, including computer architecture operating systems, files systems, software engineering, and computer networking as well as legal procedures that describe criminal and civil litigation, cyberlaw, and rules of evidence (Kerr, 2009; Whitcomb, 2002). Digital evidence comes from a variety of sources, including computer devices, network servers such as websites, electronic email and social networks, and network hardware (Casey, 2011; Brown, 2010).

Conly (1989) argues that collecting digital evidence can be challenging for a number of reasons: Firstly, digital evidence can easily be altered, copied, stored, or moved. Secondly, because computers use electricity, thus, power interruption may cause harm to digital evidence. Even when they are switched off, computers may be harmed. Thirdly, magnetic fields may harm or destroy magnetic storage media. Furthermore, Huang and Frince (2007) provide other challenges that digital evidence provides in comparison to physical evidence as follows: Firstly, digital evidence may exist for a period of time, ranging from a fraction of a second to many years. Secondly, digital evidence might be found in an amount of data ranging from a single bit to a multi-gigabyte file. Thirdly, all of the relevant digital evidence may be found in a single
cluster on a hard drive or spread across many servers on the Internet. Adding to the problem of collecting digital evidence, it is said to have negatively impacted by way of claiming for the nature of technology errors, technical malfunction, and prejudicial interference (Walden, 2010).

In fact, the issue of collecting evidence from abroad can be practically implemented by the following two alternative approaches. First, Police officers have to make a formal request that has historically been used to obtain evidence in the same way as in transnational criminal cases. The other option is to make an informal request for cooperation. However, each method will come up with several difficulties. For example, the first method requires a significant amount of paperwork and must progress through a number of process gates such as Prosecution Office, Judge’s Office, Ministry of Justice, Ministry of Foreign Affairs and so on, thus, it will take a long time. In addition, a letter request has to be clear as to its requirements and contain sufficient evidence for a foreign authority to understand that a crime has been committed and the evidence sought that relates to that crime is located or existed in the country requested for assistance. Furthermore, the formal letter and related documents must be translated into the language of that country. In the partner country, they may have a number of processes similar to Vietnam since they receive many such formal requests. Once the evidence has been collected, it will follow the same process. Thus, the problem of this formal approach is time consuming.

The second approach involves informal cooperation between Police organisations in the respective countries. This is considered the most effective way of obtaining evidence from abroad in cybercrime investigations (Brenner, 2010). The single greatest advantage of this approach is the speed with which evidence can be preserved and collected (Brenner, 2010). However, this approach depends very much on the relationship between Vietnamese Police officers and Police officers in the country in which the evidence is located. Further, it depends to a great extent on the relations that exist between the two countries.

Arresting suspects in cybercrime cases can provide other challenges for Vietnamese Police. Similar to collecting evidence, arresting suspects in cybercriminal case can be a significant challenge posed by the nature and characteristics of cybercrime. The key challenge is how to arrest suspects when they are located in other countries.
Arresting suspects in cybercriminal investigation cases is also an important task of the Police. Arresting a suspect will generally be applied to bring crimes to justice, prevent further crimes, or if it is believed a suspect would cause difficulties to the investigation or prevent them from continuing to commit other offences (Criminal procedure code, 2009). However, arresting suspects in cybercriminal investigation cases will not be easy, and may be extremely difficult, due to the fact that the suspect will be located in other countries or even multiple jurisdictions. Although Police can, in fact, have two alternative methods to gain custody of a suspect who is in another country. One is to rely on extradition, the formal approach that is historically used to transfer a suspect from one country to another. The other option involves informal, unilateral action by the country seeking the suspect. However, these approaches will create a wide range of issues that any such Police investigation will be faced with.

The extradition approach requires a treaty between countries. Thus, it will not be considered without an extradition treaty. In fact, not all countries have extradition treaties with other countries, even developed or developing countries, Vietnam is no exception. The importance of international cooperation in combating transnational crime, including cybercrime, was identified in Part 8 of the Penal Procedure Code of Vietnam (Chapter 36 and Chapter 37) that regulates international cooperation in criminal proceedings. This part provides the basic principles for international cooperation between Vietnam and another country in criminal proceedings. This is the legal basis for Vietnam’s competent authorities to carry out mutual legal assistance in criminal issues, extradition of criminals and extradition of offenders to foreign countries. Pursuant to the provisions in the Penal Procedure Code of Vietnam, mutual legal assistance in criminal matters between Vietnam and other countries is implemented on the basis of international conventions that Vietnam is a contracting party, on the principle of reciprocity and international practices. Even when Vietnam has an extradition treaty with another country, the implementation of extradition is often a hard task and with more complicated processes, many government organisations could be involved.

In addition, Vietnamese Police may practically be faced with the refusal of a request to extradite a suspect who is located in another country, especially that country’s own citizens. Each country has its own legal reasons to refuse extradition requests, even in the international formal agreements between countries. For example, as regards refusal
of extradition, in general, according to the Vietnamese Criminal Procedure Law (Article 334), extradition will be refused for the following cases: (1) persons requested to be extradited are Vietnamese citizens; (2) under the provisions of the laws of the Socialist Republic of Vietnam, the persons requested to be extradited cannot be examined for criminal liability or serve penalties if the statute of limitations has expired or for other lawful reasons; (3) the persons have been convicted by the courts of the Socialist Republic of Vietnam under legally valid judgments for the criminal acts stated in the extradition requests or the cases have been ceased under the provisions of the criminal procedure code, and (4) the persons requested to be extradited are residing in Vietnam for reasons of being possibly ill-treated in the extradition requesting countries on the grounds of racial discrimination, religion, nationality, ethnicity, social status or political views. Therefore, it can be understandable that many countries have several reasonable reasons for refusing an extradition request. Therefore, the competent authorities of Vietnam can implement a request of mutual legal assistance in criminal matters with states that Vietnam has not signed a convention on the principle of reciprocity, but in contravention of the laws of the Socialist Republic of Vietnam, international laws and international practices.

At present, Vietnam has signed 14 bilateral treaties of mutual legal assistance of criminal cases, of which 13 treaties contain provisions of mutual legal assistance and criminal extradition. Moreover, apart from eight international conventions related to the prevention of terrorism, Vietnam has signed the UN Convention for fighting against transnational organized criminals and the UN Convention for fighting corruption which have many provisions on mutual legal assistance and criminal extradition.

Other challenges for Police investigations are resource limitations, in terms of staff, equipment, training and funding. Police are not only faced with the problems of lack of jurisdictional and technical difficulties, they are also confronted with the problems of dealing with a huge number and variety of victims of cybercrimes, and many locations, regardless of borders. The victims of cybercrime include individuals, businesses, various agencies, corporations, organisations and governments. Funding is essential for supporting law enforcement agencies. Lack of funding can be one of the main obstacles to effectively regulate cybercrime in terms of providing training, and of providing high technology equipment and travel.
4.5.2. The challenges for prosecutors

According to the Vietnamese Constitution and Penal Code, as well as the Vietnamese Criminal Procedure Code, and the Law on organisation of the People’s Procurator, the people’s procuracies perform several functions and tasks. However, in terms of criminal investigation, they have an important role to play in “exercising the right to prosecute and supervise the observance of the law in investigation and adjudication of criminal cases”, and “supervising the observance of the law in the execution of judgments and decisions of the courts”, and “directly conducting investigation in some types of offences against judicial activities, committed by officials of judicial bodies” (The Vietnamese constitution, Article 137; Vietnamese criminal procedure code, article 37).

From the legal text above, it can be said that Vietnamese prosecutors play a vital role in the Vietnamese criminal process, including cybercrime cases. As mentioned already in this thesis, there are several challenges facing Vietnamese law enforcement agencies such as Police investigation officers, prosecutors, and judges today, who seek to successfully investigate, prosecute, and judge cybercrime cases. These challenges include: i) Implementation of relevant provisions of cybercrime law; ii) Understanding the digital evidence; iii) Collecting evidence abroad; and, iv) Being able to arrest suspects from abroad. However, based on the primary role of prosecutors to decide whether or not to approve the decisions of investigating bodies and judges, this research is going to examine how challenges Vietnamese prosecutors are faced with when implementing their power as it is prescribed in Vietnamese law. At the same time, this thesis will examine the challenges for Vietnamese prosecution authorities in dealing with the problem of jurisdiction in order to successfully prosecute cybercrime cases. In fact, before exploring the challenges for Vietnamese prosecution authorities created by cybercrime, it is necessary to describe briefly the notion of jurisdiction.

According to international law doctrine, the jurisdiction of a state is broadly regarded as a certain power (Beale, 1923), authority (Westlake, 1904) or competence (Brownlie, 2008) of the State. In particular, jurisdiction can be understood as ‘the power of the state under international law to regulate or otherwise impact upon people, property and circumstances’ (Shaw, 2008). This jurisdiction confers the legal power to a state, to make, implement, and adjudicate laws. This power is generally most effective when it is exercised within a state’s territorial borders (Henkin, 1993). This means that every
nation has complete authority to regulate its nation within its borders. Outside a state’s borders is, of course, another nation, with complete authority over its own territory, foreclosing the exercise of jurisdiction by any other nation.

The nature power of prosecutors in Vietnam is based on its national laws, meanwhile laws, indeed, are based on borders and jurisdiction. For instance, the Vietnamese Criminal Procedure law “prescribes the order and procedure of instituting, prosecuting... criminal cases”, and “functions, tasks and powers of” the prosecution office. The law (The Vietnamese Criminal Procedure law, Article 2) also confirms that “the Criminal procedure law applies to all criminal proceedings on the territory of the Socialist Republic of Vietnam”, including the action of prosecutors of Vietnam, save for those exceptions provided for/ by the international agreements which Vietnam has signed or acceded. Similarly, Article 5.1 defines Vietnamese criminal law as being applicable to all criminal acts committed within the Vietnamese borders, and may also be able to apply to criminal acts committed outside of Vietnam by Vietnamese citizens (Article 6), save for those exceptions provided for/by the international agreements which Vietnam has signed or acceded (Article 5.2). Traditionally, jurisprudence on jurisdiction assumes that the law is made for a definite group of people residing in a certain territory where the government of that territory will prescribe the law and execute the law. Legal rights and responsibilities are therefore largely dependent on where one is located. Reflecting these ideas into the Vietnamese context, one could say that Vietnamese laws are made for Vietnamese people residing in Vietnamese geography, and the Vietnamese government is given power to regulate all acts within its borders. It can be seen in the principle of both Vietnamese criminal law and criminal procedure code as being applicable within the whole territory of the Vietnamese State. They are also both concerned with “protecting the socialist regime, safeguarding the interests of the state, the legitimate rights and interests of citizens, organising and protecting socialist legal order” (Article 1, The Criminal Procedure Code, Article 1, The Vietnamese criminal law). It is therefore essential to define where the offence was committed.

As mentioned in this research, with the growth of Internet based activities, notions of borders and jurisdictions are becoming increasingly irrelevant. The virtual world brings people together from all over the world and transnational activities commonly become a part of daily life, including transnational criminal activities such as cybercrime. Cybercrimes have increasingly eroded the traditional elements of legal authority.
Traditionally, the Vietnamese prosecutors on behalf of their government, are given the power to regulate cybercriminal activities, but this is significantly challenged by the question of how do Vietnamese prosecutors implement its power to prosecute cybercrime, and how can they apply relevant laws to prosecute cybercrime?

As mentioned previously, the power of Vietnamese prosecutors is prescribed in Vietnamese law. If any criminal action appears, the prosecution authorities must use its power to impose relevant sanctions. The implementation of this power depends on the ability of the Vietnamese prosecution authority to exercise physical control over, or to otherwise impose, coercive sanctions on cybercriminal activities. The implementation of its power, traditionally, exists in the physical world, over Vietnamese territories, and Vietnamese citizens or others who live or stay in Vietnam. However, cybercrime is not the same as traditional crime which the prosecution authorities deal with on a daily basis. Cybercrime has distinctive characteristics which have been offered by the advanced technology associated with the Internet. Boundaries in the virtual world do not necessarily correspond to the geographical boundaries of the physical world. As a consequence, the power of Vietnamese prosecution authorities, which has been based on physical control, becomes inadequate.

In addition, the most fundamental characteristics of cybercrime are its global reach. Cybercrime can make crossing borders easy, perpetrators working through the Internet can instantaneously operate anywhere in the world. Simply put, cybercrime eliminates the physical limits of time and space. Meanwhile, traditional crime is always subject to conditions of time and space constraints. Moreover, the extent of the harm caused by traditional crimes has generally been limited within the certain physical boundaries of the jurisdiction. The law of jurisdiction therefore regulates actions that are most likely to have effects solely in that jurisdiction. This means that its physical borders can limit the scope of the effect of traditional crime. However, the effect of cybercrime may not necessarily take place and have their effect within a confined geography. Cybercrime can take place anywhere, via the Internet. This means that cybercrime defies the notion of geography and distance. Consequently, the effects of cybercrime may be felt immediately throughout the world, regardless of location. Its effects are not merely confined to a certain localised area. These can have an impact on every location on the Internet instantaneously. It is easily viewed as “A declaration of the independent of
cyberspace”\textsuperscript{38} such as “Cyberspace does not lie within your borders” (Para. 3), cyberspace is different as it “is a world that is both everywhere and nowhere, but it is not where bodies live” (Para. 6) or even, “...legal concepts of property, expression, identity, movement, and context do not apply to” (Para. 9) cyberspace (Barlow, 1996).

To sum up, the phenomenon of cybercrime is eroding the link between geographical locations and creates challenges for Vietnamese enforcement agencies on behalf of the Vietnamese government to regulate it. Especially, the prosecution authorities are limited to exercise their power to prosecute cybercrime by the characteristics of cybercrime. Taking into account the problem of jurisdiction for the limitation of the prosecution authority to exercise its legal rights to prosecute cybercrime cases, this can further increase the opportunity for cybercrime to expand.

4.5.3. The challenges for judges

In the previous two sub-sections, the challenges posed by cybercrime to ISPs, as well as Police and prosecutors, have been presented. This sub-section explores the challenges for Vietnamese judges in regulating cybercrime. The challenges for Vietnamese judges in regulating cybercrime can have many different aspects. However, this research is keen to explore two important aspects which are identified as central to cybercrime regulation in Vietnam. Firstly, the challenges of understanding and applying digital evidence in cybercriminal cases will be faced. Secondly, the impartial independence of judges can be another challenge for judges in Vietnam.

Judges play a crucial role in criminal process in Vietnam. They play a part at the final stage of the criminal process. In other words, judges play a gatekeeper role in finally determining whether or not persons are convicted of any crime that is prescribed in criminal law. Evidence is considered as a primary aspect as regards the final determination of the judge in criminal cases. Evidence helps judges make their determination on criminal cases (Kerr, 2009). Therefore, judges are required to have a deep knowledge, and understanding of, the evidence on which to base their final decision. In cybercriminal cases, judges are not simply facing physical evidence as they

\textsuperscript{38} A declaration of the Independent of the cyberspace; see: https://projects.eff.org/~barlow/Declaration-Final.html (accessed 26/12/2016).
would do daily. They are facing a different type of evidence – digital evidence. Digital evidence is said to be a different context than other forms of forensic evidence because it exists only in the form of zeros and one, whereas other evidence has a physical manifestation (Kerr, 2005). This difference means that digital evidence can be perceived and understood differently from one to one judge in terms of handling and explanation (Kerr, 2005; Saferstein, 2009). An understanding of how digital evidence is derived is a critical factor in weighing the probative and prejudicial value of digital evidence as used in court (Cohen, 2008, 2010; Frowen, 2009; Kerr, 2009). This is a big challenge for judges in Vietnam. The challenges of understanding digital evidence are included, and not necessarily limited to, the characteristics, collection, preservation and application of digital evidence.

The challenge of understanding digital evidence requires an understanding of both the technology and the vernacular (Kerr, 2009). An understanding of both the technology and its language is not easy, and can be especially hard for judges, who traditionally deal with physical evidence. However, this is considered as the most important step in computer forensics, that of making a forensically correct copy of the evidentiary medium (Brown, 2010). It also ensures that the original evidence is not compromised in any way, a copy of the evidence medium is created, and the forensic examination and analysis are performed on the copy (Ieong, 2006; Casey, 2011).

The challenge for judges in proving the accuracy and reliability of digital evidence is exacerbated by the fact that this typical evidence is sometimes neither accurate nor reliable. The reliability, accuracy, and integrity of digital data can be affected by variability in forensics software, errors in processing, and differences in examiners’ knowledge (Casey, 2002; Cohen, 2008, 2010). Timestamps can easily be viewed as an example of the unreliability of digital evidence. Because timestamps are metadata associated with a file and maintained by a digital device’s operating system, this might indicate the time and date, how, when and by whom, a particular file was received, created, last accessed, and/or last modified; and how the file is formatted, and the type of content in the file (Brown, 2010; Casey, 2011). Some metadata, such as file dates and sizes, can easily be seen by the users of the computer, while other metadata is embedded in file locations requiring special software tools or user knowledge to be revealed (Brown, 2010; Casey, 2011). File timestamps can be important evidence because they provide a timeline of activities. However, the reliability of digital evidence can be
negatively impacted by the interpretation of those activities (Cohen, 2008, 2010), and the inaccuracy of the forensic software (Van Buskirt & Liu, 2006). In addition, not all programs update all instances of file timestamps in a consistent fashion, and even normal file system operations can provide seemingly contradictory timestamp information, such as when a file’s reported last access time precedes the file’s creation time (Brown, 2010; Casey, 2011).

As gatekeepers, judges face challenges in determining the reliability of reports and analysis gathered from forensics software (Jones, 2009; Kerr, 2005). This means that judges are required to develop or possess a wide understanding at a high level of both the technology and its language, as it relates to computers, computer networks and so forth. This seems to create a challenge for not only judges in Vietnam, it is also a challenge for judges in every single country in the world.

As mentioned above, cybercrime is a new phenomenon for ISPs, as well as Police and prosecutors in Vietnam. It is also a new issue for judges in adjudicating cybercriminal cases. Specifically, the issues of understanding digital evidence and the application of digital evidence in the criminal court have posed a number of challenges for judges.

A further challenge for judges in regulating cybercrime in Vietnam can be the interference of the Vietnamese Communist Party (VCP). In the other words, the involvement of VCP can provide significant limitations in efforts to regulate cybercrime. The involvement of VCP can be traced back through the history of legal development in Vietnam. Vietnam is a typical model of a single party Communist state since Vietnam announced itself to be a single party state since becoming independent from the French, after over 80 years of domination (1858-1945). The latest Constitutional Law 2014 has reasserted the nature of the involvement of VCP “...is force leading the state and society” (Vietnamese National Assembly, 2014, Article 4).

Put in a different way, the VCP is allowed by law to directly interfere in any aspect of Vietnamese society. Thus, the VCP does seem to have a critical involvement with the Vietnamese judges through the Vietnamese court system. For example, the Revolution No.08/2002 of the Politburo of the Communist Party of Vietnam on Justice Reform has stated “the party shall lead the judiciary closely” and “guarantee that judicial activities follow the guidelines of the party and state law” (Resolution No.08/2002, 2002). Even though the VCP has been pushing forward judicial reform by recognising many challenges and weaknesses in playing the gatekeeper role, the VCP nonetheless still...
reaffirms that “judicial reform must be put under the leadership of the party” (Resolution No.49/NQ-TW, 2005). In addition, more than 90 per cent of Vietnamese judges are members of the VCP (Ba, 2001). The judges are, of course, responsible to the party.

4.5.4. The challenges for ISPs

As indicated above, the emergence of the Internet and associated technological advances has been accompanied by new opportunities for criminals, as well as new challenges for law, and law enforcement agencies. The global characteristics of the Internet, its inexpensive transmission of information, and the relative anonymity of its users, contributes to an uncertain and difficult environment for law enforcement. However, to connect to the Internet, and join with the world of the information age, users must come through a select group of gatekeepers, known as Internet Service Providers (ISPs). As gatekeepers, ISPs are different from their users. ISPs are readily identifiable and susceptible to sanction. Regarding these characteristics of ISPs, they are believed to be in a good position to regulate cybercrime.

It is argued that the critical role ISPs could play in cybercrime regulation in Vietnam have not yet, on the whole, been recognised. There are some reasons for the lack of attention to the role ISPs can play regarding cybercrime regulation in Vietnam. Firstly, the liability of ISPs is not imposed by any specific legal regulation in Vietnam. Secondly, the ISPs can easily avoid the liability despite the fact that they are in a favourable position to monitor and control cybercrime. Thirdly, the economic barrier, or simply cost issues, are considered as a significant challenge for ISPs to provide additional security facilities its users.

In the context of Vietnam, Internet providers include (1) Internet Service Providers (ISPs); (2) Internet Exchange Providers (IXPs); and (3) Online Service Providers (OSPs) (Decree No.55/2001/ND-CP, 2001). Internet Service Providers are enterprises that are granted an Internet Access Service Provision License by the Ministry of Post Telecommunication (later Ministry of Information and Communications). ISPs must conform to regulations of the Decree No.55/2001 and other regulations on Internet Access Service Management regulated by the Ministry of Post Telecommunication.
It can be seen that ISPs can play an important role in preventing cybercrime or security in the information age. However, in the Vietnamese context, Vietnamese authorities seem to neglect to play proper attention to the role of ISPs in cybercrime regulation. The lack of attention to the role of ISPs in relation to cybercrime prevention may be that there is no specific legal regulation creating liability for ISPs in regulating cybercrime. Although, there are existing legal regulations and policies related to the Internet, such as the 2006 Information Technology law, Copyright law, and laws on transactions, trade, telecommunication, and so on. However, there is as yet no clear liability of ISPs for any illegal activities committed by users. Moreover, this lack of attention is understandable because ISPs operate in a virtual world, a ‘no-man’s’ land in terms of laws, legislation and even national jurisdiction (Mann and Belzley, 2005). This issue is not particular to Vietnam. It is a common issue in most countries in the world. The Convention of Cybercrime is an international legal recognition framework that has indicated that liability for ISPs would only be for aiding and abetting if the ISP shared the metal state with the perpetrator (Magnin, 2001). The standard for aiding and abetting requires the defendant to have (1) substantially assisted another who committed a violation of international law and (2) known that his action would assist in the illegal or wrongful activity at the time he provided the assistance (Magnin, 2001).

Another reason might explain why Vietnamese authorities pay less attention to ISPs in regulating cybercrime. They may simply misunderstand how dangerous cybercrime can be to Information Technology (IT) development, and how many organisations, governments, businesses, and individuals confidently use IT applications for their business with little thought for the dangers and risks relating to cybercrime and cyber security. However, in the context of Vietnam, this is understandable. One of the main reasons as mentioned above, that after the re-unification of Vietnam in 1975, Vietnam faced an economic crisis, including serious food shortages. In the following years of the late 1970s and early 1980s, Vietnam’s economic development was characterised by high inflation, low productivity, low quality export standards, energy shortages and inefficient management of the economy (Levinson and Christensen, 2002). Furthermore, food supply fell short of national demand, and in some areas Vietnam suffered from chronic food insecurity. In response, Vietnam began to find a suitable path of development and started focusing on its reconstruction. In this context, IT was and is identified as an enabler, as a crucial economic sector, and as part of the
infrastructure of the national economy. Firstly, IT is considered as one of the most important driving forces for economic development. It is seen as one of the quickest ways to achieve national industrialisation and modernisation goals, and provides an important contribution to national security (The Directive No.58 CT/TW). Secondly, as an economic sector, the development of IT makes an important contribution to economic growth, helps other sectors develop, and enhances technology’s capacity in industrialisation and modernisation nationally. Furthermore, IT can be a key element to help Vietnam quickly transform its socio-economic structure to become an advanced country in terms of a knowledge based economy and information society, and greatly contributes to the success of the country’s industrialisation and modernisation process (Decision 264/2005/QD-TTg).

Given the importance of the IT sector in the country’s development, the Vietnamese authority has made significant efforts to support it. Directive 58 is considered as the earliest manifestation of IT policy foundation for the IT development in Vietnam. Following Directive 58, a series of government documents have subsequently been enacted to guide the implementation of Directive 58. For example, Resolution 07/2000/NQ-CP; Decision 128/2000/QD-TTg; Decision 81/2001/QD-TTg; Decision 95/2002/QD-TTg and national strategy for ICT as well such as The Strategy on Vietnam Information and Communication Technology Development to 2010 and orientations towards 2020 (Prime Minister’s Decision No. 246/2005/QD-TTg on Oct 6, 2005); Decision No. 1755/QD-TTg on Sep 22, 2010 approving the national strategy “Transforming Vietnam into an advanced ICT country” in 2020.

However, in the early stages of the Internets’ operation in Vietnam, ISPs are encouraged to be responsible for “strengthening the access to education, propaganda and guidance for Internet service users regarding the retrieval and use of information on the Internet in line with the laws” (Decree No.55/2001/ND-CP)39. At the same time, ISPs also are responsible for preventing violations forbidden as follows by Article 11 (Decree No.55/2001/ND-CP):

1. Disturbing, destroying equipment systems, preventing the provision and use of Internet services,

2. Stealing and illegally using passwords, code, keys and private information on the Internet of organizations and individuals,

3. Taking advantage of the Internet to fight against to the Socialist Republic of Vietnam; causing chaos and security disorder; degrading national virtues and traditional good customs; and committing other violations of the law,

This legal text also mentioned other laws and legal documents such as the law on Information Communication, the law on Information Technology, Decree No.97/2008/ND-CP, and Decree No.72/2013/ND-CP. However, the question should be asked here is - how would ISPs prevent such violations as above.

Taking these requirements into account, ISPs in Vietnam might make an effort to provide or create a system for notifying infected computers, provide up-to-date threat information, resources for end users or security software to its users. However, this can become a big challenge for ISPs in terms of economic costs. Although some people argue that ISPs provide a variety of services to its user and must contribute the best practices to protect its customers or ISPs are believed to in a good position to protect its users’ network (Rowe et al., 2011; Moore and Anderson, 2011). Furthermore, the nature of the position of ISPs are considered as gatekeepers to allow users to access send and receive email, information through the World Wide Web (WWW). As gatekeepers and by being the parties with the greatest visibility and information, ISPs play a critical role in maintaining security in cyberspace. They can immediately and directly allow users in, or remove users from, the digital age (Circular No.04/2001/TT-TCBD, 2001)\(^40\). Without ISPs, no businesses, no users and no criminals would get online (Shachtman, 2011; Murray, 2013). As a result, it can be argued that ISPs have their own relationships with the cybercriminals as they provide the actual gateway to the Internet for perpetrators (Peterson et al., 2014). For example, malware is the most common form of cybercrime in Vietnam. It therefore represents the most prevalent way in which cybercriminals interact with ISPs. Malware can take a number of forms, such as viruses, worms, Trojans, and spyware. A virus, for example, reproduces as it spreads across computers deleting and stealing data as it travels (Mann & Belzley, 2005). A virus can

be attached to an executable file which remains dormant until the end user opens the file or program.

As mentioned above, ISPs are seen as being in a good position to protect their users, and are required to provide more security facilities to its users. However, ISPs may lack the incentive to act because victims may be using other networks or in another country (Shachtman, 2011). Furthermore, the significant costs involved in providing additional security facilities mean that ISPs might have trouble making a return on their investments (Huang et al., 2007). The significant costs involved may include, but not be limited to, technical costs, customer service costs and legal issues (Rowe et al., 2011). The technical costs include the cost of both identifying incidences of cybercrime, and preventing or stopping cybercrime. In both cases this represents very complex tasks. Moreover, cybercriminals continue to adapt their techniques to evade detection, this generates further cost. In addition, even the challenges of sending notices or warnings to its users can be another problem and represent a significant task. Indeed, even if sent, warnings might be ignored or mistaken for spam as marketing material. Finally, by using or providing additional security facilities, ISPs risk compromising user’s privacy.

4.6. Conclusion

As computer technology and cybercrime have evolved, certain forms of cybercriminal activities present problems not only for the Vietnamese Penal Code, but also for the Vietnamese criminal justice system. These problems arise from the difficulty in encapsulating new forms of criminal activities as well as traditional forms of criminal activities within the existing criminal law of Vietnam. Although the Vietnamese Penal Code has been amended several times in response to cybercrime, the law has not effectively regulated cybercriminal activities because many of the characteristics of cybercrime are incompatible with existing Vietnamese criminal law. In addition, Vietnamese criminal law has not yet criminalised some important acts, such as online gambling and prostitution, child pornography, cyber-terrorism, terrorist-websites or the commission of organised crime by using information systems and information networks and so on. Furthermore, the issue of legal linguistic is also identified as an obstacle for Vietnamese authorities in seeking to understand and apply the law in response to
cybercrime. In other words, in dealing with cybercrime, the effectiveness of Vietnamese
criminal law is reduced.

In particular, cybercrime can be trans-jurisdictional, sophisticated, either committed
without any crime scene or maybe with multiple scenes. In addition, cybercriminals can
easily conceal their identities. By contrast, Vietnamese criminal law and the Vietnamese
criminal justice system focuses on the domestic landscape, is concerned with preventing
traditional criminal behaviours, and based on the existence of identifiable perpetrators
and crime scenes. Thus, Vietnamese law enforcement agencies face a significant
challenge in effectively responding to, and regulating, cybercrime.

It is clear that neither Vietnamese criminal law nor the Vietnamese criminal justice
system will provide an entire solution to the problems posed by cybercrime. Each will
come with its own limitations. Although they still have limitations they are not
redundant. Each has a role to play in protecting rights and the legitimate interest of
individuals, organisations and the State. Each of them has a role to play as both a
symbolic tool of deterrence and a practical tool of management and guidance. For the
complicated problems presented by cybercrime, it is necessary to have a comprehensive
and flexible approach can be used to reduce the growth of cybercrime.
Chapter 5. Findings

5.1. Introduction

This chapter presents the findings of the series of face-to-face semi-structured interviews across seven regulatory institutions between July and November 2015. Thirty-five interviewees, who were high-level professionals working across seven regulatory institutions, were recruited for interview. These institutions included:

(1) The Ministry of Public Security - The Department of Cybercrime Prevention (coded as PO);
(2) The Ministry of Justice (coded as MJ);
(3) The Ministry of Information and Communications (coded as MT);
(4) The Supreme People’s Procuratory (coded as VK);
(5) The Supreme People’s Court (coded as TA);
(6) The Vietnamese Post and Telecommunication (coded as SP1-5); and
(7) The Corporate for Financing and Promoting Technology (SP5-10).

Based on the research methodology discussed in Chapter 3, a ‘thematic analysis’ approach was chosen as the appropriate method for data analysis. This analytical approach is widely used by criminological researchers. Thematic analysis is a flexible approach that can be used in both inductive and deductive methodologies for the interpretation of data collected (Braun and Clarke, 2006). The purpose is to extract information to determine the relationship between variables and to compare different sets of evidence that pertain to different situations within the same study. Hence, this research makes use of thematic analysis to interpret the collected data and to identify relevant themes in such a way as to meet the research aims as well as to provide answers to the research questions.

The chapter begins with a descriptive overview of the research participants (Section 5.2). Section 5.3 provides details of the attitudes and perceptions of the participants towards the definition of cybercrime, including the nature of cybercrime, the importance and dangerousness, and impact of cybercrime. Section 5.4 focuses on the attitudes and
perceptions of participants towards current Vietnamese cybercrime regulation policies. Section 5.5 delivers the interview results on participants’ views relating to current Vietnamese cybercrime regulation mechanisms - covering the role of the four key players in regulating cybercrime, and possible improvements to current cybercrime regulation mechanisms. Section 5.6 provides a summary of the chapter.

5.2. Descriptive overview of the research sample

As mentioned above, a series of interviews were undertaken at the time of the fieldwork trip. The research set out to interview 35 participants high-level professionals who were working across seven key regulatory institutions (listed in Figures 3.1 above). A total of 35 selected interviewees agreed to participate in this research study. Figures 5.1 to 5.4 summarises the demographic characteristics of participants within the final sample. These characteristics include gender, age, educational level, years of work experience, and level of computer literacy.

As can be seen from Figure 5.1, the sample was predominantly male (72%). Only 10 female respondents took part in the interviews (28%). Although the sample was selected according to practical considerations, the proportion of female participants interviewed is representative of the whole population. The majority of participants in the sample (40%) belonged to the 30-39 age range, 31.4 % were in the 18-29 age range, with 28.6% in the 40-49 age group. There were no participants in the 50-59 or the over 60 age group. The interviewees were selected based on the recommendation of each institution’s authority, with interviewees in the 18-39 age ranges believed to be more adaptable to new technology (and also having more technical knowledge than those within other age groups).
With such diverse education and social backgrounds, and levels of professional and technical experience, participants’ views are valuable if current Vietnamese cybercrime regulation policy, as well as cybercrime regulation mechanisms, are to be effective in response to cybercrime.

As shown in Figure 5.2 below, 100% of participants held at least a Bachelor’s Degree qualification. Approximately a third of the sample (31.5%) held a Postgraduate Degree (MA) but only a very small number of participants held a PhD qualification. With all participants holding at least a Bachelor’s Degree qualification, it could be assumed that all respondents are able to understand social and legal issues and related government policy. However, holding a Bachelor or even a Master’s Degree does not mean all participants were able to understand technical issues well enough to support their work. Nevertheless, the participants can be considered representative of the overall research population, adding further weight to the research findings.
Figure 5.2 indicates that a prerequisite for becoming an employee of any of the seven institutions was a qualification at Bachelor’s Degree level. In other words, in order to work for each institution above, applicants are required to have a certain level of understanding of social and legal problems, and related government policies. The key reasoning to support this assumption is that those people holding a Bachelor’s Degree qualification would have been required to study intensively at University, including some specific subjects related to their present jobs. For example, a participant holding BA in Criminal Law would have been required to study such subjects such as legal studies, criminal law, criminal procedure law, social security and so on.

In relation to years of working experience, Figure 5.3 below shows that participants’ work experience ranged from at least 5 years up to 19 years. No participant had less than 5 years work experience, nor any participant with more than 20 years work experience. This suggests that the people working for these institutions are neither very young nor very old. They are, therefore, assumed to be confident in dealing with issues of cybercrime regulation, and the information they supplied within interviews would be valuable and credible.
All respondents were asked to rate their own computer literacy. Respondents used a 5-level Likert scale, with 1 equating to the lowest level of computer literacy (beginner level) and 5 equating to the most literate (expert level). Figure 5.4 shows that over half of interviewees considered they had an ‘advanced’ level of computer literacy (54%), with a lower proportion indentifying themselves as ‘experienced’ in terms of computer literacy (6%). No respondents considered they had an ‘expert’ level of computer literacy, only two respondents classed themselves as ‘beginners’ (6%), while 34% of the sample indicated they had an ‘intermediate’ level of computer literacy. Based on these findings in conjunction with those on educational qualification, it is suggested that respondents were able to provide strong and credible views on issues of cybercrime regulation, as well as the challenges they face in the regulation of this form of crime – and thus could provide data that would help to address the research questions.
In addition, levels of computer literacy among respondents may also determine the actions of participants when dealing with cybercrime. Higher levels of computer literacy might encourage a more proactive approach toward the fight against cybercrime. Figure 5.4 also suggests that the participants working for these institutions are required to have a certain level of computer skill, understanding and literacy in order to perform their work effectively.

5.3. Attitudes and perceptions toward definitions of cybercrime

As mentioned in the introductory chapter, identifying how cybercrime is defined in Vietnam is very important. It indicates the outer limits of the subject and also distinguishes cybercrime from other types of traditional crime. In addition, respondents’ understanding of cybercrime helps to establish the most appropriate terminology to be used. Furthermore, understanding the term of cybercrime will enable identification and investigation responsibilities. As Shinder and Cross (2008) conclude: “To successfully fight cybercrime, as with any other type of crime, we must first understand it. Know thine enemy is good advice, regardless of the type of war we plan to wage. The first step in developing a plan to fight cybercrime is to define it both generally and specifically” (p. 29).
The definition of cybercrime is highly dependent on the purposes for which it is used. In Vietnam, cybercrime is known by different names, such as computer crime, e-crime, Internet crime, electronic crime, and high-tech crime. All of these terms refer to crimes in which computers or electronic networks are used to perform attacks, or when networks themselves are attacked. It can be seen that the participants (35 people) in seven regulatory institutions with diverse backgrounds and purposes (such as legal, information technologies) may have varying understandings of cybercrime and may use associated terms differently.

Based on the findings, there were two main approaches to defining cybercrime in Vietnam:

Based on the findings, they were significantly divided in their perceptions of the concept of cybercrime. Despite that, participants addressed the definition of cybercrime in a number of ways. However, there were two main approaches to defining cybercrime in Vietnam.

1) A definition of cybercrime based on referring to the convergence between crime and networked computer technologies, particularly the Internet; and

2) A definition of cybercrime that refers to a specific crime which is forbidden under the Vietnamese Penal Code.

Initially, there were 30 participants (85.7%) who addressed the definition of cybercrime in a number of ways. However, most definitions of cybercrime were based on the relationship between crime and networked computer technologies. Here are some particular examples of the first approach that were emphasised in a number of ways, as follows:

*Cybercrime is simply a crime that uses a computer or computer networks to commit or assist its criminal activities.* (PO3);

Some participants described as such:

*As I understand, cybercrime is a crime that either uses information technology to commit criminal activities or uses technology to enable them to facilitate the committing of the crime.* (SP1);

*Cybercrime is any illegal activities performed with either the use of the internet or the use of computer technologies.* (PO2);
I simply understand cybercrime is a crime that can commit its illegal acts by using computer, computer networks. (PO4);

Particularly, others not only mentioned the role of the computer or computer network as a definition of cybercrime, but also considered wider reasons including ‘other technological’ or ‘any device connected with the internet’.

Cybercrime is a crime that uses a computer or computer network, and other technological tools to commit criminal activities. (SP3); and

Cybercrime is a type of crime that uses any digital device connected with the internet to commit or complete its illegal acts. (TA1).

In this approach, the participants’ perception denotes a broad array of illegal activities that involve networked computers including: firstly, technological acts against networked computers, computer data or computer systems (for instance, malware, denial of service attacks); secondly, traditional crimes that are committed using the instrumentality of networked computers (for example, fraud, child pornography); and thirdly, traditional crimes where networked computers play an incidental role providing evidence of the crime.

Furthermore, these definitions suggest that the common denominator underlying cybercrime is the role of networked computer technologies and computer data, computer systems, and computer networks in the committing of a crime either as target, instrument or evidence of the crime. However, these understandings can also cause confusion because, for instance, it would cover traditional crimes such as theft.

The remaining participants (only 5 participants, 14.3%) provided a definition fitting the second approach to defining cybercrime. For example, they defined it as:

A harmful act that is forbidden under the Penal Code and that makes the offender liable to punishment by the Penal Code (MJ4);

Cybercrime is a type of crime that is using computers, computer networks to do some illicit acts that are prohibited by the Vietnamese Penal Code. (PO5);

As I understand, cybercrime is a crime like spreading computer virus, or creating obstacles to prevent the normal operation of computer systems and so on that are prohibited by the Penal Code. (TA2);

while another commented that cybercrime was:
a criminal act that has been committed by using a computer as the main tool to get something of value. (SP5).

Despite these attempts to define the term ‘cybercrime’, most participants have described cybercrime by focusing on the use of a computer system to commit a crime, or specific crime described in the Penal Code, or on the motivation behind the attack, such as the pursuit of something of value. However, looking at a wide range of cybercrimes motivated by technological challenges and creativity, these views of cybercrime are somewhat limited.

As outlined in Chapter 2, there is a wide range of discussion and understanding of cybercrime - both at international and national levels. However, there is no agreement on the definition of cybercrime, and there remain two ways in which to understand it: one in a narrow sense; the other in a broader sense. Nonetheless, the term ‘cybercrime’ has gained wide acceptance and usage over and above other terms and concepts. Cybercrime is, more importantly, the preferred term for most national and international legal instruments, although the definitions contained therein are either wide or narrow, and open to debate and new definitions.

Adding to the understanding of cybercrime, the participants were asked to provide answers to a number of opening questions relating to the nature and impacts of cybercrime. All interviewees considered the globalised nature of cybercrime to be the key factor that impacts not only how the consequences cybercrime can bring. It is also the difficulties and challenges cybercrime can create. The global nature and impact of cybercrime were explained in terms of the ways in which cybercriminal activities are carried out via the Internet. For example, some participants, particularly, Police offices, frequently highlighted:

At the present, we totally witness the power of the internet networks as well as advanced technologies, by using any digital device connected with the internet cybercriminals can commit their illegal act at anytime, at any place, even different places at the same time, without physical face to face with the victim. (PO4);

As we can witness cybercrime can occur anytime, anywhere via the internet networks without any physical barrier, thus, the consequences of causing cybercrime are unpredictable. It can effect on people privacy, reputation and
credibility life; the way people live. It also effects on social security order, national security. (PO5);

Cybercrime can occur at anytime and anywhere because of the internet networks by a single touch on a smart phone, or digital device, thus, it is difficult to estimate exactly how much damage cybercrime causes. However, generally, we can see that it is connected with the internet, cybercrime can disrupt normal business operation, administrative operation systems, and further can create error for transport, traffic systems. Thus, the consequences caused by a cyber-attack clearly can be unpredictable. (PO3);

As far as we can see that with a simple smart phone connected with the Internet, criminal can easily undertake illegal acts that mean cybercrime can occur anytime, anywhere via the Internet networks, thus, the consequences of cybercrime cannot be limited. In particular, cybercrime can damage intangible objects in nature which means it is not possible to quantify how much damage cybercrime can cause, such as damaging the reputations of people, organisations, even create a bad image for the country which cannot be recovered in a short time. In addition, cybercrime can drive away foreign investment. (PO1).

Interviewees stated that cybercrime facilitates hidden identity, with perpetrators being able to commit cybercrimes remotely from anywhere in the world without physical contact with victims. In other words, cybercriminal activities can be committed easily with few resources, and within any jurisdiction without the perpetrator necessarily being at the scene of the crime. The research participants did not only give their clear views on where and, how cybercrime can be committed. They also expressed what consequences and damages cybercrime can cause. Put differently, they claimed that the global nature of the Internet contributes to the enormous scale of cybercrime giving rise to the large number of both offenders and victims. For example, a computer virus can adversely affect millions of computer users in a country or even worldwide. Similarly, a single spam communication is sent to millions of people instantaneously. Additionally, a cybercriminal can automatically duplicate an attack thousands of times with a single click. Thus, cybercrime can have a more devastating impact on a much larger number of victims without any additional effort on the part of a perpetrator.
As noted in Chapter 2, there is widespread research that demonstrates how the global nature of the Internet helps to differentiate cybercrime from traditional crime. The differences between cybercrime and traditional crime have been identified under three major categories: multiple opportunities; global; and anonymity. Some scholars, such as Brenner (2010, 2012), Wall (2015/2013/2007), Yar (2013, 2005) asserted that unlike traditional crime, the target of cybercrime is mainly digitally stored and transmitted information, which is intangible. Scholars also emphasise that not only are the targets of crime in cyberspace shifted from tangible to intangible, but also the place where crime is committed is changed from the terrestrial world to cyberspace, in which there are no states or international geographic borders (Brenner, 2010, 2012; Wall, 2015/2013/2007; Yar, 2013, 2005). Simply put, cybercrime can take place on the personal computer of the offender or the victim, or on any kind of computer network. This means the location of cybercrime is in cyberspace, which is characterised by having no clear-cut or identifiable boundaries. Sharing a similar view, Yar (2013) points to this “anti-spatial” feature of cyberspace noting there is “zero difference between all points”; once you are on the net, you are there and you are anywhere in the world, no matter where you connect from (p. 18).

Another special characteristic of cybercrime offered by the nature of the Internet is anonymity. The Internet features an abundance of ready-to-use tools to conceal users’ identities and disguise their activities, such as encrypted communication, anonymous remailer or zombie computers. This makes it extremely difficult, if not impossible, to identify and trace offenders that use such cyber technologies (Grabosky & Smith, 2001; Wall, 2007; Yar, 2013).

One of the interesting findings is that technological developments appear to make cybercrime transforming from one to others easily with more complicated and sophisticated methods. The findings suggest that the development of technology has not only helped Vietnam to integrate worldwide, but it also contributed to the economic development of the country. However, it also brought more opportunities for cybercriminal activities committing its acts easily and taking fewer risks. Here are some examples:

*There are various toolkits offered for cybercriminals to use to perpetrate their act. For instance, they can use some special software to give themselves a backdoor and also assist them to cover their presence in your computer whenever your system is*
on. With this, they can see what you do, unfortunately, you cannot notice their presence. (SP1);

From my understanding, I think cybercrime has changed over time because advanced technologies are increasing development of smart phones, smart devices, as well as more and more sectors now relying on advanced technologies. This has led to cybercriminals moving away from simply stealing credit cards to the perhaps more profitable, large-scale implementation of demanding money. Meanwhile the management of ICTs, legal protection have not adjusted to follow such developments. (PO5);

As far as my understanding goes, I think cybercrime has changed over time as advanced technologies are increasingly developed and levels of using varieties of advanced technologies have increased as well, and become even more complex, sophisticated. For instance, if previously, cybercrime was simply a computer virus, it has now turned to become more complicated and in the form of malware, bon net. (PO2);

In my view, I think cybercrime has changed over time because of the advancement and development of technology; a cybercriminal will always take the huge opportunity to facilitate the committing of the crime by increasingly using advanced technologies for themselves, and making them sophisticated. (PO4);

In my point of view, cybercrime changes over time as newer, modern technology is used to assist or commit criminal acts and because advanced technologies change and develop on a daily, even hourly, basis. In addition, the level of using such IT has improved .... In this country, criminals’ use of technological advancement has become increasingly diverse, including hacking into bank databases to steal passwords or money, and tax evasion. Criminals are even linking up with foreign individuals and organisations to establish transmission networks via advanced telecommunications devices to commit criminal acts. (MJ2);

Another participant, with a background in information technology, indicated:

“Cybercrime has changed over time alongside the development of advanced technologies and their use within different sectors. It is clear that the developments of technologies are helping to provide various tool/techniques for cybercriminals to make committing criminal acts easier. A mathematic model is one of many
examples to use for designing a program using Tree diagram, a statistical tool in order to get victim information and pin numbers." (SP3).

A number of scholars have conducted more in-depth research on this aspect. For example, Beck (1992) labels the contemporary world as both an ‘industrial’ and ‘risk’ society. The indiscriminate use of technology has associated risks which are not traceable, yet because of the complexity of society and technological advancement, new crimes, especially cybercrime, have grown creating new types of risk for individuals, organisations and for society.

Wall (2007) suggests that new technology generates great anxiety. He asserts that information technology influences crime and the criminal in three main ways: firstly, it is a vehicle for communication which sustains existing patterns of harmful activity, such as drug trafficking and human trafficking; secondly, information technology has created a transnational environment that provides new opportunities for criminals; and thirdly, the nature of the virtual environment, particularly, creates distances between time and space irrelevant in cyberspace.

Majid (2006, 2013) illustrates a sound and concise view of cybercrime as follows: “New crimes appear at a rapid pace and old crimes disappear or change their form and what counts as a crime varies across societies.”

As discussed above, cybercrime has certain characteristics that set it apart from traditional crimes. These differentiating characteristics are derived from the very nature and design of information technologies. These characteristics, in turn, are linked to the many challenges which cybercrime presents to policymakers when trying to regulate against this type of crime. These characteristics also create many difficulties for law enforcement agencies in their quest to investigate and prosecute cybercriminals.

To expand our participants’ understanding of cybercrime, they were asked to evaluate the consequences of cybercrime. Unsurprisingly, the majority of interviewees stated that the impact of cybercrime depended on the purpose of the criminal act. It can be a financial loss or interruption of normal system operations of private businesses, organisations or government services. It may even damage individuals, organisations, and government’s reputation. Furthermore, it might represent a threat to national security. Moreover, at some point, the participants explained that the greatest
consequences caused by cybercrime cannot be predicted. In this aspect, two participants commented:

*cybercrime can damage intangible objects in nature which means it is not possible to quantify how much damage cybercrime can cause, such as damaging the reputations of people, organisations, even create a bad image for the country which cannot be recovered in a short time. In addition, cybercrime can drive away foreign investment.* (PO1);

*ICTs can be used in almost any sector of society, thus, the consequence of cyber attacks can be unlimited, such as losing money by several means through things like system operation recovery, interrupting normal system operations, wasting time and so on.* (SP3).

The consequences of cybercrime can be either tangible consequences such as financial loss, or intangible consequences such as reputational damage to individuals, organisations or even governments, making people lose trust and confidence. For example, a participant warned that cybercrime can “threaten national security [and the] social security order” (MJ2).

The data generated by interviews possibly suggests that the impacts of cybercrime in Vietnam can be placed into three categories: economic, social and political. Firstly, there is the economic impact of cybercrime in Vietnam. This impact can be linked to the attacks by cybercriminals which damage the reputation of individuals, organisations or even the Vietnamese government. Some illustrations given were:

*Cybercrime can create a bad image for Vietnam as it can put Vietnam on the list of countries with a high risk of cyberattack. As a consequence, it will drive away investors due to the fact that in most aspects of life, things are done electronically and if someone can attack your database, then they have everything about you at their disposal.* (PO4);

*If we look at the damage cybercrime can cause and how people can be affected by cybercrime, I would think cybercrime can have other consequences such as distressing people, damaging reputations of individuals, firms, organisations and productivity reduction and so on.* (PO2);

*As cybercrime occur anytime, anywhere via Internet networks … the consequences of cybercrime can be very difficult to evaluate. Especially, intangible damage*
cannot be counted... such as damaging the reputation of people, firms, organisations and even a nation. (TA2);

I think cybercrime can have other consequences such as distressing people in terms of their psychological well-being, and have a negative impact on young people. Additionally, cybercrime has caused serious damage and threatened Vietnam’s image and credibility, creating a barrier for attracting foreign investments into Vietnam. (PO1);

Well, I believe that cybercrime could have other consequences. As we all know cybercrime can have either tangible consequence such as financial loss (fraud, online banking transactions) or intangible damage, such as damaging the reputation of personal individuals, organisations, making people distrustful, effect of the way people live, culturally and so on. (PO3);

... The consequences of cybercrime can have negative effects ... losing data, assets, stability, and reputations of individuals, firms, industries, markets, and more importantly critical national infrastructure, is a real and present consequence, and is only expected to grow. (PO5).

The second category of consequences comes in the social impacts of cybercrime. These social impacts can disproportionately affect developing countries like Vietnam. The reason for this is that preventing cybercrime demands substantial additional resources for law enforcement, but at the same time there are other important social projects that would be of benefit to Vietnamese society that also require funding and should not be sidelined. However, if the Vietnamese government does not allocate sufficient funds for the regulation of cybercrime (including prevention measures), Vietnam might become a greater target of cybercrime, and a prime location for cybercriminals. As a consequence, the international reputation of Vietnam could be damaged and foreign investment will be reduced, which in itself will have a detrimental impact on Vietnamese society.

Another social impact arises from the threat and insecurity posed by cybercrime; people might avoid using technology in order to protect themselves from cybercriminal acts. Effectively, this can close the doors of opportunity to Vietnamese citizens and place them at a disadvantage in a globalising world.
One other social impact of cybercrime manifests itself in the lives of young people. Some young people may view cybercrime as a route and a means by which they can achieve a ‘good life’ for themselves and their families. Failing to realise the full implications of such acts could become a social problem.

The third category of the impact of cybercrime is political, this could affect Vietnam in particular. The political impacts of cybercrime in Vietnam include issues such as reducing the likelihood and willingness of international organisations to invest resources in Vietnam, and creating a bad image for Vietnam. For example, Chinese hackers recently attacked the Vietnamese government’s websites after political events relating to Vietnam-China relations (Vietnamese News, 2015, 2016). The following section continues to show how the characteristics of cybercrime can create challenges for Vietnamese policy-makers.

5.4. Attitude and perception toward the policies of cybercrime regulation

There were a number of ‘open’ questions used to establish the views of participants on current Vietnamese Cybercrime Regulation Policies (VCRPs) as a way in which to tackle cybercrime. Some key themes emerged from the data generated by interviews, as follows:

1. The nature and limitations of the VCRPs; and
2. The inadequacy of the VCRPs.

The nature and limitations of VCRPs can be understood in terms of the limitation of jurisdiction. As indicated above, the global nature and characteristics of cybercrime pose new and significant challenges to a traditional legal philosophy. The global nature of cybercrime is also described as ‘transnational’. Vietnamese legal regulations are traditionally premised on its geographical borders and jurisdiction. Traditional jurisprudence on jurisdiction assumes that Vietnamese law is made for Vietnamese citizens, residing within Vietnamese boundaries, where the Vietnamese authorities will prescribe and execute the law. Legal rights and responsibilities are therefore largely dependent on where one is located. However, with the growth of Internet-based activities, these elements have become increasingly irrelevant. In fact, some of the traditional elements of legal authority have been demolished by the global nature of
cybercrime facilitated by the Internet. The reasons for this increasing irrelevance are described below.

The power of Vietnamese authorities underpins Vietnamese law. If a piece of legislation is violated, the Vietnamese authorities must have the power to impose sanctions in respect of that violation within the Vietnamese jurisdiction. Vietnamese legal authority, in turn, depends on the ability to exercise physical control over, or otherwise impose coercive sanctions, on violators. Based on legal regulation, Vietnamese authorities derive their power from physical control over Vietnamese territory or the Vietnamese people, objects and actions located within Vietnamese boundaries. In principle, a Vietnamese authority wishing to impose a set of policies relating to cybercrime regulation should ensure the integrity of Vietnamese boundaries in order to protect national, organisational and individual interests from illegal activities.

In fact, cybercrime has a special transnational aspect compared to other crimes because of the nature of developments and advancements in technologies. Boundaries in cyberspace do not necessarily correspond to the geographical boundaries of the physical world, and thus the power of the sovereign nation’s legal authorities (based on physical control) become outdated. Thus, the Vietnamese authorities wishing to enforce laws on, or in, cyberspace find that they simply do not have the necessary physical control over the Internet. This was strongly emphasised by 25 participants (71.4%) and this issue was viewed in various ways. Here are some particular examples:

- *[Regulation]*will be impossible when it occurs out of Vietnamese boundaries.* (PO4);
- *Because the Vietnamese Penal Code only applies within its own boundaries, we are not allowed to apply it to other countries. Therefore, we are actually facing difficulties when responding to cybercrime.* (PO3).

In addition, tracing and tracking down cybercriminal suspects is not only problematic but almost impossible because the Internet operates logically rather than geographically. The Internet functions by finding the logical location of a computer, not its physical location, nor the address at which it is registered or the person residing at that address. Therefore, cybercrime can remain anonymous and evade detection by authorities.

Adding to the issue of the anonymous nature of cybercrime, two particular Police officers strongly highlighted it as follows:
Cybercrime can take place at anytime without physical boundaries to prevent it. Moreover, the global nature of advanced technology allows cybercriminals to hide their identity easily, and allows cybercriminals to attack multiple users in different places at the same time. (PO1);

...by using any digital device connected to the internet, cybercriminals can commit their illegal acts at anytime, in any place, even different places at the same time, without being physically face to face with their victims. (PO4).

Similarly, Furnell (2003) points out that the nature of the Internet makes it accessible from any geographical location throughout the world while legislation has a comparatively limited effect and reach. Furnell provides three inherent reasons why legislation is less effective in regulating cybercrime. Firstly, legislation is national in nature; when a particular country enacts laws those laws can only have an effect within the national bounderies of that country. Secondly, although different countries may have different laws, it is difficult to trace the exact geographical location of a cyber attack, and hence within which country’s jurisdiction it falls. Thirdly, even when the location of a cyber criminal is known, it may require the criminal’s extradition so they can face charges for their crime/s, but this is often very difficult to achieve between certain countries, not least because the formal legislative requirements may not be well-articulated.

There is another reason why Vietnamese law has been limited by Vietnamese geography. Traditionally, the extent of the harm caused has been generally limited within the physical boundaries of the Vietnamese jurisdiction. Vietnamese law regulates actions that are most likely to have effects solely on, or within, Vietnamese boundaries. This means that there is a strong connection between jurisdiction and the effects of certain activities. However, the global nature of cybercrime means that it may not necessarily take place, and have impact, within a defined/confined geography. Moreover, the speed and interconnected nature of the Internet means that information communication via this medium is becoming increasingly easy and convenient. This means the notion of geography and distance is totally defied and, consequently, the effects of illegal actions such as cybercrime may be felt immediately throughout the world regardless of the location of origin. This means that the effects of cybercriminal activity are not merely confined to a certain localised area, they can be felt anywhere, in
any location on the Internet instantaneously. This aspect of cybercrime was expressed by participants in a number of ways. For two examples:

*Cybercrime is a borderless crime, the scope of its commission is unlimited in that it is not dependant on any location, country. In the other words, it can be anywhere.* (MJ2);

*With simply a smart phone connected with the internet, criminals can easily commit illegal acts which means cyberime can occur anytime, anywhere via Internet networks.* (PO1).

In relation to the nature of the limitations of law when dealing with cybercrime, Koops (2012) explains “One of the most fundamental tenets in criminal law is national sovereignty. More than any other area of the law, criminal law is tied up both with the cultural values of a nation and with the sovereign exercise of power over citizens of a territory. There is an obvious tension between the global character of the Internet and the nation-based exercise of criminal law” (pp. 359-360).

According to the results of interviews, more than half of respondents (57.1%) emphasised the inadequacy of legal regulations to be another factor that makes cybercrime difficult to regulate. These problems included: not addressing all aspects of cybercriminal activities or not covering all cybercriminal activities; the rapid development of advanced technologies. When talking about the VCRPs, participants, especially, Police officers and Ministry of Justice officers, tended to be clear about what caused them difficulty and challenges when regulating cybercriminal activities. They addressed the inadequacy of legal regulations of Vietnam in various ways, for example:

*In my opinion, the policy of cybercrime regulation of Vietnam does not address all aspects of cybercriminal activities, in particular the Vietnamese Penal Code where it defines crime and punishment. Why I say that is because the Vietnamese government has proposed amending and supplying some articles, including some new articles in regard to cybercriminal activities, in order to improve its laws to protect people from cybercrime, on the one hand. On the other hand, the development of advanced technologies has created many ways for criminals to exploit and commit illicit acts while the policy of cybercrime regulation is slowly developed or created to apply for such illicit acts.* (MJ2);
... laws always stay behind the development of ICTs, [and] could not catch up with new forms of cybercriminal activities. Thus, it is understandable that the laws in Vietnam have not covered a full range of cybercriminal activities. (PO1);

Personally, I think the Vietnamese Penal Code does seem to be inadequate in response to cybercrime because there are a number of cybercriminal activities that have not been regulated yet. For example, at this time, the Penal Code has been revised and is waiting for the National Assembly’s approval. At the time of revision, the Penal Code has had inserted some cybercriminal activities that already occurred in Vietnam and that previously has not been regulated. In addition, advanced technology is rapidly developing and a new form of cybercriminal activity can be expected to appear afterwards, while the Penal Code remains the same. Thus, a new form of cybercriminal activity will be missed. (MJ5);

Laws will always stay behind the development of ICTs, and thus covering all aspects of cybercriminal activity is most difficult and challenging ... because the development of advanced technologies are increasing quicker. Meanwhile, crime always exploits newly modern technology for criminal acts. It is understandable that the laws in Vietnam have not covered a full range of cybercriminal activities. (PO2);

In my opinion, the laws in Vietnam have not covered the full range of cybercriminal activity because although information technology is increasingly developing meanwhile laws take time to review or build.” (MJ1);

If you look at the Penal Code, for example, you could see only 6 articles regulating cybercriminal activities, meanwhile cybercriminal activities can exist in many forms, including assisting traditional crime. (MT2).

Meanwhile, other respondents explained that the policies relating to ICT were just focused on interpreting the legal application for ensuring ICTs can be applicable in assisting the social and economic development rather than addressing cybercriminal activities. They commented:

*I am of course aware of the law on ICTs when I deal with cybercrime issues. They are important legal documents both in relation to information technology and to telecommunication. The law on information technology was created to ensure*
information technology application and development, and rights and obligations of agencies, organisations and individuals engaged in information technology application and development activities. The law on telecommunication focuses on telecommunications activities, including telecommunications investment and business. These laws are to focus on the application and development rather than addressing cybercriminal issues. (TA5);

Additionally, there were a number of legal protections in regard to information communication technology created, however, they do seem to be concerned with legal interpretation rather than regulating cybercriminal activities. (MJ3).

The main reason for this is that modern technology develops quicker and faster in comparison to legal policy. As discussed in the analytical framework, legislation related to cybercrime in Vietnam has not been operational for long. It came to the attention of the Vietnamese government for the first time in 1999, when the Penal Code 1988 was revised by supplying three regulatory provisions focusing on cybercriminal activities. The Code underwent its second revision in 2009 by increasing the regulatory provisions related to cybercrime this was due to some emergent forms of criminal activity. Although the Penal Code has been revised twice, one participant claimed:

*The technological developments have gone far beyond what the Penal Code could have envisaged at the time of its enactment.* (PO5).

Therefore, there is no doubt that when the Penal Code was enacted it did not take into account the current cybercrime threats. In other words, the Penal Code currently does not cover the full range of cybercriminal activities.

Furthermore, the regulatory provisions related to cybercrime are incorporated in the Penal Code under the chapter titled “Crimes of infringement upon public safety, public order”. This means cybercrime is treated as a crime against public safety or public order. As a result, the Penal Code does not fully address all the features of cybercriminal activity because:

*At this time, cybercrime is not simply a crime against public safety, or public order, it can be perpetrated against any legally protected interest such as property, moral, liberty, security, financial and so on.* (PO3).
In other words, at this time, cybercriminals perform illegal acts in various sophisticated forms; thus many cybercriminal activities are beyond regulation by the law and the law is therefore outdated.

However, in some ways, it can be argued that at the time of revising the Penal Code, technological development was at an embryonic stage in Vietnam, as it was not integrated into all aspects of life. At that time, the diffusion of social media had not penetrated Vietnam. Thus, the use of computers and computer networks could not be considered as involving specific security issues linked to criminal conduct. Similarly, issues of cyber security would not have been viewed with a sense of urgency. It is not surprising that Vietnamese policymakers could not have anticipated the pace of technological change over time in the ensuing years.

Recently, the Vietnamese Penal Code has been revised for the third time to regulate some new forms of criminal activity. At the same time, a law on online information security has been approved. Both laws came into effect from January 2016. This does seem to demonstrate efforts by the Vietnamese government to improve its legal policy in relation to cybercriminal activity in order to protect its country, organisations and citizens from cybercrime on the one hand. On the other hand, it is considered to be a confirmation that Vietnamese cybercrime regulation policy has its limitations.

Moreover, Vietnamese policy on cybercrime regulation is said to be unclear, even hard and difficult to understand in terms of its legal language. This unclear legal policy can be inconsistently interpreted and implemented in a number of ways, including for personal interest (Malinasky, 2012). As a consequence, legal authorities can use laws arbitrarily, including cybercrime regulations. It is worthwhile using an example of the seriousness of issues of bribery and corruption in Vietnam. In an evaluation in 2014 by the United Nations of countries with corrupt practices, Vietnam was placed 119 out of 175 (United Nations, 2014). Many legal authorities, including members of the Central Executive Committee have been involved in committing crimes of corruption. In the Namcam trial in 2003, for example, the Vice-president of the People’s Procuracy and the Vice-president of the Ministry of Public Security, as well as the
Deputy of Police of Hochiminh City, were convicted of corruption (The New York Times, 2003). Although this example is outdated, it still remains relevant.

In fact, legislation affects everyone and makes no exception for individuals. Thus, legislations need to be clear, and easy to understand otherwise as one participant suggested:

... it means professional users can find the law complex, hard to understand and difficult to comply with. (PO3).

Another participant suggested:

... these laws seem to be difficult to understand. Because the legal language used does not seem to be clear enough or even difficult [to understand], they can conflict with each other. Thus, these laws need to have a legal interpretation. (TA3).

Therefore, it is not surprising that users and practitioners often need help or guidance in understanding the raw material of law. Unclear legislation presents further opportunities for criminals to find ways around and subvert the law and commit criminal activities.

Although there can be guidance to help with the interpretation of legal documents, this guidance can take some time to be issued, often years. As a consequence, Vietnamese authorities face more confusion, and difficulties implementing legislation in practice. For example, although the 2006 Law on Information Technology of Vietnam was approved on 29 June 2006, and came into effect on 1 January 2007- Decree No:07/2007– which provided details and guidance for the implementation of a number of articles of the legislation – was not issued until 3rd July 2007. In particular, while cybercrime was defined in the 1999 Vietnamese Penal Code, the official document guidance for applying this Code, specifically articles relating to cybercriminal activities, was not in fact produced until three years later. The legislation itself can, therefore, create barriers for regulating cybercrime in Vietnam. It might be also considered as presenting an opportunity for many more cybercrimes to be committed.

---


42 Joint Circular No. 10/2012 / TTLT BCA-MOD-TT-BTP-BTT & SPP-SPC dated 10/09/2012 of the Ministry of Public Security, Ministry of Defense, Ministry of Justice, Ministry of Information and Communications, the inspectorate the Supreme people's Procuracy and the Supreme people's Court guiding the application of the provisions of the criminal Code of some criminals in the field of information technology and telecommunications.
5.5. Attitude and perception toward the current Vietnamese cybercrime regulation mechanism

Streamlining and strengthening procedures for cybercrime investigation, and eliminating the factors that make Vietnamese law enforcement mechanisms difficult and challenging, are important prerequisites to achieve effective responses to cybercrime. Arguably, effective regulation of cybercrime requires a two-pronged approach. One is criminalisation of cybercrime itself and the other is a law enforcement mechanism approach to respond to cybercrime. The previous section summarised how current Vietnamese cybercrime regulation policy in general, and the Penal Code in particular, were insufficient to address all forms of cybercriminal activities, as well as other issues relating to Vietnamese cybercrime regulation policies. There is a need and demand for a comprehensive cybercrime regulation policy. Creating a comprehensive legal policy, however, is only half the solution. The other half is the (in)ability of current law enforcement mechanisms to respond effectively to cybercrime. This section further continues to explore the key factors that create challenges for current Vietnamese cybercrime regulation mechanisms. At the same time, this section aims to identify the role four key players should play in regulating cybercrime, and what could possibly be done to make the current cybercrime regulation mechanisms more effective in controlling cybercrime.

Both traditional crime and cybercrime are similar in nature because they both result in violations of the rules and laws of Vietnam. However, cybercrime differs from conventional crime in terms of its reliance on modern technology and computers as essential key elements. As a result, current Vietnamese law enforcement mechanisms are facing complex challenges; particularly as cybercriminals are often educated, organised and well-equipped, making it difficult to regulate their activities, gather evidence, locate criminals and prosecute offenders.

5.5.1. The Police - Role and challenges

In relation to identifying Police agency’s role in responding to cybercrime in Vietnam, all participants, including Police officers, were asked the opening question “Who is
responsible for cybercrime? The Police agency, the providers? The Corporation? The individuals?” In response to this question, there were 31 participants (91.4%) who considered the Police have an important role to play in combating cybercrime because the Police, on behalf of the Vietnamese government, manages national security, social security and social order in order to protect the nation’s legitimate interest, and those of organisations and individuals.

All Police officers (100% of the sample) identified themselves as having the main responsibility for cybercrime prevention and investigation. The simple reason for this is that Vietnamese Police agencies are empowered in “the protection of national security, ensuring order, social security, the fight against crime” (Articles 14, 15, the Law on the People’s Police). In addition, in criminal processing, Police agencies are the first to be given power to investigate incidents of cybercrime. In relation to cybercrime investigation, the duties of Police agencies consist of arresting and questioning cybercrime suspects, as well as interviewing victims and other people related to a cybercrime case. At the same time, Police agencies need to collect as much evidence as possible to support potential prosecutions and bring the cybercriminals activities before a court of justice. The collection of evident takes place via search and seizure. This means the Police have to take action by identifying, where possible, where cybercrime takes place and where evidence will be stored. It may be a place where a suspect lives or works or in public places such as coffee shops or restaurants. Undeniably, Police agencies are viewed as having the lead role in the investigation and the prevention of criminal activity, including cybercriminal activities. In this regard, the majority of participants claimed that the police should be responsible for preventing cybercriminal activities. For instance:

We are, of course, the special unit; we mainly take responsible for cybercrime prevention. (PO4);

As you can see cybercrime is such a complicated phenomenon. Indeed ... we are living in an interconnected world and this is only going to likely increase as everything linked to the Internet becomes a reality. We are mainly responsible for cybercrime prevention. However, our ability to deal with this typical threat is limited in terms of human resources, budget, because the developments of advanced technology help cybercriminals commit crime and to carry out attacks in any place or multiple places at the same time. (PO5);
Traditionally, we as the police agency are given the power to prevent any type of crime, therefore, we take mainly responsible for preventing cybercrime. (PO2);

For me, although each individual, organisation and provider should take their own role in relation to the fight against cybercrime ... police agencies should take the main and leading role because of their total duties. (SP7).

As discussed above, the global nature and characteristics of cybercrime, as well as the nature of legislation in this area, have created significant challenges for law enforcement mechanisms, including those used by the Police. Although, the Vietnamese Police agencies play the leading role in the prevention and investigation of cybercriminal activity, they face some key challenges in performing this task.

These key challenges were identified within the series of interviews. Traditionally and principally, the first important step within an investigation is to identify the suspect. This is a vital task for the Police investigator, before any criminal sanction can be imposed. The Police cannot impose any criminal sanction without identifying who is possibly responsible for an illegal act. In addition, without knowing who is responsible for an illegal act, no Police investigation can be undertaken. The point being emphasised here is that, in so far as the identities of cybercriminals remain unknown, no legal action can take place. The Vietnamese Penal Code was principally created to apprehend and prosecute cybercriminals, thus, if the criminals are unidentifiable, the Vietnamese Penal Code cannot be enforced. Moreover, by identifying a cybercrime suspect, the Police can both stop the suspect continuing their criminal acts and prevent other criminal acts which might give rise to other serious consequences. In some circumstances the Police should take legal action to protect the public from suspects of cybercrime in case they are dangerous and may harm themselves or their victims (if they are aware that they are being investigated or caught acting illegally).

In fact, identifying suspects of cybercrime can pose a huge challenge for a Police investigation. Unlike a traditional crime, cybercrime can take place anywhere, or even multiple locations at the same time. In addition, the virtual world is an invisible environment, operating in an invisible electronic space, not in any one physical location. This means that the identity of suspects of cybercrime can be hidden, and suspects can easily remain anonymous. Cybercriminals can take any name, put/use any information without the prior approval of any authority. Technically, cybercriminals can use
different telecommunications equipment and software to hide their identity. As a consequence, identifying cybercriminals is increasingly difficult, and sometimes impossible. It can take time, costs money and is a considerable expense, as illustrated by participants’ comments set out below:

At the present, we totally witness the power of internet networks as well as advanced technologies. By using any digital device connected with the internet, cybercriminals can commit their illegal act at anytime, at any place, even different places at the same time without being physically face to face with the victim. As a result, the demand for an effective response to cybercrime is significantly difficult to meet because we need more staff travelling to different locations at the same time in order to protect crime scenes and to collect the evidence. This will be impossible when it occurs outside of Vietnamese boundaries. (PO4);

...the nature of developments in advanced technological help cybercriminals in the form crimes can take and to attack any or multiple places at the same time. (PO5).

Another participant commented:

Cybercrime can take any place at any time without physical boundaries to aid prevention. Moreover, the global nature of advanced technology make it easy for cybercriminals to hide itheir identity, and to allow them to attack multiple users at different places, at the same time. (PO1).

Another impediment to Police investigations of cybercrime emerged in relation to the ‘search and seizure’ of cybercrime evidence. Search and seizure is a crucial task within the investigation process, involving the discovery of evidence to identify a connection between the suspect and the crime that has occurred. According to the Vietnamese Criminal Procedure Code, evidence is that which tends to prove the existence of certain facts. It may consist of testimony, document evidence, physical evidence and admissible evidence. However, search and seizure evidence in a cybercrime case is increasingly a challenge for the Police as it raises the questions of where to search, and what to search for. Even knowing where and what to search for, there remains a challenge when that search is not located within the boundaries of the nation state.

The determination of the location to search is challenging for the Police investigator, not least when issuing a search warrant with or without the approval of the appropriate prosecuting office. One reason is that most individuals, organisations, and businesses
rely on computers for daily work (for example, for communications, financial transactions such as online banking, shopping, social network activities, education and entertainment) and thus various actors will be significantly affected by search and seizure procedures, because electronic information and computer technologies are an integral part of their daily lives and business operation. Taking search and seizure action can cause interruption and/or serious harm to that activity.

When the search location is in another country, or even in multiple countries, the challenge to law enforcement is greater. As mentioned above, the global nature and characteristics of cybercrime enable cybercriminals to cross borders and commit crimes without actually moving from their home location, whereas Vietnamese law enforcement mechanisms are restricted and can only be exercised in relation to crimes committed within Vietnamese boundaries, and located within Vietnamese jurisdiction. This challenge can, however, be resolved by taking mutual legal assistance from other countries, although it is not always easy to do so and depends very much on legal, political and cultural factors within each country where searches are to take place. In relation to political factors, Smith, Grabosky and Urbas (2004) state:

“…If relations with one’s counterparts in another country are not close, one is less likely to go the extra mile. Even where a treaty places an obligation on parties to cooperate…when authorities in another country are disinclined to cooperate, for whatever reason, investigations can be complex and legally murky” (p. 57).

Even when mutual legal assistance takes place, it involves a long process and can take a long time before a search can be conducted. During that delay, cybercrime evidence may be changed, removed or even destroyed. The primary reason is due to the intangible and often transient nature of the information and data especially in a network environment. Advanced technology makes it possible to record information and data on the one hand, on the other hand it also renders the process of investigation for evidence vulnerable to defence claims of technical errors, detrimental interference, malfunction or fabrication.

In respect of investigating cross borders, Smith, Grabosky and Urbas (2004) have identified a number of challenges for Police agencies. One of these challenges relates to cybercrime evidence which can be stored on a remote server located in one or more other jurisdictions.
The lack of human resources and funding can be another key challenge for Police agencies. In fact, there are significant differences between investigating cybercrime and traditional crimes. Unlike traditional crimes, the global nature and characteristics of cybercrime allow cybercrime attacks to be undertaken in multiple places with a large numbers of victims, all at the same time, without physical barriers. Thus, an effective response to cybercrime demands a large number of Police officers, spending a lot of money travelling to different locations at the same time to gather evidence, before that evidence may be damaged, removed, or even destroyed. This will be significantly difficult when multiple locations relating to the cybercrime under investigation are located outside of the country. Some cases are imposible to investigate. In this regard, the respondent explained:

“Our ability to deal with this typical threat is limited in terms of human resources and budget because the nature of developments of advanced technological that help cybercriminals, the crimes they can take and the way they can attack any or multiple places at the same time. (PO5);”

In fact, Police agencies ability to investigate is arguably limited, as they are not capable of covering all aspects of cybercrime even if they have an educational background in information technology. In addition, cybercriminals always look for weaknesses within legal and criminal justice systems so as to circumvent preventative measures and to avoid detection. The typical explanation for lacking ability, sufficient skills and techniques was described as:

... our ability is limited, meanwhile if we can get help from others who have sufficient skills and techniques, it will be better for us to be able to effectively tackle cybercrime. (PO3).

Similarly, another Police officer highlighted the need for more staff and resources to combat cybercrime in different locations, even other countries:

“At present, we can totally witness the power of internet networks as well as advanced technologies ... cybercriminals can commit their illegal acts at anytime, in any place, even different places at the same time. As a result, demand for an effective response to cybercrime cannot be met because it is significantly difficult because we need more staff travelling to different locations at the same time in
order to protect crime scenes, and collect the evidence. This will be impossible when it occurs outside of Vietnamese boundaries. (PO4).

In short, when asked about who should be responsible for cybercriminals, almost all participants believed that the Police should play the leading role in regulating cybercriminal activities. In their view, the Police have not only been given the power in law; they are also facilitated to deal with criminal activities, in general and cybercriminal activities, in particular. However, they face many challenges when dealing with this typical crime.

5.5.2. The Prosecutor – Role and challenges

It cannot be disputed that the Prosecutor plays a significant role in relation to cybercrime regulation in Vietnam. According to the Vietnamese Criminal Procedure Code and the Law Organisation of the People’s Procurator, prosecutors shall exercise their right to prosecute via criminal procedure and before a court. Prosecutors have duties to ensure that all criminal acts be handled in time. (The Law Organisation of the People’s Procurator, 2014).

Although, there were no specific questions asked about Vietnamese prosecutors, based on the prosecutor role and the global nature and characteristics of cybercrime, the research has revealed two key significant factors that pose challenges for Vietnamese prosecutors when dealing with cybercrime issues.

The first factor surrounds levels of computer literacy. The Prosecutor’s role is empowered by Vietnamese law as exercising the right to prosecute and supervise the observance of the law in investigation and adjudication of criminal cases, and supervising the observance of the law in the execution of judgments and decisions of the courts (The Law Organisation of The People’s Procurator, 2014). This can be understood as the prosecutor being required to have a deep understanding in every aspect of cybercriminal activities, as well as the relevant law, in order to determine whether or not to approve the actions and decisions of Police investigation agencies and judges. In addition, cybercriminals are usually educated, well-equipped and up-to-date in terms of computer skills and techniques. Thus, there is a need for the prosecutor in
Vietnam to have deeper, regularly updated computer knowledge, skills and techniques in order to help undertake their duties more efficiently and effectively.

In fact, the results of interviews surprisingly showed that the level of computer literacy among prosecutors was lower than for other Vietnamese law enforcement officers. There were only two prosecutors who considered themselves as having an advanced level of computer literacy; two assessed their computer literacy as being at intermediate level; and one indicated they were at beginner level. In addition, only two of these interviewees were intensively trained in the use of Microsoft Office and Excel. Furthermore, all prosecutors backgounds were in criminal law and none had any specific training in relation to computer networks and technology. Therefore, it can be understood that prosecutors face difficulties when dealing with cybercrime issues.

5.5.3. The Judge – Role and challenges

Within the Vietnamese criminal justice system, judges have a role to play in the final criminal proceedings. Judges’ roles are crucial in cybercrime regulation because they make the final determination as to whether or not the suspect is convicted of any cybercriminal acts prescribed in the Penal Code.

Similar to Vietnamese prosecutors, judges were not directly asked about their role and the difficulties they faced in dealing with cybercrime in this study. However, Vietnamese judges are given a special role in the criminal processing and without this criminal sanctions cannot be imposed on criminals and cybercriminals.

5.5.4. The Internet Service Providers (ISPs) – Role and challenges

As mentioned in Chapter 2, the role of ISPs is changing and expanding. ISPs are transforming themselves to offer a wider range of service to their customers. Undeniably ISPs have a vital role to play in protecting their users as well as their networks from cyber attacks. Taking a vital role in regulating cybercrime, ISPs in a gatekeeper or observer sense, and in providing or improving security for their users, does seem to contradict the idea of the convergence of the three factors in Cohen and
Felson’s (1998) ‘Routine Activity Theory’. As previously mentioned, the reduction in the growth of cybercrime will be effective when the opportunities for criminals can be controlled, even removed, through either legal actions, technological advances or the users themselves. As discussed, a number of difficulties were found to currently exist when applying legal actions to regulate cybercrime. This subsection examines ISPs liability/responsibility for providing additional security protection to guarantee their networks, as well as their users, in order to reduce the growth of cybercrime.

Unsuprisingly, the majority of respondents (23 respondents, 65.7% of the sample) admitted that ISPs have a critical role to play when it come to Internet security. The key reason for this is that ISPs provide the means and venue for cybercriminals to operate. In other words, ISPs facilitate the transmission of cybercrime traffic by removing a significant barrier for individual perpetrators. It can be made easier to understand by using the most common form of cybercrime – Malware - as an example to illustrate the most prevalent means by which cybercriminals interact with ISPs. Malware has three primary forms. First, a ‘virus’ reproduces as it spreads from one to other computers, deleting and stealing data as it travels. Secondly, ‘worms’ which are similar to a virus, except that they do not rely upon other files, and thus they are often able to expand across vast computer networks. Finally, trojans convince users that they are not harmful to computer programs. Trojans often provide a means for cybercriminals to infiltrate the network.

Ensuring network security and protecting customers from cyber attacks can be easily achieved by ISPs through the provision of additional security equipment. One of the main reasons for this is that ISPs are well placed to detect and deter bad or illegal acts because they are the gateway to networks and potentially monitor almost all user acts. In addition, ISPs can impede access to their network operation, control or prevent any malicious or illegal acts by using equipment security protection, such as firewalls and computer virus software. In doing so, ISPs have the capability of being guardians on the one hand, while on the other hand, they can also help users make themselves more difficult to be targeted by cybercriminals. In recognising the role of ISPs, some participants acknowledged:

_Cybercriminal acts can be committed via the internet or computer networks. We, as ISPs, control the gateways, we have a role to play in protecting our customers from cyber attacks. We especially have the equipment and the expertise to monitor and_
block any unauthorised or illegal access. Staying on the users’ side, we can see that in Vietnam users do not have the knowledge and expertise to handle security of the internet, except a very small number. Even though some users have the knowledge, they stay far behind the increasingly sophisticated threat of attackers. (SP1);

Look, how cybercrime can attack? Is this only via the Internet? We run this service, we should take care of our service as well as our customer. Because if our customer is attacked, our service also will be affected. We have the technical expertise to do so. (SP5).

In relation to increasing ISP network security, other interviewees suggested the use of an indirect method by producing more information on how dangerous cybercrime attacks are, and how to recognise and avoid them, to urge users to protect themselves from cyber attacks. In addition, the participants also recommened that ISPs should also provide users with advisory services to which they should address concerns and report suspected attacks by cybercriminals. In other words, ISPs should enable their customers to counter cybercrime. For two examples:

*We are ISPs, we provide services to the user; thus, we should take care of our users as well as our networks. Doing so, I think we should provide more information about how dangerous cybercrime is, how to recognise a dangerous website and how users can protect themselves at a basic level, as well as making available an advisor to users on where and who they should come forward to contact if they are attacked. (SP9)*;

*Personally, I think ISPs play an important role in regulating cybercrime because cybercrime might only be committed via the Internet, computer networks otherwise, it is just traditional crime. Meanwhile ISPs provide its services to its users, thus ISPs should take care of their users as well as their networks. I think ISPs should provide more information about how dangerous cybercrime is and how to recognise dangerous websites and how users should protect themselves at the basic level. (SP7)*.

Despite ISPs felt that they should take care of their customers by providing additional security to users, this would not be easy to implement due to the significant costs involved. In particular, interviewees were asked to outline what role ISPs should play in regulating cybercrime issues, and how this should be undertaken. The majority of
interviewees acknowledged that providing additional security to users would be the most significant cost for their services, although ISPs were in a good position to observe traffic flowing into and out of their services and that it would be relatively easy to apply technical support to stop suspicious traffic from entering their network services and so on. For that reason, some participants commented:

As you may know, we have expertise in this area, we can provide our best services to customers, including security protection such as antivirus programs. However, in terms of protecting customers from cyber attacks, we need to spend more money on that. The money we spend is not only for identifying the attacker, but also how to stop them, as well as adapting and developing new technical prediction software to improve protection against future attacks … in order to catch up with the new and even complicated techniques that attackers were using in order to avoid detection enabled by the developments and advances in technology. (SP2);

Personally, I think ISPs play an important part in regulating cybercrime because ISPs provide their services to users, and should take care of them as well as their networks. In addition, not all users have the same level of technical expertise required to properly patch or upgrade operating systems and software, update antivirus programs, and install hardware and software firewalls. Possibly, as ISPs, we could consider providing security to customers; however, we will face difficulties in doing that as it is costly providing equipment and possibly providing training in professional security. (SP10).

Following the results of the interviews above, it is reasonable to suggest that ISPs should provide some security services to their customers. However, barriers preventing ISPs from becoming more involved were found to be the most significant cost issue involved including the cost of identifying attackers, providing equipment to stop cyber-attacks as well as training in professional security. Therefore, it can be difficult and costly for ISPs to implement.

5.6. Reducing the growth of cybercrime in Vietnam – some possible approaches

The interview findings identified users as playing a significant role in relation to reducing the growth of cybercrime. In order to identify the users’ role, participants were
asked the question “What role should users play in the response to cybercrime?” Interestingly, 33 participants (94.2% of the sample) acknowledged that users have a primary, and crucially, important role in responding to cybercrime. A variety of reasons were given to explain why users play this important role. One of many interviewees explained the significant role a user plays in the whole cybercriminal process. Others considered that users have dual roles in relation to cybercrime: one not to create opportunities for cybercrime and the other to help reduce or even prevent cybercrime. The following below are specifically two examples:

*From my point of view, I would say human elements are a vital factor in every aspect of life, especially in preventing crime in general and cybercriminal in particular. Users have such an important part to play in the response to cybercrime because … users have two effects. One is creating opportunities for crimes to take place, the other or at the same time, users can act as a significant barrier to stop crime occurring. Thus, we can see that if users are aware of the risks of cybercrime, they can protect themselves, avoid creating any opportunity for cybercrime to take place. They also know where they can get help if they become victims of cybercrime. (PO3).*

*If user is aware of an attack before it happens, user can evacuate their sensitive data to safer places, so the cybercriminals cannot steal it even though they have broken into user system. (SP9).*

Similarly, other participants asserted the important role of human actions in relation to the appearance of crime in general, and cybercrime in particular. Thus, users can either be part of the cause of cybercriminal acts, or help to reduce them:

*We all see that a human element always plays a crucial role, even with the development of technological advancement; cybercrime could not exist without human actions. The core problem is that users act and react. In the other words, users’ acts can either create more opportunities or reduce the opportunities for cybercrime. If users are aware of the dangers they can face, they can be careful when they go online and prepare to protect themselves in order to avoid becoming a suitable target of cybercrime. Even if they do become a victim of cybercrime, they would know where to go and who they should advise that they were a victim. (PO1).*
In particular, one interviewee not only commented that user reaction was the best approach to fight back against cybercrime and that they should employ advanced technology to respond, but as a long-term response to cybercrime, user awareness needed to be increased and that simple precautions can be the most effective way of defending oneself from a cyber-attack. Simply put:

*Look, the human component is so important in the response to any crimes types. Thus, I would suggest that users have an important part in the response to cybercrime because user reaction is the best approach in place to fight back against cybercrime - although advanced technological development is no doubt successful in the fight against the cyber attacker. However, the increase of user awareness and users taking simple precaution can be the most effective defence in the long term. In doing so, I think users should be educated. Let me take an example to make it clear why users need to be educated ... in the physical world, we are all aware and suspicious of an item left unattended because we all know the potential consequence if it happens to be an item purposely left behind by a terrorist. In contrast, in the information age, it is very hard, even impossible to see the unattended item. Thus, if people are aware of or know the consequences of opening a suspicious email attachment or clicking on an untrusted website, they will then be more careful and reduce their chances of becoming a victim of cybercrime." (PO2)*

*I do believe that users play a vitally important role in the response to cybercrime because users are the most important factor in the complete process of response to cybercrime. Users can be the victims of cybercrime; users can also be the suspects of cybercrime. (SP3)*

*User have such an important part to play in responding to cybercrime because users can have two effects ... one is by creating opportunities for criminal acts to take, the other is to act as a significant barrier to stop crime occurring. Thus, we can see that if users are aware of the risks of cybercrime, they can protect themselves, avoid creating any opportunity for cybercrime to take place. They also know where they can get help if they become victim to cybercrime. (PO3).*

Expanding the role users can play in relation to reducing the opportunities for cybercrime, other interviewees expressed that users should be provided with
information on how they felt either by increasing user awareness on the dangers of cybercrime and/or how user safety could be improved through the use of available protection software. One interviewee described it as follows:

If users understand how ICTs system work and how dangerous cybercrime is, they might then protect themselves, create less opportunities for cybercriminal activities when operating in insolation. (SP10).

Another interviewee said:

“Users play a vitally important role in the response to cybercrime because they are aware of the dangers of cyber attacks, they can protect themselves at least from minor attacks or not go into the critical dangerous websites.” (SP5).

Technically, another interviewee suggested:

When users are aware of, or understand how to use ICTs safely, and use some of the available equipment such as firewalls, antivirus and anti-spyware software, then users can act as a solid gate to keep out cyber attacks or at least make themselves less likely to become a target of cybercrime. (SP7).

And one interviewee claimed that using software protection could be a form of guardianship:

It is similar to traditional crime – criminals are always seeking ways to commit criminal acts. Therefore, if users can have good security, such as using anti-virus software, a protection system, they will be able to prevent themselves becoming a victim of cybercriminal activities. (SP6).

Based on the findings from interviews, it appears there are possibly two main ways in which to reduce the growth of cybercrime via the role of users. The first is increasing the level of security measures via physical security. In other words, users should take action against cybercriminals by increasing the level of their computer security. The reason is that cyberspace is not so different from traditional space, and physical security measures should be used - computer security installed - to protect against cybercrime. Today, people should take action to protect themselves from cybercriminals by equipping their computers with one or more of the many kinds of available software, such as firewalls, and anti-virus packages. Failure to do so will potentially mean that users will become victims of cybercrime (Choi, 2008). Indeed, it cannot be denied that
in a computer connected to the external world via the Internet, security software is crucial to protect its users and its systems from malware, hackers and criminals.

Increasing levels of personal computer security are identified as part of ‘capable guardianship’ in Lifestyle Routine Activity Theory (LRAT). Guardianship can be subdivided into three categories as the following: formal controls, informal controls and target hardening activities (Cohen et al., 1981; Choi, 2008).

Formal control is the first category of guardianship, whereby law enforcement mechanisms plays the role of the guardian personal. As mentioned above, law enforcement mechanisms in Vietnam need to take more action in protecting individuals from being victimised by cybercriminals. However, the nature and characteristics of cybercrime create difficulty and challenges for investigators and prosecutors. In other words, the intangible nature of cybercriminal activities make it different from traditional crime in its nature. In addition, the consequences of cyber attacks can be intangible in nature; they are difficult to evaluate and predict. Furthermore, in order to regulate cybercrime effectively, law enforcement mechanisms are required to have a certain level of understanding of computer technology, and computer network literacy. Put differently, law enforcement mechanisms, even when equipped with the knowledge necessary to identify the suspects of cybercrime, need to obtain and process the digital evidence needed for an effective cybercrime investigation and prosecution. In fact, the increasing of number of cyber attacks year after year in Vietnam has illustrated the limitations of its law enforcement mechanisms. So, it is difficult to find formal guardianship provided by law enforcement.

Increasing the level of computer security can provide better protection for users against cyber attacks, such as malwares (virus, Trojan, worm or spyware) or hacking. In fact, maintaining security requires encompassing a wide range of activities, technical support and tools - such as using strong passwords, using digital security protection, for instance firewalls, intrusion detection systems, anti-virus, and anti-spyware software. However, it can be argued that the increasing level of computer security is not enough to protect users from cyber threats because anti-virus software and protection systems are limited by their design and each of them only deals with certain types of cyber threats and attacks (Cox, et al, 2009). In addition, as previously mentioned, cybercrime can change over time, manifest itself in different forms and become increasingly sophisticated. Therefore, protection systems need to be renewed or updated regularly in order to keep
up with new threats. In some cases, the time between the release of a new virus and finding a solution can be just long enough for the virus to spread or expand across the Internet, and in some instances solutions for a particular threat may not be possible (Wall, 2007). It leads to the possible conclusion that although technical guardianship is not enough for protection, if technical guardianship is kept up-to-date and employed correctly it can be crucial in helping to keep users more secure - in other words, it can help to reduce the rate of growing cybercrime. The role of users is not only important in terms of the proper use of technological protection, but also for changing the situation in which users potentially become victims. For example, Cox (2009) states:

“The capacity to change in response to circumstances and events is what makes the human effective as guardians. No matter how sophisticated and complex the “guardians” for the users of the Internet are, these are all mechanical devices. They are reactive. They designed to prevent actions that are already identified. They cannot respond to new instructions and criminal activity” (p. 313).

Increasing the level of computer security as an aspect of guardianship is well-supported by a wide range of empirical research (Grabosky & Smith, 2001; Yar, 2005; Holt & Bossler, 2009; Cox, et al., 2009), and although increasing the level of computer security is not completely effective in protecting users, it is still a crucial weapon to win the battle against the cybercriminal. Wall (2007) argues for “the use of technological means to change the physical environment of criminal opportunity so as to reduce it” (p. 192).

The second possible aspect is the increase of user awareness via education. As mentioned in Chapter 2 which sets out the analytical framework increasing user awareness via education is one useful method to control the growth of cybercrime; otherwise users can easily become either victims or offenders (Wall, 2008). The reason for this is that education is an effective method to transmit information, knowledge, skills, and laws to users in order to make them more confident to deal with the issues they might face online. In regulating cybercrime, the increase of users’ awareness provides basic information and advice to help them be more knowledgeable about computers, computer networks and their dangers.

Technological prevention is one possible method to protect the user from cyber attacks. However, if users lack a certain level of knowledge about the operation and limitations of antivirus software or the need to update it, then computer protection will be
ineffective. In relation to user awareness, if users are unaware of the need to take safety precautions and then disclose sensitive personal information via social networks or respond to an email asking for their bank account details – then they will be at increased risk of becoming a victim of cybercrime, even if they have installed the latest versions of computer protection software.

5.7. Conclusion

This chapter presented participants’ attitudes and perceptions in relation to cybercrime in general and the key factors that make cybercrime difficult and challenging to regulate. The findings gathered from a series of face-to-face interviews have allowed this research to establish the key challenge factors for regulating cybercrime in Vietnam as the following:

(1) Inconsistency in defining cybercrime can cause confusion when dealing with cybercrime issues. Participants provided their best understanding of the term cybercrime, and its associated terms. However, two approaches to understanding the term cybercrime appear to exist and it is still open to debate and for new definitions to emerge.

(2) The global nature and characteristics of cybercrime - trans-border, anonymity, advancement of technologies - appear to present the most significant challenge for policy-makers as well as Vietnamese law enforcement agencies.

(3) Limitations of current policies on cybercrime regulation can also create difficulties for Vietnamese authorities in their response to cybercrime.

(4) The inadequacy of policies on cybercrime regulation arises from the nature and character of cybercrime, the nature of the legal system and its inadequacy in addressing a wide range of cybercriminal activities forms, as well as simply unclearly worded laws and policies.

In addition, the research also found that Vietnamese law enforcement agencies are ill-equipped to regulate cybercrime due to a lack of human resources, training, and funding.
Chapter 6. Discussions

The overarching aim of this research is to explore the phenomenon of cybercrime and its regulation in Vietnam. This thesis was divided into four specific aims, as discussed in Chapter 1. A qualitative research approach has been adopted to achieve these four specific aims. An initial document analysis was undertaken followed by interviews to explore the perceptions and opinions of individuals from key regulatory institutions in Vietnam including Police, Prosecutors, Judges, ISPs, MIC and MOJ. A prominent outcome of the study was the value of gaining the points of view of such people directly involved in dealing with cybercrime in a variety of ways. They are the most likely people to understand the difficulties and challenges posed by cybercrime and the means by which current approaches could be improved in order to reduce the growth of cybercrime in Vietnam.

From the interview data, it can be seen that the transnational nature of cybercrime, not only contributes to making cybercrime difficult to define, but it also contributes to creating unlimited negative impact on individuals, organisations and the Vietnamese government. Two main ways of defining cybercrime were found in Vietnam in line with a number of research studies in different countries (Brenner 2010, 2012; Yar, 2013, 2005; Wall, 2015/2007). The transnational nature of cybercrime and the limitations of cybercrime regulation policy in Vietnam were also identified as the two key difficulties faced by the Vietnamese authorities in responding to cybercrime. In responding to the difficulties and challenges faced in dealing with cybercrime, there were two possible regulation approaches that could usefully be adopted towards reducing cybercrime in the Vietnamese context, as follows:

1. applying technical know-how and the necessary equipment to respond to cybercrime,
2. increasing awareness among internet users via education.

In the following sections, discussion of the research findings will be used to illustrate and highlight these two approaches. The four research questions presented in Chapter 1 are used to guide the discussion.
6.1. Research question 1: How is cybercrime perceived by high-level professionals from key regulatory institutions in Vietnam?

6.1.1. Defining cybercrime - perceptions of high-level professionals from key regulatory institutions in Vietnam.

With reference to the definition of cybercrime, the results of the interviews, unsurprisingly, show the existence of two ways to define cybercrime in Vietnam. One approach is more common than the other. The most common definition of cybercrime is based on the relationship between crime and networked computer technologies, particularly the Internet (85.7% of participants). Simply put, cybercrime arises from consideration of the role of computers, computer networks and the Internet in relation to criminal activity. From this perspective, the interview findings suggest that cybercriminals could appear in any of the following three situations. Firstly, cybercrime can occur where the computer is an instrument used to assist in the commission of traditional crimes such as fraud, identity theft, child pornography and so on. These crimes are, somehow, ‘traditional crimes’, but the perpetrators are taking advantage of new technologies to commit these crimes. However, they are not easy to respond to, or detect, because physical proximity is no longer intrinsic to committing the crime and the criminal’s capacity is now amplified by advanced technologies. They may commit the crime anonymously and without leaving a single trace. Thus, traditional investigation procedures, including searching and seizing, may not be suitable to detect crimes.

Secondly, cybercrime occurs where the computer is incidental to the commission of the crime. This includes all traditional crimes that are merely facilitated by advanced technology. This type of crime, in fact, can be committed without utilising cyberspace or advanced technology. The use of advanced technology just helps criminals to complete these criminal acts more quickly, and makes their crimes more difficult to detect. Thus, the computer system network is neither the principal factor in the crime nor the core of the crime. However, the use of advancing technology such as encryption or digital software make it easier to conceal or hide criminal activities and make them harder to be traced and investigated.
Finally, cybercrime occurs where the computer is the subject or target of crime. This consists of those forms of criminal conduct in which the victim’s computer is the actual target of criminal action. In fact, this includes traditional crimes such as theft and criminal damage. In this way, the victim’s computer is simply a property and the criminal’s purpose is to steal or damage the victim’s computer. On the other hand, the target of the crime may not be to steal data or software, but instead, to alter the data or the software contained in the victim’s computer by such means as, for instance, a destructive virus or denial of service attacks.

A second approach to defining cybercrime was identified by the remaining participants (14.3% of participants) and focuses either on a specific type of cybercriminal activity or on the motivation behind the attack. This approach is limited to the scope of whichever act or law the activity is determined to be criminal by the Penal Code. This approach suggests a more limited scope of cybercriminal activities in comparison to the others. In other words, some cybercriminal activities have not yet been classified as a cybercrime.

The findings in relation to the definition of cybercrime in Vietnam was viewed as similar as the other studies conducted in other countries (Brenner, 2012, 2010; Yar, 2013; Wall, 2015/2007). All came to conclude that there does not yet seem to be any formal agreement upon the definition of cybercrime at a national or international level. Thus, two ways of defining cybercrime still exist. For example, Thomas and Loader (2013) define cybercrime as “computer-mediated activities which are either illegal, or considered illicit, by certain parties and which can be conducted through global electronic networks” (p. 3); Vito & Maahs (2015) define cybercrime as “a criminal act that is committed using a computer that occurs over the internet” (p. 296); the UK government defines cybercrime as follows it “can be either cyber-dependent crime - committed only through the use of Information and Communication Technology devices, where the devices are both the tool for committing the crime, and the target of the crime; or cyber-enabled crimes that are traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT” (HM. Government, 2016, p. 17).

It can be seen that both approaches to cybercrime provide unique common features that, regardless of being either first or second approach, make them different to criminals in the physical world. These characteristics present a challenge to Vietnamese citizens, businesses, the Vietnamese government, and the Vietnamese criminal justice system in
keeping pace with cybercriminals. Previous studies, such as Goodman (1997); Grabosky & Smith (2014, 2001); Moitra (2005); Wall (2015/2013/2007/2001); and Brenner (2010, 2012) have suggested that the unique characteristics of cybercrime not only make it distinct from traditional crimes, but also provide a key reason for its complexity. The unique characteristics of cybercrime also make prevention, policing, investigation and prosecution more difficult.

6.1.2. Unique characteristics of cybercrime - perceptions of high-level professionals from key regulatory institutions in Vietnam

6.1.2.1. The global nature of cybercrime

Interestingly, all participants within this research clearly stated that the global nature of cybercrime is one of its unique characteristics. This unique characteristic is related to the ways in which cybercrimes are committed. For instance, some Police officers suggested that cybercrime can ‘occur anywhere’, and that cybercriminals can operate in ‘different places at the same time without any physical barriers’. One participant asserted that cybercrime is a borderless crime. In other words, the scope of opportunity for cybercriminals to commit crime is significant or even unlimited. It can happen anywhere within Vietnam’s physical boundaries, but it can also be outside of Vietnam’s boundaries. For example, malicious software can spread to millions of computers within Vietnam or other countries with ease, through emails or social networking sites. Child sexual abuse images can be made available in every country, including Vietnam that has Internet connectivity, with a single click. This issue was explored (Wall, 2015/2013/2007; Brenner, 2012, 2010; Yar, 2013, 2012, 2006; Holt et al., 2015; Clough, 2015, 2010.) All have concluded that cybercriminals can act freely from both geographical and physical constraints.

In relation to this, 100% of Police officers reported that this global feature is a problem for them when they deal with cybercrime. The participants have addressed the problems caused by this feature which can include legal jurisdiction problems, problems for Police officers in identifying where cybercriminals are located, problems identifying exactly who is responsible and problems in determining the best means of collecting evidence. Typically, in relation to the legal jurisdiction problem, 71% of interviewees...
agreed that the Vietnamese legal system cannot regulate cybercriminal activity when it is situated outside of Vietnam’s physical boundaries. Only 29% of interviewees did not mention this, even if they agreed with the idea that the transnational aspect of cybercrime is a distinctive feature.

The legal jurisdiction problem was highlighted by a majority of participants. They explained that Vietnamese law defines a ‘criminal act’ as set out by Vietnamese law and located within Vietnamese boundaries. This means that if some illegal activities are not regulated by Vietnamese law, they could not be considered as a crime in Vietnam, even if the illegal act is located within Vietnamese boundaries. Additionally, the power of law is limited by Vietnam’s physical borders. In other words, cybercriminal acts that are located outside of Vietnam’s physical borders cannot be subject to criminal sanctions by Vietnamese laws. Thomas et al., (2015) mentions that the global reach of cybercrimes offered by advanced technologies has created substantial difficulties for law enforcement agencies at the national and international level in enforcing cybercriminal law globally. This is due both to the natural limitations of law and the natural characteristic of cybercrime as offered by advanced technology. This issue will be further discussed in the sections below.

Problems in identifying criminal suspects were reported by all Police officers interviewed. They explained that the identification of a criminal suspect and where the criminal act is located are vital tasks for the Police. Criminal sanctions can only be imposed when a criminal suspect is identified and without either a suspect or a location/scene of crime, it is difficult for an investigation to move forward. The aim of identifying criminal suspects is crucial to stop the suspect from committing further criminal acts and to deter other criminals that might offend. A further problem in this regard is that the Vietnamese police agency is territorially-based and operates within Vietnamese legal jurisdiction. Supporting this argument, research studies in other countries (Brenner, 2012; Clough, 2016, 2010; Yar, 2013) have shown that every law enforcement agency is located in, and derives its authority from, a particular country. Thus, it can be understood that a law enforcement agency from one country has no legal authority to conduct a criminal investigation within the territory of another country. Because of this it is usually difficult, or even impossible, for law enforcement agencies to apprehend cybercriminals who are located in another country. Police officers also
stressed the problem of demand: that it was difficult to provide an effective response to
cybercrime without recruiting more staff and more resources.

Similar to identifying criminal suspects, collecting evidence is also considered to be a
problem for Vietnamese law enforcement officials, especially, when it involves
collecting evidence from another country. Collecting evidence is an important task for
Police officers. Evidence can be collected via search and seizure. Being able to search
for, and seize, evidence requires the identification of a victim, a suspect, or even just a
scene of crime. The Police officer needs to know where to search, and what to search
for, in order to obtain search warrant approval. In addition, there can be different
conceptions of what constitutes evidence between legal systems. Police officers also
pointed out that even when they know who, where and what to search they still can be
challenged by the fact that some, or all, of the evidence exists in another country, and
even where a reciprocal arrangement exists, it is still a time-consuming and costly
procedure.

The issues highlighted above were also found to relate to the matter of collecting digital
evidence which can be easy to remove, exchange or even destroy. Some scholars
(Brenner, 2012; Casey, 2011, 2002) have warned that digital evidence can be
manipulated easily or altered either maliciously or accidentally by offenders during
collection. In relation to digital evidence, some Police officers said that they needed to
have a new form of facility which can support and store digital evidence safely, this
suggests a need for more resources. They also pointed out that not all Police officers
have sufficient computer networking skills, therefore, it can be even more difficult
when dealing with cybercriminal evidence.

6.1.2.2. The issue of anonymity

There were 27 (77.1%) participants who found that anonymity is a distinct and difficult
phenomenon to be addressed. They explained that cybercriminals can conceal or
disguise their identities in a way that is impossible in the real world. There is, in fact, no
requirement to force users to reveal their identity when using the Internet. In addition,
cyberspace allows cybercrime to be committed from a distance, that is to say, a high
degree of anonymity is achievable. Furthermore, cybercriminals can take advantage of
the rapid development of advanced technologies to hide their identities by using special services or software, such as encrypted, remailers or zombies, which makes it even more difficult to identify and apprehend cybercriminals. Anonymity could be maintained from the beginning to the end of the process of committing a crime. Anonymity could potentially enable criminals to commit large-scale offences with fewer personal risks and costs. Meanwhile, traditional criminals have to use various techniques to avoid revealing their identity and to disguise certain crime scenes. The findings confirmed a clear distinction between traditional criminals and cybercriminals, indicating that this can be a key challenging factor for investigations in identifying where cybercriminals were situated, and who exactly was responsible for a crime. The findings of this research were found to be similar to others (Grabosky & Smith, 2001, Wall, 2015, 2007; Yar, 2013, Thomas and Loader, 2013). It is surprising that no one has mentioned the general misconception that online activities are, in fact, not anonymous. Actually, “networked technology leans in the opposite direction, to the point that we are now in danger of experiencing what has been described as the ‘the disappearance of disappearance’ (Haggerty & Ericson, 2000, p. 605)” (Wall, 2011/2007). Starting from cybercrime, since it is enabled or dependent on the Internet, gradually all crime opportunities can be pro-actively designed out of new software technologies (Wall, 2011/2007). This is especially relevant with the arrival of the Internet of Things (IoTs). It is clear the Vietnamese authorities have not foreseen a future of crime regulation, wherein code is law (Lessig, 1999, 2001).

6.1.2.3. The advancement of technology

Technological advance was found to be another factor facilitating cybercrime as reported by 26 (74.28%) participants. They explained that cybercrime used various tools and techniques in order to commit criminal acts more easily than before. The development of technology has changed criminal behaviour over time. In addition, advanced technology has made it more difficult for law enforcement agencies to deal with crime as it requires using even more specialised technical equipment. In doing so, this required agencies to find more money to buy similar or even higher-level technical equipment and was also very time-consuming. This is consistent with the literature in Chapter 2 – cybercrime in general and Chapter 4 – cybercrime in Vietnam. All came to
emphasise that advanced technology creates more ways and more opportunities for criminals to commit their crimes.

This finding is supported by a number of research studies (Clough, 2015, 2010; Wall, 2015/2012/2007; Brenner, 2014, 2012, 2010; Gillespie, 2016; and Yar, 2013, 2012). They all illustrate that advanced technologies have transformed criminal behaviour to become automated, professional and even de-skilled. The development of advanced technology is creating more opportunities for cybercrime by changing the skills level required (Wall, 2015). For example, a few years ago, cybercrime required a criminal to have a certain skill level to commit criminal acts but now this is changing dramatically. Cybercrime can now be committed by renting or buying software, programming skills/toolkits via crime aware-as-a-service (Wall, 2015). Cybercrime is increasingly sophisticated, and allows criminals to commit many crimes or a large crime with little risk to themselves.

As explained in Chapters 2 and 4, the scope/scale of cybercriminals is potentially expanded by key characteristics such as globalisation and anonymity. Advanced technologies add to ‘scale’ by allowing contact with a vast number of people worldwide creating new forms of networked social relationships. Thus, cybercrime can act as a ‘force multiplier’ and advanced technology can be a powerful tool for cybercriminals (Yar, 2013, p. 11; Clough, 2015, p. 6). In other words, advanced technology represents a formidable challenge for law enforcement agencies (Wall, 2015).

The advancement of technology is considered as an important aspect to facilitate social and economic development. This, indeed, is especially true in the case of Vietnam. As pointed out in Chapter 4, the Vietnamese government has prioritised the development of advanced technology, encouraging individuals, businesses, organisations, and government agencies to apply advanced technology in their work, businesses, and services. In so doing the Vietnamese government has considered the development of advanced technology as a national plan and created several projects to implement such a plan. As a result, the number of Internet users has increased year after year, and many social networks have also appeared, dramatically increasing their numbers of users (please see Chapter 4). Vietnam has also become a hotbed of cybercriminal activity.
6.2. Research question 2: How adequate are the current policies responding to cybercrime in Vietnam?

The perception of high-level professionals from key regulatory institutions regarding cybercrime regulation policies in Vietnam plays a vital role in identifying how efficient or not cybercrime regulation policies are in Vietnam. Therefore, gathering the points of view of high-level professionals from key regulatory institutions above current cybercrime regulation in Vietnam is significantly valuable. It not only serves to show how the current Vietnam Cybercrime Regulation Policies (VCRPs) are implemented as a way in which to tackle cybercrime, it also assists Vietnamese policy makers to improve future cybercrime regulation policies if required.

Outcomes regarding Question 1 are very closely related to Question 2. As already identified in subsection 6.1.2 there were several aspects of cybercrime which provided challenges for Vietnamese legal authorities to manage it. The result of the interviews has indicated that the viewpoints of participants are influenced by individuals' backgrounds and where they work. In regard to the discussion of the current VCRPs, therefore, what they considered the natural aspects of cybercrime were very much related to what they have faced in order to perform their tasks in dealing with cybercriminals effectively. Therefore, the point of view of each participant on the current VCRPs has been identified. According to the interview results, two main factors were found to affect the current VCRPs. The following subsections below illustrate the two key challenges regarding the response of the current VCRPs.

6.2.1. The natural limitations of the VCRPs - Jurisdictional/Transnational issues – a major factor that reduces the effectiveness of VCRPs.

As previously mentioned, the nature of the Internet is considered to be the major factor that not only impacts on the ways in which people, businesses and organisations interact with each other, it also significantly affects the Vietnamese legal system and law enforcement agencies. The significant effect of the nature of cybercriminal activities offered by the Internet was, in one way or another, indicated by the majority of participants, especially Police officers. They agreed that the transnational characteristic
of cybercrime imposes many difficulties and challenges for the Vietnamese traditional legal system, and Vietnamese law enforcement also. The transnational characteristic of cybercrime possibly even demolishes some aspects of Vietnam’s traditional law enforcement system. The nature of cybercrime was identified by participants in this research study, including characteristics such as: transnationality, anonymity and advancement of technology.

In relation to the current Vietnamese cybercrime regulation policies, all participants were asked the same questions: some ‘open’ and others ‘very closed’. The interview results suggested that the effectiveness of Vietnamese law in relation to cybercriminal is limited by the three characteristics cited above. As mentioned above, the transnational characteristic of cybercrime is a crucial factor that has a significant effect on the effectiveness of the VCRPs. In other words, the transnational characteristic of cybercrime becomes an obstacle for Vietnamese law enforcement agencies to undertake their legal powers to protect Vietnamese citizens. Police officers, for example, explained that cybercriminals can be anywhere within and beyond physical Vietnamese borders. They, further, pointed out that the Vietnamese legal policy cannot be used to deal with cybercriminal activities committed outside of Vietnamese borders.

As demonstrated previously, cybercrime extends far beyond national boundaries, including Vietnam’s. In other words, the nature of transnational cybercriminal defies notions of geography and distance. The effect of a cybercriminal action may be felt immediately throughout the world regardless of location, it is not merely confined to a certain localised area. Rather, it can have an impact on every location within the cyberspace environment instantaneously. Thus, the effect of cybercriminal actions are naturally not limited by geography, because distance is largely irrelevant in cyberspace. In contrast, the effectiveness of the VCRPs is based on its boundaries and jurisdiction. This means that the effectiveness of the VCRPs is completely limited by physical geography. Vietnamese authorities cannot undertake their own procedures on illegal action which happens outside of Vietnamese boundaries. Other requirements such as a reciprocal legal arrangement can be put into place but even this is significantly complicated and sometimes even impossible to achieve.

Similar to the effects of VCRPs, the powers of the Vietnamese authorities are naturally limited to Vietnamese borders. The ability of Vietnamese authorities to exercise their physical power exists only within Vietnamese boundaries and jurisdictions as described
in law. The Vietnamese authority cannot impose any sanction to any harmful/illegal activity that is not within Vietnamese jurisdiction. Even if a harmful/illegal activity is found within Vietnamese jurisdiction and borders, a Vietnamese authority is still challenged by tracking down and finding offenders as the Internet is designed to operate openly and logically rather than geographically. In other words, the Internet is primarily programmed to deal only with finding the logical location of a computer; it is not the physical location of the computer with that address or the person behind that address.

Consistent with previous studies (Furnell, 2002; Brenner, 2013, Wall, 2007) the transnational characteristics of cybercrime are evidently key factors that make cybercrime regulation policy less effective in response. The transnational characteristic of cybercrime appears to be regarded as a significant challenge by the majority of participants, which may be a reflection of the difficulties they have faced in regulating cybercriminal activity. Cybercriminals make geography irrelevant and make themselves difficult to identify in the whole criminal chain therefore making it difficult to secure sufficient evidence to undertake prosecution. It is also increasingly difficult to enforce national laws against activities which are considered offensive or harmful to local taste or culture (Katyal, 2003).

Furnell (2002) identified that legislation is naturally less effective in response to cybercriminal activity by three inherent aspects: 1) legislation is national in nature and legislation can only take effect within national boundaries 2) inconsistency of laws, regulations and procedures across countries can make it difficult to establish cross-border investigations; and 3) the criminal’s extradition may be required in the event of identifying their geographical location and this requirement is not easy to achieve.

In addition, the aim of the VCRPs is to deal with criminal activity that violates Vietnamese law, this means that crimes and criminals must be identifiable. However, cybercriminals can take advantage of the relative anonymity provided by the Internet, and some can enhance this using high tech procedures such as software encryption to completely remain anonymous in order to avoid detection (Brenner 2004, 2012; Grabosky & Smith, 2001; Wall. 2012/2007/2001; Yar, 2005, 2013). Anonymity was viewed as another factor that created a challenge for VCRPs to deal with it. It is viewed as both a cause of increasing the volume of offending and obstructing efforts to identify culprits (Brenner, 2008; Casey, 2002).
6.2.2. The inadequacy of the Vietnamese Cybercrime Regulation Policies (VCRPs)

Inadequacy of the VCRPs was, in particular, found to be another key factor that make the VCRPs less effective in regulating cybercriminal activities. Contributing to this, the interview results suggested two main aspects, 1) that all aspects of cybercriminal activities have yet to be fully covered, and 2) unclear legal provisions. The following subsections below present these in more detail.

6.2.2.1. The lack of coverage

The majority of participants with experience in making cybercrime regulation policy and cybercrime regulation in practise noted that key factors which make the VCRPs inadequate to address all aspect of cybercriminal activities to be included: (1) the development and expansion of ICTs into almost all aspects of socio-economic life have gone far beyond the development of the VCRPs; (2) the VCRPs mainly focus on interpreting the legal application for ensuring ICTs can be applicable to assist social and economic development rather than addressing cybercriminal activities.

When talking about how the current VCRPs respond to cybercriminals, the majority of participants (74.8%) tended to blame the development of technology which is quicker and faster in comparison to legal regulations. This can be a reasonable complaint, due to the fact that the development of technology in Vietnam has rapidly increased since the country announced its political reform in 1986. More importantly, as mentioned in Chapter 4, the Vietnamese government has strongly recognised, and believes the development of advanced technology to be a crucial aspect to assist the country is its continued development. It not only improves the lives of Vietnamese citizens and makes businesses, and other services work more efficiently; it is also a significant part of the process to assist in Vietnam becoming a modern and industrialised country. Thus, the Vietnamese government has given more priority to the development of advanced technology.

Adding to the problem of legal policy always lagging behind the development of technology is the matter of legal processing. According to the Law Commission of
Legal Documents, the creation and announcement of any legal document is obviously a long process. It can take several months or years, depending on the type of legal document, and level of authority behind it. For example, the Law on Information Security was proposed and drafted in 2012, but was only approved in late 2015. Yet there is no guarantee that during the period of obtaining legal approval, there is either no appearance of new technology or a new emergent form of criminal activity.

Moreover, as an illustration of how the current VCRPs fail to cover all aspects of cybercriminal activity, the majority of participants provided an explanation as to how far and how many times the Vietnamese Penal Code has been revised, and how many laws in relation to ICTs activity have been created. In fact, the Vietnamese Penal Code has been revised several times. For example, in 1999, for the first time, the Vietnamese Penal Code had three provisional regulations inserted in relation to cybercriminal activity. Then, in 2009, the Vietnamese Penal Code was revised a second time to include more provisional regulations regarding cybercriminal activity. The Penal Code was recently revised in late 2015 to supply more provisional elements in respect to cybercriminal activities. Generally, it can be agreed that the latest revision of the Penal Code is comprehensive and describes more cybercriminal activities. The Penal Code is still behind the development of technology for a number of reasons previously mentioned. In addition, during the period between 1999 and 2016, there were two specific legal regulations in relation to ICTs activities created, one was enacted in 2006, (the Law on Information Technology) and the other was recently enacted in late 2015 (the Law on Online Information Security).

As suggested in Chapter 4, the Vietnamese government has considered and given priority to the development of ICTs in the way in which ICTs can help the country’s economic progress. This is a reason why ICTs have been applied and the use of the Internet has been expanding in almost every economic sector, including that of the individual user in Vietnam. Furthermore, the VCRPs were mainly viewed as focusing on the legal application for ensuring ICTs can assist social and economic development, rather than addressing cybercriminal activities. There was no explanation from interviewees as to what the key reason was for the Vietnamese government doing this. However, looking at the context of a transitional country like Vietnam it is understandable. Because the country had experienced a long and devastating war for many years, and a long period of poverty, starvation, and low living standards, all
policy and strategic priorities were for economic development. Vietnam devoted all its efforts, including creating its laws and regulations, to contribute to the concentration and the development of the economy and other sectors to improve living standards for its citizens.

It is worth noting that the Vietnamese government has made every attempt to harmonise its laws in order to protect its citizens from the harmful activities of the Internet, in order to integrate with the international community. However, the technology, and the criminals who use this technology, are moving faster than legislation. It does seem to be that the findings in this regard are consistent with other studies which have been carried out by a number of scholars (e.g., Moitra, 2005; Nasheri, 2005; Wall, 2007; Brenner, 2012). All conclude that legislation dealing with cybercrime has had a very limited deterrent effect and has been very slow to catch up with the problems exposed by the cybercriminals.

In short, the interview results suggest that without an appropriate level of law and policy to keep up with developments, the Vietnamese Penal Code is less effective in responding to cybercriminals. In other words, without an appropriate level of cybercrime regulation policy, including an up-to-date regulatory framework, cybercriminal acts are more likely to continue to increase in Vietnam.

6.2.2.2. The complex nature of legal language

Despite the problems described above, the Vietnamese Cybercrime Regulation Policies (VCRPs) were viewed as an important tool in response to cybercrime. It nonetheless requires greater clarity and transparency to ensure that it is widely used by the general public and the legal authorities, legal regulation is generally viewed as a formal tool to combat criminals. The VCRPs are, of course, the formal legal tool to deal with cybercriminals in Vietnam. In the light of Routine Activity Theory (RAT) (Cohen & Felson, 1979), the VCRPs are a formal legal framework for Vietnamese law enforcement officers to use in order to tackle cybercriminals, and to protect the legitimate interests of individuals, organisations and nations. It seems to be a major legal tool not only for Vietnamese legal authorities to deal with cybercriminals, but it
also seems to be used by the general public in order to protect themselves or to avoid becoming either a victim or a potential cybercriminal.

As the major legal tool, the VCRPs do seem to significantly influence how Vietnamese enforcement agencies react to cybercriminals. The majority of participants were aware of the existence of the VCRPs and would apply it in attempting to regulate cybercriminals. However, participants perceived that the current VCRPs were limited in a number of ways, and that, in turn, limited law enforcement agencies in their ability to combat cybercriminals effectively. The main limitation of the VCRPs was that they were “unclear, hard to understand in terms of its legal language used” negatively influencing law enforcement agencies’ responsibilities and abilities to react to cybercrime and perform tasks.

Meanwhile, awareness of the VCRPs is seen to be vital to respond effectively to cybercriminals. In fact, research participants, particularly Police officers, raised this issue to indicate that they were aware of the VCRPs, particularly, the Law on Information Communication Technology and the Penal Code that could be used to regulate cybercrime. However, as already noted, they also claimed that these legal regulations were hard to understand, and difficult to implement.

6.3. Research question 3: Who should be the key players in the regulation of cybercrime in Vietnam?

Interviews with a wide range of people working across seven institutions focused on gaining more insight into the perception of responsibility for cybercrime regulation in Vietnam. These interviews added greater depth, not only in understanding the key factors influencing the growth of cybercrime in Vietnam, but also understanding which should be the key role players in relation to cybercrime regulation in Vietnam. An ‘open’ question was used to address these issues. The most notable finding from the interviews was that the role of the prosecutor and judge were considered less important in relation to preventing cybercrime by the research participants. As there was insufficient evidence around these roles, they will not be discussed further.

Interestingly, Internet users were not considered to be the principal focus of this research; however, the interview findings indicated a perception among participants that
there is, or should be, a significant role for users in reducing the growth of cybercrime in Vietnam. The interview results also show that Police institutions and ISPs are the key players in reducing the growth of cybercrime in Vietnam. This is consistent with previous research, which has identified that Internet users (Marcum, 2008; Choi, 2008; Holt & Bossler, 2009; Reyns et al., 2011; Bossler, Holt & May 2012); ISPs (Schachtman, 2011, Rowe et al., 2011; Moore and Anderson, 2011; Murray, 2013) and the Police do have, should have, or are regarded as having, significant roles to play in reducing the growth of cybercriminal activities in Vietnam. In the light of RAT (Cohen & Felson, 1979) these groups (users, the Police, ISPs) can act as capable ‘guardians’ in slowing or stopping the growth of cybercriminal activity. The subsections below outline aspects related to each role as they emerged from the interviews.

6.3.1. Internet users

The role of Internet users was regarded as significant in reducing the growth of cybercrime (91.4%). Participants suggested that users play a role in preventing, facilitating or initiating criminal acts as both victims or offenders. It was suggested previously that Routine Activities Theory (RAT) could be used to explain how and why cybercrime occurs, in general, and in the Vietnamese context in particular. According to RAT, users can be the most effective and capable ‘guardians’ in terms of reducing the growth of cybercrime. Users can be the most effective means of crime prevention, reducing the opportunities for cybercrime. As suggested from the interview results, users can become capable guardians by either: i) increasing the level of their own security measures or; ii) increasing awareness of using computer networks. These findings are consistent with previous studies (Marcum, 2008; Holt & Bossler, 2009; Reyns et al., 2011; Bossler, Holt & May 2011, Wall. 2010/2007). Users can undertake preventative action by employing or installing software solutions such as anti-virus software, and firewalls. Whether or not users take such action may be a reflection of their own perception of the risk of using computer networks.

Choi (2008) identified the positive influence that users can have on the reduction of cybercrime by applying antivirus, antispyware and firewall programs. Similarly, this research suggests that using available protection equipment such as firewalls, antivirus,
and anti-spyware software, users increase their security measures making themselves a harder target to attack. Whilst the impact of using available protection equipment was not assessed within the present study, the majority of participants claimed that using protection programs could help users avoid becoming ‘a target of cybercrime’ and ‘a solid gate’ to keep out cyber - attacks.

The role users play was associated with developing knowledge, particularly regarding understanding the risk of using computer networks, as well as using the potential availability of protection products in order to become a hard target. As Felson (2006) argued, for guardians to be effective in crime prevention, the user must be knowledgeable about their immediate surroundings and the context. In the context of the Internet, the user must be able to recognise what act can be observed as criminal or deviant. In doing so, the user should be properly educated, in other words, users should increase their awareness of using computer networks and cybercriminal threats via education.

Increasing levels of user awareness is a crucial factor which needs to be added to the role of the capable guardian. As mentioned in the literature review chapter, increasing a user’s awareness is the first and foremost measure to protect the user from cybercrime. Although increased awareness of users does not seem to have an immediate outcome, it is valuable in the long-term for regulating cybercrime. The fact is that cybercrime is about users’ acts. An individual’s acts are dependent on their awareness/perception. In turn, an individual’s awareness impacts very much on their reactions and leads individuals to constrain their behaviour. Similarly, individuals’ actions are the result of the choices they make based on anticipated consequences (Cook, 1986). Increasing awareness of individuals about threats or dangerous online environments, in turn, prompt individuals to take defensive measures (Rountree & Land, 1996). In other words, if individuals are aware of dangerous cybercriminal activities or consider themselves at risk of cybercrime, they will conduct their activities online more carefully, using more security tools and taking more precautions (Cohen & Felson, 1979; Ferraro, 1995; Hindelang et al., 1978). Moreover, human acts are a natural cause of occurrences of crime or the prevention of crime. Thus, increased awareness of course can help users to identify whether their computer has, for instance, correctly installed security software, or to assess the security of a particular website as they go online. In other words, awareness helps them to avoid becoming victims of cybercrime. It also
helps users to know where to go to be able to report an attack by cybercriminals and to get advice in such instances.

6.3.2. Internet services providers (ISPs)

The role of ISPs in the context of cybercrime regulation in Vietnam was naturally recognised and understood to be important in ensuring the security of networks and regulating online illegal activities, by relevant participants, and especially by members of the ISPs themselves. The majority of participants (77%) suggested ISPs have an important role in relation to controlling cybercriminal activity. This involvement reflects the natural position ISPs have in securing the Internet.

The results of the interviews identified two key features in which the role of ISPs can act to increase their security services, and protect their customers from cybercriminal activities, including providing and using additional security protection, and providing security advice services. In other words, ISPs can provide defensive measures against cybercriminal attacks. Providing defensive measures identified by the participants in this research, such as firewalls, antivirus software, security advice and security information, can all contribute to improving the protection of users against cybercriminal attacks. ISPs were in a position to enable users to improve their understanding of how to use computer networks safely, how to protect themselves from cybercriminal attacks, and even where and who they should go to report attacks and seek advice. Providing defensive measures improves the early identification of online crimes or of new security vulnerabilities. Early detection and monitoring can prevent possible attacks or minimise their impact. Providing security measures was identified as important to help users become less vulnerable to cybercriminal attacks; and it was suggested that this should fall within the ISPs role. ISPs’ staff expressed the opinion that ISPs are in a good position with their facilities and professional experts to become a ‘hard layer’ to prevent/disrupt cybercriminal attacks. This expression was similar to that found in previous studies (Lichtman & Posner, 2004; Institute for Homeland Security Solution, 2011) where, providing either fully external or internal, or even partially internal/external security solutions was identified as central to increase the security of ISPs’ networks and the protection of ISP users.
The findings of the present study reinforce previous research findings which suggest that ISPs are in good position to protect their customers’ network (Shachtman, 2011, Rowe et al., 2011; Moore & Anderson, 2011; Murray, 2013) because they connect users to the Internet, they have their own relationships, and ultimately, although not intentionally, they provide the venues from which, and in which, cybercriminals can operate (Peterson et al., 2014). In addition, they have the equipment and the expertise to monitor their services and influence online behaviour (Wall, 2011). This highlights the nature of the position of ISPs and also the potential power of ISPs that can be put in place to reduce the growth of cybercriminal attacks. It seems important therefore, to encourage ISPs to take on these roles, in order to ensure security within their networks, even though ISPs are naturally immune from liability for this role.

Applying RAT (Cohen et al.; 1979), providing defensive measures through ISPs can indeed constitute ‘capable’ guardianship. According to Cohen et al. (1981) using defensive measures either by their presence alone, or by some sort of direct or indirect action, will reduce the occurrence of cybercriminal activities. In other words, users will be more protected or secured by the increased use of any defensive measures. In contrast, Cohen et al. (1981) indicated that users are less guarded either by any defensive measures which means it is considered as a suitable target by offenders because they show little or no resistance to crime. Defensive measures appear to be very important for reducing the opportunities for criminals, which in turn decreases the numbers of crimes committed (Miethe & Meier, 1994).

Providing additional security measures was found to be a ‘hard layer’ of capable guardianship to protect users or make cybercriminal attacks difficult. However, this approach, on the other hand, was also identified as a significant cost for ISPs. The cost was found to include the cost of identifying the attacker, the cost of providing and updating equipment to stop cyber-attacks, and the cost of training personnel and users in professional security.

Additionally, providing information about cybercrime was seen to be vital in relation to the protection of users, although it does not necessarily have an immediate effect. Information helps users to be aware of, amongst other things, the seriousness of cybercrime, the consequences of cybercrime for the victim and how to recognise dangerous websites.
6.3.3. The police

Unsurprisingly, all of the Police officers interviewed considered the Police to play a leading role in regulating cybercrime. Meanwhile, all participants were asked, ‘who should be responsible for combating cybercrime?’ 88.5% responded by saying that the Police had an important role to play in regulating cybercrime in Vietnam. According to RAT, the Police constitute a formal capable guardian in terms of criminal investigation and crime prevention.

Traditionally, Police play an important role in protecting the legitimate interests of a nation, organisations and individuals, and maintain social order. In Vietnam, the Police are a government institution. On behalf of the government, the Police are responsible for managing social and public order in the country, securing the country and preventing any harmful activities by enforcing national law. This role is clarified by the Vietnamese constitution, the Penal Code and other legal documents.

From the Police officers’ perspective, their legal role is determined and recognised by Vietnamese law and society. In other words, the Police are a formal capable guardian as they are empowered locally to undertake legal action within nation states, and under national laws to maintain social order, protect the legitimate interest of individuals, organisations, government and nation. Additionally, the Police play an important role in enforcing criminal sanctions upon offenders, including online criminals, even if they play a comparatively small role (Wall, 2011).

Playing a leading role in response to cybercriminals, it was suggested that the Police would benefit from receiving greater support from other parties, such as individuals, organisations, and ISPs. In particular, support from skilled people and organisations would help the Police respond to cybercrime more effectively.

The interview results also indicate a number of key challenges for the Vietnamese Police. The key challenges were found to include identifying suspects, the searching and seizure of evidence, and human resources.

The results from interviews indicated that identifying the suspects of cybercriminal activity was the most challenging task in cybercriminal investigations. Identifying suspects is always the first task in a cybercriminal investigation. Police officers focused
more heavily on how to identify suspects in order to take action such as arrest or search and seizure. They also stressed the importance of preventing such criminal acts being committed again, or to prevent new criminal acts from taking place. This reflects on the role that Police officers have as formal guardians. However, identifying the suspects in cybercriminal cases is, as already identified, a complicated task because of the nature of cybercriminal activity such as transnationality, anonymity, and automated activity.

The searching and seizure of evidence was found to be another challenge for Vietnamese Police agencies. Criminal evidence is crucial to criminal investigation in determining whether a criminal act was committed or not. However, evidence in cybercriminal cases is also digital evidence, that is, beyond physical form. As illustrated previously, evidence in cybercriminal cases can easily be altered, copied, stored or removed and digital evidence can be easily or naturally affected by using electricity (Conly, 1989). Digital evidence is not as simple and easy to manage as traditional evidence, because digital evidence has little or no physical manifestation (Kerr, 2005). Additionally, digital evidence sometimes exists only for a period of time, ranging from a fraction of a second to many years. Thus, the combination of the unique feature of cybercrime with the special features of digital evidence creates extreme challenges for the Vietnamese Police in collecting evidence especially when collecting evidence from abroad. It can be a complicated and bewildering process (Grabosky & Smith, 2001). As a result, collecting digital evidence requires a set of rules beyond those which apply to normal physical evidence.

An additional problem is that Police investigators are required to be knowledgeable in a variety of ICT areas (Casey, 2011) because digital evidence comes from a variety of sources, such as computer devices and cellular telephones; network servers and network hardware (Brown, 2015, Casey, 2011). This knowledge is not usually based on formal training and education but on personal experience involving the use of computers and networks such as the Internet (Cohen, 2008, 2010). Thus, differences in peoples’ knowledge can affect the reliability, accuracy, and integrity of digital evidence (Casey, 2002; Cohen, 2008, 2010).

A further factor that was noted as affecting cybercriminal investigations was the limited capacity of Police investigators and the limitation of human resources and budgets. Generally, criminal investigations undertake several tasks, such as identifying locations, the suspects of cybercrime, the search and seizure of evidence, the arrest of suspects,
interviewing witnesses and so on. Depending on how big and complicated the criminal case is this could require a number of investigators, as well as substantial financial and other resources, to support a successful investigation. However, cybercrime is usually complicated and unpredictable due to the unique characteristics of cybercrime already discussed. Thus, it was perhaps unsurprising that most Police officers admitted ‘our ability is limited’, ‘we need more staff travelling to different locations’. As demonstrated above, the characteristics of cybercrime such as transnational, anonymity and automated activity, have significant effect on the abilities of the investigating Police officers. To improve the responses to cybercrime, the police require better resources, more personnel, and better, and more up-to-date equipment.

Addition to the problems described above is the fact that the Department of Cybercrime Investigation was established relatively recently. More importantly, the Police officers belonging to this department come from different departments. Thus, they generally have either legal or technical backgrounds. There are, in fact, a very limited number of people who have both a technical and a legal background. Thus, the availability of capacity and sufficient knowledge, skill and expertise to deal with cybercriminals was found to be a factor impacting on regulating cybercrime.

An impression given by the Police participants was that financial strain is a serious obstacle to conducting cross-border operations utilising special investigative means. This is especially true in relation to cybercrime, because cybercriminals can be in, or from, multiple nations and usually adopt the latest technologies. In order to effectively tackle cybercriminals, Vietnamese Police officers not only require more investment in the latest technology, but also training and better maintenance of equipment. However, as mentioned previously, in the context of Vietnam as a developing country and devastated from years of war, many aspects of life in Vietnam require, and compete for, limited available support. In general, the role of the Police based on the Peelian Paradigm needs to be re-examined in order to catch up with new needs arising from cybercrimes. Certainly, the needs of the Police in regulating the Internet is far more than catching up with the latest technologies and their criminal impacts. In fact, new local, national, and international relationships with other agencies need to be established in order to enhance its effectiveness and position in the policing of crimes of the current era (Wall, 2011/2007).
6.4. Research question 4: What possible responses can be put in place in terms of cybercrime regulation in Vietnam?

Following on from the above, the research findings and discussion have indicated that cybercrime is a complicated phenomenon which cannot be defined by any single law. This thesis has also charted the attempts of the Vietnamese Penal Code to control cybercriminal activities. In doing so, it is situated within the framework of the existing Penal Code and concluded that cybercrime cannot effectively be regulated by the Vietnamese Penal Code alone, because there are a number of incompatibilities between the nature of cybercrime and the nature of the Vietnamese Penal Code. Furthermore, the Vietnamese Penal Code suffers from many defects, formulates a less than ideal coverage of cybercriminal activities and lacks clarity in terms of legal linguistic definitions. This suggests that the Vietnamese Penal Code is only, or can only, be a partial means of control. In addition, the complexity of advanced technology, difficult jurisdictions, and resource limitations reduce the effectiveness of law enforcement in response to cybercrime.

However, looking at developed countries, with more experienced and comprehensive legal regulations in dealing with cybercrime issues such as the UK and the USA, they have also faced similar challenges due to the nature of technology and criminal law. For a wide, complicated issue such as cybercrime, it is necessary to develop a reflective and cohesive approach. In seeking to do this, this research suggests two possible approaches of cybercrime regulation: 1) using advanced technological measures, and, 2) increased awareness via education. These emerged from the interviews as important potential measures to reduce the growth of cybercrime in Vietnam, and are discussed further below.

6.4.1. Technical solutions: To apply advanced technologies

As mentioned above, technological advances can be used for legitimate and illegal purposes. Those technologies may create better opportunities to commit crime, or can be used by potential targets to protect themselves. Thus, this research suggests that
making use of technological advances can be one of the best possible solutions to reducing the growth of cybercrime.

There are several reasons to suggest that using technology to control cybercrime is an easier and more effective way than legal regulation. Firstly, technology can disrupt criminal activity, forcing criminals back to negotiate different paths and goals (Latour, 2000). For instance, some websites require users to give information, requiring a password before gaining access to that website; in others, ‘user identification’ might be required in order to access it. Some websites allow users to choose a certain kind of language that only the users can understand. These features are the product of the code, software or architecture that are created by code writers. Secondly, technology, code or architecture is malleable; it is easily shaped by users that have access to its control (Wall, 2007). Thirdly, the way in which technology imposes constraints on how users can behave is more pervasive and immediate than laws (Wall, 2007). Fourthly, users seem to be more readily and rapidly adaptable to technology than to law. Technology then can control criminal and sub-criminal behaviours; and technology is also claimed as a native form of regulation, making it less debatable than legal instruction (Wall, 2007).

Digital architecture can be used as a regulator to control cybercrime (Katyal, 2003) when the ‘code’ is utilised by actively designing in security/crime prevention measures without changing the hardware (Wall, 2007). The role of code as a regulator is a central theme of Lessig’s argument (Lessig, 1999). He argued that ‘code’ is identified as the invisible hand that might be able to construct an architecture that perfects control and makes possible highly efficient regulation (Lessig, 1999). He also emphasised that ‘code is law’ and argues that ‘Some architectures of cyberspace are more regulable than others; some architectures enable better control than others. Thus, whether a part of cyberspace generally can be regulated turns on the nature of its code’ (p. 20). It can be said that if the ability to regulate is the aim of the state and some architectures are more amenable to regulation than other, the state will be then likely to use some technical architectures more than others (Fafinski, 2009).

Katyal pointed out that solutions to cybercrime must involve trying to exploit the characteristics of networked technology, especially its potential for natural surveillance, territoriality, and its capacity for building online communities without doing damage to the Internet’s principal design innovation – its openness (Katyal, 2003, p. 2264-8). Wall
(2007, p.190) also argues that the characteristics of networked technology can be used to generate ‘a range of automated active policing tools that seek to identify wrong doing’. The honeynets,⁴³ for example, consist of a wide range of honeyposts; their aim is to improve the security of the internet by detecting attempts at illegal activity of attackers, analysing these attacks, and sharing the findings in order to support users to defend themselves against cybercrime. These honeyposts include a computer, data, a site to appear as a part of a legitimate network and they seem to comprise rich and valuable information for attracting attackers. These honeyposts socially engineer users who are able to access the site and pass through various levels of security, indicating their intention and willingness to progress at each stage, and signalling that they are aware of the content. Their details, at the end, will be recorded and will be used for investigation if appropriate.

However, using technology to respond to cybercrime cannot avoid all problems. It is very hard to measure how effective an intervention has been at the first stage of technology creation, especially in trying to identify what functionality is primarily determined by software and its accompanying procedures rather than by the hardware itself (Wall, 2007). Therefore, the negative effect from technological design cannot be ignored and it should be taken into consideration when they interfere with the free flow of information (Wall, 2007). Using technology to control cybercrime is claimed to create conflict between the level of security provided and functionality of the product, and it is even argued to conflict with the public interest (Wall, 2007). Indeed, responding to cybercrime through the use of technology can trigger the issue of infringement of individual rights of privacy and freedom of speech (Akdeniz and Walker, 2001; Fafinski, 2009). As Akdeniz and Walker (2001) comment ‘there is no compelling state interest in such an invasion of privacy, as the perpetrators have been detected and evidence gathered without any new powers to survey or research’. Encryption technology is even claimed to circumvent the legal powers of interception afforded to the state (Fafinski, 2009, p.271). As Akdeniz and Walker (2000) have argued, ‘technology can be so effective against oversight that law enforcement agencies have begun to voice concerns about the viability of future crime detection in cyberspace’.

Overall, it is clear to see that the application of technologies to control cybercrime has provided many advantages, at the same time; it has also created some new problems as mentioned previously. For instance, ‘Cryptography surely is the best of technology and the worst of technology. It will stop crimes, and it will create new crimes. It will undermine dictatorships, and it will drive them to new excesses. It will make us all anonymous and will track our every transaction’ (Baker and Hurst, 1998, XV). As a result, it can be concluded that cybercrime cannot be entirely controlled by using technology, though technology is considered as an important alternative form of response to cybercrime. Moreover, using technology to respond to cybercrime is not without the problems of technological complexity and high cost. An alternative then, is to increase awareness among users.

6.4.2. Education: To increase awareness

The second possible measure which is identified as a potential approach to reducing cybercrime, is that the raising of awareness. This measure was clearly expressed by the majority of participants. The participants considered that users can either become a contact point of, or barrier to, criminal activities. The majority of Internet users are unaware of how harmful the online world in which they participate can be (Furnell, 2002). This means they lack a basic understanding of how the system works and they may not even want to understand. Some may even feel that they do not need a deep understanding of the technology as they simply want to use it. As a result, the risk will be increased. Thus, Furnell opined that the opportunities offered by computers and the Internet could only be realised by an informed population. Uninformed users are also more vulnerable to risk. Therefore, understanding or raising awareness of the risk of using technology is necessary for all in order to avoid falling foul of online criminals.

Increasing awareness or common sense prevention measures are the first and foremost measures. This was first seen in the early 1960s (Parker, 1983). It is still valuable for criminal prevention measure. Parker has given a clear explanation of why he contends that the raising of awareness is the solution to reducing cybercrime. He explains as follows:
“If any single solution is to be drawn from the 11 years of research and consulting, it is that computer security is not primarily a technological subject. It is a subject of psychological and sociological behaviour of people. As I have said repeatedly in my worldwide lecturing, computers do not commit errors, omissions, or crimes; only people can do these things that my subsequently be manifested in computers. Solutions to these problems also must come from people, their actions, and their attitudes” (Parker, 1983).

Giving the same viewpoint, Mendell (1998) also emphasises awareness as the most effective prevention method, because computer crime is about people and whatever security countermeasures are developed, computer criminals always appear to be one step ahead.

In criminological studies, there are a number of theories that seek to account for how and why crimes occur. RAT, already described, is one of many criminology theories that can be applied to cybercrime and be proven by a number of empirical researches in the field of cybercrime. RAT essentially, provides explanations as to how crime occurs, based on the convergence of three elements; a motivated offender, a suitable target and the absence of capable guardianship. Convergence of these three elements creates opportunities for criminal and deviant activities, and increases the likelihood of occurrence in cybercrime offences. However, it is illustrated that the absence of one of the three factors above will be sufficient in preventing the occurrence of criminal acts (Cohen & Felson, 1979; Messner & Blau, 1987; Miethe & Meier, 1994). In other words, criminal activities will be prevented if the convergence of these elements can be separated.

Raising awareness would seem to be a guardianship to prevent the occurrence of cybercrime. As Cohen et al. (1981) define guardianship as “the effectiveness of persons (e.g., housewives, neighbours, pedestrians, private security guards, law enforcement officers) or objects (e.g., burglar alarm, locks, barred windows) in preventing violations from occurring, either by their presence alone or by some sort of direct or indirect actions” (p. 508). Thus, guardianship has both social and physical dimensions (Miethe & Meier, 1994). According to Cohen et al. (1981) a person is less guarded either by social or physical means to be considered as a suitable target by offenders when they show little or no resistance to crime. As a result, individuals who have greater guardianship are less likely to become victims of cybercrime. The availability of both
social and physical guardianships is very important for decreasing opportunities for criminals (Miethe & Meire, 1994).

Increasing awareness via education is identified as one of the most useful methods in response to cybercrime. Awareness can be improved by providing basic information and advice to users to understand their computers and be aware of computer networks, and their risks (Wall, 2005). This is a basic foundation allowing users to make up their own minds and express their own choices in order to deal with their own safety and security online. In some countries such as the UK, and many European countries, education is considered to play a role as one of the functions of both Computer Emergency Response Teams (CERTs) and Warning, Advice and Reporting Points (WARPs) to provide advisory services to their customers (Fafinski, 2009). Furthermore, education is attributed to be also a means by which the law can change social norms (Lessig, 1999). As Thurgood (1958) stated ‘Education is not the teaching of the three R’s. Education is the teaching of the overall citizenship, to learn to live together with fellow citizens and above all to learn to obey the law.’ Thus, education can be understood to be a means by which certain social norms may be supported, the content of which is regulated by law (Lessig, 2006). Moreover, it can be argued that the law can conceivably intervene to compel a certain level of education in regard to the issues surrounding protection from computer crime (Lessig, 2006). As a result, education is considered as a vehicle to transmit information, knowledge, skills, and laws to people in order to make them more confident to live together and deal with the issues they face in their life.
Chapter 7. Conclusion and the implications

7.1. Summary of key findings

This study has explored the phenomenon of cybercrime and its regulatory framework in Vietnam within the boundaries of time, extent and cost associated with doctoral research. As such, it has required a conscious effort to bind its scope. Particularly, the fieldwork component involved a relatively small number of participants. These participants were chosen for their expertise, thereby maximising the potential insight and value that they could add to the study as a whole.

It was noted that there has been little comprehensive research on cybercrime and its regulation in Vietnam. Although a small number of studies on cybercrime, or its related subjects in Vietnam have been carried out, there has been no specific research on cybercrime and its regulation, to date (January, 2018). This study is, therefore, the first primary research study on the phenomenon of cybercrime and its regulation in the Vietnamese context.

The findings of this study are expected to provide practitioners and academics with some fresh ideas, particularly, regarding the nature of cybercrime and how cybercrimes are currently regulated by Vietnamese legislations and policies through evidence-based on perception of Vietnamese authorities, such as the Police, Judges, Prosecutors and ISPs who are directly or indirectly concerned with cybercrime. Additionally, this research study may also help academics and practitioners to develop and propose regulatory mechanisms appropriate to the Vietnamese context. Furthermore, the result of this research would be generalised to other societies, especially, ASEAN and South East countries.

This research has therefore contributed to the current debate and literature on the regulation of cybercrime, especially in Vietnam. As the substantive chapters have shown, a number of important findings have emerged from this research. The results are the direct or indirect answers to the research questions.

With reference to the Research Question 1, “How is cybercrime defined by individuals from key government regulatory institutions in Vietnam?”. Chapter 2 highlighted why
cybercrime has always been a typical and hot topic not only for academics but also for the general public. It indicated that there is no consistent definition of the term cybercrime, and there is no national or international consensus on what cybercrime actually is. Despite the fact that many scholars and policymakers have proposed definitions of cybercrime, there is, to date, no unifying standard definition of cybercrime.

Similarly, this research found that there is no authoritative or generally accepted definition of cybercrime in Vietnam (see Chapter 4 & Chapter 5). There are two very different perspectives that allow a better understanding of the concept of cybercrime. One is more widely accepted than the other because of the rapid emergence of new technology-specific criminal behaviours and their diversity. These findings do seem to be consistent with other research conducted elsewhere in the world (see Chapter 2). In addition, despite Vietnamese authorities and other countries’ authorities, including academic researchers, have sought a proper and generally accepted definition of cybercrime, its unique characteristics and its relation to the Internet and associated advanced technologies, make defining it a very difficult task. Therefore, it remains necessary to develop a universal definition of cybercriminal acts that come within the confines of cyberspace in order to facilitate effective international collaboration.

Research Question 2 asked “How adequate are the current policies responding to cybercrime in Vietnam?” As outlined in Chapter 4, the number of Internet users in Vietnam is increasing rapidly. At the same time, the quantity and sophistication of cybercrimes are also increasing. The Chapter has shown the efforts of the Vietnamese government has made in responding to cybercrime. Particularly, the Vietnamese government has created several laws in relation to cyber activities, for example, the Law on Electronic Transaction (2005), the Vietnamese’s Intellectual Property Law (2005) and the Law on Information Communication Technology (2006). The laws, however, just focused on creating a good and open condition of attracting and promoting economic development in Vietnam rather than regulating cybercriminal activities. That is not to say these laws do not have an important role to play, especially in the field of information communication technology. These laws are recognised as marking a significant step toward the regulation of internet activities in Vietnam, in regard to cybersecurity, enhancing the security of computers and networks.
Furthermore, the Vietnamese government has revised the existing Vietnamese Penal Code several times and this law, indeed, could better deal with some types of cybercriminal activities. However, the Vietnamese Penal Code still faces some difficulties particularly in relation to newer types of cybercriminal activities that were unforeseen at the time of its revision. Moreover, this law was formulated primarily to protect property and tangible objects against traditional criminals rather than intangible objects. It is, therefore, reasonable to conclude that current legislation still does not cover all cybercriminal activities, mainly because cybercrime is invisible, new, and the victims are almost intangible, this is partly due to rapid technological development.

Besides, the limitations of legal language used in the country’s legal policy and the matter of legal processing are viewed as obstacles to make Vietnamese cybercrime regulation policies less effective in responding to cybercrimes.

Moreover, the research discovered that transnational/jurisdictional issues are a major factor reducing the effect of Vietnamese cybercrime regulation policies. As previously mentioned, Vietnamese regulation policies are traditionally premised on its geographical borders and jurisdiction. Vietnamese law is made for Vietnamese citizens, residing within Vietnamese boundaries, where the Vietnamese authorities will prescribe and execute the law. Legal rights and responsibilities are therefore largely dependent on where one is located. However, cybercrime has a special transnational aspect compared to other crimes because of the nature of, and advancements in, technology. Cybercrime often crosses multiple jurisdictional boundaries. Therefore, Vietnamese legal regulations cannot be applied.

Thus, the key factors that have been identified in this research that make cybercrime a challenge for Vietnamese authorities to regulate, are: (1) the global nature and characteristics of cybercrime; (2) the anonymity provided by use of the Internet and related technology; and (3) the advancement of technology. These key factors do not only make cybercrime different from crime in the physical world, they also challenge the capabilities of the current Vietnamese legal and law enforcement systems to keep Vietnamese society safe from the threats posed by cybercriminals and to impose effective criminal sanctions. The difficulties and challenges posed by these characteristics include legal challenges, problems in identifying cybercriminal suspects, and evidence collection.
In response to Question 3 “Who should be the key players in the regulation of cybercrime in Vietnam?”, the research findings addressed the roles that internet users, Police institutions and ISPs currently play in tackling cybercrime, and the roles they could play in the future to reduce the growth of cybercrime in Vietnam.

Although the role of Internet users was not a central focus in this research study, the majority of participants seemed to think that users should, and could, have a significant role to play in the reduction of the growth of cybercrime. This could explain that human factors play a crucial role in preventing cybercrime for two main reasons: i) most cybercriminals exploit advanced technology to commit crimes; and ii) the failure or unawareness of users to take necessary precautions that could prevent cyber threats is key. In that sense, this study found that increasing user awareness and knowledge of cybercrime and appropriate protection methods can significantly reduce and prevent the damage caused by cybercrimes.

Although it might require further examination, the study suggested that users can become more effective in reducing the growth of cybercrime by either i) increasing the level of their own security measures or; ii) increasing their awareness of using computer networks. Increasing the level of security measures can include: employing or installing software solutions including anti-virus software and firewalls. In terms of increasing user awareness of the risks of using computer networks, this could include providing better basic information about how to use computer networks safely; how to identify acts that could be criminal or deviant; and how to be more aware of the availability and potential of protection products and how to use them. Most security tools do not require advanced computer knowledge, and ordinary computer users can easily use them. User initiative is essential and individuals may take that initiative only when they are fully aware of possible threats and use protective means to prevent these threats.

The role of ISPs was found to be important in ensuring the security of networks and regulating online illegal activities in the context of cybercrime regulation in Vietnam. In other words, ISPs play an important role in regulating cybercrime. As discussed in Chapter 6, two types of approach can be used to increase ISP security: providing and using additional security protection, and providing security services. Put differently, ISPs can provide defensive measures against cybercrime. Providing defensive measures can include firewalls, antivirus software, security advice, and security information. All
can contribute to improve the protection of users against cybercrimes or making cybercrime attacks more difficult.

The police were, unsurprisingly, found to play a leading role in regulating cybercrime in Vietnam. The police are responsible on behalf of the government, for managing social and public order, securing the country and preventing any harmful activities by enforcing national law. This role is totally clarified by the Vietnamese Constitution, the Penal Code and other legal documents. They are also formally and legally viewed as a ‘capable guardian’. In their leading role, the Police are faced by a number of key challenges such as identifying suspects, search and seizure of evidence, and the human resources available for investigations. The reasons for these challenges are not necessarily limited to the unique characteristics of cybercrime, such as transnationality, anonymity, and automated activity. They also include the form of evidence – digital evidence, human resources, and budgets.

Interestingly, and in contrast, there was little suggestion in the interviews that prosecutors and judges could, or should, play a greater role in reducing the growth of cybercrime in Vietnam. In other words, the role of prosecutors and judges in relation to regulating cybercrime was regarded as less important than that of users, the Police and ISPs.

To the final Research Question 4, “What possible responses can be put in place in terms of cybercrime regulation in Vietnam?”, the results of interviews carried out during this research have clearly shown that besides the central role suggested for users, Police and ISPs to reduce the growth of cybercrime in Vietnam. There are certain ways to prevent cybercrime. Although no measure can effectively regulate all types of cybercriminal activities, certain measures can have an effect on some cybercriminal activities. Two measures that emerged from this research as particularly important are: i) the application of advanced technologies; ii) working to increase the awareness of users via education.

This study supported that making use of advanced technology can be one of the best possible solutions to reduce the growth of cybercrime within the Vietnamese context. It might come with an immediate outcome because technology cannot only disrupt criminal activity, it is also shaped by the users having access to its control. In addition, the user’s behaviour can be more pervasive and immediate in its impact than laws with
the user able to adopt new behaviours that reduce the risk of cybercrime in their daily lives.

This research also supported a second, related measure with potential to reduce cybercrime: the raising of awareness. Raising awareness is, in some ways, the first and foremost measure. Although it does not seem to have an immediate outcome, it is worthwhile and valuable in the long-term for regulating cybercrime. Awareness is the basic foundation allowing people to make up their own minds and express their own choices in order to deal with their own safety and security online. User awareness impacts very much on the users’ actions and leads people to constrain their own behaviour.

Raising user-awareness may be carried out in a number of ways. Education does seem to be an especially effective way, because educating users is viewed as a vehicle to transmit information, knowledge, skills, and laws to people. It is important to educate individuals beginning at an early age. Users then gain more confidence to deal with any issue they might face in their daily life. Although, educating users may take any of several forms, training, seminars and publications can be the best education for users. This can be done via private organisations, government agencies including CERTS, Warning, Advice and Reporting Points, ISPs, and the Police.

7.2. Implications

The Vietnamese government continues to develop and use internet-based services and reliance on these services will continue to grow. This reliance on computer network systems and other digital technologies will bring an increased vulnerability to cybercrime and cyber-attack. Although, Vietnam is working towards curtailing these threats though policies, institutions, and legislation. These efforts are still in their initial stages and inadequate in comparison with rapid changes in advanced technology and the growing threat of cybercriminals. To strengthen the regulation of cybercrime in Vietnam, comprehensive work must be done. Following the results and discussion of the interviews, this research suggests:

(1) Cybercrimes take advantage of jurisdictions that lack comprehensive legal frameworks on cybersecurity in general and cybercrime in particular. Vietnam must
speed up its proposed comprehensive cybercrime law while avoiding the piecemeal and scattered legislative approach, which makes interpretation difficult and is an obstacle to enforcement.

(2) Laws, cybercrime policies, and law enforcement alone will not suffice in preventing or investigating cybercrime. The Vietnamese law enforcement authorities ought to be adequately equipped with the necessary legal, technical, financial and human resources. Law enforcement officials should be fully informed on emerging trends in cybercrime by participating in regular and up-to-date training courses.

(3) Combating cybercrime is an extraordinarily difficult task that requires coordination, cooperation and focused efforts. Specialised units within law enforcement agencies should take the lead and work in partnership with other actors, such as ISPs and private businesses in order to effectively detect, investigate, and prosecute cybercriminals.

(4) The Vietnamese government should promote cybercrime awareness and establish effective means to offer advice on online safety and provide timely information regarding cybercrime to the public. At the same time, the Vietnamese government should provide accessible and user-friendly reporting mechanisms.

(5) The Vietnamese government should support and encourage research, forums, and workshops on cybercrime issues involving all stakeholders including those from law enforcement, academia, business, civil society, and end users to deal with this problem.

7.3. Directions for future research

Considering the limited amount of research on this issue prior to this study, this research provides important insights regarding issues of cybercrime regulation in Vietnam, from both theoretical and methodological perspectives.

From a theoretical standpoint, it is recommended that more focus could be placed on investigating specific factors, such as the transnational aspects of cybercrime, and the problems posed by digital evidence. Conducting in-depth interviews on specific factors would allow a clearer picture of the current situation regarding cybercrime regulation in Vietnam and a fuller, evaluation of the key factors that make cybercrime a challenge to the Vietnamese authorities. Additional information from both the private sector and
government needs to be considered in further research, in order to explore in more detail, the key factors cited above.

From a methodological perspective, a larger and wider study across a greater number of institutions, business organisations, and the general public would provide further insights into understanding the key challenges, factors and the role of key players in regulating cybercrime in Vietnam.
Appendix 1: Interview schedule for Police Officer/Prosecutor/ Judge

I. Demographical information

1. Job title:

2. Gender: F/M

3. Could you tell me how long have you been doing this job in years?

4. To what extent do you think you are computer literate?

5. Could you tell me what professional or other relevant qualifications do you hold?

6. Could you tell me what professional or other relevant training have you done?

7. Could you tell me do you belong to any professional bodies associated with computing?

II. Cybercrime in general

This section of interview will focus on the phenomenon of cybercrime in general to discover the perspective of interviewees on cybercrime’s nature, importance, danger and influences. In order to do so, there are several open and close questions will be asked as bellows:

1. In your personally view, could you tell me what do you understand by the term ‘cybercrime’?

2. Do you think that cybercrime has changed over time? If so, why? In which way?

3. Could you tell me what are the greatest dangers resulting from cybercrime do you consider/ or deal with?

4. How many cases in relation to cybercrime have you dealt with? If so, how many cases are successful that you have dealt with?
4. Do you think that cybercrime can make other consequences? If so, what kind of other consequences can cybercrime make?

5. In your opinion, who is responsible for regulating cybercrime? The police agencies? The providers? The corporation? The individuals?

6. Do you think your views are similar to others in your organisation? And your views are also similar to other organisations?

III. Cybercrime and its regulation

This section will discuss with the participant views on some of cybercrime regulation policies

1. Cybercrime regulation policy
   + Could you tell me what do you think about the adequacy of legal protection from cybercrime?
   + Are you aware of the law on information technology and the law on telecommunication when you deal with cybercrime issues? If so what is your view of these laws?
   + Could you tell me does Vietnamese criminal law effectively regulate the issue of cybercrime? If not, why not?
   + Could you tell me do these laws in Vietnam cover a full range of cybercriminal activities?
   + Do you believe that these laws have any deficiencies? If so, what are they?
   + Do you think that these laws should be amended? If so, in what way?
   + What would your ideal of amending law be in relation to cybercrime?

2. Cybercrime regulation mechanism
   + How would you consider your role in regulating cybercrime?
   + Could you tell me have you ever dealt with cybercrime case? If so, what did you do and what was the result?
   + Could you tell me what are the key differences in regulating cybercrime and traditional crimes?
+ Could you tell me do you face any difficulties in regulating cybercrime? If so, what are they?

+ Could you tell me are you aware of any of the specialist local, national or international units who deal with cybercrime? (National hi-tech crime unit, Interpol) If so, in your views, could you tell me what is your understanding of their role in dealing with cybercrime?

+ Could you tell me do you as a police officer and/or law enforcement officer need to be trained? If so, What kind of training shall you need?

+ Do you think as a police officer/prosecutor/judge do you need help from others in regulating cybercrime effectively? If so, who are they?

+ What role should users play in the response to cybercrime?

+ Have you got any further comments in relation to the issue of cybercrime and these cybercrime regulation policies as well as cybercrime regulation mechanism that have not been raised in the interview?
Appendix 2: Interview schedule for Policy maker

(Ministry of Justice and Ministry of Information and Communications)

I. General information

Coded name: ____________________________  Gender:

Job title:


2. Gender: M/F

3. Could you tell me how long have you been doing this job in years?

4. To what extent do you think you are computer literate?

   1 to 5 (5 being most literate; 1 being least)

5. Could you tell me what professional or other relevant qualifications do you hold?

6. Could you tell me what professional or other relevant training have you done?

7. Could you tell me do you belong to any professional bodies associated with computing?

II. Cybercrime in general

This section of interview will focus on the phenomenon of cybercrime in general to discover the perspective of interviewees on cybercrime’s nature, importance, danger and influences. In order to do so, there are several open and close questions will be asked as follows:

1. In your personally view, could you tell me what do you understand by the term ‘cybercrime’?

2. Do you think that cybercrime has changed over time? If so, why? In which way?

3. Could you tell me what are the greatest dangers resulting from cybercrime do you consider?
4. Do you think that cybercrime can make other consequences? If so, what kind of other consequences can cybercrime make?

5. In your opinion, who is responsible for cybercrime? The police agencies? The providers? The corporation? The individuals?

6. Do you think your views are similar to others in your organisation? And your views are also similar to other organisations?

III. Cybercrime and its regulation

This section will discuss with the participant views on some of cybercrime regulation policies

1. Cybercrime regulation policy
   + Could you tell me about the cybercrime regulation policy in Vietnam?
   + What do you think about the adequacy of legal protection from cybercrime?
   + Do you think that cybercrime can have special characteristics that make challenges for policy maker? If so, what are they?
   + Could you tell me do Vietnamese cybercrime regulation policies effectively regulate the issue of cybercrime? If not, why not?
   + Could you tell me do these regulation policies in Vietnam cover a full range of cybercriminal activities? If not, why not?
   + Do you believe that these cybercrime regulation policies have any deficiencies? If so, what are they?
   + Do you think that these cybercrime regulation policies should be amended? If so, in what way?
   + What would your ideal of amending these policies be in relation to cybercrime?

2. Cybercrime regulation mechanism
   + Could you tell me what role should you play in regulating cybercrime?
   + Could you tell me any difficult aspect of cybercrime would you ever experienced in making cybercrime regulation policies? If so, what are they?
   + Could you tell me are you aware of any of the specialist local, national or international units who deal with cybercrime? (National hi-tech crime unit, Interpol) If
so, in your views, could you tell me what is your understanding of their role in dealing with cybercrime?

+ Could you tell me do you as a policy maker need to be trained? If so, What kind of training shall you need?

+ Do you think as policy makers need help from others in order to making a good cybercrime regulation policy? If so, who are they?

+ What role should users play in the response to cybercrime?

+ Have you got any further comments in relation to the issue of cybercrime and these cybercrime regulation policies that have not been raised in the interview?
Appendix 3: Interview schedule for internet provider services

I. General information

Coded name: ___________________________ Gender:

Job title:


2. Gender: M/F

3. Could you tell me how long have you been doing this job in years?

4. To what extent do you think you are computer literate?
   1 to 5 (5 being most literate; 1 being least)

5. Could you tell me what professional or other relevant qualifications do you hold?

6. Could you tell me what professional or other relevant training have you done?

7. Could you tell me do you belong to any professional bodies associated with computing?

II. Cybercrime in general

This section of interview will focus on the phenomenon of cybercrime in general to discover the perspective of interviewees on cybercrime’s nature, importance, danger and influences. In order to do so, there are several open and close questions will be asked as the following:

1. In your personally view, could you tell me what do you understand by the term ‘cybercrime’?

2. Do you think that cybercrime has changed over time? If so, why? In which way?

3. Could you tell me what are the greatest dangers resulting from cybercrime do you consider as an internet provider service?
4. Do you think that cybercrime can make other consequences? If so, what kind of other consequences can cybercrime make?

5. In your opinion, who is responsible for cybercrime? The police agencies? The providers? The corporation? The individuals? And Why?

6. Do you think your views are similar to others in your organisation? And your views are also similar to other organisations?

III. Cybercrime and its regulation

This section will discuss with the participant views on some of cybercrime regulation policies

1. Cybercrime regulation policy

+ Could you tell me what do you think about the adequacy of legal protection from cybercrime?

+ Are you aware of the law on information technology and the law on telecommunication when you deal with cybercrime issues? If so what is your view of these laws?

+ Could you tell me does Vietnamese cybercrime regulation policy regulate the issue of cybercrime effectively? If not, why not?

+ Could you tell me does Vietnamese cybercrime regulation policy cover a full range of cybercriminal activities? If not, why not?

+ Do you believe that these policies have any deficiencies? If so, what are they?

+ Do you think that these laws should be amended? If so, in what way?

+ What would your ideal of amending law be in relation to cybercrime?

2. Cybercrime regulation mechanism

+ Could you tell me as an internet service provider what role should you play in regulating cybercrime?

+ Could you tell me have you ever reported in relation to cybercrime? If so, what was the result?

+ Could you tell me are you aware of any of the specialist local, national or international units who deal with cybercrime? (National hi-tech crime unit, Interpol) If
so, in your views, could you tell me what is your understanding of their role in dealing with cybercrime?

+ Could you tell me as an internet provider service do you need to be trained to prevent cybercrime issues? If so, What kind of training shall you need?

+ Do you think that do you need help from others in order to prevent cybercrime issues? If so, who are they?

+ What role should users play in the response to cybercrime?

+ Have you got any further comments in relation to the issue of cybercrime and cybercrime regulation policies that have not been raised in the interview?
Study Title: Cybercrime in Vietnam: A critical analysis of its regulatory framework

My name is Hai Van Nguyen and I am a research student in the University of Portsmouth. I would like to invite you to participate in an academic research study of cybercrime and its regulation: the case of Vietnam. I will conduct the study myself and hope to learn about the working experiences of yourself and others in handing cybercrime regulation issues in your institution.

The interview will last about 45 minutes. If you decide to participate, you are free to withdraw your consent and stop the interview at any time.

I guarantee your confidentiality and anonymity. If you give us your permission for the interview by signing this document, I may include material from the interview for writing up my PhD thesis and other relevant publications. Any material will be presented in such a way that you and your office could not be identified.

If you have a concern about any aspect of this study, you should ask to speak to me and I will do my best to answer your questions. My contact detail is: Van.Nguyen@port.ac.uk. If you remain unhappy and wish to complain formally, you can make your complain and send to the Research Ethics Committee, University of Portsmouth. Detail can be obtained from hhh://www.port.ac.uk.

If you have any questions, please feel free to ask me.
Thank you very much for giving your time for this interview. I would be grateful if you could sign two copies of this consent form. One is for you and the other is for our record.
Consent Form

Key Contacts:

Hai Van Nguyen (Researcher)
van.nguyen@port.ac.uk

Dr Victoria Wang (Supervisor)
victoria.wang@port.ac.uk

Study Title: Cybercrime in Vietnam: A critical analysis of its regulatory framework

Name of Researcher: Hai Van Nguyen

Please initial box

1. I confirm that I have read and understand the information sheet dated Date    month    2015 for the above study. I have had the opportunity to consider the information, ask questions and have had these answered satisfactorily.

2. I understand that my participation is voluntary and that I am free to withdraw at any time without giving any reason.

3. I understand that data collected during the study, may be looked at by Individuals from University of Portsmouth, or from regulatory authorities. I give permission for these individuals to have access to my data
4. I agree to take part in the above study.

Name of Participant       Date       Signature

Researcher               Date       Signature
Appendix 5: The letter of introduction for assessing to the five institutions in Vietnam

MINISTRY OF PUBLIC SECURITY
BUREAU OF SECURITY AND INVESTIGATIVE SERVICES

SOCIALIST REPUBLIC OF VIETNAM
Independent – Freedom - Happiness
Hanoi, January 22, 2015

To Whom it may concern

Bureau of security and Investigative services – Ministry of Public Security would like to introduce Mr Nguyen Van Hai who is a member of Bureau of security and Investigative services – Ministry of Public Security. Mr Hai is currently undertaking a PhD course at the Institute of Criminal Justice Studies, University of Portsmouth, United Kingdom. His PhD thesis is ‘Cybercrime and its governance: The case of Vietnam’.

The objective of his research is to find the factors that make cybercrime difficult and challenges for governing it. At the same time, his research offers the possible methods of governance which may contribute the reduction of the growth of cybercrime in Vietnam. In order to do so, with your allowance, some members’ staff of your office who is involved in governing cyber crime will be interviewed. The result of the interview would be greatly valuable for his research. The Bureau of Security and Investigative Services does hope that you will allow your staff to participate in the interview and let them share their skills and experience in dealing with cyber crime with him for the purpose of this research.

Thank you for your cooperation./.

Colonel Nguyen Chien Thang
Appendix 6: Ethical Review confirmation

Mr Van Hai Nguyen
PhD Candidate
Institute of Criminal Justice Studies
University of Portsmouth

REC reference number: 14/15:45

Please quote this number on all correspondence.

19th June 2015

Dear Mr Nguyen,

Full Title of Study: Cybercrime in Vietnam: A critical analysis of its regulatory framework

Documents reviewed:
- Consent Form
- Ethics self-assessment
- Interview Schedule
- Invitation Letter
- Participant Information Sheet
- Protocol

Further to our recent correspondence, this proposal was reviewed by The Research Ethics Committee of The Faculty of Humanities and Social Sciences.

I am pleased to tell you that the proposal was awarded a favourable ethical opinion by the committee.

Kind regards,

FHSS FREC Chair

Dr Jane Winstone
Members participating in the review:

- David Carpenter
- Richard Hitchcock
- Geoff Wade
- Jane Winstone
Appendix 7: Research ethics review checklist

**FORM UPR16**

**Research Ethics Review Checklist**

Please include this completed form as an appendix to your thesis (see the Postgraduate Research Student Handbook for more information).

<table>
<thead>
<tr>
<th>Postgraduate Research Student (PGRS) Information</th>
<th>Student ID: 726127</th>
</tr>
</thead>
<tbody>
<tr>
<td>PGRS Name: HAI VAN NGUYEN</td>
<td></td>
</tr>
<tr>
<td>Department: ICJS</td>
<td></td>
</tr>
<tr>
<td>First Supervisor: DR VICTORIA WANG</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Start Date: (or progression date for Prof Doc students)</th>
<th>February 2014</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Study Mode and Route:</th>
<th>Part-time</th>
<th>MPhil</th>
<th>PhD</th>
<th>MD</th>
<th>Professional Doctorate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Title of Thesis: Cybercrime in Vietnam: A critical analysis of its regulatory framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thesis Word Count: 70,980 (excluding ancillary data)</td>
</tr>
</tbody>
</table>

If you are unsure about any of the following, please contact the local representative on your Faculty Ethics Committee for advice. Please note that it is your responsibility to follow the University’s Ethics Policy and any relevant University, academic or professional guidelines in the conduct of your study. Although the Ethics Committee may have given your study a favourable opinion, the final responsibility for the ethical conduct of this work lies with the researcher(s).

**UKRIO Finished Research Checklist:**

(If you would like to know more about the checklist, please see your Faculty or Departmental Ethics Committee rep or see the online version of the full checklist at: http://www.ukrio.org/what-we-do/code-of-practice-for-research/)

<table>
<thead>
<tr>
<th>a) Have all of your research and findings been reported accurately, honestly and within a reasonable time frame?</th>
<th>YES ☒ NO ☑</th>
</tr>
</thead>
<tbody>
<tr>
<td>b) Have all contributions to knowledge been acknowledged?</td>
<td>YES ☒ NO ☑</td>
</tr>
<tr>
<td>c) Have you complied with all agreements relating to intellectual property, publication and authorship?</td>
<td>YES ☒ NO ☑</td>
</tr>
<tr>
<td>d) Has your research data been retained in a secure and accessible form and will it remain so for the required duration?</td>
<td>YES ☒ NO ☑</td>
</tr>
<tr>
<td>e) Does your research comply with all legal, ethical, and contractual requirements?</td>
<td>YES ☒ NO ☑</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Candidate Statement:</th>
</tr>
</thead>
<tbody>
<tr>
<td>I have considered the ethical dimensions of the above named research project, and have successfully obtained the necessary ethical approval(s)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ethical review number(s) from Faculty Ethics Committee (or from NRES/SCREC):</th>
<th>14/15:45</th>
</tr>
</thead>
</table>

If you have not submitted your work for ethical review, and/or you have answered ‘No’ to one or more of questions a) to e), please explain below why this is so:

---

**Signed (PGRS):** [Signature]

**Date:** 04/2019

UPR16 – August 2015
REFERENCES


Cooper v. Aaron [1958] 358 U.S. 1


http://www.telegraph.co.uk/technology/facebook/9068166/Facebook-criticised-for-hurting-cybercrime-investigation.html


