1. Introduction

China on the Hunt for Taiwanese Hacker
– Global Times, October 30, 2007

> There were 1,295 infected computers that reported to the control server [Ghostnet]. The infections were spread across 103 countries. Taiwan reported the most infections followed by the United States, Vietnam and India.
> *– Information Warfare Monitor*[1]

1.1 RESEARCH BACKGROUND

Cairncross (1997:26) in her book *The Death of Distance* stated that the technology revolution would make it easier for people to contact each other, to discover information, to learn new things, and to acquire new skills. The same technology revolution would make it easier for people to turn their initiatives and ideas into business ventures:

> This is a revolution about opportunity and about increasing human contact. It will be easier than ever before for people with initiative and ideas to turn them into business ventures. It will be easier to discover information, to learn new things, to acquire new skills. Above all, it will be easier to find somebody to talk to – to communicate, whether with friends or strangers, relatives or customers. As a result, the world will, in all probability, be a better place.

The Internet ranks as one of the great inventions that have affected human life. The development of computers and the Internet has transformed the way we live and do business. No matter whether you are searching for travel information or buying concert tickets, you can easily perform these functions at any time and in the convenience of your own home.

The Internet bridges the communication divide. People can contact their friends or family members whenever they wish. At minimal cost they can even have 'face to face' conversations. Moreover, with the Internet eroding national borders, making new friends in other countries has become simple.

[1] Retrieved from Information Warfare Monitor (2009:41).

The Internet also has become almost indispensable to companies and governments around the world. With the help of computers and the Internet, companies are now able to provide immediately and precisely most of their services to customers. They are able to provide product or service information at an unprecedented level of efficiency.

However, the Internet has also become the proverbial 'double-edged sword'. Along with convenience comes the inconvenience of computer crime. Not only are conventional crimes such as disseminating child-pornography, illegal online-gambling and fraud facilitated by computers and the Internet, the Internet itself has also attracted a new breed of users.[2] As Tapscott and Williams (2007:16) argued, 'criminals and terrorists can conspire over the Internet to wreak havoc on our daily existence'.

As pointed out by Professor Lawrence Lessig in his famous book *Code and Other Laws of Cyberspace,* the Internet was built for research and not commerce. Its founding protocols are inherently insecure (1999:39). The devolution of access to the computer network from government and research to the domestic arena has provided a unique gateway to cyber criminals and cyber deviant entrepreneurs.

Reputedly, the term 'hacking' was first used at the Massachusetts Institute of Technology in the 1970s and was originally defined by the *Oxford English Dictionary* as 'the use or programming of a computer as an end in itself, for the satisfaction it gives' (Ayto, 2007:190). Someone who did this was called a 'hacker'.

Hackers evolved from users wishing simply to show off their superior computing abilities into criminals who steal data or who illegally obtain financial benefit. We can see this evolution via the transformation of the definition of the word 'hacker' in the *Oxford English Dictionary*. The definition of 'hacker' changed in the 1980s to 'someone who uses their skill with computers to try to gain unauthorized access to computer files or networks' (Ayto, 2007:216).

Whenever institutions store, process or transmit personal or classified data on computers or through the Internet, they become a favourable target for hackers to gain profit by stealing that data. This is especially so for those institutions with large personal data files, such as government agencies, banks and telecommunication companies.

Unlike most individual users who can reformat their computer system to restore a compromised computer, governments and companies are in a more

---

[2] For research purposes, this book will not address conventional crimes which may be facilitated by the Internet. This book will mainly discuss crimes and criminals which target computers.

awkward situation when faced with information security breaches. It is often not possible for them to take measures an individual would take, such as simply reformatting their computer system. Reducing the harm caused by malicious activity and building a capacity for resilience have therefore become important to both government and business.

As most Internet users are using proprietary software and systems such as Microsoft Office or XP, they face identical computer security and data protection problems. Malware,[3] such as computer viruses, Trojans, and bot programs, that are created to target breaches and vulnerabilities within systems and software, are similar to bacteria and viruses in humans. There is always a risk of malware and it might not be possible to prevent it from infecting a computer system. What is important is to reduce harm caused by malware once it is discovered.

However, in a risk society, it is not sufficient to rely simply on a governmental approach to harm reduction and containment of the problem. Cooperation with non-government users, especially organizational users, and the use of convert external resources for organizational risk management, such as an early warning system, are vital (Ericson, 2007:6–11).

The decision-making process for an organization assessing organizational risk and harm reduction options involves a cost–benefit analysis. However, this is often based on non-scientific forms of knowledge, as Ericson (2007:9) argues:

> It is highly doubtful that people simply calculate risks and then choose among alternative risk–return possibilities. Rather, decisions are made on the basis of values, institution, emotion, aesthetics, morals, speculations, context, timeline, accessible information, reputation of information resources, attention capacity, and so on. In other words, cost–benefit analyses of risk are made in the context of local cultures and contingencies of uncertainty.

Consequently, in order to establish a feasible pre-warning system, it is necessary to determine the key issues relating to reporting both in the government and private sectors.

The activities of hackers have become particularly pronounced in the People's Republic of China (China hereafter) and the Republic of China (Taiwan hereafter). In 2006 and 2007, according to reports published by Symantec, one of the leading information security companies, China had the world's greatest number of bot-infected computers. In 2007, Beijing was the city with the most bot-infected computers; with about 7 per cent of the worldwide total. China has become a major international target for

---

[3] Which will be further explained in Chapter 2.

hackers. It ranked second only to the USA on the list of countries experiencing cyber attacks (Symantec, 2006, 2007d, 2008b).

The government of Taiwan has enthusiastically embraced Internet technology. Taiwan is one of the highest ranked e-governments in the world, holding the top ranking in 2002, 2004, and 2005 (West, 2001, 2002, 2003, 2004, 2005, 2006, 2007). Therefore, it is not difficult to explain why Taiwan has become a country that hackers, especially from China, particularly like to target. According to Symantec (2006), Taiwan was ranked fourth with respect to bot-infected computers, following China, the USA, and the UK. Taiwan was also one of the top ten countries targeted by Distributed Denial of Service attacks (DDoS).

Reports have shown that most hacking into Taiwanese computer systems is initiated from within China and most hacking into Chinese systems originates within Taiwan (Boxun News, 2009; Crime Investigation Bureau, 2004; Mazanec, 2009; Schneier, 2008; Zhang, 2007). However, it is important to note that these statistics do not prove that all hacking from China into Taiwan is done by Chinese hackers, or *vice versa*.

Hacking into the banking systems of Taiwan and China is sometimes performed with the cooperation of hackers from both countries. There are several reasons for this (Chao, 2010; Symantec, 2007a, 2008a):

- Taiwanese and Chinese nationals share a common language and culture;
- in recent years, there have been increasing business and economic links across the Taiwan Strait; and
- it has become more economical to base high-tech crime operations in China compared with Taiwan.

Regardless of the motives of these hackers, the inconsistency of laws and regulations against transnational cybercrime has become an obstacle for formal mutual assistance between governments in cybercrime investigation and prosecution. The issue of dual-criminality, which refers to behavior that is criminalized in both the requesting and the requested countries, has drawn the attention of international and regional organizations (Smith, Grabosky, and Urbas, 2004:51). Various international organizations have drafted a number of conventions and agreements in an attempt to solve transnational cybercrime.

This book will show that the sensitive political situation between Taiwan and China makes the problem of cybercrime difficult for both governments to address. To start to understand cybercrime across the Taiwan Strait, it is necessary to have a basic understanding of the nature of Taiwan–China relations and the legal status of Taiwan. The nature of bilateral relations

explains in part the level of malicious activities across the Strait while the legal status of Taiwan explains in part the difficulties of cross-Strait and broader international cooperation.

The Government of the People's Republic of China claims sovereignty over Taiwan. China advocates peaceful reunification with Taiwan, but refuses to rule out the use of military force if this cannot be achieved. Taiwan has undertaken, under the Presidency of Ma Ying-Jeou, to maintain the status quo in the Taiwan Strait and this approach has improved cross-Strait relations since 2008 (DFAT, 2010b). Notwithstanding the recent improvement in relations, the sovereignty claim remains and we should bear in mind that sovereignty claims are a common reason why nations have, historically, gone to war.

Most countries recognize the People's Republic of China as the sole legal government of China. Only 23 states recognize Taiwan as the Republic of China. Under its 'one-China policy', recognition of China requires acceptance of Taiwan as a province of China. For example, Australian Government policy towards Taiwan is based on its Joint Communiqué with the People's Republic of China of 21 December 1972. Under the terms of the Joint Communiqué, Australia recognizes the Government of the People's Republic of China as the sole legal government of China and acknowledges the position of the Chinese Government that Taiwan is a province of China (DFAT, 2010a, 2010b; Government Information Office, 2009).[4]

However, as treaties are concluded between independent nation states, the countries which recognized China are unable, under the terms of their recognition of China, to enter into binding agreements with Taiwan. Taiwan is excluded from most international organizations, including the UN, and is therefore not accepted as a signatory for most international conventions. This clearly precludes Taiwan from pursuing the most typical means for formalizing bilateral or multinational cooperation between nation states with most countries in the world and many conventions, including the Council of Europe's *Convention on Cybercrime*, cannot be used to address cross-Strait cybercrime.

There has been some progress in cooperation in combating conventional crime as the political situation between Taiwan and China has improved. Unfortunately, that cooperation has not been constant or timely. And because of the sensitivity of cybercrime, which is considered as a national

---

[4] Chapter 7 of *the Republic of China Year Book 2009*, Cross-strait Relations, has a detailed description on the political situation and relationship between Taiwan and China. Also see 'Political status of Taiwan', Wikipedia, http://en.wikipedia.org/wiki/Political_status_of_Taiwan.

security issue in China, there has been a lack of mutual assistance. In other words, the governments of Taiwan and China have failed to act as capable guardians.

The lack of constant and timely cooperation between Taiwan and China has enabled both countries to become havens for criminals wanting to launch cyber attacks on the other country. Cybercrime between Taiwan and China will not be deterred by threats of punishment. Even with strict laws and regulations against cybercrime, criminals know that there is a very low probability of being convicted.

The establishment of long-term cooperation and trust between China and Taiwan to combat cybercrime has become an urgent issue for both governments. This book will argue that, until official mutual assistance between the two Governments becomes a reality, it is important to determine whether cooperation through third parties, such as international organizations or companies, might be feasible.

This book suggests that another strategy to prevent cybercrime involves strengthening target computers to make them less vulnerable to cyber attack. As Routine Activity Theory suggests, a crime happens when a motivated offender meets a suitable target and when a capable guardian is absent (Cohen and Felson, 1979; Felson, 1994, 2000). With the lack of capable guardians, such as that which could follow from cooperation between Taiwan and China in investigation, the strategy of building a secure system to avoid being victimized becomes even more important as regulatory responses are weak.

Target hardening and incident response mechanisms cannot be provided efficiently by individual government agencies or companies. As most organizations are using proprietary software, collaboration between users and software companies to discover and report system breaches and vulnerabilities, and the establishment of a pre-warning system to reduce the spread of malwares are necessary. However, as Ericson (2007) argued, this is a cost–benefit exercise for all participants. In order to make a pre-warning system feasible and to encourage organizations to take part in it, research needs to be done on the concerns of, and incentives faced by participating organizations.

1.2 AIM OF THE RESEARCH

This book aims to identify and assess the viability of regulatory and other responses that government agencies and private companies can take in order to combat cybercrime in the Greater China region, especially Taiwan and China. Under the special political situation where formal mutual assistance

might not be workable between the two governments, it considers how to establish a feasible pre-warning system and how to encourage the public and private sectors to cooperate in strengthening their capacity against cybercrime.

It begins with an account of the extent and nature of cybercrime between Taiwan and China, especially on the prevalence of bot-nets in Taiwan and China. Following the structure of Routine Activity Theory, and given the existence of motivated offenders, it will analyse Chinese and Taiwanese legal responses to cybercrime, mutual assistance between the two countries and cooperation through a third party, to see if there are alternative capable guardians. Inspired by the concept of 'risk commonwealth',[5] it will not only suggest the desirability of a pre-warning system between government agencies and private companies to build resilience and make targets less vulnerable and suitable, but also examine concerns and incentives to attract organizations to participate and share information on security incidents.

For research purposes, this book will not address conventional crime facilitated by computers and the Internet, such as online drug dealing, disseminating child pornography, illegal online gambling and fraud. The narrative of cybercrime discussed in this book will mainly focus on topics relating to new types of crime, such as hacking, malicious activities and issues relating to information security protection. It will focus on cybercrime against government agencies and private companies.

Most cybercrime research conducted in Taiwan and China focuses on the technical aspects of cybercrime prevention. That research discusses how computer code can be used to prevent cybercrime or to protect information security. Other research has focused on the study of applicable laws and regulations. However, little empirical research has been conducted on the phenomenon of cybercrime in Taiwan and China.

The study of comparative laws, coupled with empirical research conducted in the Greater China region, is still a new field. Little research has been done on the difficulties confronting mutual cooperation or on the possibility of establishing, officially or through third party cooperation, a cybercrime prevention model for the two countries. That might arguably be because the issue of cybercrime is particularly politically sensitive and data is very difficult to acquire. Such research also requires an interdisciplinary background.

From an interdisciplinary perspective drawing on sociology, criminology, epidemiology, regulatory science, and organizational management, along with empirical study, this book will contribute to our understanding of

---

[5] This will be explained later on Chapter 2.

the nature and extent of cybercrime in and between Taiwan and China, the possibility of cooperation between the two governments through third parties, and provide a new approach to cybercrime prevention which is different from the existing crime prevention measures.

1.3 METHODOLOGY

The main narrative of this book relies on secondary data analysis, comparative law studies, and face-to-face interviews in both China and Taiwan. By re-interpreting statistics gathered by government agencies, non-government organizations, and information security companies, the research will endeavour to explain trends in cybercrime between Taiwan and China. Using comparative law study, the book will analyse the legal responses of Taiwan and China in combating cybercrime. Semi-structured interviews revealed the reasons behind the difficulties facing both governments as they seek to prevent and control cybercrime.

1.3.1 Secondary Data Analysis

Limited by financial and time constraints, the research was not able to collect quantitative data. Therefore, open source data on the information security problems facing Taiwan and China has been used in this book. The main narrative used in subsequent chapters to address the information security problems of Taiwan and China relies heavily on regular reports issued by Symantec (Symantec, 2006, 2007a, 2007b, 2007c, 2007d, 2008a, 2008b, 2009a, 2009b). Supplementary information has also been obtained from reports issued by IBM, Trend Micro, McAfee, CNCERT, and official statistics released by the Chinese and Taiwanese Governments (Choo et al., 2007; Cisco, 2009; CNCERT/CC, 2008, 2009; Gordon, Loeb, Lucyshyn, and Richardson, 2005; IBM, 2009; Information Warfare Monitor, 2009; MessageLabs, 2008; Sun, 2007; Trend Micro, 2009).

Symantec Internet security reports have been selected as the main resource for information security statistics because they are the only reports which regularly present information on security problems in Asia (including Japan) and the Pacific region (the APJ region hereafter)[6] and unlike

[6] The APJ region in this book follows the definition of Symantec. According to 'Symantec APJ Internet Security Threat Report', the APJ region includes Australia, New Zealand, China, Hong Kong, India, Indonesia, Japan, Korea, Malaysia, Philippines, Singapore, Sri Lanka, Taiwan, Thailand, and Vietnam.

most other reports, they include separate statistics for Taiwan. Most other reports include Taiwan in the statistics for China.

Some methodological concerns might arise on the validity of using data published by commercial companies. Reports published by commercial entities may have limitations. They may be subjective in order to reach their special goals, such as exaggerating the number of information security incidents to induce people to use their products (e.g. anti-virus or anti-malware programs). Also, their data is not collected through random sampling methods. For example, the data collected by Symantec is based mainly on data derived from the Symantec Global Intelligence Network, which includes the Symantec DeepSight Threat Management System, Symantec Managed Security Services, and the Symantec Honeypot Network (Symantec, 2007a).

The statistics reported here are mainly used to highlight trends in information security problems in the APJ region and the situation in both Taiwan and China. This book is not focused on the absolute number of incidents occurring in Taiwan and in China. Consequently, the regularly published Symantec Security Report, with its consistent data collection methodology, fits the needs of this book.

Reports released by other commercial companies such as IBM, Trend Micro, McAfee as well as official statistics or statistics released by non-government organizations, are used to supplement the interpretation of the information security situation in Taiwan and China. This may minimize any concerns regarding the subjectivity of the data published by Symantec.

1.3.2 Qualitative Interviewing

Qualitative interviews are based on conversations with individuals or with groups, either face-to-face or through telephone interviews, with the researcher asking questions, listening and reflecting on the respondents' answers. They can be structured, semi-structured, or unstructured (Fontana and Frey, 2000; Mason, 2002; Rubin and Rubin, 2005).

For an 'elite' study, where the interviewees are powerful members of society such as government officers, IT managers in the private sector, police officers, prosecutors and other professionals, the semi-structured interview is recognized as appropriate to explore a complex phenomenon. By using open-ended questions, interviewees with a professional background in information security may be encouraged to respond freely with their viewpoints (Crow and Semmens, 2008; Fafinski, 2009; Odendahl and Shaw, 2001).

The interview data used in this book was collected in 2008–9 through in-depth and semi-structured interviews with individuals and small focus

groups. Most interviews were done 'face-to-face' while two interviews were conducted over the telephone in China and Taiwan.

1.3.2.1 Semi-structured questionnaire and interview process

The questions asked included, but were not limited to:

(1) the experience of the interviewees, such as work experience and the relationship between their work and cybercrime;
(2) types of cybercrime occurring in the public and private sectors;
(3) the goals and methods used by hackers;
(4) evaluation of laws and regulations for combating cybercrime;
(5) the difficulties encountered when constructing an information sharing system between the public and private sectors in Taiwan and China; and lastly,
(6) a suggested approach to government agencies and the private sector.

All interviews were conducted in Mandarin and sometimes mixed with Taiwanese and English. Most recorded data was transcribed in Mandarin. The quotations within the interview data were translated by the researcher himself. While all interviewees agreed to be recorded, 'off-the-record' was sometimes requested by an interviewee when certain sensitive issues were discussed. This 'off-the-record' data was not used in this book.[7]

Some interviewees were interviewed more than once. Measures such as following up via email to get more specific data and information were also adopted. Based on the *guan-xi* and *gang-qing* (which are discussed below) established at the first time, second time (or even third time) interviews and following up via emails not only helped obtain more data, but they also made the information provided more reliable and valid.

1.3.2.2 Data collection

As shown in Table 1.1, 38 interviews (including four focus groups, one in China and three in Taiwan) with a total of 44 interviewees were conducted in Taiwan and China during the years 2008 and 2009. All the interviewees interviewed in Taiwan are coded with the letter 'T' while those in China are coded with the letter 'C'. The number following the letter means the case record. For example, T001 means the first interview done in Taiwan.

[7] Most off-the-record data relates to specific cases easily identifiable, even with the names removed. At the request of the interviewees, they were not used in this book.

Table 1.1 Categorization of interviews

	Private sector	Public sector	Law enforcement	Other professionals	Total
Taiwan (T)	10	5	4	4	23
China (C)	7	0	3	5	15

Interviewees were selected purposely based on their work experience or background. People with knowledge of information security and cybercrime were potential subjects for this research. These included but were not limited to IT people in government agencies and private companies, police officers, prosecutors, and other professionals in cybercrime and information security, such as professors, managers of legal compliance in companies, and information security experts in big accounting firms which audit information security and conduct staff training in organizations. They were categorized into four groups: public sector, private sector, law enforcement, and other professionals.

For qualitative research, sample sizes can vary. An appropriate way to decide when to stop interviewing a class of candidates is based on the concept of 'data saturation (or theoretical saturation)' (Auerbach and Silverstein, 2007; Guest, Bunce, and Johnson, 2006; Marshall, 1996; Morse, 1995). According to Morse (1995:147), '[s]aturation is defined as "data adequacy" and operationalized as collecting data until no new information is obtained'. Also, Auerbach and Silverstein (2007:102) point out that '[t]heoretic saturation is the research sampling strategy in which you can continue to study new research samples until you are simply confirming the theory that you have already developed, rather than modify or elaborating it'.

This concept of data saturation has been adopted by this book as the basis to decide the sample size for interview. Except for the interviews in the categories of public sector and law enforcement agencies from China, interviews in other categories all reached the point of theoretical saturation. In Taiwan, there were 23 interviews with 28 interviewees. There were only three interviewees with less than ten years experience in information security or related areas. All other interviewees in Taiwan had more than ten years working experience in this area. Four participants were female.

Among all the interviews in Taiwan, ten were conducted with 12 participants from the private sector; five interviews were conducted with seven participants from the public sector; four interviews were conducted with five participants from law enforcement agencies such as the police and

prosecutors; and four professors were interviewed who were experts in law, information security issues or criminology.

In China, 15 interviews were conducted and 16 people participated. Seven interviews were conducted with eight participants from the private sector; three policemen were interviewed as well as five professors. With regard to the experience levels of the interviewees in China, only two had experience in the related area of less than ten years. In terms of gender, only one interviewee was female.

There were no government agencies willing to be interviewed. As well, there were no Chinese prosecutors interviewed. However, in lieu of formal prosecutors, some professors interviewed were also concurrently serving as deputy chief procurators. Their data helps overcome the lack of data from government officers and prosecutors in China.

1.3.2.3 Difficulties in getting data

It came as no surprise that people in China are not comfortable being interviewed. Although the methodology of interview is not a foreign concept in China, it is argued that 'modern fieldwork that adheres to Western ideals and principles has only recently developed in China' (Liang and Lu, 2006:158). Unlike the Western individualist concept which emphasizes individual autonomy and is concerned with personal privacy and rights being protected, Chinese people, in particular people from mainland China, are more collectivist. They are defined not by who they are, but how they fit into the social system. That is, individuals might cooperate not because they want to cooperate, but because they wish to maintain personal ties. For example, they would cooperate if a superior wanted them to cooperate (A. Chen, 2005; Liang and Lu, 2006).

Guan-xi,[8] which resembles the idea of social capital, plays a very important role when doing research in Chinese society.[9] As Yang (1988:411) noted, the term *guan-xi* literally means relationship. However,

---

[8] The concept of *guan-xi* and its related concepts such as *ren-ging* (favour), *gang-qing* (affect) and *main-zi* (face) will be introduced here as they connect to the discussion later in Chapter 5.

[9] There are doubts on the similarity and differences of *guan-xi* and social capital, especially in the field of anthropology, where some argue that *guan-xi* is an essential and defining elemental part of Chinese culture, while others believe that *guan-xi* is little more than a Chinese word for social capital which can be found in all societies, see more discussion at e.g. Gold, Guthrie, and Wank (2002), Jacobs (1979), King (1991), Smart (1993), Yang (1988). Here, the original expression *guan-xi* is used to avoid any misunderstanding that may arise by using other words like social capital.

she argued that in the context of the gift economy, 'it has the sense of social connections, connections which must be carefully initiated, preserved and renewed through the giving and receiving gifts, favours and dinners or banquets' (1988:411). It builds on pre-existing relationships such as classmates, people from the same native-place, relatives, superiors and subordinates in the same working place and so on (1988:411).

The function of *guan-xi* is not exclusively instrumental. True *guan-xi* must possess an effective component, *gang-qing* (the quality of the relationship), which controls the 'closeness' and 'distance' of the relationship (Gold et al., 2002:7; Jacobs, 1979:242).

Indeed, as a Chinese proverb says: *You guanxi jiu mei guanxi* (There is nothing to worry about if you have *guan-xi*). If a researcher does not have any ties with Chinese people, in particular those with high social status such as government officers, professors or high ranking police officers, then it will be very difficult to do empirical research in China. Therefore, building up good *guan-xi* is important for doing research in China, just as the second sentence of the proverb says: '*Mei guan-xi jiu gao guan-xi*' (If you don't have *guan-xi*, try to build up some).

However, *gao guan-xi* usually relies on intermediaries who have good *guan-xi* with the person you want to build *guan-xi* with. In order to give *ren-qing* (favour) and *mian-zi* (face) to the intermediaries, the person you want to build *guan-xi* with might talk to you and give you some support (Huang, 1987; Jacobs, 1979; King, 1991; Yang, 1988). Yet, the *guan-xi* built up through intermediaries is usually with distance as there is a lack of affection between the two. Only if the requester builds up *gang-qing* with the person he wants to have *guan-xi* with, will there be close *guan-xi* between them (Jacobs, 1979).

The discussion above accorded with my experience in conducting research in China. Before I went to China for fieldwork, I sought professors in Australia and Taiwan, and classmates and relatives as intermediaries to help me build *guan-xi* with professors in China. When I arrived in China and visited them, based on *ren-qing* and in order to give *main-zi* to the intermediaries, they welcomed me. However, at that stage, they were only willing to talk to me about my trip, my research and life in Australia. I sensed that they were not so willing to introduce me to people they knew as they might still have had concerns about me. The *guan-xi* between the professors and myself was at the point where *guan-xi* existed but the affection was absent. Distance between the potential interviewees and myself still exists.

However, I felt that the *guan-xi* improved over the next month as I kept meeting with them and having meals with them. Giving gifts and inviting them for lunch or dinner were the strategies I used to harden the *guan-xi* and

to make the relationship close. Toward the end of my first trip one of the professors offered to introduce me to some of his students who were working in police and prosecution agencies but I did not get the opportunity to meet with them on that trip. However, I met those police and prosecutors during my second trip to Beijing. I could feel that the *guan-xi* between the professors I met during the first trip was now established and had improved. They were more willing to talk to me and introduce me to key persons who might be helpful to my research.

However, even with *guan-xi*, the sensitivity of this particular research topic still made interviewing difficult. Although I succeeded in interviewing 16 people in China including three who were working in law enforcement agencies, most people from the public sector introduced by professors in China were willing to talk to me in private but not willing (or possibly they are afraid) to be formally interviewed. This had nothing to do with *guan-xi* but with the sensitive nature of the topic.

Some interviewees from China told me that if they were researching a similar topic, they would also find it difficult because information security issues are usually tied up with national security issues, and national security issues are forbidden areas for research. Even with *guan-xi*, people would not agree to be formally interviewed and one would not be able to get the data needed.

Moreover, my Taiwanese identity made the interviews even more difficult, especially with government and law enforcement agencies. I encountered the embarrassing situation where someone had agreed to be interviewed but subsequently refused after realizing that I was Taiwanese. However, in order to address any ethical concern that might arise, all data used in this book is based on interviews where the interviewees knew that I was from Taiwan.

1.3.3 Comparative Law Approach

Cooperation between States when combating transnational crime is difficult if the respective States have different views on the offence being pursued. That is, dual-criminality, which requires that an offence must be recognized as a crime by both countries when providing mutual assistance, would be the first concern encountered.

In order to understand the basis for cooperation in crime investigations, a comparative law approach will be used in the book to examine substantive criminal laws and procedural laws in both Taiwan and China. They will also be compared with the first cybercrime convention, the *Convention on Cybercrime*, drafted by the Council of Europe.

By comparing criminal laws and criminal procedural laws in both Taiwan and China, this book seeks to determine whether dual-criminality is an issue between Taiwan and China in terms of cybercrime investigations. Additionally, with the support of interview data, this book will also examine the sufficiency of laws and regulations used by the Taiwanese and Chinese Governments to combat cybercrime. The similarity of those laws to international legal trends on combating cybercrime will also be addressed.

1.4 CHAPTER STRUCTURE

This book is divided into four parts:

(1) setting the scene;
(2) the cybercrime situation in Taiwan and China;
(3) regulatory responses to cybercrime; and
(4) measures to prevent cybercrime.

Part I will provide background to the research, describe the research methods and introduce the theory employed.

The following chapter, Chapter 2, is divided roughly into two parts. The first part will provide a short introduction to the emergence of the Internet and cybercrime. A variety of definitions of cybercrime will be discussed and the focus of cybercrime in this book will be defined. Significant types of malware as well as the evolution of the hacker from a well-meaning amateur to a profit-oriented criminal will be introduced. The limitations of laws and regulations for combating transnational cybercrime will also be addressed.

The second part of this chapter will, based on criminological theory, explain how cybercrime happens and which measures should be adopted to combat cybercrime. The concept of a risk society and the framework of Routine Activity Theory (RAT) are adopted to explain why cybercrime occurs. Guided by RAT and risk-based crime prevention, this book will also propose possible measures for the Taiwanese and Chinese governments to take which may be effective in cybercrime prevention.

After the introduction, background and methodology, Part II will focus on cybercrime and information security problems currently occurring in Taiwan and China.

Chapter 3 will examine cybercrime problems in Taiwan and China. Trends in malicious activities will be examined using statistics provided by information security companies, in particular Symantec. Emphasis will be placed on bot-net distribution. Bot-nets, a new type of organized crime in the virtual world, have become the most serious internet security problem in

Taiwan and China. This chapter will compare the structure of organized crime in the real world and bot-nets in the virtual world. It will suggest that bot-nets can be regarded as organized crime in the virtual world, even if the bot-net is constructed by fewer than three people.

The chapter will also, by analysing interview data, determine the reasons why bot-nets are so popular in Taiwan and China. The chapter will also discuss the control of bot-infected computers and concludes that no longer can we say 'seeing is believing'.

After gaining a clear picture of the extent of cybercrime between Taiwan and China, Part III will focus on the regulatory responses against cybercrime across the Taiwan Strait. According to RAT, establishing a capable guardian is an important element in preventing a crime from happening. This part will examine Taiwan's and China's legal responses to cybercrime and mutual cooperation, to see how laws and regulations could work efficiently as capable guardians to reduce motivated offenders from perpetrating cybercrime.

Chapter 4 will focus mainly on a comparison between criminal law and criminal procedural law in Taiwan and China, and on the UN Treaty and the first international convention relating to cybercrime – the Council of Europe's *Convention on Cybercrime*. The chapter will introduce the criminal law and criminal procedural law relating to cybercrime in Taiwan and China. It will then compare those with the Convention. Then, using interview data, the chapter will discuss the limitations of the law and express concerns on cybercrime investigation and prosecution. Through the comparative law approach, this book will examine the issue of dual-criminality between Taiwan and China and their compliance with international conventions.

Although the USA has ratified the *Convention on Cybercrime,* thus affording the convention greater international status, neither Taiwan nor China is a party to it. The chapter will also discuss why Taiwan and China have not adopted the Convention.

Following Chapter 4 on legal responses to cybercrime, Chapter 5 will discuss existing mutual cooperation between Taiwan and China. Hindered by the sensitive political situation, there is no official mutual assistance between Taiwan and China. However, the Red Cross Society and other designated organizations have worked as intermediaries.

The chapter will discuss the model used by those intermediaries and consider whether they might play a role in bridging the gap between Taiwan and China in combating cybercrime. Apart from cooperation through designated non-governmental organizations, the chapter will also examine

other possibilities for cooperation through third parties, such as international corporations. The extent of and limits to the use of third parties will also be discussed.

Part IV will draw attention to crime prevention from the perspective of target-hardening. It will not focus on the elimination of cybercrime, but will discuss how to reduce the impact of cybercrime and how to prevent it from spreading.

Chapter 6 will discuss the necessity of establishing a pre-warning system and how to make it effective. Malicious computer activities are identified by this book as resembling an infectious disease in the real world. Most users (including government agencies and companies) use proprietary software and therefore are more vulnerable to hacking or a cybercrime event through any breach in that software. That is, hacking of one computer may mean the hacking of many computers.

Cybercrime challenges the 'mind your own business' approach to security. It becomes essential to think in terms of 'mind our business'. Prevention requires victims to share their problems in order to prevent others from becoming victims. However, government agencies and enterprises have concerns about sharing their information on security incidents.

The chapter will, based on institutional theory and responsive regulation theory, discuss the forming of an institution to encourage sharing. It will examine the existing information sharing systems in Taiwan and China through the regulatory pyramid and the strength-based pyramid. From interview data, the chapter will also highlight issues and concerns that may hinder or induce companies or government agencies to share their security problems. A feasible model for an information sharing platform will be proposed.

Finally, Chapter 7 will provide suggestions on what the public and the private sectors might do to combat hi-tech crime. It will also discuss whether laws and regulations should be modified. from interview data, and endeavour to provide some practical suggestions on the building of a feasible cooperation model for fighting hi-tech crime between Taiwan and China.