POLICING INTERNET FRAUD: A study of the tensions between private and public models of policing fraudulent activity in cyberspace with particular focus on South Korea and special reference to the United Kingdom and the United States

Tae Jin Chung

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

The University of Leeds
School of Law

December 2008

Acknowledgements

I wish to express my sincere appreciation for the opportunity to work with my thesis supervisor, Professor David S. Wall. His constant support and dedication to my work have remained a constant inspiration for me during my doctoral studies. I would like to acknowledge the support of my other supervisor, Professor Clive Walker. Thank you for your helpful comments for creating a basic structure for the thesis. I believe that your comments during the upgrade process enlightened me.

There are special people who have been supportive during my academic career: to the respondents who participated in the interviews and shared their experiences, a sincere acknowledgement is offered. Special appreciation also goes to the government agencies: CTRC, ICIC, NCSC, KISA, FSA, KrCERT/CC, KFTC, KSRC. Without the assistance of these people and agencies, this research could not have been accomplished. In the private sector, internet crime and security experts in Ahnlab, Koscom, CONCERT, Auction Corp., BC Card, Daum, GCN and YMCA participated and provided valuable information for this research.

My father, Min-Taek Chung, deserves special memory. He passed away during my Ph.D. study in the United Kingdom. I remember him so much. I would like to thank my mother Ki-Hwa Kim who spiritually supported me throughout the Ph.D. course and my grandmother Young-Shin Kim, lovely wife Hyun-Jung and daughter Selynn who inspired the value of an academic achievement, which sustained me during this research. Their continual support and encouragement will be remembered.

Abstract

As more people obtain online access and the finance sector becomes transformed by networked technology, opportunities for internet fraud grow. In recent years we have seen the maturation of new digital environments in which financial transactions can take place while at the same time we have seen an explosion in incidences of identity theft. This unprecedented rise in internet fraud is depressing growth in e-commerce activities and is creating growing demands by governments, the commercial sector and also the public for an appropriate model of policing. This thesis will explore the policing of internet fraud and it will argue the scope of police work with regard to white collar crime, because the public believe that police forces do not effectively control internet fraud and non-internet fraud.

By drawing upon various global sources this thesis analyzes the tensions between the respective interests of the public and the private sectors. Such tensions raise concerns about how public resources are most effectively allocated in the public interest. Although internet fraud is a globalized phenomenon and indeed the UK and the US are notably mentioned, the analysis has specially focused on South Korea.

At the core of the thesis is the observation that a major conflict of interests emerges when the private and public models of policing compete for "ownership" over internet fraud, so before exploring the laws, rules and enforcement models for policing internet fraud, it is first necessary to remove the tensions that exist between and within policing bodies.

Two significant tensions were examined: firstly, the tension caused by different characteristics and objectives of private and public models of policing. Whereas the public police pursue the public interest thorough a public model of justice, the private sector polices problems in their own private interest along a private/corporate model of justice. Secondly, tensions are also created within the public policing sector by intra-governmental competition. For example, the South Korean National Police have attempted to obtain independent investigatory powers while the Prosecutors' Office strongly defends its ownership of investigatory powers.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

BJA/ USA	Bureau of Justice Assistance
CIPAC/ USA	Critical Infrastructure Partnership Advisory Council
CNI/ UK	Critical National Infrastructure
CNSA	Contact Network of Spam Authorities
COE	Council of Europe
CPNI/ USA	Centre for the Protection of National Infrastructure
CTRC/ Korea	Cyber Terror Response Center
DHS/ USA	Department of Homeland Security
ENISA	European Network and Information Security Agency
FSA/ Korea	Financial Security Agency
FSC/ Korea	Financial Supervisory Commission
FSS/ Korea	Financial Supervisory Service
FTC/ USA	Federal Trade Commission
IC3/ USA	Internet Crime Complaint Center
ICIC/ Korea	Internet Crime Investigation Center
ISAC	Information Sharing and Analysis Center
IFCC/ USA	Internet Fraud Complaint Center
IWF/ UK	Internet Watch Foundation
KISA/ Korea	Korea Information Security Agency
KSRC/ Korea	Korea Spam Response Center
KFTC/ Korea	Korea Financial Telecommunications and Clearing Institute
MFE/ Korea	Ministry of Finance and Economy
MGL/ Korea	Ministry of Government Legislation
MIC/ Korea	Ministry of Information and Communication
NCL/ USA	National Consumer's League
NCIS/ UK	National Crime Intelligence Service
NCS/ UK	National Crime Squad
NCSC / Korea	National Cyber Security Center
NFIC/ USA	National Fraud Information Center
NFRC/ UK	National Fraud Reporting Centre
NHTCU/ UK	National High Tech Crime Unit

NIS/ Korea	National Intelligence Service
NPA/ Korea	National Police Agency
NSC/ Korea	National Security Council
NW3C/ USA	National White Collar Crime Center
SFO/ UK	Serious Fraud Office
SPO/ Korea	Supreme Prosecutors' Office
SOCA/ UK	Serious Organised Crime Agency
WCCRC/ USA	White Collar Crime Research Consortium

Chapter 1: Introduction - Internet Fraud and the Information Age

1.1 Background

Internet fraud has become one of the major threats to online shoppers and e-business markets as more people and businesses use the internet as a major vehicle to purchase and sell their goods. It has decelerated the development of e-commerce activities. The reported loss from internet fraud in 2007 was $239.09 million dollars (IC3, 2007) with a median value of $680 per complaint in the US which was more than the loss from other crimes. This was noticeably increased from 2006 ($198.44 million). In the UK, monthly internet shopping sales rose by 80 percent to £4.2 billion from £2.34 billion in July, 2006. Annually, online retailers pay £580 million in response to internet fraud (Samport, 2008). While e-business industry pays huge amounts for the prevention of internet fraud, fraudsters have developed new methods to deceive innocent consumers. However, existing counter-measures for internet fraud are very limited. The most well-known method is the chip and PIN system for credit card transactions used in the UK. It has significantly decreased credit and debit card related frauds. Therefore, fraudsters have moved their focus to card-not-present transactions.

Despite the fact that internet fraud has a significant impact on e-commerce activities worldwide, the policing of internet fraud has not been written about in the criminal justice literature. Existing literatures simply introduce internet fraud as a type of cybercrime and consider the policing of cybercrime as a whole. There appears to be no further study about policing fraudulent activities in cyberspace. Therefore, this thesis particularly argues that whether the public police have adequate capabilities to deal with internet fraud or not, the private sector has much better knowledge and resources to deal with internet fraud. This thesis suggests an effective cross sector partnership model for policing internet fraud in the course of removing tensions residing between the two sectors. Consequently, the introduction of an ideal model for policing internet fraud in South Korea is the focus of this research.

1.2 Brief outline of existing literature

With regard to this thesis topic, no research on policing internet fraud appears to have been done in South Korea and other nations. Fortunately, similar work (although it does not focus on internet fraud) has been done by McKenzie (2006). His thesis introduces an ideal partnership model for the policing of electronic crime. Despite the fact that it does not directly detail the topic of internet fraud, it provides useful ideas about partnership policing for electronic crime. For the panoramic vision, David Wall's (2007) 'the internet's order maintenance assemblage' model inspires the construction of this thesis. His thesis shows the role of each participant with regard to policing cyberspace. For the basic concept of policing, the idea was borrowed from Reiner (2000) and Wall (1997: 223) 'cybercrime is not routine activity of the public police which includes cross border investigation'.

Grabosky and Smith (2001: 29) reported that 'security in cyberspace depends on the efforts of a wide range of institutions, as well as on a degree of self-help by potential victims of digital crime' and it is more likely to depend on a 'mix of law enforcement, technological and market solutions'. Technological intervention such as biometric authentication and filtering software can be good counter-measures to prevent and to control internet fraud (Grabosky and Smith, 2001; Green, 2001). Recent research by Burns et al. (2004) show that 64.2 percent of participants reported that there was very effective cooperation among law enforcement agencies. These findings indicate the need for a central clearinghouse of information available to all law enforcement agencies. A clearinghouse of information in which agencies involved with internet fraud enforcement efforts could share 'technical information, the names of expert witnesses, advice from experienced prosecutors, or the location of available labs which would greatly assist law enforcement effort' (Burns and Whitworth, 2002: 18).

Private and public sector partnership was strongly recommended by Grabosky and Smith (2001) who suggested that public awareness programmes by relevant public agencies and financial institutes are needed. For better coordination and cooperation, the Financial Services Antifraud

Network Act of 2001 was established in the US (Burns et al. 2004). However, it is less effective for the private sector. Recently it has been discussed that law enforcement agency oriented information sharing has to be expanded to the entire criminal justice agency (Burns et al, 2004). An international level of response by Europol and Interpol has been observed. however, more efforts at the international level of cooperation have been emphasized. The international levels of law enforcement agencies have shown efforts to adapt to the policing of cybercrime, while the local level of response has still been below the appropriate level.

1.3 Summary of the problem

As suggested by the literature review, public police do not have sufficient resources and knowledge to deal with internet fraud. Cross sector partnership is imperative to perform appropriate levels of policing. However, there are various tensions residing between the two sectors. Without removing those tensions, effective partnership of policing internet fraud cannot be achieved. In particular, the local level of response against internet fraud is far behind that at the international level of response due to those tensions. It was also found that few nations have specialized law enforcement units to handle internet fraud. Unlike the public sector, the private sector has performed much better in policing and investigation activities. According to Williams, the 'Forensic Accounting and Corporate Investigation (FACI) industry' (2005: 317) has positioned itself as a supplier of a unique and highly specialized form of investigative and quasi-juridical labour geared to the resolution of 'business troubles' ranging from the theft of intellectual property, to the misappropriation of corporate assets, to breaches of financial security. However, Brodeur and Kempa (1995; 1999) argued that the public-private dichotomy fails to account for the diversity and heterogeneity of actors participating in the governance of security or policing, including the policing of internet fraud. The distinction between public and private forms of policing are increasingly difficult to maintain and have been proven somewhat outdated, given the emergence of complex and multi-dimensional 'security-networks' (Johnston, 1996: Shearing, 1996; Loader, 2000; Newburn, 2001) or forms of 'nodal governance' (Johnston

and Shearing, 2003: 18). Therefore. policing internet fraud has to be studied in the light of the 'order-maintenance assemblage' suggested by Wall (2007).

1.4 Scale of the study

This research is a partially comparative study. I choose the United Kingdom and the United States to compare with South Korea, mainly with regard to: *How they police internet fraud? Who polices internet fraud?* and *What laws they use for the control of internet fraud.* There are three reasons for choosing these countries. First, the United Kingdom and the United States are historically and politically strong alliances to South Korea. Korean government does not have any negative preoccupations with their systems Therefore, comparison of the policing model and laws of these countries is applicable and admissible in South Korea. Second, most available resources for this study are to be found in the United Kingdom and the United States. Although a large volume of useful information is available in Australia, South Korean people are not familiar with Australian systems, so it was not chosen as a primary comparable subject for this study. Third, the researcher of this study studied in the United Kingdom so it was more reliable and comfortable when conducting the research.

1.5 Objectives of the study

The primary aim of this thesis is to identify the tensions that surround the policing of internet fraud, such as lack of trust, different investigation philosophies and negative publicity. These have negatively influenced the maintenance of the correct balance between the private and public models of policing internet fraud. Each sector has different interests and cannot abandon its policing authority. In order to provide a more effective and efficient method of internet fraud control, we also aim to suggest an appropriate level of policing internet fraud for the two sectors.

In order to establish the above mentioned aim, the following objectives have to be achieved:

- Identification of tensions produced by internet fraud.

- Definition and classification of internet fraud because internet fraud does not fit into the existing category of white-collar crime.
- Identification of correct balance of policing internet fraud.
- Examination of governance of internet fraud.
- Examination of relationship existing between and within the public sector.
- Investigation of major faults and lack of the South Korean policing system in respect to its treatment of internet fraud.
- Analysis of factors that promote and resolve tensions.
- Examination of internet fraud control at the local, national and international level.

This thesis will also examine the laws, rules, and policing strategies that could help to eliminate these tensions. Suggestion that the removal of tensions may achieve effectiveness and efficiency in policing internet fraud provides good grounds for academic debate. This legally and politically sensitive issue may catch the attention of many policy makers, law enforcement staff and criminal justice scholars.

1.6 Research questions

Research questions about resolution of tension and an appropriate policing model for the response to internet fraud will be answered by using existing data and informational sources for South Korea, the UK and the US, while an additional qualitative study for Korea will be undertaken as very little existing literature considers the current situation in Korea.

Both private and public police have hypothesized that removing tensions between the private and public models of policing will enhance the effectiveness and efficiency in enforcing correct behaviours on the internet. In order to prove this hypothesis, it is necessary to develop pertinent research questions for the interviewees. Therefore, the main research questions ask: *How do tensions influence policing? How do tensions influence your work in terms of your working practices for response? Why it is important to remove tensions?* Since 'tension' in policing internet fraud is

not well known to the general public. the term 'tension' needs more conceptual building in order to address the issues properly. Using a vague meaning of tension in the research would confuse interviewees. Therefore. some examples of tension need to be addressed.

There are also additional questions asking: *Why are tensions produced? How can tensions be removed? Can the government or your organization do anything to help remove these tensions? How can partnership policing be promoted?* These questions will find out the best solutions to reduce or remove tensions.

If negative tensions are found to be impeding the effective and efficient policing of internet fraud, it will suggest the adoption of an appropriate policing model by which these tensions could be removed. The correct balance of policing internet fraud should aim to be mutually beneficial to the private and public sectors while preserving their interests.

It is believed that cross-sector partnership policing is the best way to maintain the correct balance for policing internet fraud. However. there has not been any standard upon which to decide the correct balance between the two sectors.

The following sections outline the design of a programme of qualitative research that aims to critically examine the questions and issues raised by tensions between the private and public models of policing internet fraud, from which normative guidelines for implementation might be proposed.

1.7 Methodology

The research questions in this thesis call for qualitative study and normative analysis, which is an analysis based on a judgment about what is desirable and what is not desirable. Simply, normative analysis suggests how policing internet fraud ought to be. Tension is a normative concept. that is: 'evaluative, denoting or implying goodness, desirability. what ought to be. or the negation of these denotations. Compassion, equality. and exploitation

are such normative concepts. Clearly, the same concept may be used descriptively or normatively depending on context and intent. However, some concepts have a built-in evaluation that even a careful descriptive analysis may not avoid, such as with the concepts murder, torture, exploitation, charity, and love' (Rummel, 1981: 320).

Normative analysis 'attempts a rational and principled exploration of moral/political justifications for a given course of action' (Bottoms, 2000: 48). It is not simply to find true explanations of social phenomenon. Normative theorists should consider whether there is a relationship between the normative proposition and real-life situation or not. Without justification of reliable criteria, rational, normative analysis cannot be implemented. As stated in McKenzie (2006: 95), 'it is also crucial to provide explanatory accounts of current practice' of investigation of electronic crime. According to Berg (2000: 230), 'explanatory case studies are useful when conducting causal studies. Particularly in complex studies of organizations or communities, one might desire to employ multivariate cases to examine a plurality of influences'. Tensions are a good example of the independent variable. The concept of tension can be directly observable and as such may be viewed as an objective in policing internet fraud although it 'requires consideration of the individual's own perception and understanding' (Berg, 2001: 11).

Positivists assume that reality is objectively given and can be described by measurable properties that are independent of the researcher and his or her instruments. Positivist studies generally attempt to test theory in an attempt to increase the predictive understanding of phenomenon (Myers, 1997). Removing tensions in policing internet fraud is a predictive phenomenon so therefore a positivist perspective is appropriate and valid for this research.

1.8 Qualitative research strategy

The researcher used a qualitative research method to obtain the core research values that determine the balance between those mentioned three models of policing internet fraud. 'Qualitative methods allow a researcher to

share in the understandings and perceptions of others and to explore how people structure and give meaning to their daily lives' (Berg, 2001: 7). According to Noaks and Wincup (2004: 15), the qualitative research method 'helps to inform the development of policies of crime control'. However, the main reason why the researcher chose a qualitative research method is because it is the most efficient and effective method to obtain necessary answers to the research questions, from the private sector of security experts (such as CSOs (Chief Security Officers), IT security staff, risk management staff at financial institutions, corporate legal department lawyers, and corporate marketing department staff) and the public sector of security experts (such as public police officers, public prosecutors, government and intelligent agents), perceiving the tensions between and within their domains.

It would not be easy to obtain clear answers from respondents since the topic of the thesis is politically sensitive in the study focus area – South Korea. Since most research questions require non-numerical answers, a qualitative research method is the most appropriate for this research. A qualitative research method reflects real-life that includes 'not only emotions, motivations, symbols and their meanings, empathy, but also other subjective aspects associated with the naturally evolving lives of individuals and groups'. These elements may also represent 'their behavioural routines, experiences, and various conditions affecting these usual routines or natural settings' (Berg, 2001: 10- 11).

In order to undertake a qualitative study of tensions between the private and public models of policing internet fraud, it was necessary to adopt a research method that would ensure an in-depth understanding of tensions affecting the policing of internet fraud. Qualitative interviewing fits this research purpose because respondents provide valuable information that cannot be experienced by others. The respondents most appropriate for this study are experts in policing cybercrime. Their role is not simply to reveal their own views in relation to an event, but to describe what actually happens in the policing of internet fraud.

Prior research revealed a distinct lack of research that attempts to explore tensions affecting the policing of internet fraud. Similar researches conducted tended to deal with partnership policing of e-crime and found factors affecting the investigation of e-crime to include detection of incidents, under reporting of e-crime, prioritization of different types of e-crime, obtaining evidence, and inadequate staffing (Mckenzie, 2005).

After examining various possible research methods, qualitative interviewing was chosen as the most useful and creditable means to obtain the necessary information required answering the research questions. Other methods, such as survey or self-administered questionnaires, were considered to be insufficient.

In this study, the semi-structured interview was mainly used to obtain information from respondents. It has an advantage in that interviewers are allowed freedom to wander; 'interviews are permitted to probe far beyond the answers to their prepared and standardized questions' (Berg, 2001: 70).

The interview schedule consisted of four sections. The first section asked demographic information about the respondent with a structured interview schedule. The second, third and fourth sections asked about the nature of tensions, appropriate policing models and the resolution of tensions. Throughout the interview, respondents were encouraged to speak their opinion based on their experience. The semi-structured format of the interview schedule allowed the order of questions to be varied in accordance with the direction and 'flow' of any given interview. The purpose of the interviewing process was to attempt to access the perspectives of the subjects, rather than those of the interviewing researcher; and the less structured form of the interview allowed subjects to define the world in their own perspectives. The key point of this qualitative research is to obtain an in-depth understanding of tensions between the private and public models of policing.

Interview schedule

Tensions between the private and public models of internet policing found in this study cannot be applied to other non-police organizations or agencies since partnership policing is different from other business collaborations. Partnership policing creates interplay of disagreement, power play and inter-dependency (Mckenzie, 2006). Therefore, in the light of these considerations, the research method in this study, including the primary instrument of the interview schedule was appropriately designed (See Appendix 2).

An interview schedule was developed that was designed for interviewees of the private and public sectors. Interview schedules aimed to answer questions such as: *What are the most serious tensions? What is an appropriate model of policing Internet fraud? How can tensions be removed?* As mentioned earlier, the interview schedule consisted of a pool of questions divided into four sections:

- Section 1: demographic information of respondent;
- Section 2: questions on tensions;
- Section 3: questions on policing internet fraud:
- Section 4: questions on resolution of tensions.

The first section was structured, with a mix of closed and open questions, and the other three sections were semi-structured, with a mixture of closed and open questions. Usually, obtaining demographic information of respondents does not require open questions. However, for this research, it was important to know respondents' daily activities and experience. These could not be described by 'yes' or 'no' answers.

The pilot study

A pilot study was undertaken prior to the data collection phase and the first two interviews with the private and public sector personnel. The purpose of sample interviews was to evaluate the interview schedule in terms of whether it covered the full spectrum of policing internet fraud; whether its questions were properly formulated, and what adjustments might be

required with respect to them; what sequence of questioning would work best; how best to establish a good rapport and confidentiality between interviewer and subjects; what would be the best way of taking down notes; and what time-frame would be required to complete the interview.

Since in-depth interviews might prove more intrusive and involved in terms of qualitative methods, and because of possible subject discomfort and sensitivity of the subject matter involved in the interviews, the study was carefully explained to each of the two subjects prior to obtaining their agreement to participate in the pilot study. The subjects were each informed that their respective interview would be confidential and that they could terminate the interview at any time. They were also advised that they could answer, choose not to answer, or go into further detail, on any question that might be asked in the interview. Additionally, throughout the course of the actual interview process, the subjects were repeatedly asked if they were comfortable to continue with the interview. Neither subject expressed uneasiness during the course of the interview. It was clear that they did not feel pressured by the interview or by the questions posed to them in the interview; quite to the contrary, they easily identified with the objectives of the larger study, as well as with those specifically attached to the interview itself. The fact that most of the questions were not of a personal nature, but rather, were directed at the subject's experience of policing internet fraud and of the factors (tensions) surrounding that event, could have been contributory to the creation of an image of a hostile relationship between private and public sectors that prevailed throughout the interview.

During the course of the pilot study, it was found that overall the proposed questions were valid for the formal research. The researcher asked questions such as: *What are the most serious tensions? Why are those tensions produced?* and *When is it appropriate to involve (a) private rather than public policing mechanisms (b) public rather than private policing mechanisms?* Interviewees believed that those questions were relevant to the aim of this research.

However, it was found that some questions contained the same meaning. For example: *How do those tensions influence your working practices for response?* and *Is it important to remove tensions? If so, why?* The researcher recognized that those questions could be expected to reveal almost the same answers so one had to be deleted. The researcher deleted the latter one: *Is it important to remove tensions? If so, why?*

The duration of the interviews varied from twenty-five to thirty-five minutes, which was thought to be generally within the expected duration that had been scheduled for them. The recording of the interviews was done through note taking only since it was done informally. Since the changes that needed to be made to the interview schedule and process were only minor in character, the decision was taken to include these cases in the total sample of research cases that were analyzed and interpreted in the study. The pilot study was an important phase in the research process of the study, one that allowed the researcher to familiarise himself with appropriate interview techniques, so that the quality of the data collected in the study could be improved.

Sampling

Most data for this research were collected between November 2006 and January 2007 from both the private and public sectors through face-to-face interviews in Korea. Overall, 16 people in the private and public sectors of security were interviewed who were considered to be internet crime investigators or IT security experts. There was no specific job title of internet fraud investigator since internet fraud investigation does not exclusively belong to an independent agency or organization. There are many policing bodies participating in the policing of internet fraud as a part of their overall policing activity in cyberspace.

The researcher selected interviewees based on the nature of the organization. The rationale for selecting samples from those organizations is that they can not only represent each category of sectors, but also address fraudulent activities of each sector in the literature review of this thesis.

For the private sector, eight experts were interviewed. Interviewees were selected from IT security companies (Ahnlab), ISAC (Koscom).CERT (CONCERT), an online auction company (Auction Corp.), a major credit-card company (BC Card), a famous portal site (DAUM). non-profit organizations: GCN (National Council of the Green Consumer's Network in Korea) and YMCA (National Council of YMCA's of Korea). Each interviewee was selected from internet fraud response related organizations. They are reliable and valid human resources to provide evidence for the research questions.

Separately, a corporate legal department lawyer and a member of corporate marketing department personnel were also interviewed in order to obtain an answer for the question regarding tension between corporate legal department lawyers and corporate marketing departments. However, the researcher was not able to obtain any valuable information from them since they do not want to answer for the sensitive questions so that the question about tension between corporate legal office and marketing department was deleted.

For the public sector, eight experts were interviewed. Interviewees were selected from the National Police Agency (CTRC), the Supreme Prosecutors' Office (ICIC), the National Intelligence Service (NCSC), the Korean Information Security Agency (KISA), the Financial Supervisory Service (FSA), Korea Internet Security Center (KrCERT/CC), the Ministry of Finance and Economy (KFTC), Korea Information Security Agency (KSRC). A public cyberpolice officer, the public prosecutor's internet crime investigator and other government agents represent the public sectors. The researcher believes that interviewees have profound knowledge and experience that will enable them to provide reliable information.

Gaining access to the subjects

The nature of the research question can be a politically sensitive issue so it was not easy to arrange interviews without special recommendation. Some places, such as NCSC/NIS (National Cyber Security Center of the National Intelligence Service) do not allow other people to contact and visit their

office to get information, whether it is classified or not. Generally, NCSC/NIS is publicly known as an impregnable fortress. It is almost impossible to access the NCSC/NIS as an individual researcher. However, the researcher's long-term membership of criminal justice societies, such as Korea Police Studies Association, Digital Forum of the National Congress and an alumni relationship made it possible to access the respondent's office without any official procedure. The initial interviewee at the NCSC was changed unexpectedly due to his regular reassignment. However, the new agent at his office was very cooperative and agreed to the interview. The interview was held at the NCSC/NIS office in Seoul, but he did not allow the researcher to look around their operation room. The respondent was a high-ranking agent of NCSC and understood the overall Korean situation regarding this research topic. The interviewee provided a very analytical perspective of policing cyberspace and crime.

Access to the CTRC/NPA (Cyber Terror Response Center of the National Police Agency) was relatively easy in comparison to other agencies since the researcher is a member of the Digital Forum of the National Congress. Through the previous conference, there was a close rapport between the researcher and the interviewee. The interview was held outside the National Police Agency. The interviewee provided very useful information that was pertinent to the research question without any concealment of the nature.

For the interview with the prosecutor, the researcher visited the Cheong-Ju District Prosecutors' Office. It was located about one and a half hours from Seoul. The interviewee was officially dispatched to the Ministry of Information and Communication as a legal advisor before relocating to the Cheong-Ju District Prosecutors' Office. He was famous for investigating and prosecuting many cybercrime cases. He used to work closely with the NIS for industrial espionage cases. Because of his various legal experiences, the researcher was able to obtain information on legal issues related to the policing of internet fraud.

Other non-police public agencies welcomed the researcher because those agencies are open to the public and their nature of work does not include

highly confidential matters. Therefore, the researcher conveniently visited their offices for the interviews without any problems. Among those agencies, KISA (Korea Information Security Agency) has subsidiary units such as KSRC (Korea Spam Response Center), KrCERT/CC (Korea Information Security Center), and PRIVACYNET. The researcher was able to conduct four interviews in the same building.

Most respondents in the public sector are linked via membership of the Korean National CERT council which is formed by nine government agencies: National Intelligence Service, National Police Agency, The Supreme Prosecutors' Office, Korea Information Security Agency, Korea Financial Telecommunications and Clearings Institute, Defence Security Command, Ministry of Information and Communications, Ministry of Science and Technology, Ministry of Government Administration and Home Affairs.

The public sector is well linked so each respondent tended to know each other officially or unofficially. During the course of the interviews, it was easy to identify the correct respondent who could provide reliable information regarding this research. Overall, the interview process in the public sector was relatively easy and comfortable. Most respondents showed a very friendly manner during the interview process. It was assumed that the individual researcher would not complete the research unless there was special recommendation by the higher authority. Fortunately, the researcher's long time maintained human network in the Korean Police Studies Association helped this research without any obstacle or delay. Some respondents recommended finding another useful topic for the thesis.

While the public sector respondents were linked by the membership of the Korean National CERT council, most private sector respondents were linked by the membership of the CONCERT (Consortium of CERT)[1]. Unlike the public sector, private sector respondents were more cautious and unfriendly. It may be attributed to the nature of their work in that they

---

[1] Consortium of CERT (Computer Emergency Response Team)

protect the most important business information of their company. Each company had different perspectives and interests in terms of why and how they deal with internet fraud so it was necessary to convince each company of the benefits of this research for the private sector. After the explanation, respondents expressed their interest in balancing private and public models of policing internet fraud. They agreed that it is essential to remove tensions for promoting effective and efficient policing.

The first interview was held at CONCERT since it is known as a hub for private IT related companies and organizations. The president of CONCERT is a leading expert of Information Security and currently is working at SungKyunKwan University as a professor of the computer science department and a director of the telecommunication bureau. The interview was held at the interviewee's university office where he spends most of his time teaching and working. The interview appointment was made through his university secretary. The researcher was welcomed by the interviewee. The interviewee expressed interest in the fact that this research will contribute to promoting the policing of internet fraud. His expert perspective was remarkable and can be used as a good reference for further research.

The second interview was held at the CTRC (Cyber Terror Response Center in the National Police Agency in Korea) because CTRC is the first government office to begin policing cybercrime[2]. A veteran cybercrime investigator was introduced by the director of the CTRC. The interviewee was also a very well known police liaison officer in both the private and public sector. He was aware of current issues and knows almost everybody who works in online security. The researcher was satisfied that the first two interviews were held with the right people. Through these two interviews, the researcher also confirmed that other interviewees would be good selections for the research.

---

[2] Hacker investigation division was found in October, 1995.

Interviews with other respondents were subsequently scheduled. Most respondents in the private sector and from private companies required permission from higher authorities in order to be interviewed by the researcher. Some respondents attempted to confirm the identity of the researcher. The researcher provided a copy of identification or a letter for cooperation with the research. The majority of respondents did not require confirmation of the identification of the researcher since the researcher introduced himself through e-mail or telephone when the researcher arranged interviews. Compared to other organization's access, NGOs (Non Government Organization) did not have any high threshold through which to delay the timetable of the interview. Approval of the interview was almost made at the time of request. NGO respondents were very cooperative since they are not profit organizations. They provided an objective perspective through which to address the current issues of policing internet fraud.

Respondent demographics

Despite the fact that the research used a small number of participants these respondents represented experts in the policing of internet fraud and cybercrime in Korea. It was unnecessary to involve invalid samples in order to inflate the number of the sample, which would not enhance the validity of this research.

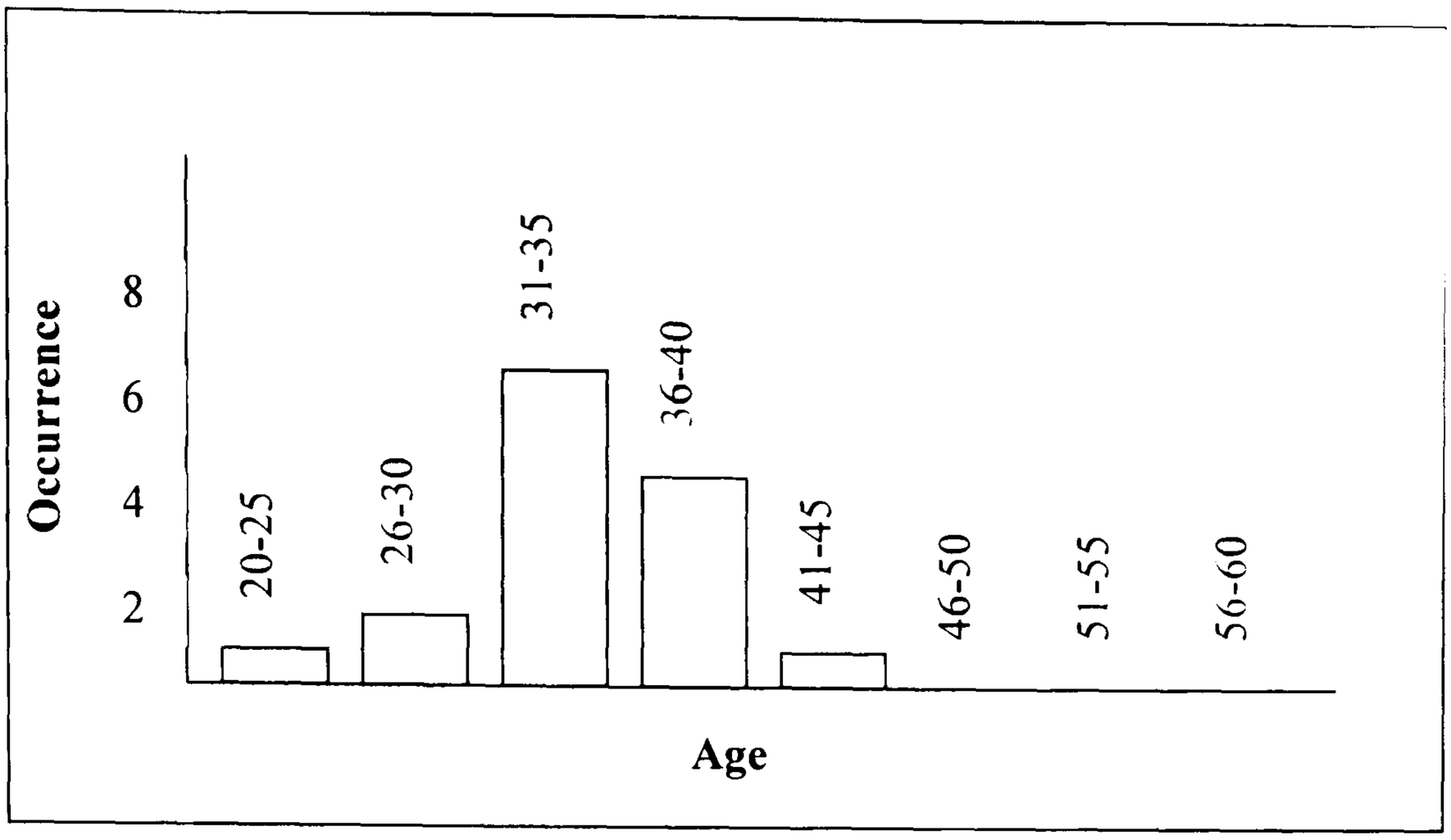
Table 1-1 displays information regarding the 16 respondents who participated in the study. All security experts interviewed from both the private and public sectors were well known within the IT security, fraud prevention or internet crime investigation.

Table 1-1: Respondents by sector

Sector	Organization	Frequency	Percent
Public Sector	CTRC	1	6.25
	ICIC	1	6.25
	NCSC	1	6.25
	FSA	1	6.25
	KFTC	1	6.25
	KISA	1	
	KSRC	1	6.25
	KrCERT	1	
			6.25
			6.25
Sub-total		8	**50**
Private Sector	Ahnlab	1	6.25
	KOSCOM	1	6.25
	CONCERT	1	6.25
	Auction	1	6.25
	BC Card	1	6.25
	Daum	1	6.25
	GNC	1	6.25
	YMCA	1	6.25
Sub-total		**8**	**50**
Total		**16**	**100 %**

Figure 1-1 indicates that the majority of respondents were between 31 and 40 years of age; this majority (12 respondents) makes up 75% of the following sample.

Figure 1-1: Age of respondents



Most respondents (under the age of 40) reported that they had no other job experience before joining their current office. They could be considered the 'true' IT generation. In contrast, older respondents (over the age of 40) reported that they had other job experience before joining their current office. Their skills upgraded accordingly as technology advanced.

It is also assumed that age and experience are not in direct proportion. Thus, older experts do not necessarily have more experience than younger experts since the emergence of the internet is a recent event.

Compared to the terrestrial level of policing, respondents in the private sector reported that they had no law enforcement experience before joining their current company. This implies that previously there were not many IT security experts in the law enforcement field.

Table 1-2 indicates that respondents in both the public and private sectors consisted predominantly of male security staff members (n=13, 81.25%). There were more female respondents in the private sector; 25% of females work in the private sector, whilst only 12.5% of females work in the public sector. This is indicative of the fact that the private sector permits more females to participate in policing cyberspace than the public sector. The public sector tends to have a notably more conservative environment that

the private sector. Other than the IT security division, female employees are outnumbered in IT related companies in Korea.

Table 1-2: Sex of respondents

	Male	**Female**	**Total**
Private Sector	6 (37.5/75)	2 (12.5/25)	8 (50/100)
Public Sector	7 (43.75/87.5)	1 (6.5/12.5)	8 (50/100)
Total	13 (81.25%)	3 (18.75%)	16 (100%)

Table 1-3 demonstrates that all private and public sector respondents had attained an undergraduate university degree or higher, with 63% of respondents having obtained a Masters or PhD degree. Participants were asked whether any special qualifications or training in relation to the policing of internet fraud was required for their role. Law enforcement agency respondents (police, prosecutors, and intelligence agents) reported that they had special training after they joined their offices. Other respondents reported that they had received IT security training before commencing work at their current positions. It seems that the public sector needs more advanced techniques to respond to internet fraud.

Table 1-3: Higher education attained by respondents

	Private Sector	**Public Sector**	**Total**
PhD	2 (12.5)	2 (12.5)	4 (25)
Master	3 (18.75)	2 (12.5)	5 (31)
Bachelor	3 (18.75)	4 (25)	7 (44)
High School	0	0	0
No response	0	0	0
Total	**8 (50%)**	**8 (50%)**	**16 (100 %)**

Although many people in IT security institutions have higher education, displacement of human resources is a common occurrence, especially in the public sector. For example, a prosecutor or investigator who is assigned to the Internet Crime Investigation Center (ICIC) usually does not stay there

more than two years due to regular personnel transfers performed by the Supreme Prosecutors' Office.

Compared to other parts of occupation, it indicated a much higher educational level of respondents. The majority of respondents achieved their academic degrees before joining their current offices. Respondents were qualified as experienced or professional when they were employed by each sector. Demographic information gathered, including respondents' level of education, was very important for this research in order to determine whether the reliability of the respondents was consistent across sectors. This data collection procedure shows the validity of the sample. Therefore, profiles of respondents show that they are well-educated elite people in Korean society and their responses for this research are trustworthy and valid.

Interviewing

All of the interviews were conducted face to face at the interviewees' place of work or near the perimeter. Prior to the appointment with interviewees, it was impossible to know in advance whether there would be any potential subject available for interviewing on any given day. Fortunately, using the human network in Korea, every interview was tightly scheduled. Interviews varied in length, but most of them were less than one hour. It was difficult to have longer interviews since respondents claimed their workloads were too heavy. Before each interview began, the researcher explained to the interviewees the main purpose of the research and how it contributed to policy making for internet fraud. All personnel were aware of the aims of the research project and were given assurance of anonymity.

Prior to the interview beginning, interviewees were asked to read and sign an informed consent form. They were informed that the interview would be audio taped for later review by the researcher, but assured that their responses would be confidential. Interviewees were informed that they did not have to answer any questions that made them uncomfortable and that they could withdraw from the interview at any point without loss of experimental credit. From the beginning of the research, every single part of

the process was based on voluntary participation. This type of research guarantees that no manipulation is involved.

A digital tape recorder was used in interviews and for documenting conversations. Recording took much less time than typing or writing would have done, it interfered or disturbed the process less, and allowed a precise record to be made of the interviews. Interview notes were written up on the scene and were often checked for validity by asking participants for clarification of comments and accuracy of recorded notes. Some additional notes were made upon completion of the interview. In these notes, interview acts were conceptualized, and descriptions and analyses of the interview process were recorded.

In general, the interviewees gave impressions of self-confidence. They were able to relate to the researcher in a friendly manner, and they seemed to discuss most topics and questions openly and in relation to personal experience. Some of them, however, were nervous at the beginning of their interview. Later, they relaxed as the interview progressed and eventually become completely involved in the interview. There was no delay during the interview due to note taking because the interviewer only recorded key words and concepts that were emphasized. However, some respondents opposed to the use of a digital recorder for their interviews. Especially, respondents in the public sector expressed more opposition to the use of a digital recorder. It was guaranteed that all audio tapes, notes and copies of transcripts would be destroyed on completion of the research.

Conversation between the interviewer and the interviewee was not always easy to record, as some voices were more easily captured on the digital recorder than others. This became obvious when attempts were made to record interviews with a few subjects who were softly spoken. In the case of these subjects, to continuously request that they speak up was disruptive, and it was stressful for both parties. Therefore, the researcher allowed the loss of some words from the subject's responses rather than have to request the subject to raise their voice and speak louder, particularly as key concepts were also being recorded in note form.

Ethical issues

Before conducting the interview, the researcher collected secondary data related to internet fraud and overall cybercrime information from CTRC/NPA, ICIC/SPO and NCSC/NIS websites. These resources are open to the public and do not require any approval to see them. The Korean Information Disclosure Act established in 1996 and in force in 1998 allows the general public access to most governmental information, except information directly related to national security. The researcher also collected secondary data from the private sector. Secondary data collected from private companies were examined carefully to avoid data that could be biased or manipulated because the private model of policing focuses on the private interest only. The psychological well-being of an individual participating in research was not negatively influenced by participation. The researcher protected their rights, interest, sensitivities and privacy based on the ethical guidelines of the British Society of Criminology (Gelsthorpe, Tarling, and Wall, 1999).

A researcher has responsibilities not only to the principles of pursuing the truth and searching for knowledge, but also to the subjects of the research. The research has also always to take into account the effect of the research and of the researcher's action during the research process, upon those subjects; and must act in such a way as to preserve the rights, dignity, and integrity of the subjects as human beings. Given that this research interviewed policing internet fraud experts as research subjects, it was possible that information obtained could subsequently harm a subject who had taken part in the study. This possibility raised a range of potential problems, involving the issues of informed consent, assurances of confidentiality, and dissemination. According to the BSC code of ethics, a 'researcher should endeavour to avoid contractual conditions that limit academic integrity or freedom'.

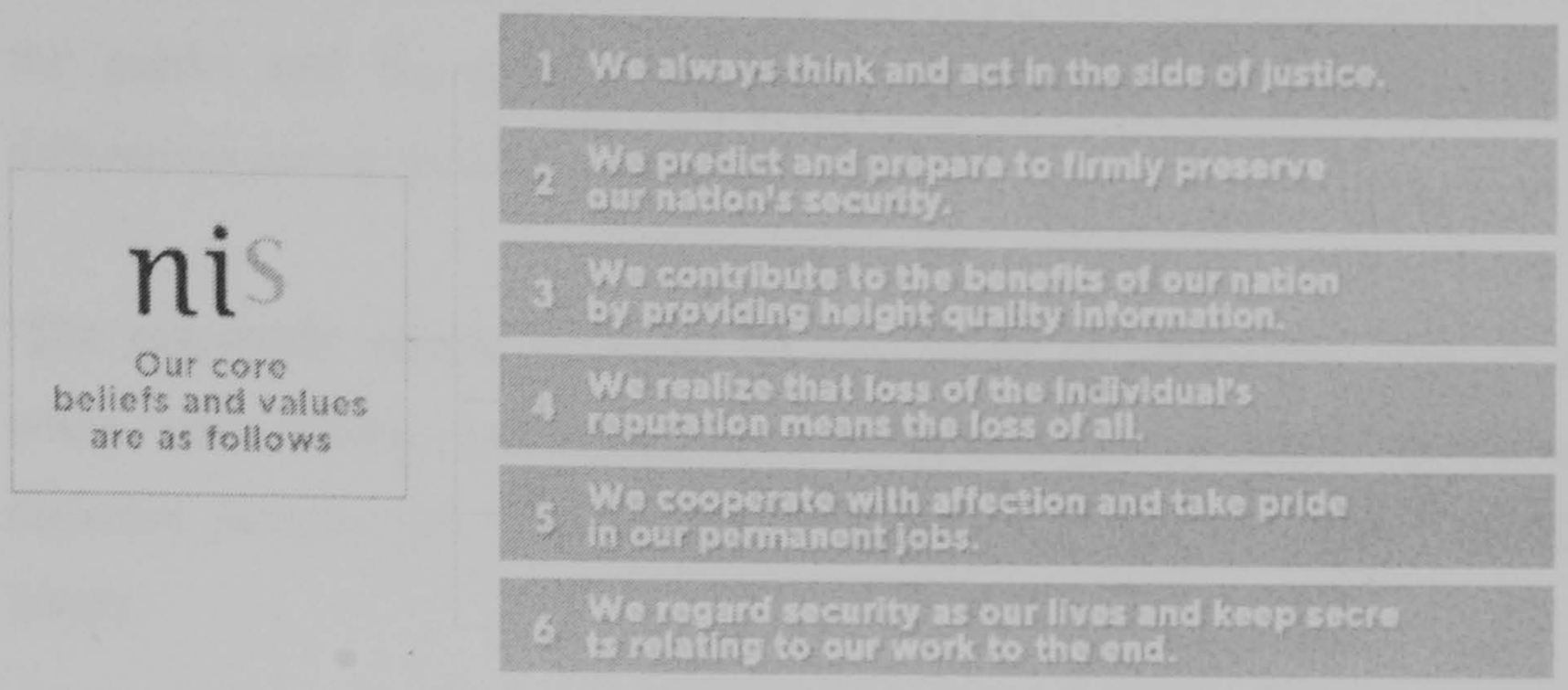
The ethical guidelines of the British Society of Criminology (2005), and of the British Sociological Association (2002), both state that participation in criminological research should be based on the freely given, informed consent of the subjects of the research. The British Society of Criminology

(2005) further defines informed consent, as requiring that the researcher carefully practice their responsibility to explain as fully as possible, and in terms understandable and meaningful to the potential participating subjects, the following key aspects of the research: who the researcher is; what the research is about and why it is being undertaken; what will be required of participating subjects in respect to the research; how and in what form, any findings of the research are to be disseminated; and what, if any, are the anticipated potential consequences of the research. The guidelines of these British professional bodies, also state that researchers should make fully clear to potential participating subjects, that interviewees have the right to refuse permission whenever and for whatever reason they wish.

For this research, the participation of each interviewee was voluntary, and permission from them to conduct the interview, was obtained on an individual basis. The researcher kept in mind that interviewees must not be adversely affected by participation this research and the responsibility to ensure the physical, social and psychological well-being. Before participating, the researcher asked each interviewee for verbal consent, and this process was audio taped, as well as the subsequent interview itself. The researcher did not contact higher-level staff members of the participant office to obtain interview permission. However, some interviews had to be approved by their agencies. Some public agencies and private companies misunderstood the fact that this research was an evaluation of their job performance. However, that was not the intent of this research. In order to resolve this problem, the researcher sent an interview schedule for approval.

Some agencies, such as NCSC/NIS have very strong regulations regarding the protection of information. NIS agents cannot reveal or disclose any information obtained during their service by law. This law applies even after their termination of duty. For this research, the Deputy Director of NCSC was interviewed. Interviewing with a field agent is almost impossible since he or she has no authority to decide his or her participation in the interview. The NIS code of ethics requires a high standard of job performance including confidentiality of their work. However, the Deputy Director did not ask about any part of the agreement of confidentiality.

Figure 1-2: Staff ethics of the National Intelligence Service



Source: http://eng.nis.go.kr/docs/about/ethic.html

In particular, participants in the police, prosecutors and intelligence were likely to ensure that their information would not be used for anything other than the original purpose of this research. It was mentioned that without participant's permission, individual data would not pass to any third party. The researcher explained the degree of anonymity and confidentiality for the research. It is known that providing anonymity and confidentiality to participants are key points in gaining valuable data that represents an objective viewpoint (Gelsthorpe, Tarling, and Wall, 1999). Some respondents in the private sector asked for more anonymity and confidentiality than the public sector respondents. They were concerned that what they said about current policing may irritate the public sector agency.

Most respondents were interested in 'how the research results would be used?' The researcher discussed any potential use of data by other researchers in advance. Respondents were informed that the research result might be published in a few journal articles such as 'Journal of Criminal Justice', 'Journal of Criminal law and Criminology' and 'British Journal of Criminology'. However, respondents' identities would not be disclosed and sensitive information would not be included. It is also assumed that the research results may be used as good guidelines for future policy and law making. All participants agreed that the research result would be disseminated for the public interest purpose.

Although it may not happen in this research, it is very useful to know additional information regarding internet research. 'When conducting Internet research, the researcher should be aware of the boundaries between the public and the private domains, and also any legal and cultural differences across jurisdiction' (BSC, 2005)

'The researcher should be aware of the additional difficulties that occur when undertaking comparative or cross-national research, involving different jurisdictions where codes of practice are likely to differ' (BSC, 2005).

Transcription and analysis of data

First, it was decided that digitally recorded interviews would be transcribed in the Korean language. Since the researcher required more profound familiarity with the contents of the digital recorder, transcription was made by the researcher without any assistance. This provided a means to discover practical understandings of meanings and actions. In order to discover patterns of human activity, action, and meaning, the researcher organized and reduced the data appropriately. When it came to selecting quotations from the completed transcription, it was decided to exclude 'overstated' words, 'repetitive phrases', or 'related encumbrances' that significantly obscured the clarity of the meaning of that mentioned by the interviewee.

The next stage, translation of written interviews from South Korean text to English text was important. It was not easy to translate from Korean to English since some nuances cannot be fully expressed in other languages. However, the research confirmed the translation by undertaking a reverse translation from English to Korean. For this process, the researcher asked a person whose major is English translation. It was found that there was not much difference between the Korean and English version of the interview transcription. Minor differences found that English transcription was more direct and simple in character compared to the Korean transcription. This might have been due to linguistic differences.

In terms of actually analyzing the transcribed recording, the first level of this analysis took place while the recording was being listened to during transcription. Interview recordings were replayed and reviewed many times, particularly if any statement was unclear. The transcription had to be analyzed with repetitive listening, writing and reading. The second level of analysis occurred when the process of transcription was completed. In this stage, key words/codes were analytically developed or inductively identified in the data and affixed to sets of notes or transcript pages. The selected key words/codes were examined for both the commonalities and disparities that emerged across the responses of the different individual subjects. In this stage, all materials were examined to separate meaningful patterns and processes. These key words were also transformed into categorical labels or themes.

This categorization constituted the third level of analysis. In this level, the researcher examined the small sets of generalizations established and identified patterns in the light of previously established conceptual frameworks and research expectations. The themes that emerged through this process include those such as 'tensions', 'appropriate policing', 'resolution of tension', and so on. This confirmation stage was able to determine whether the original research aims and objectives had been maintained or not.

Finally, the researcher accomplished the data analysis with coding frames and analyzing any correlations between respondents' answers and the main research questions. Initially, the researcher thought of using an Nvivo 7 programme to analyze the data. However, it was not used due to the relatively small size of data. Wincup (1997: 69) stated that a 'software package consumes too much time for sorting and retrieving data at the expense of writing'. The concept of data display was used to accomplish this analysis. Data display involves 'tables of data, tally sheets of themes, summaries of proportions of various statements, phrases, or terms, and similarly reduced and transformed groupings of data' (Berg, 2001: 36). Data display helps the researcher to understand the pattern of data and to determine whether additional analysis or actions are required. The

researcher used the concept of data display from the beginning of the research to monitor the overall research process.

Criteria for 'trustworthiness' of the research

This research was tested for 'trustworthiness' by four criteria (credibility, transferability, dependability, conformability) suggested by Lincoln and Guba (1985). This research result satisfied those four criteria since the subject of this research was accurately identified and described; the conclusion of this research can be generalized; the process of this research was well documented and reasonably stable over time; and neutrality of research and minimization of bias are in the research.

This study made every effort to maintain a high standard of research integrity and 'trustworthiness', in accordance with the four criteria described. The credibility of the findings of the study was largely grounded in the scientific methodology used for data collection and analysis, in the meaningfulness of the descriptions given in conjunction with that data collection and analysis, and in the way in which the results and findings of the study were systematically linked to the conceptual framework. With regard to transferability, the qualitative approach followed in the study did not allow for generalization applied to a population wider than that involved in the study. However, in as far as the findings were congruent with, or confirming of, the conceptual framework of the study, it is possible to speak of the study having analytical validity; and this may allow for theory-connected transferability of findings. Dependability of the study was enhanced by the fact that the research questions, research strategy, and conceptual framework of the study, were all constructed on a strong theoretical basis, within clearly defined research parameters. Finally, to increase the conformability of the study, the research design, methodology, and procedures that guided the research process, including the collection, processing and analysis of the data, were well described and documented, and were executed in the most objective manner possible.

1.9 Expected contributions

I believe that this thesis will provide a useful contribution to the development of internet fraud prevention in the design of South Korean internet fraud law and policing policy. Although South Korea is recognized as a strong IT nation, its current laws, rules, and policing strategies are insufficient to deal with the rising level of internet fraud. Since internet fraud shares a characteristic of transnational crime in that it is not constrained by national borders, the results of this research may well be applicable to other nations' policy making.

1.10 Overview of the thesis structure

Chapter 1 introduced the subject of policing internet fraud and aimed to familiarise the reader with the purpose of the study and the intended structure. This chapter also explained the method and considered the questions to be answered through the qualitative research strategy. One of the main objectives of this chapter was to describe and explain the qualitative interviewing process used in the study, and how that process was customized to suit the particular requirements and conditions of the study as a whole. The qualitative interview method used in this study was designed to obtain a distinctive and informative perspective on tensions between the private and public models of policing internet fraud in South Korea. The techniques of data collection and analysis have been documented, and relevant ethical issues were also addressed.

Chapter 2 aims to introduce the current situation of internet fraud in South Korea, the United Kingdom and the United States. This chapter discusses the definition of internet fraud, types of internet fraud and statistics of three nations. Different types of internet fraud which are prevented through different jurisdictions are discussed and introductions to major incidents can help us to see the trends of internet fraud. Comparison of statistics will show that internet fraud has rapidly increased regardless of jurisdictions.

Chapter 3 discusses the main theme of this thesis about 'policing internet fraud' in South Korea. It first introduces policing cyberspace in the sense of 'the internet order-maintenance assemblage' model by David Wall (2007). Subsequently this thesis introduces internet fraud regulation, policing bodies and internet laws in South Korea. Finally, an explanation of the historical background and reform of the criminal justice system reveals why the Korean police force is struggling over the ownership of policing cybercrime.

Chapter 4 examines the UK policing model for internet fraud which illustrates a much more fragmented and specialized form of policing compared to the South Korean policing model. This chapter also indicates the relationship between private and public sectors, multi-agency cross sector partnerships and barriers to hinder the development of partnership policing. Particularly, this chapter discusses tensions produced between sectors while taking part in policing internet fraud.

Chapter 5 examines the US policing model for internet fraud which focuses on public security and crime prevention by the public policing bodies. This chapter shows how enhancement of national security shapes the laws related to cybercrime. Kozlovski's 'designing accountable online policing' model emphasizes the transformation of policing cybercrime. It compares traditional law enforcement model strategies and structures to the cyberpolicing model. It shows why the current criminal justice system has to be changed in order to respond to cybercrimes. Finally, it introduces the US model of multi-agency cross sector partnership through illustrating the CIPAC (Critical Infrastructure Partnership Advisory Council) that 'provides the operational mechanism for carrying out the sector partnership structure.

Chapter 6 examines serious tensions between private and public models of policing internet fraud in South Korea. This chapter identifies the most serious tensions between and within the two sectors. The chapter explores the origin, resolution of tensions and ideal partnership from the local to the international level. The interviews reveal cultural differences in policing internet fraud and other policing activities.

Chapter 7 proposes the promotion of effective partnership policing and correct balancing of policing between the two sectors in order to provide the most appropriate policing model to the general and corporate victims. The chapter recommends the ideal model of policing internet fraud from the local to international level in both sectors. The International Internet Fraud Control Agency (IIFCA) would become a hub agency for policing internet fraud.

Chapter 2: Internet fraud problems in Korea, the UK and the US

2.1 Introduction

The policing of Internet fraud may be simply explained with words such as the regulation of internet fraud or internet fraud control. However, the concept of 'policing' is more appropriate here to help understand the tensions between private and public policing models. In order to appreciate the main research question about tensions between private and public models of policing fraudulent activities in cyberspace, it is necessary to examine the characteristics of internet fraud, private and public policing models, internet fraud regulation and tensions surrounding the policing of internet fraud.

In addition to the benefits it has brought, the emergence of the internet has had some negative impacts on society. It 'has not only radically changed the means by which one communicates, conducts business, and engages in recreation, but has also brought new avenues for criminal pursuits and new forms of victimization' (Burns et al., 2004: 477). Internet fraud has attributed to a significant loss of e-commerce (FTC, 1998) and is a significant impediment to commercial growth. Recent research reports that internet fraud is on 'the increase and that a lack of awareness, and inappropriate, limited or absent countermeasures have aggravated the negative impact of Internet fraud on society' (Malakedsuwan and Stevens, 2003: 18).

The emergence of the internet has made fraudulent activities easier than ever, because internet fraud does not require office space, employees, or long periods to convince target audiences. The internet saves time and money. Furthermore, it does not require people to congregate. The internet has attracted many people to commit fraud in cyberspace. Cohen (2002: 5-6) said that 'throughout the centuries, people have perpetrated frauds of all sorts in order to gain through taking advantage of others'. The crime, having

moved to the internet, is made more diffusible and harder to identify readily as a real threat.

According to the Confederation of Asian and Pacific Accountants (2001), reports of consumer based internet fraud indicates that between 5 to 10 percent of online transactions may involve fraud. Internet fraud affects all members in society in a number of ways that are different to traditional street crimes because of a lack of victims' computer networking knowledge and vulnerable targets, such as retired seniors, homemakers and children. Furthermore, victims may be unaware that they have been victimized. There are no corresponding estimations for fraud involving business and government transactions conducted electronically, although it is likely that fraud rates would be similar.

Smith and Urbas found high rates of concern about internet fraud risk among consumers, businesses and government agencies, and these concerns continue to hinder the development of electronic commerce globally (Smith and Urbas, 2001). This demonstrates how internet fraud can cause fear of crime even in the digital era. Therefore, it is necessary to understand the nature and implications of internet fraud as a crime.

As described in the following section, internet fraud can display different characteristics to traditional economic crime and therefore requires new strategies for detection and prevention. Non-reactive strategies would require private and public agencies to work together in ways that would most likely transcend the traditional private/public dichotomy (Brenner, 2004).

2.2 Defining internet fraud

Internet fraud has characteristics that are completely different to those of traditional fraud being, for example, impersonal, anonymous, instantaneous, accessible, and convenient. Baker (2002) reported that the internet enables fraudulent, low cost schemes to be circulated to a wide audience. Wall (2006: 12) stated: 'they are small-impact, bulk-victimizations with a large

aggregated loss, but spread out globally across a range of jurisdictions'. Corbett (2006) similarly stated that internet fraud cases often involve multiple one-time victims who have only lost a small amount of money. The internet offers more ranges of products to buy as well as providing more opportunities to commit fraudulent activities.

Internet fraud is also different from the traditional forms of fraud in terms of the use of technology in the criminal act and shares some characteristics with what Wall called 'hybrid' and 'true cybercrimes', respectively those criminal behaviours that are either traditional crimes transformed by networked technologies or wholly new forms of criminality such as spamming, phishing and pharming (Wall, 2006). True cybercrime is a type of crime that would disappear if the internet was removed, thus internet fraud is not a part of true cybercrime as fraud will always remain a form of crime. These new forms are distinguished from more traditional forms of criminal behaviour which only use the internet for communications.

According to Wall (2007), cybercrime tends to fall in one of three basic sub-criminologies: *computer integrity crimes, computer-assisted crimes* and *computer content crimes*. Internet fraud falls into the category of computer-assisted crimes, which use networked computers to commit crimes. In particular, many auction frauds use manipulated sites to entice innocent victims. However, the distinctions are not always so clear because true cybercrime, such as 'phishing', involves more than one of these three basic categories. Wall (2007: 49) explained that 'offenders engage their victims through spam (integrity), steal their personal information (computer-assisted) by deceiving victims into logging on to a bogus website (content) which they think belongs to their bank. Phishers then assault the integrity of the victim's own financial system to perpetrate a fraud'.

However, internet fraud does not conveniently fit into existing categories of crime. It is therefore classified as a white-collar crime since there is a preconception that the internet is only used by well-educated groups of people. However, although it shares minor characteristics, since internet

fraud contains unique attributes that contrast with conventional fraud, it is not easily classified as white-collar crime. Its differences are four fold.

- Internet fraud has a global reach capable of targeting a wide range of victims (Fried, 2003) virtually instantaneously.
- Internet fraud requires a wide range of policing since it transcends individual jurisdictions.
- Internet fraud requires a relatively small amount of money to commit crimes. 'No longer there is a need to rent office space, hire employees and spend hours on a telephone pitching to targeted audiences' (Fried, 2003).
- Internet fraud does not require high levels of education or training to commit crimes. Actually, modern computers make it possible to commit fraud easily without any professional assistance. Computers provide not only the device for the fraud, but also new opportunities for fraud.

These characteristics are similar to the general characteristics of cybercrime. These show us that internet related fraud should be treated differently from the traditional criminological point of view.

Although internet fraud shares a large proportion of characteristics with white collar crime, it does not mean that it has to be dealt with through the same method of crime prevention and investigation. Internet fraud is a new type of crime in the digital era. Therefore, it needs distinctive analysis in criminology. The following section addresses how internet fraud is to some extent linked with white collar crime.

Historically, Sutherland coined the term 'white collar crime' in 1939. Marx and Engels recognized that the powerful and the privileged commit 'crimes'. Such crime is associated with the character of the capitalist economic system and the special status of the privileged (Friedrichs, 1996). Ross (1907) promoted the notion of 'the criminaloid' that inspired Sutherland: the businessperson who committed crime to maximize profit under the camouflage of respectability and piety. Sutherland criticized 'those

behaviours and actions of "big business" that corrupted and threatened the laudable aspects of the American economic system' (Sutherland, 1949: 1983: 90-93). The generally accepted definition is that white-collar crime is the illegal and harmful actions of elites and respectable members of society carried out for economic gain in the context of legitimate organizational or occupational activities (Friedrichs, 1996). Another definition by Tombs and Whyte (2001: 319-20), is: 'a heterogeneous group of offences committed by people of relatively high status or enjoying relatively high levels of trust, and made possible by their legitimate employment'.

White-collar crime refers to acts defined by criminal law and adjudicated in criminal proceeding (Tappan, 1947). There are conceptual controversies over whether white-collar crime should refer to acts committed by higher status individuals or institutions, or those committed in the context of a legitimate occupation, regardless of socioeconomic status: whether it should refer to acts involving economic and financial activities only, or other acts involving physical harm as well: and whether it should refer to acts of people only, or organizations only, or both (Friedrichs, 1992).

Traditionally, white-collar crime has been perceived as less serious than conventional crime (Schlegel and Weisburd, 1992). The public tends to be unconcerned about business crime and even expresses sympathy with the offenders after they have been arrested. White-collar crimes involving fraud, illegal price fixing, or other purely financial losses have tended to be regarded as less serious than those causing physical harm. However, if a significant amount of money is involved and it was obtained under false pretences, it might be considered more serious than housebreaking (Levi, 1991).

It is believed that 'white-collar crime victimization is diffusible and victim's attributes are especially heterogeneous' (Mcshane and Williams, 1992: 262). 'Not all crimes committed with high technology are white collar crimes, but techno-crime/ hi-tech crime has been described as a subset of white collar crime, or alternatively as a distinctly new form of white collar crime' (Parker, 1980; Wasik, 1991). According to Reichman (1993) the internet

plays a chief role in insider trading cases by providing the facilities to hide illegal profits and market positions, transfer money to offshore bank accounts, and to park stocks and hide stock ownership.

The internet has been used as a tool for developing fraudulent businesses (Attaran, 1999). Online business is favoured by the fraudster since it does not need a physical space, office supplies or staff. The mobile technology of the internet attracts more fraudsters making policing of internet fraud even more difficult. It is common that offenders, servers and victims are located in different countries. Therefore, fraud in the information age must be treated in a different way to that of conventional fraud, because the criminal environment has changed significantly with the emergence of information technology in the last few decades (Cohen, 2002). Each type of crime needs a different formula and level of policing. However, it is not easy to determine what level of policing would appropriately fit to a specific type of crime. It is a very difficult research question since there has been insufficient previous work done to date.

Internet fraud is equivalent to the traditional form of fraud in that it incorporates deceptive behaviour (Grazioli and Jarvenpaa, 2003) that causes financial damage to innocent people. One advantage of using the internet as a tool is the offender can distance him or herself from the victim. Impersonal and anonymous contact between the offender and victim can be one of the factors helping to facilitate internet fraud. Internet fraud is also defined as any act of dishonesty or deception carried out with the use of the internet, or directed at the technologies that support the internet. By definition, internet fraud takes place in a 'virtual environment' (Williams, 2000).

Internet fraud has similar general characteristics to traditional fraud, but in being reorganized into the virtual environment it is fundamentally transformed (Cohen, 2002). It is more a technology based crime in contrast to traditional cybercrime which is computer based. The nature of this transformation depends on what particular features of the internet are exploited. The internet is used by both those with an interest in efficient

exercises of 'traditional' criminality as well as by those familiar with the possibilities of altogether new forms of criminality (Grabosky. 2000). Potential internet fraud is encouraged by a failure on the part of policy makers to realize that the internet offers access to an area beyond the reach of traditional policing and traditional legislative frameworks (Grabosky. 2000). Therefore, we need more studies about the legal response to internet fraud. How to regulate internet fraud in cyberspace without infringing other innocent internet users' rights is a priority matter.

Just about every facet of commerce has been transformed by the internet; we now have many more opportunities to undertake e-commerce through the internet. However, it appears that online securities utilized by the private and public sectors do not perfectly counter internet fraud. As more people use the internet to purchase and sell their goods identification theft is also increasing. We have often heard that large portal sites or companies' websites have been hacked and customers' personal information has been stolen.

According to the long tail theory by Chris Anderson (2007)[3], the emergence of the internet enables anybody to easily access useful information that he or she has never accessed previously. The internet has provided unlimited opportunities to deceive vulnerable groups of people without spending the high cost normally incurred by fraudsters. Easy access and the low cost of using the internet have enabled fraudsters to find new victims in cyberspace. According to the Anti Phishing Working Group (APWG), phishers no longer only exploit the famous banking brand names. The study indicated that 80 percent of fraud concentrated on the 15 top brands but 20 percent of fraud aimed at previously unknown brands. This shows the long-tail effect started in cyberspace crime (Broersma, 12/09/2006). Foremski (22/03/2008) said that 'long-tail businesses are based on aggregating huge numbers of micro market'. The cost of maintaining a micro market is low and the cost of data storage and servers are rapidly becoming cheaper. He believes that 'long-tail businesses' will eventually collapse e-commerce. Because of this

---

[3] Editor in chief, 'Wired' magazine and author of 'The long tail' (Hyperion and Random House).

reason, a fraudster's business can be seen as a micro-market based 'long-tail business' which will eventually disintegrate the level of e-commerce activities.

It is evident that it is difficult to narrowly define internet fraud, but with a broad idea of its characteristics, the following section now aims to introduce different types of internet fraud and consider their impact on individual internet users' e-commerce activities.

2.3 Types of internet fraud

Major internet fraud includes identity theft, credit card fraud, online auction fraud, short firm fraud and advanced fee fraud, as described below with reliable data from trustful agencies such as APACS – the UK payments association, Australian Credit Card Fraud Survey (ACCFS), National White Collar Crime Center (NW3C), Federal Trade Commission (FTC), National Consumer's League (NCL), Federal Bureau of Investigation (FBI), and Internet Crime Complaint Center (IC3). These data sources provide an overview of major internet fraud activities in the United Kingdom, the United States and Australia.

Identity theft

According to an APACS (2005: 28) report, '15 million adults used internet banking and 22 million adults purchased goods or services over the internet' in 2004. This reflects the fact that more people are using the internet as a major means for managing their financial affairs. Therefore fraudsters have used the internet to defraud banks using loan frauds and through money laundering and identity theft.

As credit cards have become a more widely used payment method, fraudsters have focused on credit and debit card payment fraud. With more technologies being used by fraudsters, credit and debit card payment fraud has become a true cybercrime. This fraud is mainly divided into two types: input and output fraud. Input fraud relates to a fraudster accessing credit

card information while output fraud is 'to obtain goods, services or money' (Wall, 2007: 72).

Recently, phishing and pharming have been used by fraudsters to collect personal information (passwords and account details) of credit card holders. Wall (2007) stated that this has brought about the automation of cybercrime. Phishing emails usually direct someone to a deceptive URL and ask for the recipient's personal information in order to protect them from potential risks from an urgent security breach, while pharming automatically directs recipients to a bogus website. 'DNS poisoning', 'cache poisoning' or 'DNS spoofing' are also other names for pharming. Pharming does not use social engineering methods to obtain the victim's information. Pharming emails contain malicious codes that poison or hijack the domain name server (DNS). The main point of pharming is to confuse recipients so that they are 'signposted to internet sites different to those intended, or their e-mail may be rerouted to mail servers not authorized to receive it' (Wall, 2007: 77).

Those two methods are based on automated technology used by fraudsters. In order to protect innocent internet users from those harmful activities, public awareness programmes provided by the government, financial institutes and other relevant private entities are important. Because most phishing and pharming fraudsters target credit card and auction site users (Murphy and Murphy, 2007), these companies have to prepare advanced internet security systems.

Following identity theft, credit card fraud, online auction fraud and Nigerian advance fee fraud are the most notorious offences in terms of seriousness and size of loss (Smith, Holmes and Kaufmann, 1999). There are many complaints from consumers who use internet shopping mall and auction sites. However, the statistics of victimization appear to show that it is in inverse proportion to the actual number of victims due to lack of reporting by victims.

Credit card fraud

The most frequently committed type of online financial fraud involves the use of a credit card fraud as the payment instrument; it is flexible and can target anyone from the individual consumer to the large corporation.

According to APACS statistics in 2007, internet card payments (using a credit card payment or debit card) by UK customers increased by 400 percent between 2003 and 2007, to 34 million. As more customers have the facility to use internet card payments, e-commerce activities have globally developed. More people are also purchasing goods from the online market in which businesses are not locally based. For example, Korean customers are using e-Bay and Amazon to purchase items. However, prosperous e-commerce activities have increased risks when using internet card payments (Smith and Urbas, 2001). Customers' risks and liabilities have also increased while e-commerce activities have become major business methods. However, financial institutions do want to take any risk for paying customers' losses from internet fraud so customers have to take all financial burdens in terms of liability for loss (Gibbons, 2001; Lang, 1999; Parliament of Victoria, 2002).

The absence of face-to-face confirmation of internet transactions has promoted the development of online trading by credit card (Gibbons 2001; Shankar and Walker 2001). For online transactions, customers are only required to provide their name, address, credit card number and expiry dates. This non-personal contact and transaction has facilitated internet fraud (Gibbons, 2001; Smith, 1999; Westpac, 2000).

A United Kingdom study found that 57 percent of businesses had reported online credit card fraud incidents to police (Experian, 2001). It is difficult to assess the losses associated with online credit card fraud since losses are associated with card-not-present frauds. However, the introduction of chip and pin decreased the loss from CNP (card-not-present) fraud from 219 million pound to 209 million pound in the first six months (APACS, 2006).

There is another problem that promotes online credit card fraud and this relates to the demographic information gathered from fraud; traders are under reporting and absorbing the fraud cost (Kennedy, 2000). Until they receive a chargeback from their financial institution, they are not aware of their liability and risks (Levi, 2002).

The Australian Credit Card Fraud Survey (ACCFS) in 2003 indicated that the prevalence of online credit card fraud does vary by business type, with 11 percent of florists, 17 percent of booksellers, 15 percent of recorded music retailers, 11 percent of toy and game retailers, 13 percent of computer hardware small retailers, and between 26 and 43 percent of online businesses having been victims of fraud (Australian Institute of Criminology, 2003). In spite of the risk of online credit card fraud, and the potential consequences of an incident of fraud, most online traders were largely satisfied with e-businesses. Only 5 percent indicated that they were likely to discontinue online trading in the future. More than 50 percent of businesses believe that online trading has significantly increased sales in their businesses and expect more businesses will join e-commerce within the next two years (Charlton and Taylor, 2004). This indicates that the rapid growth of e-commerce will not be deterred, despite the fact that some significant adverse effects, such as internet fraud, have occurred.

The recent Interpol website for a Universal Classification System for Counterfeit Payment Cards provides up-to-date information on trends and techniques for forgery of payment cards and fraud (Broadhurst, 2005). This site has a unique clearinghouse function and serves as an example of how international agencies can assist with essential tasks, such as secure shared intelligence, and the potential role of the individual in the prevention of financial crime.

Online auction fraud

The internet's new digital commercial environments, such as eBay have created new criminal opportunities for online auction fraud. In addition to generating public concern, auction fraud is a useful example of the new generation of cybercrimes. Although auction fraud existed before the

emergence of the internet, the onset of digital auction environments, such as eBay, has required the establishment of new bidding systems and safe payment methods, such as PayPal (Wahap, 2004).

In the US, the National Consumer's League Internet Fraud Watch (1998) reported that the largest number of complaints relating to fraud in e-commerce concern online auction sites (NCL, 1999) and noted that fraud involving online auctions occurred far more frequently than other forms of internet fraud, and there was an average loss per complaint of $518 in 2001 (Internet Fraud Watch, 2002). According to an FBI report in 2002, online auctions account for the majority of complaints about internet fraud. The Internet Fraud Complaint Center, a joint operation of Federal Bureau of Investigation and the National White Collar Crime Center said it referred 16,775 complaints in 2001. 'These statistics indicate the significance of Internet fraud and the need to identify the readiness of law enforcement at all levels to prevent and control Internet fraud' (Burns and Whitworth, 2002: 1). The monetary loss associated with fraud more than tripled, to $54 million from $17 million, in the same period. Auction fraud accounted for 46 percent of complaints referred to law enforcement. Internet auction sites have strengthened user responsibility by reinforcing the real-time name verification system and adopting strong countermeasures to minimize fraud cases. According to IFCC, internet fraud comprised 71 percent of referred complaints and 190,143 complaints referred to law enforcement in 2004 (NW3C, 2005). The total loss from internet fraud was $68.14 million with a median dollar loss of $219.56 per complaint. The average loss per person increased from $527 in 2003 to $895 in 2004. Websites were still the most prominent medium, with 75% in 2005, utilized for conducting fraud (NCL and NFIC, 2005).

According to Gregg and Scott (2006), the FTC's (Fair Trade Commission) internet auction fraud data comprised 71.2 percent of the reported complaints with an average loss of $765 in 2004. After auction fraud, non-deliverable merchandise and non-payments were the second largest category, accounting for 20.3 percent of complaints. In 2005, IC3 received 231,493 complaints, 62.7 percent related to online auction fraud where 41 victims

lost an average of $385 and most related to online auction complaints about non-delivery of ordered items and manipulation of reputation systems (Chau, Pandit and Faloutsos, 2006; Zhang and Zhou, 2008).

The majority of online auction fraud occurs on eBay because it is the biggest auction site: eBay had roughly 69 million registered users worldwide and $1.2 billion of net revenue in 2002. Nearly 8 million bids are placed everyday (Kirshner, 2003). These auctions range from small toys to consumer durables and antiques. 'eBay promotes itself as a community where people come to shop, get to know others, discuss issues of mutual interest, and have fun' (Duh et al, 2002). In its mission statement, eBay 'offers a wide variety of educational tools, features, and services that enable members to buy and sell on the site quickly, safely, and conveniently. These services include online payments by PayPal, tips on safe trading, and the Developers Program for community members who would like to develop their own technology solutions' (eBay, 2006).

The FBI (2006) reported that auction fraud outnumbered any other type of cybercrime. Approximately 45% of reported cybercrimes come from auction fraud. According to the IC3 statistics, 86,000 complaints were officially reported to the law enforcement agency. The average loss per victim was $724, totalling up to $198.44 million, $15 million more than 2005 losses. Complaints rose by around 21% from 2005.

Along with its fast growing market and business volume, the number of complaints is increasing. In response to these complaints, the FTC started a database to gather and organize online auction complaints for legal enforcement purposes (Guidera, 2000). As is the case with most internet fraud, the fraud on auction sites is diffused and varied, making it difficult to counteract.

There are many different forms of auction fraud including shill bidding, bid-siphoning, bid-shielding, refusal to pay, misrepresenting characteristics of goods offered for sale, and selling illegal or stolen items. According to the National Consumers' League (2001), among the various kinds of fraud,

shilling is the hardest form of auction fraud to detect (Kauffman and Wood, 2003). Shilling is the most widely reported fraud in online auctions. It is the practice of sellers posing as buyers and submitting bids to drive up the price. For example, the seller may register under another alias and submit bids that appear to come from an independent buyer (Duh et al. 2002). Bid siphoning is the practice of a seller posting an item for sale and observing the e-mail addresses of interested buyers, and then contacting them with intent to sell directly to avoid the auctioneer's service charges. When a seller receives money, however, the buyer never receives the item and does not have the remedy of reporting the swindle through eBay's feedback system (Ray, 2000). In bid shielding, two or more bidders plan to keep other legitimate buyers from bidding. The high bidder withdraws his bid just before the end of the auction giving some excuse, and his partner gets the item for the lowest price that he or she bids. eBay could discourage bid shielding by allowing sellers to specify a price above which bids are automatically accepted when the auction terminates. Refusal to pay is another problem. Since eBay conducts no credit checks, a person can bid any amount of money on any item, even without the means or intent to pay for them. Sellers are often accused of misrepresentation of goods or failing to supply the item listed for sale to the winning bidder (Simpson, 2000). Some eBay users have formed a 'shill group' to expose suspected frauds on an internet discussion group by requesting the actual user name behind the screen name from eBay (Simpson, 2000). According to Duh et al. (2002: 14), 'Failing to pay, using stolen credit cards, improper employee behaviour, and misrepresenting the quality or characteristics of goods are more common and occur in a wide variety of e-commerce websites'.

A feedback forum and an escrow programme are the key mechanisms with which eBay deals with fraudulent behaviour. The feedback forum is a unique feature of eBay. When the successful transaction is completed, the buyer and seller are encouraged to record feedback about their counterparts. The character of feedback records makes them a powerful enforcement tool. It has also stimulated some competing participants to try to manipulate the feedback by getting their colleagues to post positive feedback, or by painting their competitors in unfavourable terms. Shill feedback, feedback

extortion and feedback solicitation are some obvious possibilities (Dennehy, 2000). eBay deals with such behaviour by allowing buyers to file complaints and takes disciplinary action, but 'for legal reasons, the result of the investigation may not be disclosed or shared with eBay users' (Kaiser and Kaiser, 2000: 142). eBay does not have many direct disciplinary options other than to refer offensive behaviour to the police, or expel the offending party from their website. eBay also does not compensate the deceived buyers (Levy and Stone, 1998). Online auction sites are powerless once a crime has occurred. As a result, various user groups have made increasing calls for government regulation of the internet auction business (Bywell and Oppenheim, 2001).

Compared to other economic crimes, which pursue the private model of justice, online auction companies more often invite the public police investigation to deal with auction fraud in their virtual markets. Because online auction fraud involves many individual participants, including sellers and buyers, it is completely different from the typical style of Business-to-Business (B2B) commerce. Online auction fraud is difficult for authorities to investigate and victims rarely recover the money they have lost. Online auction companies with their private model of justice and security management cannot handle all fraud cases without public police intervention. Online auction fraud can be a good example of cybercrime that strongly demands cross sector partnership between public and private policing.

As described in this section, constantly increasing numbers of online auction fraud incidents show that more attention is needed to protect online shoppers and vendors while e-commerce is taking place in our society. Cross-sector partnership policing between private and public poling models is essential to respond to it because victims of online auctions vary from individuals to businesses so that any single sector alone cannot effectively cover the reported incidents.

Short firm fraud

This fraud directly relates to auction fraud and long-firm fraud that 'fraudster sets up in business as wholesaler, and place orders with suppliers with the intention of evading payment' (Merseyside Police. 2008). For example, an internet shopping mall may sell good items at a lower price for a while and build customer trust, and then may advertise to sell more expensive items at lower price but the items will never be delivered. By manipulating the reputation system poor quality items are sold at very expensive prices. Use of the reputation management system is very important since more people are using auction sites for selling and buying useful items. There is usually no better system for trusting the reputation of the vendor than from the perspective of online customers (Wall, 2007). It appears that short firm fraud is an auxiliary fraud for online auction fraud. Without online auction fraud, short firm fraud does not exist. In contrast to short firm fraud, long-firm fraud entails a fraudster setting up in business as a wholesaler and purchasing goods from suppliers for resale with the sole intention of evading payment.

Advance fee fraud

This section on advance fee fraud will illustrate how the internet can transform an existing crime to an upgraded form of crime. Previously, advance fee fraud was conducted by sending letters to their potential victims. These frauds annually result in the loss of hundreds of millions of dollars internationally (Buchanan and Grant, 2001).

Advance fee fraud is also known as the '419' scheme, named after a statute in the Nigerian criminal code that prohibits obtaining property by false pretences (Oriola, 2005). Hence the reason why it is often called 'Nigerian advanced fee fraud'. In the United States, the Secret Service, who estimate that one quarter of the major frauds under investigation involve Nigeria, has primary responsibility for dealing with advance fee fraud (Smith, Holmes and Kaufmann, 1999). Where the victim has suffered financial loss, the Secret Service initiates an investigation (US Secret Service, 2007).

The National Internet Fraud Information Center reported that '8 percent. or 985 out of 12,315 fraud complaints were about Nigerian money offers' in 2005 (Wall, 2007: 92). According to IC3, they received 207,492 complaints in 2006, a decrease of 10% from the 2005 figures of 231,493. The average loss per victim was $5,100. This fraud typically begins with an unsolicited letter or email. The confidential message purports to come from a government official or ex-official, a doctor or a tribal chief (Emery, 2002). The letters are addressed personally to a potential victim explaining that a 'mutual business associate' has suggested that the writer contact the addressee confidentially. The letter requests the recipient's assistance in transferring large sums of money in exchange for a percentage (Buchanan and Grant, 2001). The letters usually contain the following similarities:

- there is a large sum of money, known only to the writer, waiting to be paid out of the government coffers as a result of accounting shenanigans or over invoicing;
- the writer is a member of the government or military trying to move the money out of the country but needs help from abroad:
- the writer is willing to share the money with the recipient who provides assistance;
- secrecy is an absolute must because other corrupt officials would seize the money for themselves if they knew of its existence.

The amounts represented are usually in the area of $35 million but may be as much as $75 million. In return for the help of the addressee, the writer promises anywhere from 20% to 30% of the total. In other words, the addressee is offered $7-10 million for very little effort and virtually no risk. (Buchanan and Grant, 2001: 40):

After a number of communications and an appropriate amount of time to establish trust, the fraudster will report that the money is finally available for transfer. However, an unpredicted problem occurs, and advance payment fees are needed to clear the final obstacle. If the victim sends money, some other problems will occur until the victim is out of cash or realizes he or she has been deceived (Buchanan and Grant, 2001).

There is a popular misconception that many of Nigeria's 120 million people were actively involved in the '419' frauds. However less than 1 percent of households have a personal computer, while internet connectivity and accessibility is one of the lowest in Africa (Oriola, 2005): most of the fraudulent emails are sent from public internet cafes and some of them come from outside Nigeria. For example, in 2002, a US law firm was swindled of $2.1.million, by someone who claimed to be an official with the Ministry of Mining in Pretoria, South Africa, who convinced their bookkeeper to assist in the transfer of $18 million from South Africa to the United States. She had been promised a commission of $4.5 million (Ashenfelter, 2002). Because of its seriousness, the United States House of Representatives proposed a Bill to tackle the problem. The Bill was to be known upon enactment as the 'Nigerian Advance Fee Fraud Prevention Act of 1998' (Emery, 2002). The proposed law emphasized the necessity of international cooperation and public enlightenment campaigns to combat the fraud. The Bill also indicated that the Nigerian Government had responsibility in the advance fee fraud and considered the possibility of imposing economic and other sanctions on the Government of Nigeria as a means of restricting the fraud. However, there are jurisdictional problems that prevent transnational cybercrime governance and explain the US Congress's preference for international cooperation, diplomacy and possible economic sanctions against Nigeria. The Money Laundering Act and Mail Fraud Act cover some parts of the violation, so the law was not passed (Oriola, 2005).

In the United Kingdom, the Serious Fraud Office's West African Fraud Section took action; 111 individuals were prosecuted in 1997 (Smith, Holmes and Kaufmann, 1999) and approximately 25,000 complaints were received in 2001. This report indicates total losses of 10.5 million pounds, with an average loss per victim of 146,000 pounds. The City of London Police arrested over 500 advance fee fraudsters in 2004 (The Hindu, 2004). Smith, Holmes and Kaufmann (1999: 5) reported that 'the British Postal Service is also acquiring new powers to intercept and destroy advance fee letters'.

However, before postal service intervention, as part of public law enforcement, provision of the necessary power to police by ISPs could provide more effective proactive policing against Nigerian advance fee letters. While some people believe that it is very useful that Internet Service Providers worldwide help by filtering out advance fee fraud e-mails, many Internet users oppose to the filtering of their e-mail by Internet Service Providers. It is against one of the basic principles of the internet, which guarantees free flow of information. Civil liberty groups have opposed the cybercrime treaty because they believe that its activity dramatically restricts the free flow of information (BBC, 2006). From this perspective, self-regulation of the ISP is a very sensitive agenda for the private sector. It may result in the collapse of the ISP due to the infringement of cyber-rights.

Oriola (2005: 246) suggested that countries with spam laws adapt them to avoid advance fee fraudsters because 'advance fee solicitations can be expressly designated as unsolicited non-commercial fraudulent e-mails, and outlawed'. It gives a significant impetus for strong international cooperation, since emails travel all around the world. There is no specific remedy for this violation, only international cooperation in intelligence gathering, sharing, and investigation and prosecution can be an effective counter measure to control advance fee fraud (Emery, 2002; Oriola, 2005).

These days advance fee fraud has been found in eBay auction sites. The con artist personally approaches to victims to suggest that the direct trade between seller and buyer would save commission. When the victim is deceived and has sent money or products to the fraudster, the victim will never receive the money or products they expected. Therefore, online auction companies like eBay strongly recommend using secure methods for transactions, such as Paypal.

Other advance fee frauds have also been adapted to the online environment. They are advance fee fraud in dating (looking for sex partner) and purchasing of goods (selling at a lower price). Advance fee fraud in dating usually occurs between an adult male victim and a young female offender. Particularly in Korea, a young female fraudster will offer a date for money.

When the man remits money through the Internet, the girl never shows up at the meeting place. Because of protection laws of the youth, which prohibit any sexual relationship with minors (under 19 years old in Korea). most victims tend not to report incidents to the police. Advance fee fraud in purchasing of goods is similar to eBay fraud in that the seller never sends purchased goods to the buyer after receiving money.

As described above, credit card fraud, online auction fraud, and advanced fee fraud are the overwhelming fraud cases directly affecting the public interest. However, private interest is also engaged in that corporate entities respond to these fraud cases with their own private model of justice to protect them from the negative adverse publicity and to secure market confidence.

Meanwhile, the victims of advanced fee fraud are often complicit and willing participants who have been driven by their own greed. Therefore, 'victims are seen as deserving ridicule more that sympathy' (Peel, 2006). Their seeking for the abnormal fortune provides more opportunities for the fraudsters. Whether victims of advanced fee fraud are aware or not, they significantly facilitate this kind of fraud. This makes policing it much harder.

Other types of internet fraud

- Direct investment frauds are more harmful than work at home scams. Fraudsters 'purport to be legitimate investment brokers who sign up and produce free investment reports to customers that subsequently trick them into investing their funds in dubious stocks and shares. Another direct investment fraud is the 'pump and dump' fraud whereby investors playing the stock market are deceived by misinformation circulating on the internet about real stock. This information artificially drives up the price of the stock (the pump), which is them sold off at inflated price (the dump)' (Wall, 2007: 87).

- Internet Access Services is a fraud that offers a free trial period for the Internet Service to the customer, which eventually results in a contract with the ISP, with large penalties for cancellation (Balsmeier, Bergiel and Charles Viosca, 2004). According to Internet Fraud Watch statistics compiled for 2005, Internet Access Services fraud indicates 1% with $1262 of the top 10 fraud (Internet Fraud Watch, 2005).

- Internet advertising fraud is a 'pay-per-click' advertising fraud. The aim of this fraud is to make people click. Every single click is to make money. However, each click is not made from an individual internet user but more likely done by a Third World low-wage factory worker. As technological advances occur, software is more commonly used by fraudsters. Link spamming is a good example of this fraud, which connects the specific keyword to a website such as 'pornography' (Wall, 2007).

- The repair of credit rating is a famous financial scam to entice 'many poor and financially excluded through the internet with promises to repair their credit ratings, provide credit options or credit facilities, credit cards with zero or very low interests, or instant and unlimited loans without credit checks or security' (Wall, 2007: 87).

- Drug sales scams aim to distribute counterfeit versions of drugs such as Viagra and Cialis (anti-impotence drugs) through internet sales. Sometimes spam mail and viruses to infect computers accompany the drug fraud. Particularly, this fraud also involves transnational criminality since it involves sending drugs across national borders to avoid local prescription restrictions or exploit beneficial tax circumstances (Wall, 2007).

- Travel and vacation scam is a fraud that offers a luxurious boat trip with lots of extra benefits such as a rental car, hotel and entertainment. However, they deliver lower quality accommodation and services than advertised or no trip at all. Usually a trip is

scheduled for the next year so that customers voluntarily abandon trips. Most of the time there is an additional or hidden charge in order to take an actual trip. According to the National Fraud Information Center, the average loss due to fraud in 2004 was $803 per incident. Travel frauds are the second most reported fraud after online auctions (Glink, 2005).

- Advance fee loan frauds are run by deceitful individuals who target those individuals with a poor credit history and who have been turned down for loans from financial institutions. According to law enforcement agencies in the US and Canada, 'ads and promotions for advance-fee loans suggest — or even "guarantee" — that there's a high likelihood that a loan will be approved, regardless of the applicant's credit history. But to take advantage of the offer, the consumer has to pay a fee'. Once they receive your money, they run off or their phone number will be changed (FTC, 2005).

- Prize/sweepstake fraud is a fraud whereby 'customers receive an e-mail from someone claiming to be from a law firm or a government agency. Victims are told that they have won a large sweepstakes prize but need to pay taxes up front. If they pay, they will receive another email a few days later, telling them that another winner refused to pay taxes. As a result, the prize is larger and they need to pay additional taxes'. According to the Canadian Better Business Bureau (CCBBB, 2005), it is illegal in both Canada and the United States to ask for money upfront if you have legitimately won a prize/sweepstake.

2.4 Social engineering and internet fraud

Social engineering is used as a major method to deceive others. Social engineering is 'an outside hacker's use of psychological tricks on legitimate users of a computer system, in order to obtain information he needs to gain access to the system' (Palumbo, 2000). According to Granger (2001), 'the basic goals of social engineering are: to gain unauthorized access to systems

or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. Typical targets include telephone companies and answering services, big-name corporations and financial institutions, military and government agencies, and hospitals'. Hackers and fraudsters use social engineering to obtain 'user names and passwords' to penetrate computer networks. They deceive people who can lead to them to system control programmes, database, financial or telecommunication systems. After they access the system, they erase, modify or copy the information to fit their needs (Broadhurst and Chantler, 2007).

Fraudsters develop a human relationship to obtain the necessary information. One of the most serious concerns is ID theft since true ID leads to the network or computer system (Smith, 2006). As the development of e-commerce increases, awareness of social engineering is necessary. However, study of social engineering and its defence is rarely provided in private or public sectors. Social engineering is classified into two categories: syntactic and semantic. Syntactic social engineering refers to the second wave of network attacks and relates to the operation of network and vulnerabilities such as denial of service and difficulties with cryptographic algorithms (Schneier, 2001). Barrett (1997) argues that basic security faults make syntactic social engineering possible for attacking the network. Malware and smurfing are the most common forms of syntactic attacks. Malware is a malicious code that is responsible for the distribution of viruses and worms. Smurfing is a denial of service that uses 'ping' to test an internet host's response.

Semantic social engineering refers to the third wave of network attacks (Schneier, 2001). This targets the people who operate the computer rather than the physical machine by using human-based or computer-based methods. Low awareness of personal intrusion and data collection, and ineffective security measures make semantic social engineering attacks possible (Barrett, 1997).

The most common methods of human and computer based semantic social engineering are introduced by Granger (2001):

- Phone: a social engineer calls up and imitates an employee in order to pull information out. Help desks are vulnerable to this type of attack. Hackers usually pretend to call from inside the corporation by manipulating the caller's number, so caller-ID is not useful (Granger, 2001).
- Dumpster diving: another favoured method of social engineering. A huge amount of information can be collected through company dumpsters. 'The following items are potential security leaks in our trash: company phone books, organizational charts, memos, company policy manuals, calendars of meetings, events and vacations, system manuals, printouts of sensitive data or login names and passwords, printouts of source code, disks and tapes, company letterhead and memo forms, and outdated hardware' (The LAN Times, 1995).
- On-line: the major weakness is that many users often use one simple password on every account. So once the hacker has one password, he or she can probably get into multiple accounts. One way to obtain this kind of password is through an on-line form: 'they can send out some sort of sweepstakes information and ask the user to put in a name (including e-mail address – that way, she might even get that person's corporate account password as well) and password' (Granger, 2001). Another way to obtain information on-line is by pretending to be the network administrator, sending e-mail through the network and asking for a user's password. Or a pop-up which requests that the user re-enter his username and password to fix some sort of problem. This information is re-directed to the hacker (Guenther, 2001).
- Persuasion: 'basic methods of persuasion include: impersonation, ingratiation, conformity, diffusion of responsibility, and plain old friendliness. Regardless of the method used, the main objective is to convince the person disclosing the information. The other important key is to never ask for too much information at a time, but to ask for

a little from each person in order to maintain the appearance of a comfortable relationship' (Granger, 2001).

- Reverse social engineering: this is more advanced method of gaining illicit information. A hacker pretends to be a person that appears in a higher position so that employees will ask him for information, rather than the other way around. The reverse social engineering attacks may offer the hacker an even better chance of obtaining valuable data from the employees. The reverse social engineering attack involves three parts: sabotage, advertising, and assisting. *Sabotage* the system that hackers want to break into; then *Advertise* for the service to fix it; and then *Assist* with the problem while obtaining the necessary information (Allen, 2006).

In order to defend against social engineering, several layers of protection are more effective in stopping further penetration after passing the first level (Gragg, 2002). Security policy is considered to be one of the most effective methods to respond against social engineering. Security policy assures that end users resist the fraudster's request. It must address 'information access controls, setting up accounts, access approval, and password changes. Modems should never be permitted on the company intranet. Locks, IDs, and shredding should be required. 'Violations should be posted and enforced' (Granger, 2002: 2). Besides, security policy has to define the responsibility for information or access by users or employees.

Training in the form of awareness programmes of social engineering attacks, is essential for all users, including private company's employees, government employees and individual users. They must be aware of social engineering techniques used to attack network systems (Stevens, 2001). Their confidential information should be protected. Management level should defend their employees when they refuse to provide confidential information to others. The refusal occurs when a caller asks 'to give contact information, rushing, name-dropping, intimidation, misspellings, odd questions, and requesting confidential information' (Granger, 2002: 2). They must know how to respond to suspicious requests by social engineers.

Finally, well defined security policy should enable employees to report any incident if they suspect it.

Social engineering traps are set in the system to stop attacks. Traps provide warnings for potential threats. They will prepare for the common social engineering techniques. Some recommendations for trapping the social engineer are made by Gragg (2003): First, all employees must understand the possibility of the physical presence of a social engineer in their legitimate area. They must be aware of unauthorised visitors. Second, centralised security logs must be examined on a regular basis by information security personnel. They have to monitor not only network access logs but also help desk services and customer requests. Help desks are particularly vulnerable since staff members of help desks are trained to be friendly and give out information. Third, a phone back policy will help to confirm the true identity. Employees should call back suspicious persons to check whether he or she provided a true identity.

The following table lists some common intrusion tactics and strategies for prevention:

Table 2-1: Common Intrusion tactics and strategies for prevention

Area of Risk	Hacker Tactic	Combat Strategy
Phone (Help Desk)	Impersonation and persuasion	Train employees/help desk to never give out passwords or other confidential info by phone
Building entrance	Unauthorized physical access	Tight badge security, employee training, and security officers present
Office	Shoulder surfing	Don't type in passwords with anyone else present (or if you must, do it quickly!)
Phone (Help Desk)	Impersonation on help desk calls	All employees should be assigned a PIN specific to help desk support
Office	Wandering through halls looking for open offices	Require all guests to be escorted
Mail room	Insertion of forged memos	Lock & monitor mail room
Machine	Attempting to gain access,	Keep phone closets, server

room/Phone closet	remove equipment, and/or attach a protocol analyzer to grab confidential data	rooms, etc. locked at all times and keep updated inventory on equipment
Phone & PBX	Stealing phone toll access	Control overseas and long-distance calls, trace calls, refuse transfers
Dumpsters	Dumpster diving	Keep all trash in secured, monitored areas, shred important data, erase magnetic media
Intranet-Internet	Creation and insertion of mock software on intranet or internet to snarf passwords	Continual awareness of system and network changes, training on password use
Office	Stealing sensitive documents	Mark documents as confidential & require those documents to be locked
General-Psychological	Impersonation & persuasion	Keep employees on their toes through continued awareness and training programs

(Source: http://www.securityfocus.com/infocus/1533)

Security awareness of social engineering must thus be increased. More security organizations should make social engineering a priority for their programmes. Organizations should routinely conduct security audits so that security doesn't become out of date.

Finally, Kevin Mitnick (2001) said that 'you could spend a fortune purchasing technology and services from every exhibitor, speaker and sponsor at the RSA Conference, and your network infrastructure could still remain vulnerable to old-fashioned manipulation.'

The next sections will provide an overview of cybercrime and internet fraud statistics in South Korea before discussing the loss and victimisation caused by internet fraud around the world, based on statistics provided from reliable agencies in the United States and the United Kingdom.

2.5 Internet fraud statistics (South Korea)

More than 30 million people are using the internet in Korea. This number, equivalent to 68.2 percent of Korea's population, was recorded in June 2004

by the Ministry of Information and Communications. It was noticeable that the number of users over the age of 40 had dramatically increased, as had the level of use – internet users reported that they used the internet on average for 11 and half hours per week. In terms of reasons for use, in 2005 86.6 percent of users used the e-mail function, 45.3 percent were using the internet for shopping purposes, 18.9 percent of users were using paid contents, 44 percent of users were using online chat services and 30 percent of users had their own personal blog (Ministry of Information and Communications, 2005). These statistical results indicate that many people will be naturally exposed to the risk of internet fraud. However, as yet there is not enough reliable data available to compare the progress of internet users and internet fraud in Korea.

In order to understand the policing of internet fraud in Korea, it is helpful to see overall cybercrime data for Korea. The official cybercrime statistics are managed by the Korean National Police Agency since the Cyber Terror Response Center (CTRC) is the major cyber-policing agency and deals with most cybercrime.

The NPA categorizes cybercrime into 'cyberterror' and 'general cybercrime'. According to their classification, cyberterror includes the hacking and distribution of viruses that attack a computer's information system and the network itself. General cybercrime includes internet fraud, defamation, copyright violation and stalking and intrusion of privacy (CTRC, 2005).

Table 2-2 shows the number of cases occurring from 2001 (22,651) to 2006 (62,000). There were more noticeable increases in the general cybercrime level than in the level of cyberterror. Since cyberterror requires more advanced skills and technology to commit crimes, the number of cases has slowly increased. However, general cybercrime cases have rapidly increased. this is largely because general cybercrimes do not need any special knowledge to commit crime; they depend more on 'social engineering' than technique and technology.

Table 2-2: Statistics – cases occurring

Classification	Total	Cyberterror	General Cybercrime
2006	82,186	20,186	62,000
2005	88,731	21,389	67,342
2004	77,099	15,390	61,709
2003	68,445	14,241	54,204
2002	60,068	14,159	45,909
2001	33,289	10,638	22,651

(Source: www.ctrc.go.kr)

It is assumed that general cybercrime cases will continuously increase since more computers will be used by criminals as tools for committing crimes. In the past, the computer was considered an expensive tool for everyone but popularization of the computer has reduced its price so that it can now be purchased by a much wider range of people. If someone cannot afford to own a computer, they can still use a computer by paying a small fee at a public internet café.

However, there was a statistical decrease in cybercrime from 2005 (21389: 67342) to 2006 (20186: 62000). This could be explained by the use of higher technology and hiring of more cyber police officers by the National Police Agency. Coincidently, cybercrime related conferences and symposiums have been held since the year 2005. It seems that more public attention and effort has been able to decrease the number of cases of cybercrime since 2006.

The Supreme Prosecutors' Office (SPO) has independently compiled separate internet fraud statistics, as follows:

Table 2-3: Statistics of internet fraud in total number of internet crimes – compiled by the SPO

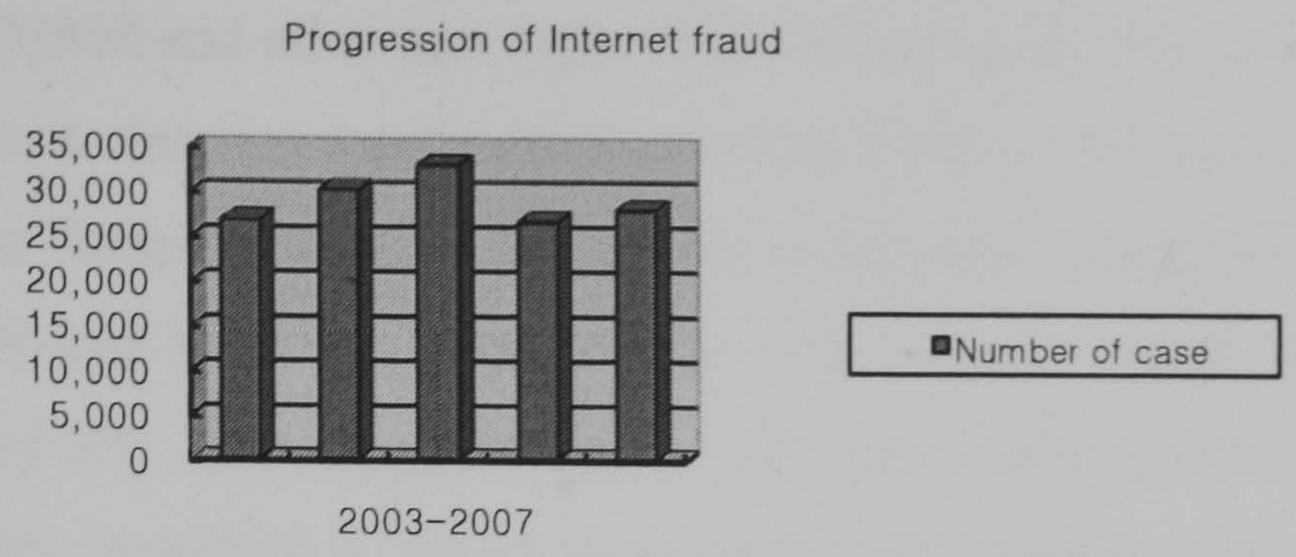
Internet fraud	**Result**		
	Year	**Number of cases**	**Number of offenders arrested / (charged)**
	2000	247	325 (66)
	2001	428	588 (146)
	2002	1,346	1,603 (680)
	2003	2,403	2,777 (846)
	2004	1,634	2,040 (323)
	2005	1,208	1,465 (203)
	Total	7,266	8.798 (2,264)
Internet crimes	2000	802	1.074 (122)
	2001	2,353	3,143 (331)
	2002	5,722	7,198 (990)
	2003	12,501	15,575 (1,745)
	2004	11,685	15,814 (1,104)
	2005	12,672	19,234 (1,766)
	Total	45,735	62,038 (6,058)
	Internet fraud (%)	15.89	14.18 (37.37)

The data from the SPO are based on the number of cases passed over from the police (see data below Table 2-4). However, SPO data does not fully reflect the actual numbers of incidents since these data were compiled based on prosecuted cases. Compared to the police data, SPO data show that relatively small numbers of offenders were legally charged. Probably, SPO did not find any concrete evidence for their offences.

Table 2-4: Statistics of internet fraud compiled by the National Police Agency (NPA)

Year	**Total**	**Internet fraud**	**Hacking/Virus**	**Violence**	**Illegal site**	**Illegal software**	**Others**
03	51,722	26,875	8,891	4,991	1,719	677	8,569
04	63,384	30,288	10,993	5,816	2,410	1,244	12,633
05	72,421	33,112	15,874	9,227	1,850	1,233	11,125
06	70,545	26,711	15,979	9,436	7,322	2,284	8,813
07	78,890	28,081	14,037	12,905	5,505	8,167	10,195

Figure 2-1: Progression of internet fraud compiled by the NPA



According to the Korea National Statistical Office (KNSO), a total of 15.8 billion dollars worth of cyber-shopping mall transactions occurred in 2007; this has increased by around 50 percent from 10 billion dollars in 2005. This indicates that more people are moving from the offline market to the online market to purchase their goods (2007). Seoul Electronic Commerce Center (2008) reported that 14,223 fraud cases were received in 2007. This figure had increased 46.7 percent from 9,694 in 2006. With the development of e-commerce activities, more internet frauds have occurred in cyberspace. The National Police Agency data indicates that a total of 28,081 internet fraud cases were reported in 2007, which was an increase of 4.2 percent from the 26,875 internet fraud cases reported in 2003. Introduction of the escrow system in April 2006 enhanced policing effort, although there was little reduction in the number of cases during 2006. However, the total amount of loss has not changed since fraudsters now appear to be targeting more expensive goods. *The Cheat*, a community response site for internet fraud, has received more than 17,900 internet fraud cases from victims since it was founded in 2006. Now it has become a very popular site among internet users for sharing internet fraud information (Baek and Lee, 2008).

In contrast to other nations, there are no statistics available to show the overall financial loss from internet fraud in South Korea. Further data and thus further research are needed to enable the response to internet fraud.

2.6 Internet fraud statistics (US AND UK)

There is broad evidence to illustrate that internet fraud is increasing as a function of the increased numbers of users online and the increasing

numbers of facilities, in addition, the rate of internet fraud is increasing because of ID theft and other new types of fraud emerging. The average loss per person due to internet fraud is $410 (Emling, 2001). The Gartner Group predicted that financial damage caused by cybercrime would increase by between 1,000 and 10, 000 percent by 2004. The Internet Complaint Center (IC3) received 206, 884 complaints about internet crimes in 2006. In 2007 this was further increased by about 20 percent or $40 million, which marks approximately $240 million of financial loss (Leyden, 2008).

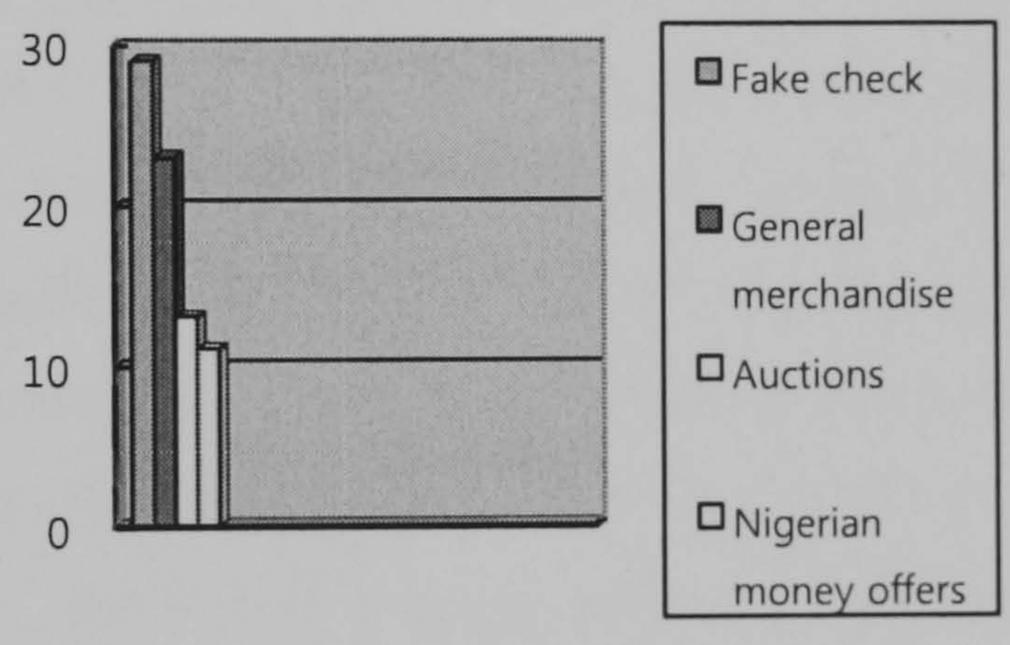
In order to respond to internet fraud, the Federal Trade Commission created 'Consumer Sentinel', which is the largest database of consumer fraud complaints in North America. US and Canadian law enforcement agencies have access to the data through a secure, searchable website, and can now easily coordinate policing efforts aimed at the most common fraud (FTC, 1998).

According to the British National Criminal Intelligence Service (NCIS) (which has subsequently become absorbed into SOCA), 'fraudsters typically exploit human misery so they invariably create human misery. They are without scruples because this is how they make money' (Matusic, 2001). Depending on the skill of the fraudster, websites can be made to look very attractive and legitimate. Phishing is a good example of this kind of fraudulent website. Litan (2004) reported that 57 million US adults have received a 'phishing' attack e-mail within the past year. More than 50% of those who responded were victims of identity theft such as credit card data, home addresses, and telephone numbers. Phishing attacks undermine consumers' confidence in the authenticity of e-mail originators, threatening consumer trust in the very foundation of internet based communications. Gartner believes that at least a million individuals may have fallen for such schemes without realizing it. Direct losses from identity theft fraud against phishing attack victims in the US were about $1.2 billion in 2003. It also reported that the failure of the implementation of anti-phishing measures, consumer distrust and annual US e-commerce growth would drop to 10 percent or less by 2007 (May 4, 2004). In order to decrease the number of cases of phishing, the public has to be aware of the importance of protecting

personal information and safe business practices. Most recent statistics of APWG (Anti Phishing Working Group) reported that 25,683 phishing attacks were received during the month of December 2007. According to a Gartner (2007), phishing attacks resulted in 3.6 million adult victims and the loss of $3.2 billion in the United States.

According to the US National Consumers League (NCL) data in 2007, the total loss of internet fraud was $17,508.480 this was significantly higher than the $13,863,003 reported loss in 2005. The graph (Figure 2.2) below shows that the top 10 scams were auction (13%), general merchandise (23%), Nigerian advance fee scam (11%), fake cheques (29%), lotteries (7%), phishing (3%), advance fee loans (3%), friendship and sweetheart swindles (1%), and Internet access services (1%).

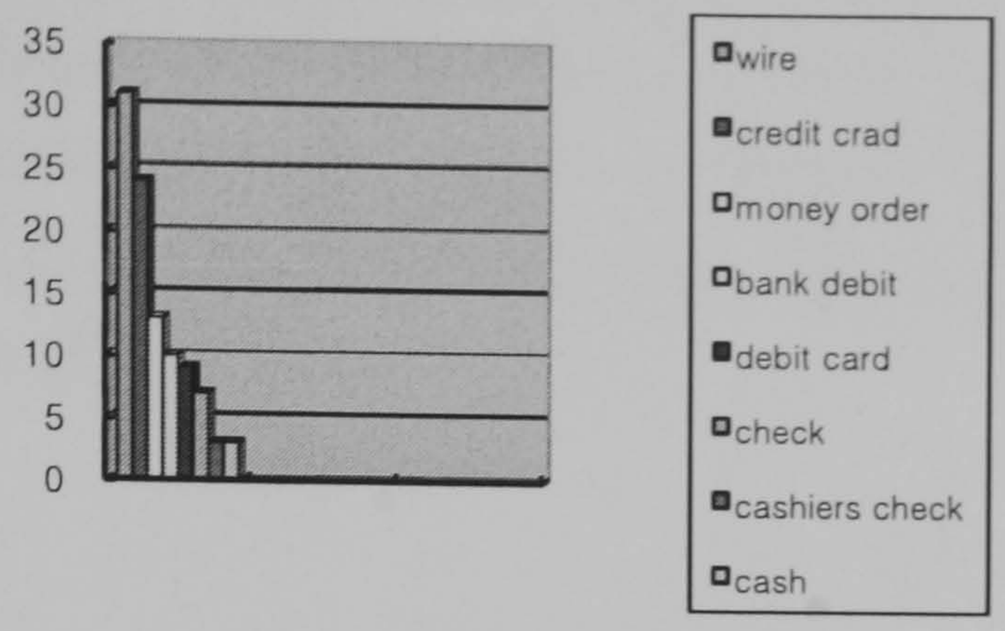
Figure 2-2: Top 10 frauds in 2005 (National Consumers League)



It was found (NCL 2005) that most consumers' aged 60 or over were vulnerable to phishing (21%), lotteries (21%), adult/information services (20%), and Nigerian advance fee (12%). These statistics show that most victims are seniors who are vulnerable to the fraudsters. In contrast to those frauds targeted at those in their senior years, work at home plans (44%) and advance fee loans (35%) mainly victimize those under the age of 30.

Figure 2-3 shows that most fraud victims use the following payment methods: wire (31%), credit card (24%), money order (13 %), bank debit (10%), debit card (9%), check (7%), cashier's check (3%), and cash (3%).

Figure 2-3: Top methods of payment in 2005 (National Consumers League)



In addition, the existing survey indicates that most offenders of internet fraud are individuals and not businesses. They are predominantly males residing in large cities (NW3C, 2005).

According to UK statistics, internet fraud comprises about 15 percent of total fraud in the United Kingdom. The *State of the Nation* paper reported that their average loss was £875 per person in 2006. This equates to a total loss of 20 billion pounds and is equivalent to 1.5 percent of GDP, as recorded in 2006. *Get online* reported that about 3.5 million internet users have been deceived. This means that around 12 percent of the 29 million internet user population have been defrauded. About 6 percent of internet users were defrauded during online shopping sessions (Andrews, 2007). APACS (2006) indicated a loss of £428 million from card fraud although this decreased by £80 million due to the introduction of chip and pin payment systems. Major card fraud is still CNP (card-not-present) fraud causing a total loss of £212.6 million. This figure includes off-line fraud such as phone and mail. So, actual level of internet based CNP fraud is less than figure cited. However, most recent statistics of APACS data indicated that card fraud losses were up by 25 percent, driven by a 70 percent increase in fraud from abroad. APACS expects that the use of chip and pin payment systems will continuously reduce the level of card fraud (Knights, 2008).

The above statistics for the United States, the United Kingdom and South Korea indicate that internet fraud is a global trend; findings show that it has risen across all jurisdictions. However, South Korean data sources do not include detailed information of financial loss. The data only indicate numbers of reported incidents to law enforcement agencies. In contrast to South Korean data, the US NCL data indicates the total loss of internet fraud ($17,508,480 in 2007) while UK APACS data indicate major loss

from card fraud (£428 million in 2006). Overall, each country compiled slightly different types of internet fraud figures or wide-ranging data so it is difficult to compare those three countries' statistics. Lack of consistent reporting systems among those three countries is considered a major factor hindering cross comparison of internet fraud.

2.7 Major internet fraud cases in South Korea

The most prominent internet fraud cases reported by the National Police Agency are online escrow, phishing, bogus internal revenue sites, internet phone services, pornographic websites, internet banking loans and internet shopping mall scams. Details of case information are described on the NPA website, as summarized below.

The online escrow website is the latest scam, which has become a serious problem since there is growing tendency of using the internet payment method. Recent escrow fraud detected by CTRC indicates that fraudsters open a fake internet shopping broker site to entice buyers to sell electronic merchandise such as LCD TVs, notebook computers and other items at below market value, and ask to pay through the most popular escrow service site. However, they advertise the escrow site on the largest portal site and its popularity ranking is manipulated. Innocent buyers then send money to the escrow account but never receive any items from the fraudsters. Over 10,000,000Won (approximately 100,000 dollar USD) was made in less than two weeks from this scam.

Phishing scams create an entire bank website in order to deceive the innocent customer. This scam is a personal identification theft, in which fraudsters open a fake portal site almost identical to the largest portal sites and collect personal information, such as KID number, age, sex, address, telephone number from the new members who recognize their site as a genuine portal site. Approximately 360,000 articles of personal information were collected and sold via internet transactions. Surprisingly, the hacker who won second place in the international hacking competition committed

this crime. He and his colleagues, who were also hackers, founded an internet security company.[4]

A bogus Internal Revenue Service site was run by the local Korean and Korean Chinese gang (Triad). They sent SMS messages or made calls to small retail business owners claiming there were tax returns for them to collect immediately. Many people were deceived as the female operator called them first and they then heard more detailed information from the supervisor who was a professional con artist. The fraudsters made the recipient go to the ATM and operate the machine incorrectly to send them money. In July 2006, the NPA found that they had duped 37 people in 50 incidents, taking more than 140,000,000 Won (approximately 140,000 USD). The police were astonished that Chinese gangs worked with Korean criminals to do their business. This case illustrates how international cooperation in policing cybercrime and internet fraud is important to strike out the criminals.

Internet-based phone scams have a technical advantage of being able to change the number of the sender anytime so that victims do not suspect calls from phony places. For example, a fraudster can manipulate his or her telephone number to be the same number of banks or credit card companies so victims provide their personal information without any hesitation. The internet phone was invented by the Israeli company 'Vocaltec' in the 1990s and was introduced in Korea in August 2005.

Pornography fraud attracts people who want to watch private adult films. According to NPA, fraudsters who set up business in Pusan, the second largest city in Korea, advertised their service, and were able to obtain 9000 subscribers within a very short period (October 2004 to May 2006) despite the fact that no site existed. The pornography site was good bait for those who wanted to enjoy special movies, and fraudsters made more 12,000,000Won (1.2 million dollars USD).

---

[4] NPA did not disclose the name of the internet security company.

Internet banking loan scams attract people in financial difficulty. A recent case indicates that a fraudster made 76,000,000Won in less than 6 months (January- June, 2005) from 234 victims, most of which had low income and a bad credit history background. Fraudsters convinced their victims to open an instalment saving account to improve their credit rate, in which a 10% cash deposit was required to apply for the loan. Victims thought that this made sense so they deposited funds and provided their bank account number, password, and security card number. With this information, fraudsters cancelled their victims' instalment savings accounts and disappeared.

Internet shopping mall scams are the most common fraud cases in Korea. Many fraudsters open internet shopping malls and advertise their items at below market value. However, customers do not receive any of the items they order, and any phone calls they make to hasten orders result in the same answer or excuse. After a couple of months victims can no longer see the shopping mall site. In one recent incident it was reported that a fraudster earned more than 460,000,000 Won (4.6 million dollar USD) in 16 days from 1,900 victims.

A popular online game, called 'Lineage', in Korea has game money called 'aden'. It is known that 1000,000 aden can trade with a value of 12000 won (approximately USD 10) in the online market. Annually, more than 1 billion won (USD 100 million) has been transacted for the cyber money. Fraudsters advertised to sell this aden at a lower price than the real value and many innocent gamers paid the price. However, they never received it. A similar case is the 'selling of a magic sword', which is also used in the online game to rescue various characters. Recently, the Korean National Police Agency busted a criminal ring that circulated in Korea online money generated in China and cashed it out of Korea. Criminals wired $38 million from Korea to China. Fraudsters produced game money in China using cheap labour and a virus programme. They took commission of 3 to 5 percent of the money trade to purchase game money. An anonymous police source said that 'the ring used a virtual private network for IP laundering. Using the network, the suspect hid their real location. The network made their China based IP look like that of an internet café in Korea' (Lee, 2008).

2.8 Major internet fraud cases in the UK and US

In the UK, among many internet scams, 'Card Not Present (CNP)' crime is one of the most commonly occurring internet frauds. According to APACS, CNP caused more than £290.5 million in 2007. The introduction of Chip and Pin has attracted fraudsters to move on CNP fraud because the shopper does not have to be physically present at the point of transaction (Leyden, 2008). Internet shopping mall fraud only scares about 20 percent of internet users who avoid online shopping, although estimated revenues were over £13bn during the Christmas season in 2007 (Leyden, 2007).

According to Garlik (2008), 90,000 incidents were categorized as online identity theft in 2006. However, approximately 90 percent of cybercrimes is not reported by victims due to absence of consistent reporting systems.

Phishing fraudsters are 'hacking into IT director's bank accounts and ordering new credit cards that are subsequently used to purchase jewellery, electronic goods, or foreign currency' (Leyden, 2007). One victim discovered that £60,000 had been withdrawn from his account at Barclays.

In the US, 'a Californian man was accused of using an automated script to open 58,800 online brokerage accounts that were linked to a handful of online bank accounts' (Goodin, 2008). He sent 'huge numbers of deposits between two cents and $1 dollar to the accounts to verify that account details of new customers are correct'. It is similar to the PayPal verifying method. He got his idea from the USA Patriot Act that requires financial institutions to verify the identity of their customers. Many fraudsters maliciously manipulate the legitimate methods to deceive others.

A different kind of advertising fraud, 'cookie stuffing' was found in auction businesses; eBay sued its business partners for it. eBay pays its partners for advertising based on the number of clicks by partner site users. However, some of those partner sites were pretending that users had clicked eBay ads when they hadn't (Out-law, 2008). Their clicks are recorded by small text files within web browsers visited. Those partners secretly redirected their

users' computers to eBay. It caused eBay cookies to be placed in the users' web browser. This fraud makes it looks as though users have clicked on ads and thus eBay paid for their advertising fees.

2.9 Internet fraud Control

Most governments have anti-fraud policies and departments dedicated to the development of electronic commerce (Sathye and et al., 2004). although the actual levels of implementation of such policies are different throughout different regions. Many studies suggest that little attention has been given to the regulation of confusing, unreliable, untruthful and fraudulent businesses in contrast to the regulation of harmful content, virus and phishing (Smith, 2001). Although some countries have updated their laws to deal with cybercrime, there is still a need for a detailed assessment and review of the current policies and regulations regarding cybercrime (Smith and Urbas, 2001).

Currently, there are three main ways of dealing with internet fraud: hard regulation involving the use of the law; soft regulation using codes of practice; and strategies based on fraud prevention (Clark, Dugdale and Sathye, 2004; Smith, 2000). Depending on the sector, agency and situation, these regulations are applicable for the control of internet fraud varying from the level of criminal prosecution to prevention strategy.

Criminal action

Criminal prosecution and punishment deters fraudsters from recidivism and deters other criminal activities. There are varieties of other consequences, which may follow the detection of internet fraud, although conventional judicial punishments are not imposed. For example, 'adverse publicity, professional disciplinary sanctions, civil action, injunctive orders and, various forms of community conferencing' are followed (Smith, 2000: 10). The seizure of offender's assets is considered as an effective means of deterrence. However, there are 'various forensic difficulties associated with gathering evidence from computers in a number of different jurisdictions that often make proceedings both difficult and costly' (Smith, 2000: 11).

Civil action

Civil action can recover the loss from internet fraud while criminal action can punish the offender (Clark, Dugdale and Sathye, 2004). Although the threat of civil action can be quite effective in that it exerts a chilling effect upon potential fraudsters, it may be impractical because to invoke formal procedure can consume excessive time and be prohibitively expensive. For the non-career fraudsters, this threat may stop or delay their activities for a while. However, serious fraudsters do not care about civil action and ignore the threat of criminal action.

In order to pursue a civil action the victim must be able to prove the loss or forfeit that caused by fraudulent activities. For example, deceptive advertisements on the internet will be held liable if the offensive content forms part of the terms of the agreement. This may cause a right to cancel the contract or sue for damages. The use of the internet raises legal issues, which are substantively the same as those which arise out of paper based advertisements and contracts. However, it is difficult to establish what transpired between the parties to an electronic transaction due to difficulties of collecting evidence and forensic investigation (Smith, 2000).

Providing concrete digital evidence is the most difficult part of any legal procedure due to lack of technology, knowledge and staff in pursuing civil action. Unlike criminal procedures, civil procedures do have less coercive legal authority to collect evidence from ISPs or private corporation data. For example, an individual auction fraud victim will have difficulty pursuing the case without hiring a lawyer, and often fails to take successful legal action (Snyder, 1999). Depending on the seriousness of the incident, corporate victims use their corporate legal service teams or hire outside law firms to carry out legal action. The majority of times, the threat of legal action will stop or deter fraudulent activities and protect their reputation and brand image. Financial compensation through legal action is not their intention.

Content regulation through filtering system

ISPs monitor the harmful material on their network with screening software or through measures (Clark, Dugdale and Sathye, 2004). These measures prevent internet users searching words, usually criminal, sexual and terrorist act related words, which are not accessible or require the use of an identification number (Bertelsmann, 1999). Although the use of screening software has been widely used to control access to obscene and offensive materials, it is more difficult to control the misleading and deceptive content. According to Smith (2000: 11), the Internet Industry Association recognizes that 'the Internet should provide a means to enable control of access to content while acknowledging it is impractical to filter all Internet content'. The Association granted means by which content can be recognized and possibly disqualified by content filter technologies as the most practical means of empowering responsible adults to control access to the internet to verify appropriate controls to content (Smith, 2000).

Certification and endorsement services

These services provide users with information as to the reliability and acceptability of online material (Clark, Dugdale and Sathye, 2004). Users can decide whether they wish to make use of the material in question. For example, the Platform for Internet Content Selection (2000) is a voluntary content rating system, which helps users, categorizes materials that conform to specific standards.

AICPA (The American Institute of Certified Professional Accountants) developed the WebTrust programme, which certifies Internet sites that indicate legitimate online business practices after extensive auditing procedure. The audit includes checking the site's security measures, privacy practices and transaction-processing systems. The service is available from any WebTrust-licensed CPA or accounting companies. WebTrust is already available in Hong Kong, Australia, Germany, England and Wales, Scotland and Ireland, France, the Netherlands, Denmark and Spain, as well as in the United States and Canada. Internationally, 15 national accountancy institutes from Europe, North America, and Asia joined the rapidly growing consortium of WebTrust providers around the world (AICPA, 2004).

Electronic security of financial service providers poses a risk to the e-commerce activities in open network infrastructure (Glaessner, Kellermann and McNevin, 2004). Certification and endorsement services provide confidence and financial security to both customers and merchants that would establish safe e-commerce activity. However, there is a problem of proliferation of services and the determination of appropriate standards (Smith, 2000). The anonymous character of the internet has negatively affected e-commerce activities so that many global corporations, such as Microsoft, have been pushing for the use of digital identity management systems. However, it appears that more studies of the interplay of international law and standards is necessary (Rundle and Laurie, 2005).

It appears that the use of hard regulation of legal actions and soft regulation of codes of practice have been dedicated to controlling internet fraud, although some questions have been raised with regard to each jurisdiction and nation's law and policy. In addition, the development of e-commerce and transformation of financial services has facilitated the demand for more effective internet fraud regulation.

Many cybercrime experts have recommended that preventive strategies are more effective and efficient ways of controlling internet fraud than reactive methods. Preventive strategies have many advantages for business entities since the use of preventive strategies have enhanced overall corporate IT security functions and avoided tough government control.

Preventative strategies

Generally, it is better to prepare preventive strategies before resorting to hard or soft regulations, as discussed above. Since most fraudsters tend to attack the private sector, these strategies are designed to protect corporate IT systems and ISPs. The majority of corporate victims of internet fraud do not know how to respond to it while the vulnerabilities of the internet may inhibit the development of e-commerce. Therefore, it is important to establish appropriate policy for use of the internet in terms of prevention of internet fraud.

2.9.1.1 Corporate fraud control policies

Establishment of fraud control policies appear to be the best ways of preventing fraud within organizations. Without appropriate internet fraud control policy, employees are embarrassed when they are unexpectedly exposed to fraudulent activities. The ethical use of information technologies and how to respond to instances of fraud are imperative to conduct a business. Particularly, it is important to develop specific policies on computer security along with appropriate guidelines on reporting computer misuse and abuse. According to Smith (2000: 13), 'policies need to deal with specific on-line behaviour of employees such as security of user authentication systems, access to and use of the computers for private purposes, personal use of electronic mail, downloading software. and the use of copyright material'. For example, Australian Standard No. AS3806-98 Compliance Programmes 'provides which organisations are able to use to identify and to remedy any deficiencies in compliances with laws. industry code and in-house company standards and to develop for continuous improvement in risk management' (Greycar and Smith, 2002: 8).

2.9.1.2 IT security enhancement

For protecting corporate information, use of the internet by employees needs to be monitored through appropriate logs of usage (Clark, Dugdale and Sathye, 2004). The use of computers for private purposes has to be prohibited from the main business operation in order to prevent fraudulent activity internally and externally. Therefore, many companies prohibit the use of MSN messenger and limit their employees outgoing e-mail size. Global corporations such as IBM monitor their employees' behaviour through video surveillance or checking e-mails and files transmitted through servers (White and Pearson, 2001). Surfwatch filtering software programmes are used to restrict employees from accessing specific content by requesting the user's ID (Smith, 2000). However, highly restrictive IT security policies block the free flow of information, infringe privacy and deprive the convenient digital life of the individual (Clarke, 1999).

2.9.1.3 Self-regulation of internet fraud

Self-regulation is the most favoured form of governance accepted by private industries such as online auction and other professional services since it is

beneficial for the organizations with natural information asymmetries (Jacobson, 2001). According to Leland (1979), self-regulation improves the quality of goods and services. The rules in cyberspace are imposed, not through sanctions, nor not by the state, but by the very architecture (design) of the particular space (Lessig, 1999).

Current research by Chua and Wareham (2002) indicates that the internet industry displays a strong degree of progressive self-interest and as a result, is highly self-regulated. They have discovered that sophisticated anti-fraud institutions have been established and only new entrants in the market who are unfamiliar with this mechanism become victimized. In addition, their research found that informal institutions are more effective than government regulation because they target fraud at its source. 'Fraud primarily occurs because of information asymmetries' (the fraudster know something auction participants do not know) and 'regulation, on the other hand, constrains behaviour by making unwanted behaviour costly' (Chua and Wareham, 2002: 10). It is not possible to constrain fraudulent behaviour without correspondingly constraining desirable behaviour because fraud occurs in numerous forms. Unless they deal specifically with information asymmetries, government regulations do not reduce fraud.

However, some studies suggested that government regulation might reduce fraud without dealing with information asymmetries. They recommended that governments collect intelligence about deviant (including terrorist) networks to establish concrete evidence of wrongdoing (Walker and Akdeniz, 2003). This will ensure the successful prosecution with hard evidence. In order to prevent internet fraud due to the information asymmetries, the government has to implement the necessary regulation in order to fundamentally block the information flow to those who potentially manipulate the law and system, while also protecting personal information. The UK Data Protection Act 1998 is a good example that 'gives people improved rights regarding personal information which others hold about them and imposes greater control over individuals or organizations that process personal information by using both manual and automated means' (South Shropshire District Council, 2003: 1). Information asymmetries can

occur not only in relation to auction fraud but also with other frauds such as telecommunications fraud, stock transfer or alteration of sales/billings (Denning, 1999). Regulation designed to financially support trader risk or punish the con artist are likely to be unproductive. Sometimes such regulation interrupts existing formal anti-fraud mechanisms and aggravates the incidences of fraud. Regulation requires people to pay more money for the implementation of services and may cause the overnight collapse of the market due to the flexibility of the internet auction market (Chua and Wareham, 2002: 10). Government regulations may transfer the cost of fraud to taxpayers who are protected by government institutions and frequently engage in riskier behaviour (Calomiris, 1990). They concluded that the 'individual must investigate the auction, the trader, and the community of practice' (Chua and Wareham, 2002: 10) in order to protect him or herself from fraud.

Self-regulation can occur when the self-regulating body can enforce the policies, while the formal regulation of internet fraud can take place under the legal and political support by the state or by the international organization. According to Lessig (1999), cyber-law has new characteristics such as anonymity, competing jurisdiction, abundance of ambiguity, and minimalism of internet architecture (a political decision about disabling control and technological decision about the optimal network design difficulty enhanced) so that it is difficult to apply universally.

Self-regulation of the internet is an alternative that has been strongly preferred, especially during the 1990s, for addressing the issue of pornography, race-hate speech and other internet derived material considered undesirable. 'A raft of techniques for self regulation was available, and includes software that will block material with more than a certain percentage of 'skin-tone' or filtering of material deemed to have 'suspect' content' (O'Brien, 2005: 153). However, there is the danger of private companies offering these filtering facilities restricting free speech by exercising a form of 'corporate censorship' via their filtering process. Self-regulation of internet fraud can use the same techniques and software to prevent and control the fraudulent activities (O'Brien, 2005).

Overall, preventive strategies described above would be the considered the best intervention for internet fraud, although there are some sensitive issues about restriction of free flow of information, infringement of privacy and promotion of corporate censorship. For self-regulation of internet fraud. progressive studies need to discuss its advantages and disadvantages in terms of protection of e-commence. More attention must be paid to particular industries, such as online auction companies, since online auction fraud has marked the most frequently occurring fraud among various internet frauds.

In summary, each tier has different target groups and sanctions for policing cyberspace. From the individual user to government-funded public police. although some of the population served are limited within their members. most internet users are policed by this order maintenance assemblage. Sanctions vary from the lightest level of moral censure to the hardest level of criminal prosecution. Most private sectors impose the removal of access rights or withdrawal of internet services. However, this assemblage does not perfectly respond to all cybercrime. Each tier has different capabilities of policing so some target populations are sometimes ignored due to lack of resources, knowledge and labour. In fact, there are many barriers interrupting the effective policing by both sectors.

2.10 Criminological theory and policing internet fraud

The convergence of technology, policing and white-collar crime (Nhan, 2006) is necessary to explain the difference in policing internet fraud compared to traditional terrestrial policing. Policing internet fraud appears to be quite different from terrestrial policing in that it invokes strong partnership policing. It appears that internet fraud needs more intervention from the private sector. Private companies and ISPs are participating in policing not only for the protection of their corporate interest but also for the protection of their customer's interest. Since cyberspace is not split into two sectors, policing by the private sector also covers the public interest area of cyberspace. The private sector has complained that over expenditure is

unavoidable if the police only symbolically exist and promise 'to serve and protect'. It seems that the public sector has to answer the question: 'why does the private sector have to spend money without delegation of power to control?' The division of policing labour has to be clearly defined and financial support for the policing of internet fraud has to be enhanced by the public sector.

As explained earlier in this chapter, internet fraud does not fit into traditional criminological theory. Internet fraud is a part of cybercrime, so it borrows the general characteristics of cybercrime. According to Wall (2005), cybercrimes appear to be fundamentally instantaneous, transnational, trans-jurisdictional and global. The discussion of cybercrime is also offence based and tends to 'cover a broad range of legal issues, many of which are the subject of civil law in addition to, or instead of, criminal law, demonstrating a resonance with the study of white-collar crime' (Wall, 2005: 87).

Theoretical concerns about criminological links between cybercrime and white-collar crime leads us to wonder whether 'cybercrime' is a part of 'white-collar crime' or not. However, logical conditions do not perfectly satisfy the theory of a link. More studies are required to find out their relation and to create new typology for internet fraud as a new crime.

2.11 Conclusion

Internet fraud statistics, statistical trends and major cases are found in South Korea, the UK and the US to be moderately different from each other. For the statistics, it seems different ways of data collection, compilation and interpretation were applied. South Korean statistics compiled by both the Supreme Prosecutor's Office and the National Police Agency do not indicate detail typology of internet fraud so it is difficult to state which fraud needs more attention or impacts more on internet users and e-commerce activities. Only through other civil organisations' data such as '*the Catchall*' and '*the Cheat*' are we informed which fraud is more prevalent and serious. Consistently, statistical trends in the three nations indicate that the total loss

from internet fraud has continuously increased. Although there was a little reduction in occurrence, total loss has never been reduced.

As the earlier part of this chapter indicated, the statistics show internet fraud incidents are increasing across jurisdictions worldwide. This shows that internet fraud is a new criminal trend, and is a rapidly growing area of online crime. The impact of internet fraud is to hinder the development of e-commerce, which is globally changing the traditional business mode. More people are purchasing goods from the online market and more businesses are looking for customers online. The use of the internet shopping mall saves customers' shopping time while it saves sellers' advertisements, logistics and store rent fees. Therefore, development of e-commerce activity will never stop as long as we use the internet. However, it is unavoidable that internet fraud is internationally dispersing and is becoming crime that is more serious. In order to respond to it more effectively and efficiently, it is necessary to analyse the characteristics and nature of various cyberspace policing methods.

Since internet fraud has characteristics of global reach, it is helpful to compare to a non-Western nation's policing model such as South Korea in order to examine similarities and differences in policing strategies and laws. While the IT business of South Korea has successfully expanded in local and global markets, the policing of internet fraud or cyber policing activities have not been known to other parts of the world outside South Korea. Therefore, an examination of the Korean policing model of internet fraud will introduce another dimension of cyber policing strategies and laws while showing also that occurrence of internet fraud is not geographically limited within South Korea.

Chapter 3: Policing internet fraud in UK Research

3.1 Introduction

Cyberspace is currently policed by multiple policing actors: 'Internet user and user groups, online virtual environment managers and security, ISPs, corporate organizations/corporate security organizations, non-government/non-police organizations, governmental non-police organizations and public police organizations' (Wall, 2007: 167-177). These entities constitute the nodes of networked internet governance because 'new technologies have accelerated the growing tendency towards networking sources of security' (Johnston and Shearing, 2003; Dupont, 2004: 76-91). Shearing (2004) stated that 'auspices' and 'providers' of governance are distinctive. Entities that authorize governance are 'auspices' and entities that shape behaviours are 'providers'. They are referred as an assemblage because they 'work as a functional entity across the network' (Wall, 2007: 167). This term 'assemblage' is borrowed from Deleuze and Guattari (2004) and Haggerty and Ericson (2000: 605).

3.2 Who polices internet fraud in the UK?

As explained in the introduction, internet fraud is policed by multiple actors from the smallest unit, the internet user, to the large corporate security. Wall's (2007) 'the internet's order maintenance assemblage' (See Table 3-1) categorises seven levels taking part in policing cyberspace. Since internet fraud is a predominant cybercrime, this concept is borrowed and applied to the policing of internet fraud. Compared to other nations, the UK model has more policing actors in the private and public sectors. This may be attributed to the reputation of the financial hub in the world. Besides, the public sector has also launched a specialized agency to respond to internet fraud. This shows how much the UK government recognizes internet fraud as a significant harm to society. This chapter explores how 'the internet's order maintenance assemblage' fits into the UK model of policing internet fraud.

Table 3-1: The internet's order-maintenance assemblage

Type (governance providers)	Population served	Sanctions (auspices)
Internet users/users groups-includes CyberAngels, Association of Sites Advocating Child Protection (ASACP), Spambursters, eBay	All internet users within interest group	Moral censure. cold-shouldering, lobbying, reporting, hacktivism
Online virtual environment managers and security-for online role playing/game playing, chat rooms, discussion lists, e-auction rooms, cyber worlds	Members of online environment	Removal of access rights, exclusion from the environment when community norms or laws are transgressed
Network infrastructure (ISPs)-Internet Service Providers, ISP orgs, domain name registries	Subscribing users/clients	Withdrawal of internet service, introduction of control software such as spam filters or content management
Private (corporate) security-banks, telecommunications, corporate entities	Own private interests/private clients	Withdrawal of services, civil recovery
Non-government, non-police hybrids/ internet Watch Foundation, CERT, CAUCE	All internet users	Withdrawal of participation, financial sanctions, reporting to police
Government-funded non-police/ customs and excise, security services, intelligence, trading standards	All internet users, business	Financial sanctions, prosecution (civil or criminal)
Government-funded public police/ police forces, national special units	All internet users	Criminal prosecution

(Source: Wall, 2007: 168, table 8-1).

Internet users and user groups

As commonly practiced in other countries, internet users and user groups police their virtual community to protect their valuable digital assets from outsiders. They routinely exchange useful information through messenger services, e-mail and community bulletin boards. Although their policing

activity is minimal and less effective, their informal networks often perform much better policing activity than that of government or corporate level. This level of policing has an advantage of using the huge volume of information from individual users and user groups which reflect the utmost priority social issues, such as bulk-victimization of internet fraud. Internet users and user groups impose sanctions of moral censure, cold-shouldering, lobbying, reporting and hacktivism.

Online virtual environment managers

As indicated in Wall (2007) online virtual environment managers mainly focus on the violation of norms or laws of their virtual community. When finding any violation, they remove access rights and exclude from the environment. Compared to South Korea, there are fewer virtual communities in the UK. The most popular websites among young internet users are facebook.com and myspace.com powered by Google, originally made by US companies. UK local online virtual environment managers monitor unusual activities on their sites. For the older internet user, seniority.co.uk provides over 50 websites that share useful information and gain knowledge from one another. This site is also policed by its monitoring staff for any illegal and harmful activities. In addition, online virtual managers are working at community chatting sites such as 'just chat' and 'wocchat' to monitor any illegal act. The 'just chat' site famously does not allow putting any sexual graphics or contents online. These people are not monitoring a specific kind of cybercrime, but rather a wide range of cybercrime, including internet fraud.

Internet Service Providers (ISPs)

The BT trial 'Webwise' promises both 'protection against online fraud and makes ads that appear on participating websites more relevant to your interests' (Sterling, 2008). In the past, London based Biblio Tech (Richardson, 1999) asked to stop spam mail to US companies and individuals. In some serious cases, they pursued legal action for any losses incurred. Pipex Internet Limited, a Tiscali UK company has a security team to monitor fraudulent activities on their website. They have exercised their power to control internet fraud by withdrawal of internet services,

introduction of control software such as spam filters or content management. ISPs are considered the best safe guard for preventing from internet fraud so the government wants to tightly control the ISPs. However. strong opposition by ISPs and internet users has discouraged government intervention.

Corporate security

The most popular private sector organization, APACS (2004) is a trade association for payments and operates a website for banking users, which assists in the protection of customers' money. The Independent Banking Advisory Service (IBAS), IBAS helps with banking related security problems. For financial fraud through internet banking, IBAS investigates any mistakes occurring with the bank. Similarly, the British Banker`s Association provides information about the prevention of fraud and money laundering. There are also smaller private organizations such as Miller Smiles and Rip-off Tip Off. In general, private sector activity is in-house security service based so it is difficult to know how each company operates anti-fraud units or whether they hire private investigators. With the development of mobile technology, telecommunication companies have monitored fraudulent activities in their service network. BT mobile. Orange and Vodafone have alerted their customers through real time warning systems. When they detect any suspected event, they have the ability to withdraw the service for offenders and pursue civil recovery.

Non-government, non-police hybrids

Get Safe Online is a joint initiative between the government, Serious Organised Agency (SOCA) and private sector website operated by Endurance Limited that introduces facts on how to use the internet safely and provides information on how to protect computers from many possible threats (Get Safe, 2007). According to Barrett (2007), 25% of the 10.8 million people in the UK registered with networking websites expose personal information. Its activity focuses more on public awareness than policing activity. Recent CIFAS (2008) is the UK's fraud prevention service that has more than 270 member companies varying from financial agencies

to retail credit agencies. CIFAS is the first international level of data sharing scheme. Members share information to prevent further fraud.

State-funded non-police groups

WARP (2008) protects internet users from online fraud through providing up-to-date advice on information security threats, incidents and solution. WARP also provides useful training on how to use the internet safely. Another state-funded non-police agency is NAFN (National Anti Fraud Network). It was created for the awareness of organized fraud in 1993 (NAFN, 2008). The UK Treasury department is monitoring and reporting fraud activities. The fraud advisory panel detects and deters external fraud. However, theses agencies do not specify their activity on policing internet fraud. For them, internet fraud is a kind of fraudulent activity. In addition, the committee on standards in public life is also involved in preventing internet fraud through examining current concerns. The FSA (Financial Services Authority) regulates most financial organisations such as banks, credit unions and insurance companies. The FSA also works with other regulators and authorities in order to tackle financial crimes. Consumer Direct provides advice on how to avoid scams through online consumer advice services. This agency is supported by the Department of Trade and Industry.

State-funded police

Policing internet fraud in the United Kingdom is carried out by various levels of public police agencies, which vary from local police forces to the national level criminal justice agencies such as SFO (Serious Fraud Office) and SOCA (Serious Organised Crime Agency). As their names betray the former focuses upon serious frauds and the latter upon organized crime.

At the local level, the Metropolitan Police Service (MPS) Computer Crime Unit was founded under the Computer Misuse Act 1990 to deal with internet related crime such as hacking and virus writing. So far, MPS reported that about 1,000 police officers have been trained to handle cases of cybercrime (Stephens and Induruwa, 2007). However, the MPS Computer Crime Unit does not deal with fraud related crimes, which are

mainly handled by the Economic and Specialist Crime OCU. Lack of resources and jurisdictional issues mean that the police have not effectively responded to fraud cases. Current reporting arrangements are insufficient to respond to fraud cases where those responsible are based overseas (MPS, 2008). Local police have limitations in investigating internet fraud so lack of continuity of response gives benefits to fraudsters. It has also been reported that fraud involving minor values within a different jurisdiction and trading standard is rarely investigated (Fraud Review, 2006). In order to upgrade the capabilities of the MPS Computer Crime Unit, the Metropolitan Police Service launched the PCeU (Police Central E-Crime Unit) in 2008. The PCeU has worked closely with the Home Office, City of London Police, and the Serious and Organised Crime Agency (SOCA) to respond to cybercrime (MPS, 2008). The major mission of PCeU is to support the new National Fraud Reporting Centre (NFRC) since 80-90 percent of cyber crimes are internet fraud related. The UK government assigned £7 million for this new agency (Vassou, 2008). Meanwhile, some local police forces, such as South Yorkshire, have prepared methods for investigating internet auction fraud on their website so that any police officer can use it. Despite local efforts, the majority of victims and police officers still do not know how to deal with internet fraud.

At the national level, the Serious Fraud Office (SFO), part of the criminal justice system and headed by the Director who is appointed by the Attorney General, handles major fraud offences in the UK. Its jurisdiction includes England, Wales and Northern Ireland. It was founded in April 1988 and its powers were created by the Criminal Justice Act 1987. Since the SFO has a limited budget and about 240 staff members, it does not deal with all fraud, only with serious fraud that involves special knowledge, wide coverage, international impact, and huge amount of loss (at least one million pounds) (Kiernan, 2005). Section 2 of the Criminal Justice Act is a special power requiring answers to questions, provision of information or production of documents for the purpose of an investigation (SFO, 2008). Recently, the SFO obtained a new computer system to deal with internet fraud investigation (Kiernan, 2005).

SOCA (Serious Organised Crime Agency) is a non-geographic police unit responsible for undertaking pro-active operation against serious and organized crime. The agency has been formed from the combination of the National Crime Squad (NCS), the National Criminal Intelligence Service (NCIS) and HM Customs and Excise. A substantial part of the staff comprises former police officers so that they have carried over the professional police quality. The agency is sponsored by, but operationally independent, from the Home Office (SOCA, 2008). Recently, SOCA has expanded their policing activity to internet crime while its major role is to tackle national and transnational organized crime (Segell, 2007). The existing National High Tech Crime Unit (NHTCU) has become a part of SOCA. There is a little difference between MPS/SFO and SOCA in that the MPS Computer Crime Unit and Serious Fraud Office have the ultimate aim to prosecute fraudsters while SOCA seeks to intercept criminals. It is in 'addition to the SIS (MI6) and the Secret Service (MI5), similar to the FBI' (Segell, 2007: 1). However, SOCA's activities give little attention to cybercrime, this is apparent since only five percent of the budget was assigned to fight e-crime (Leyden, 2008).

The UK government will establish the National Fraud Reporting Centre (NFRC) by 2009, which collates reports of all type of fraud and investigates fraud through its law enforcement arm (Leyden, 2008). The establishment of NFRC would fill the gap between fraud reporting and investigation. Previous separated systems did not prove effective or efficient in policing internet fraud.

As illustrated above, public policing agencies have systematically responded to internet fraud from the local to national level in the United Kingdom. Although they do not perfectly deal with internet fraud, it appears that their progressive effort for developing policing for internet fraud can provide positive signs for future policing. In addition, along with the public model of policing internet fraud, the private model of policing is very active in the United Kingdom.

Summary

The Fraud Review Team compiled statistics in 2006 indicating that that the following groups of investigators focused on fraud (Button; Johnston; Frimpong and Smith, 2007: 194):

- Serious Fraud Office (270 employees);
- The police (524 police officers in fraud squads);
- Serious Organised Crime Agency (SOCA) (288 employees during 2005-6);
- Other public sector bodies - Her Majesty's Revenue and Customs (HMRC) (7500 staff including drugs investigators); DWP (3250); NHS (344); Financial Services Authority (FSA) (46); Department of Trade and Industry (DTI) (150) etc.;
- Private sector (in-house investigations departments - the six largest banks alone having 2500 investigators).

According to the Attorney General's Office, internet fraud accounted for about 8 percent of all fraud while overall losses from fraud were about 20 billion pounds in the United Kingdom. Lord Goldsmith said that 'it is often confusing for victims to know who to report the fraud to, particularly if it crosses geographical or sectoral boundaries'. 'Fraudsters benefit from this lack of continuity of response. Internet fraud is a particularly good example of how a fraud can become difficult to report' (the register, 26/07/2006). For this reason, it is necessary to establish a central reporting centre so that victims can easily report their incidents without confusion and hesitation. A central reporting system would improve overall policing activities because it would resolve the under reporting problem while recording reliable incident data. Without recognizing the exact number of incidents, it is difficult to implement an effective policing strategy for internet fraud.

Compared to the US policing model for internet fraud related crime, the UK policing model appears more fragmented and well balanced between the public and private sectors. It shows how the Americans and the British respond differently to internet fraud and reveals how internet fraud has been bridged between and within the public and private sector agencies.

Overall, the model for UK policing of internet fraud appears to have improved its capabilities in both the public and private sectors. Although private industries' activities are not publically recognized, in-house security and risk management teams of large banks and corporations have gained great reputations (Button; Johnston; Frimpong and Smith, 2007).

3.3 Internet fraud law in the UK

The new fraud bill attempted to simplify existing laws by creating a new fraud offence carrying a maximum 10-year jail sentence and easing the prosecution process; the main feature of the bill (Leyden, 27/05/2005). The new offence can be committed: by false representation, which would take account of the offence of phishing; by failure to disclose information or by abuse of position. The new bill introduces three new offences that could potentially be used to deal with internet fraudsters: obtaining services dishonestly, for example by using a stolen credit card over the internet; possessing articles for use in frauds, such as a computer programme that generates genuine credit card numbers; and participating in fraudulent business.

The recent reform of the UK Fraud Act 2006 Section 2 subsections (2) (3) creates an offence covering the perpetrators of phishing attacks. The provision is designed to clarify existing laws within the new Fraud Act. A new offence of fraud, designed to reinforce the existing law and simplify the prosecution process highlights the fact that the act of sending such emails without any proof of deception or obtaining of any property will be prosecuted (Savirimuthu and Savirimuthu, 2007); this is the main feature of the 2006 Act. The offence can be committed in one of three ways: false representation (as seen in phishing attacks); abuse of position (e.g. person lifting money from the account of an elderly person under their care) and failing to disclose information (e.g. a lawyer who schemes to keep information from his client so he can make money on the side). According to this 2006 Act, fraudsters can be imprisoned for a maximum 10 years for their offences (The registers, 2006). In spite of the enhanced Fraud Act 2006,

cyber fraudsters are still able to get away with limited sentences or discharges. Lost revenue in the UK stood at around $1.2 billion a year in 2007 (Leggart, 2007). According to APACS data in 2008. card fraud increased 14 percent for the first six months of 2008 with total losses of £301.7 million; online banking fraud losses totalled £21.4 million (Crimestoppers, 2008). These increases were attributed to internet fraud. However, introduction of chip and pin has interrupted fraudulent activity and reduced losses by 35 percent since 2005. This clearly shows that law is not the perfect remedy for internet fraud but safe use of the internet and enhancement of organizational information security are better solutions for the prevention (Savirimuthu and Savirimuthu, 2007). Overall, the capability of criminal law must compete with the scale of the governance challenges that the online environment poses.

3.4 How do public and private sectors police internet fraud in the UK?

Policing internet fraud is very important subject since internet fraud has become the most prosperous type of cybercrime and influences both individuals and companies. While internet fraud requires converging criminological theory in the areas of policing, white-collar crime, and technology (Nhan 2006), it is imperative to find out what kind of policing model for internet fraud is more effective between the private and public policing models.

Policing internet fraud by the public sector

Policing internet fraud has a unique characteristic that travels across jurisdictions since internet fraud is not a specific country's issue, but an international one. It is widely recognized that the use of the internet as a tool for fraud was beyond the control of public sector regulators (Drinkhall, 1997). In the public sector, there are government-funded police and government-funded non-police agencies participating in policing of internet fraud (Wall, 2007). They comprise police forces, financial supervision services, and information and communication regulating agencies. However, internet fraud cannot be effectively regulated by the public sector due to

lack of resources, knowledge, labour, training and law. The bureaucratic and inter-agency conflicts within the public sector have hindered the response to internet fraud.

As policing internet fraud is different from the traditional type of crime, public police need to use a different design and strategy to respond to it. Law enforcement agencies are naturally bureaucratic organizations (Roberg, Kuykendall and Novak, 2002; Swanson et al., 1998). Police officers do not perceive the internet as a potential for the democratization of knowledge and growth in active citizenship (Walker and Akdeniz, 1998). Some argue that the police culture has a natural aversion to bureaucracy and show the development of UK police recruitment, training, and discipline and the reform efforts for anti corruption. However, the police have not completely escaped from the image of a bureaucratic organization (Reiner, 2000).

According to Burns et al. (2004), law enforcement agencies have adopted the sort of bureaucratic model described by Max Weber, which emphasizes 'a division of labour within organizations characterized by specified areas of competence, official duties bounded by a system of rational rules while training current and new staff' (Burns et al., 2004: 479). Law enforcement agencies are required to develop competency and rules while training current and new staff, in order to respond to internet fraud adequately (Burns et al., 2004). To accomplish these developmental goals, a significant change must occur within the bureaucratic systems of law enforcement agencies. It will also require complex and comprehensive cooperation between institutions in the public and private sectors.

Grabosky and Smith (2001: 29) reported that 'security in cyberspace depends on the efforts of a wide range of institutions, as well as on a degree of self-help by potential victims of digital crime' and it is more likely to depend on a 'mix of law enforcement, technological and market solutions'. As in conventional crime, prevention is much better than cure in cyberspace. Public awareness programmes on behalf of prospective victims are needed to provide the necessary education about what risks they may confront. Grabosky and Smith (2001: 39) stated that 'individuals or institutions

should be made aware of the potential consequences of an attack on their information assets and of the basic precautionary measures which they should take'.

Technological intervention such as biometric authentication and filtering software can be good counter-measures to prevent and to control internet fraud (Grabosky and Smith, 2001; Green, 2001). By using these technologies, systems administrators can prevent insiders and outsiders gaining access to certain types of information. However, the use of technological intervention may only create more opportunities to fraudsters, since they also use advanced technology and expertise to break into the system (Centeno, 2002). For this reason, law enforcement agencies are required to upgrade their new investigative techniques and equipment on a regular basis in order to detect and intercept fraudulent activities in cyberspace.

The collaboration and cooperation of law enforcement agencies is very important in responding to serious internet fraud, since offender and victim can be located in different jurisdictions or on the sides of the globe. Therefore, the US Congress passed the Financial Services Antifraud Network Act of 2001, in order to enhance 'the coordination of anti-fraud efforts and promote the sharing of information among state and federal financial regulators' (Burns, R. and et al, 2004). Recent research by Burns et al. (2004) show that 64.2 percent of participants reported that there was very effective cooperation among law enforcement agencies. More specifically, respondents are working with county (62.0 percent), state (54.5 percent), and federal (55.1 percent) law enforcement. It was also found that there was the least effectiveness in working with the SEC's Office of Enforcement (24.4 percent), the NCL's Internet Fraud Watch (26.8 percent), foreign law enforcement (29.1 percent), and private security (30.9 percent). Information dissemination between/among security agencies is also an important factor in preventing internet fraud. According to Burns et al. (2004), most law enforcement agencies send internet fraud awareness information to other law enforcement agencies (36.2 percent), the public (34.6 percent), and private sector businesses (25.7 percent). However, it indicates that judges

(3.3 percent) and other officials (7 percent) seldom receive such information. Meanwhile, it is also necessary to develop an accessible database of cases of internet fraud for law enforcement agencies and other criminal justice experts.

These findings indicate the need for a central clearinghouse of information available to all law enforcement agencies. Internet fraud is significantly problematic and increasing in frequency primarily in a gradual fashion. A clearinghouse of information in which agencies involved with Internet fraud enforcement efforts could share 'technical information, the names of expert witnesses, advice from experienced prosecutors, or the location of available labs which would greatly assist law enforcement effort' (Burns and Whitworth, 2002: 18).

There are a number of information clearinghouses actively operating under the supervision of international criminal justice organizations but they are not available to non-membership countries. For example, Interpol, Europol and ENISA have established criminal information networks to share the necessary information in order to respond to cybercrimes. In Europe particularly, ENISA (The European Network and Information Security Agency, which was founded in January 2004, will have a pivotal role in contributing to the development of a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organizations of the European Union (ENISA, 2005). In 2005, ENISA had a budget of €34.3 million for five years and were fully staffed for collecting and analyzing incident data (Euractiv, 2004). In Asia, APEC's (Asia Pacific Economic Cooperation) 14 membership countries have discussed how to develop comprehensive legal frameworks to combat cybercrime and to build law enforcement units capable of investigating cybercrime. However, only 50% of countries participated in the treaty revealing legal and political disparities.

Overall, it appears that the public sector has recognized the importance of policing cybercrime, including internet fraud. Many people have argued that the bureaucratic police organization has to change in order to satisfy the

public demand for the transformation of policing (Reiner, 2000): police have to develop their competency and rules while providing necessary training for officers (Burns et al, 2004). Private and public sector partnerships are emphasized when policing internet fraud. It was strongly recommended by Grabosky and Smith (2001) that public awareness programmes by relevant public agencies and financial institutes are needed. Counter measures and technological interventions such as biometric access and filtering software have been introduced. For better coordination and cooperation, the Financial Services Antifraud Network Act of 2001 was established in the US (Burns et al, 2004). However, it is less effective for the private sector. Recently it has been discussed that law enforcement agency oriented information sharing has to be expanded to the entire criminal justice agency (Burns et al, 2004). The need for a clearinghouse of information was highly recommended (Burns and Whitworth, 2002). International level of response by Europol and Interpol was observed however, more efforts on an international level of cooperation have been emphasized. Evidently, the international level of law enforcement agencies has shown their effort to adapt to the policing of cybercrime while the local level of response has still been below the appropriate level. The following section will examine the level of policing in the private sector.

Policing internet fraud by the private sector

Since the policing of internet fraud is not a typical or routine event for the police, there is limited knowledge and limited human resources available to respond to internet fraud. This situation implies that the private sector is better able to deal with internet fraud since it is in their interests to do so. Wall's (2002) study found that credit card related fraud was not reported to the police, but it was reported to the banks because they were regarded as the victims. The banks then resolved the fraud in their own way and favourably to their own interests, which prevents a negative impact of adverse publicity and preserves market confidence. The private sector of policing arguably responds more effectively to fraud in cyberspace because it applies a private model of justice.

Internet fraud has become more threatening for the private sector since e-commerce is developing rapidly and more people use online transactions for purchasing goods or services. Private organizations, corporations, banks and ISPs all make efforts to protect their customers' assets from any possible risks from internet fraud. Meanwhile, some organizations such as CAPA (Confederation of Asian and Pacific Accountants) have actively responded to internet fraud through regular base meetings that exchange information. They have acknowledged that there is a need for uniform guidelines and information clearinghouse to be established that set out desirable online practices with a view to minimizing the risks of fraud relating to electronic commerce (Smith and Urbas, 2001).

The Anti Phishing Working Group is another large international level organization against fraud and identity theft resulting from phishing, pharming and e-mail spoofing. It has established global networks to respond to internet fraud and has more than 1700 members in the public and private sectors (APWG, 2008). It has a major aim to help e-commerce activities through eliminating those fraudulent threats. APWG encourages people to report their victimisation and provides public awareness programmes to enlighten internet users to avoid phishing attacks. However, it does not have any authority to use judicial sanctions on phishers, therefore serious cases have to be passed to a law enforcement agency.

APACS is 'the UK trade association for payments and for those institutions that deliver payment services to customers' (2008). APACS represents 31 industry members and works for their benefit through lobbying activities. Forecasting payment trends and collecting statistical data for developing industry standards and best practices are their main responsibilities. In addition, one of their key responsibilities is to coordinate activities to tackle payment related fraud. Usually, their policing activities are conducted through their own membership network. Thus, 31 industry members have participated in policing activities by collecting available information from each member's business domain. Eventually, the collated information will become important data for making tactical counter measures to respond to payment fraud (APACS, 2008).

In fact, the majority of economic crimes are handled informally through private models of justice, rather than reported to the police or other regulatory bodies (Clarke 1990; Levi 1992; Punch 1996; Schlegel and Weisburd, 1992). These responses are limited to 'internal systems of corporate justice' (Henry, 1983; Selznick, 1969) and 'securing desired forms of financial security on behalf of their clients' (Williams, 2005: 320). Recent trends indicate that many allegations of financial wrongdoing are handled not by the police but by private sector agencies. They are not low level and rather unsophisticated private security agencies, but professional service firms, which consist of CPAs, lawyers, former police officers (FPOs), private investigators and computer analysts.

These are internationally famous firms in terms of sizes, assets, and large number of employees, namely: KPMG, Kroll Associates, Ernst & Young, Deloitte and Touche, Price-Waterhouse and Control Risks Group. They put a different name on their banner, such as 'forensic accounting', 'risk management consultancy' and 'security consulting'. According to Williams (2005: 317), 'these firms have positioned themselves as suppliers of a unique and highly specialized form of investigative and quasi-juridical labour geared to the resolution of 'business troubles' ranging from the theft of intellectual property, to the misappropriation of corporate assets, to breaches of financial security'. Williams coined the term 'Forensic Accounting and Corporate Investigation (FACI) industry' (2005: 317), for those businesses.

In spite of a primary response to economic crime, their work has been limited to specialized accounting and legal publications. The FACI industry and its functions have been largely ignored within the sociological literature (Williams, 2005) although there are some references in discussions of risk, trust and security (Ericson and Haggerty, 1997). This industry has contributed exclusively to the investigation of economic crime as a provider of policing services in the financial field. The majority of internet fraud occurred in the financial field since fraudsters penetrate credit card facilities

and use victims' credit cards. Therefore, many financial institutes have online and offline security service contracts with the FACI industry.

According to Jones and Newburn (1999), a 'policing division of labour' has long been employed as a focus point through which the mandate, interests and logics of private versus public forms of policing have been defined and framed. In the field of security, private and hybrid organizations govern a growing share of what has become a market and continuously search for new opportunities. Brodeur and Kempa (1995; 1999) argued that the public-private dichotomy fails to account for the diversity and heterogeneity of actors participating in the governance of security or policing. The prevalence and multidimensional implications of risk and its mentality refute the idea that any single policing entity can prevent crime alone. The distinction between public and private forms of policing are increasingly difficult to maintain and have been proven somewhat outdated, given the emergence of complex and multi-dimensional 'security-networks' (Johnston, 1996; Shearing, 1996; Loader, 2000; Newburn, 2001) or forms of 'nodal governance' (Johnston and Shearing, 2003: 18).

Studies have indicated that private policing activities are very beneficial for preventing and protecting from internet fraud. However, private entities do have limited authority to enforce rules or laws against fraudsters. As indicated in Table 3.1 (internet order maintenance assemblage), their sanctions include removal from access rights, withdrawal of internet services and financial sanctions. These are relatively limited ways to effectively control the level of internet fraud. For this reason, their assistance to individual victims is limited and is often considered disappointing. In the meantime, corporations and banks have hired professional security services through the FACI industry, which will provide much more reliable services than non-profit organization services with substantial costs. However, FACI industry activities are not well known to the public (William, 2005). This reflects the fact that their activities are still restricted by some jurisdictions. As indicated in the internet order maintenance assemblage (see Table 3.1), multiple actors in the private sector participate in policing cybercrime. Therefore, some

experts report that public-private dichotomy fails to account for multiple actors participating in the governance of security or policing. The emergence of 'security networks' and 'nodal governance' is a substitute for the traditional public-private distinction (Wall, 2007).

3.5 Relationship between the public and private sectors

There are many criminal justice literatures describing the appropriate relationship between the private and public police (Marx, 1987; Gill and Hart, 1997; Golsby, 1998; Jones and Newburn, 1998; Johnston, 1999; Sarre and Prenzler, 2000; Bayley and Shearing, 2001) although this literature is not based on policing cyberspace.

According to Marx (1987), the delegation of police power to the private sector is useful to investigate cases where the police cannot reach due to legal constraints. He also argued that organizational forms distort public, private and the exchange of personnel between the policing sectors.

However, Gill and Hart (1997: 564) have argued that the police investigation work, such as guarding and patrolling service. should not be contracted out. It seems that only simple police work should be delegated to the private police. Loader (1997: 385) argued that 'the most stringently controlled private security industry might still serve to cement and exacerbate social inequalities'. Meanwhile, Golsby (1998) suggested the establishment of equal partnership and private security federation, which has a complaints system and liaison committee, would provide effective policing.

Sarre and Prenzler (2000) introduced the *regulated intersections model* to show an appropriate relationship between public and private police. Their model shows normative models for relationships between those sources. They argued that partnership is necessary but cooperation should limited and regulated in order to maximize the public interest. The model contains seven descriptive models that they suggest to consider for observed interrelation. They are the property model, the division of labour model. the

competing force model, the supplementary service model, the Ad Hoc partnership model, the combined model and the unholy alliance model.

Table 3-2: The regulated intersections model

Model	**Characteristics**
Property	Similar means of patrol and investigation but differ ent location and boundaries
Division of labour	Police focus deterrence, private focus on crime prevention
Competing forces	Compete for the market share
Supplementary servic e	The police regulate private security industry
Ad Hoc partnership	Work together whenever it is necessary
Combined forces	Two sectors combine permanently at all levels
Unholy Alliance	Corrupt relationship between two sectors

Source: Sarre and Prenzler (2000).

Among the seven models, the *division of labour model* reflects the tension between the private and public models of policing internet fraud because it focuses on how each sector approaches internet fraud differently. While the police focus on deterrence through investigation, private security focuses on crime prevention. The things that make them so different are their contrasting policing goals. The goal of private policing mainly seeks for the recovery of loss, prevention of future risk (George and Button, 2000) while the goal of public policing mainly seeks actual punishment (Reiner, 1994). In the private justice model, sanction might involve dismissal, demotion or civil penalties. Some cases can be litigious while some cannot be litigious (Stucki, 2002).

In response to internet fraud, investigative tendencies also reflect their different goals of policing activity. For example, the police would like to eradicate all connection in cases of phishing while the private security would like to reinstate normal internet services without delay or being noticed by their customers. The degree of difference in the response by each sector shows how it is difficult to mix two sectors.

The relationship between private and public sector in terms of policing internet fraud does not exist in the current law in many nations and there is no specific law to define their relationship and policing activity. Although they have pursued different goals of policing, close partnership and cooperation of the two sectors is imperative to improve the level of policing of internet fraud.

It is evident that governments and law enforcement agencies need a strong partnership with the private sector for policing internet fraud because governments cannot handle the complex problems of internet fraud without the assistance of private organizations. Neither governments nor the private sector can solve the problems alone. Lack of knowledge about internet fraud on the part of the public police and lack of legal authority for private security makes them dependent upon each other. The nature of internet fraud requires close cooperation between the public and private sectors.

Although cooperation between the public and private sector is imperative, it is also important to improve the role of public police in relation to the policing of cyberspace because traditional forms of policing cannot treat the complicated nature of cyberspace and cybercrimes required by networked security.

3.6 The development of the public police role in policing cyberspace

Policing cyberspace is characterized by 'a sense of order that results from the complex order-maintenance 'assemblage' of networked nodes of security' (Wall, 2007: 177). These networks go beyond the 'state/non-state binary' (Dupont, 2004: 76) and state sovereignty (Shearing, 2004: 6). Wall (2007) stated that networked security takes advantage of the 'natural surveillance' and has social control functions, both primary and secondary. Internationally, jurisdictional legal disparity is mediated by networked security.

Although overall the public police role is small compared to other networks, police still culturally, symbolically and politically tend to claim an ownership of policing cyberspace. Particularly, public police is being supported by 'the traditional consensual relationship with the state and the citizen' (Wall, 2007: 178). With regard to the debate over policing cyberspace, a replication was made by the terrestrial reassurance of policing debate in that the 'increasing recognition that the police alone cannot win the fight against crime and disorder and cannot meet the public's seemingly insatiable demand for a visible policing presence' (Crawford and Lister, 2004: 413). Wall (2007) argued that policing cyberspace never demands a more visible policing presence while terrestrial policing demands a more visible policing presence on the street.

According to Crawford and Lister (2004: 414), 'public police are becoming part of more varied and complex assortment of organizations and agencies with different policing functions together with a more varied and complex assortment of organizations and agencies with different policing functions together with a more diffuse array of processes of control and regulation'. This reflects the claims that 'not all policing lies in the police' (Reiner, 2000) and 'player in the broader network of security constitutes the policing cyberspace' (Wall, 2007: 178). As claimed by Crawford and Lister (2004: 426), 'much policing is now taking place beyond the auspices' of the public police and plural policing, facilitating a form of 'networked governance', that has taken placed in the networked and nodal architecture of cyberspace (Wall, 2007: 179).

Ericson and Haggerty (1997) stated that the emerging role of police is as 'information brokers' since they do not necessarily use physical force to deal with the crime but use intelligence thorough the internet. For example, 'insurance companies and their investigative units are routinely given access to police records and insurance adjusters take the lead in investigating fraudulent claims, they depend on the police for routine disclosure of relevant knowledge' (Ericson and Haggerty, 1997: 227: 231).

There is clearly a need for international cooperation to the response of internet fraud between advanced countries to make such expertise available to less developed nations and share strategic information and training throughout the world. To some extent this is already occurring, indeed some IT advanced nations' police agencies have hosted workshop and training programmes for other nations' police officers. For example, the Korean National Police Agency hosted 13 foreign police forces and provided three nations' cyber-policing training in 2006 (Kim, 2008). However, it appears that the provided training did not focus on internet fraud investigation but focused more on hacking and other types of cybercrime. It seems that internet fraud investigation is not a priority for the Korean National Police Agency. This may reflect the fact that the private model of policing internet fraud is better than the public model. Because of this reason, it is necessary to find a solution from the cross sector partnership between the public and private sectors.

3.7 Multi-agency cross sector partnerships

The purpose of 'a multi-agency cross-sector partnership is to build up networked trust relationships that engender a willingness to share information'. It should not be exclusively dominated by the state law enforcement although 'these partnerships tend to be driven by Internet security and law enforcement initiatives' (Wall, 2007: 180). For example, POLCYB (the Society for the Policing of Cyberspace) is both multi-agency and cross-sector, existing to share information across micro-networks of trusted individuals and agencies to promote cooperation between sectors which actively invite international involvement from law enforcement, corporate entities and interest groups' (Wall, 2007: 180). POLCYB (2008) is a good international forum for the policy issues while HTCC (the High Tech Crime Consortium) focuses more on discussing routine problems of cybercrime. HTCC is also more of a multi-agency than cross-sector organization (2008).

According to Hynds (2003), the private sector has spent a huge amount of money on business intelligence in order to make successful investments, new products and expand while less money is spent on the IT security that

has to be synchronized with company efforts. He suggested that a cross sector partnership would reduce the cost that private sector previously had to foot alone. Risk assessment by the public sector would provide real value to private industry. Since all information supplied comes from across the various business sectors and other intelligence sources, the private sector would obtain real value added service from the public sector.

The AGORA security group tends to discuss 'at a policy or procedure level rather than specifically sharing sensitive intelligent data; for example, developing ideas about security issues and good practice, but also identifying, even agreeing possible acceptable limits for data storage and/or provide data' (Wall, 2007: 181). It promotes more informal cross sector meetings. Sharing of commercial victimization and criminal intelligence within the forum based on networked trust relationships enhances the partnership policing. Multiple crossover memberships are common for the members who seek more information.

Charney (2005) also reported the five elements of a public and private cross-sector partnership strategy that Microsoft experienced which illustrates the role of industry and government. The five elements are:

- the existence of strong laws and adequate resources for enforcement;
- proper training of law enforcement;
- coordination among domestic and international law enforcement agencies and improved information sharing that is closely related to such coordination;
- heightened public awareness of the risks of cyberspace and proper user practices;
- improved technology (Charney, 2002: 4).

Similar to CIPAC (Critical Infrastructure Partnership Advisory Council), NISCC (National Infrastructure Security Co-ordination Centre) coordinates principle agencies in the UK. NISCC is an interdepartmental centre, which consists of Home Office, CESG (Communications-Electronics Security

Group), Security Service, MoD, DSTL (ex DERA), DTI. Cabinet Office. CCS (Civil Contingencies Secretariat), e-Envoy (CSIA), and NHTCU (National Hi-Tech Crime Unit). It was launched in February 2000 and its major aim is to minimize the risk of the Critical National Infrastructure (CNI) from electronic attack (Overill, 2001). Later, CPNI was formed in February 2007 from the merger of the National Infrastructure Security Co-ordination Centre (NISCC) and the National Security Advice Centre (NSAC - part of MI5) (CPNI, 2008). Its business philosophy focuses on information sharing. Davis (2005) emphasized that information sharing among government departments, operators, owners of CNI and system vendors would help to deal with the vulnerability. In Europe, ENISA contributes to coordinating member states in combating cybercrime associated with the private sector by developing of investigative technology (Mitrakas and Zaitch, 2006).

There is an also specific growing concern encouraging the demand for establishing specialist coalitions such as The European Contact Network of Spam Authorities (CNSA) that coordinates anti-spam enforcement internationally through building relations with the OECD and the International Telecommunication Union (Wall, 2007). Shaw (2004) reported that spam is a bothersome cross sector problem that requires international cooperation in terms of legal and technical support. Broadhurst (2006) argued a need for mutual legal assistance in the international level of response for the cross-national nature of cybercrime. Transnational policing capability for cybercrime is necessary since malicious codes penetrate into the global computer network that eventually threatens e-commerce activities.

According to Wall (2007), it is evident that there are not many multi-agency cross sector partnership organizations available at the international level. Furthermore, existing multi-agency cross sector partnership organizations such as POLCYB, AGORA, and HTCC have been launched in English culture based nations. There is no single agency or organization existing in Asia. Since cybercrime has a transnational nature, it is necessary to establish a multi-agency cross sector partnership forum or organization in order to cover the international level of the order maintenance assemblage.

In order to establish an effective international cross sector agency, it is important first to examine current policing practices in IT advanced nations. The following section illustrates how the policing of internet fraud operates in the US. This information will be used to compare other nations' policing models for internet fraud.

3.8 Barriers to the effective policing of cybercrime

The most common complaint made by police officers or law enforcement agencies is that they are not technologically equipped for the response of the high tech crimes while criminals are getting smarter and crimes are getting more complicated (Chung, 1999). Conservative police cultures and traditions have hindered the rapid change of police capability in relation to high technology (Wall, 2007).

In order to satisfy the public concern regarding emerging cybercrimes, police forces form specialist units to deal with the cybercrimes. The success of the organizational response to cybercrime depends on special knowledge and expertise within a police force. According to Wall (2007: 160), 'cybercrimes introduce a new global dimension to the relationship between police, technology and the public because they clearly fall outside the traditional localized and even national operational purview of police'.

Although the Council of Europe (COE) and international police organizations (Europol, Interpol) work at the procedural and organizational levels, there are various barriers to developing good policing of cybercrimes. There are *de-minimism*, *nullum-crimen disparities*, jurisdictional disparities, non-routine activity and police culture and under-reporting (Wall, 2007).

De-minimism is a common characteristic of cybercrimes that leads to low-impact, bulk-victimizations that cause large aggregated losses internationally because police do not investigate trivial matters. *Nullum-crimen* disparity (nullum crimen sine lege-no crime without law) is another characteristic of cybercrime that causes inter-jurisdictional problems, which arise due to cultural differences in defining crime. Some offences fall under

civil law in one jurisdiction and criminal law in another. Jurisdictional disparities are also found in many nations, hence the use of 'forum shopping' (Braithwaite and Drahos, 2000) is favoured by the police and prosecutors in order to maximize the potential of conviction (Wall, 2002: 2007). Jurisdictional venue changes have been seen in many cases since cybercrimes have involved different locations of servers, offenders and victims. Inter-jurisdictional cooperation is a key factor for a successful response to cybercrimes.

According to Reiner (2000) and Wall (1997: 2000), response to cybercrime is not a routine activity of the police, which include cross-border investigation. Wall (2007: 163) stated that 'police occupational culture is the accumulation of the collective "routine" experience of police officers and it is an important component of police work'. Since cybercrimes are non-typical events for the police officers, police culture does not appropriately support them to respond to unusual events.

Under reporting of cybercrimes to the police is becoming a serious concern. Comparison of several reliable data sets indicates that relatively small numbers of cybercrimes are reported to the police. They are mainly minor-credit card related frauds but no further investigation was taken. It appears that there is a relationship between *de-minimism* and under-reporting. The public also does not expect any successful investigation by the police due to lack of knowledge and resources. However, 'the public still regards the police as a primary emergency service' (Wall, 2007: 165). Generally, victims and other groups or organizations involved in the regulation of behaviour in cyberspace deal with the cybercrimes since most cybercrimes are actually not necessarily classified as crime, rather they are considered more harmful activities (Wall, 2007).

Police accountability, *de-minimism* and under-reporting are jointly facilitating the development of cybercrime. In addition, ambiguous classification of cybercrimes that may fall into the category of harmful activities has also provided a blind spot for the policing of cybercrime and harmful activities. Apparent classification of cybercrime is imperative to

define the role of the public police so that the public police know how to respond to it and what they have to do to prepare for it. It is very important to rethink the role of the public police with regard to the policing of cybercrime.

3.9 Tensions between private and public sectors in policing internet fraud

Nature of problem

Tensions evident while policing internet fraud have characteristics that are different from tensions in terrestrial level policing in that they are mainly occur due to lack of a legal system, lack of technological resources and lack of IT knowledge between the private and public sectors. Since the police have limited knowledge and resources for policing cyberspace they can neither satisfactorily protect the victims of internet fraud nor prevent the occurrence of crime in the first place (Parliament of Victoria, 2002). thus the responsibility of the private models of policing fraudulent activities in cyberspace has become more pronounced than ever. At the same time, the private model of policing has shifted its focus from the protection of physical assets to the protection of information (Solms, 2001). so policing by the private sector of security now plays a more significant role in the response to internet fraud than it does to conventional crime. This superiority of the private model of policing internet fraud creates serious tensions between the public and private policing bodies.

Previously many scholars have studied the tensions between private security and public police (South, 1988; Johnston, 1992; Shearing, 1992; Swanton, 1993; Greene, Seamon and Levy, 1995; Jones and Newburn, 1998; Loader and Walker, 2001; Mandel, 2002). They argued that policing involves various tensions that negatively affect the efficiency and effectiveness, public reassurance, and authority of the state. However, their studies were limited within conventional terrestrial level policing and the tensions between private and public models of policing internet fraud does not appear to have ever been chosen as a main research topic.

Despite many academic articles reporting the importance of public and private cooperation and partnership in policing cybercrime (Adamski, 2003: EURIM, 2006; IACP, 2004; Kozlovski, 2005). tensions in the policing of internet fraud have rarely been discussed in the existing literature. Lack of criminological research about tensions between private and public models of policing internet fraud suggest that criminologists may be discouraged to conduct it since it contains many sensitive issues. The only available literature regarding this topic is to be found in Wall's (2005: 87) recent work, where he comments that 'low levels of prosecutions for breaches of computer security and low levels of recorded Internet related fraud are poignant examples of this tension'.

Notwithstanding the fact that many Western countries' governments have encouraged the use of private policing, there are still tensions arising between private and public policing sectors (Shearing, 1992). Traditional public sector policing does not trust private sector policing in terms of accountability, integrity, professionalism, and public interest. According to Crawford, Lister, Blackburn and Burnett (2005), lack of coordination, duplication and poor relationships between the two sectors discourage their effectiveness.

Production of tension

According to Swanton (1993: 1), 'police and private security occupy a largely common functional domain, both are finding it difficult to prepare for the future and a degree of tension exists between them. That tension can be expected to exacerbate in an era in which charging for services hitherto considered public responsibilities finds widespread acceptance'. If the police can effectively patrol our neighbours, each individual does not need to hire private security services with the extra expenditure. However, 'tension in cyberspace arises from the power struggle for control over cyberspace in order to obtain market control and protection' (Wall, 2007: 23).

Cyberspace is a virtual world where ideas create more economic value than physical property (Barlow, 1994). According to Jordan (1999: 3), 'virtual societies have become increasingly important, taking over the existing societies and inventing their own'. More people meet, discuss and share information in cyberspace than terrestrial space. With the emergence of the internet, economic, social and political values have been reshaped and reappraised. It is not an exaggeration to say that the internet has become a most important tool for humans. 'The Internet is causing us to reformulate the ways in which we understand societal changes' (Wall 1997: 209).

Neither sector wants to compete for ownership of policing internet fraud if no interest exists between the two sectors. For the private sector, it is directly related to corporate governance and management (Von Solms, 2001). For the public sector, it is directly related to a symbol of state sovereignty (Shearing, 2004). It appears to be difficult to give up their policing authority for cyberspace since they have to pursue the different goals of justice and interests.

Types of tensions

As McKenzie (2006) reported, many more serious tensions exist between the private and public sector than between public police forces and public agencies. Their different goals and reasons for policing internet fraud create those tensions and hinder their effective partnership.

3.9.1.1 Tensions between the private and public sectors

Tensions between the private and public sector of policing bodies deter and impede the building of positive relationships. Security experts believe that lack of trust and sharing of information, different investigative philosophies, negative publicity, and adverse impact on stock are the most common tensions between the two sectors. These tensions have been noticed by criminal justice and policing related literatures (Shearing, 1992; Greene, Seamon and Levy, 1995; Connors, Cunningham and Ohlhausen, 1999; Rigakos, 2002; Crawford, Lister and Wall, 2003; Delint, 2005; Joh, 2004; Bhanu and Stone, 2004; Ferret, 2004). However, there are some gaps in this

research since tensions between private and public sectors for policing internet fraud have not been studied by many scholars.

Traditionally, the study of tension between the private and public sector was concerned with the development of private policing and the promotion of partnership policing. According to Swanton (1993), different perspectives in the way each view the world and differing interests create tensions between the two sectors. Only former police officers who join the private sector tend to have a friendly sympathy for the private sector. Usually. police see the private sector as an inferior security group. Therefore, it is difficult to unite with the police in this respect.

Later, Greene, Seamon and Levy (1995) confirmed that tension was also generated even though private and public police joined for the collective benefit of policing in Philadelphia. It seems that the generation of tension is an unavoidable phenomenon as long as two different policing models coexist. Like terrestrial policing, tension continues to be generated in the policing of internet fraud, as the only differing condition is the use of the internet as a criminal tool, the policing bodies remain the same. And. like many issues, tensions are produced when two different models of policing compete for the same target of crime.

Among the many tensions, lack of trust appears to be the most critical one highlighted in the extant literature (Loader, 1997; Johnston, 1999; Nalla and Hummer, 1999). Basically, lack of trust between the two sectors ruins efforts made toward partnership policing from the onset. Johnston (1999) reported that risk minimization in policing is attached to the element of removing lack of trust. Matthews and Cotes (2004) argued that trust is a key aspect of social capital formation at the interpersonal, community level and further institutional level. Abrahamsen (2005) argued that if institutional legal reforms proceed and obstacles such as lack of trust, corruption and cultural differences are tackled, effective partnership policing can be achieved, even in developing nations such as Kenya.

At the beginning of this chapter, lack of resources was mentioned as another tension between private and public models of policing. Previously it was thought of as an individual tension and not linked with other tensions. However, Fleming (2006) reported that lack of resources prevents trust from building in any potential partnership. Simply, insufficient technological, financial and human resources hinder the promotion of partnership policing. It is important to note that lack of trust is not only caused by political, cultural and social factors but also caused through a lack of technological, financial and human resources.

With regard to different investigative philosophies of policing, the private sector does not like to use the public police (Shearing, 1992) since interests of private security are generally client-driven and contractual, while the police are held to standards of public interest (Swanton, 1993). However, the public police, due to the consensual relationship between state and its citizens, are expected to police cybercrime. It may be more practical to establish an appropriate law and policy to define the role and scope of each sector. In particular, not only general cybercrime but also the policing of internet fraud should be clearly included. With regard to the public police, they should maintain and extend this symbolic duty to protect the public interest (Prenzler and Sarre, 1998) and so apply this to internet fraud.

As mentioned above, negative publicity is another factor significantly affecting partnership policing. Usually, private companies are concerned with negative publicity and the subsequent adverse impact on stock value (Braithwaite and Fisse, 1983). Many believe that incident reports to the police have often been disclosed to the public. Therefore, they are reluctant to report incidents despite the fact that immediate reporting makes it easier to police internet fraud. This under-reporting could deter cooperation between private and public policing bodies in the response to internet fraud (Wall, 2006).

According to Sarre and Prenzler (2000: 107), 'law enforcement and corporations that use private security often have incompatible goals and guiding principles, especially when it comes to the issues of reporting crime

and prosecuting offenders'. Private security prefers to deal with Internet fraud through informal justice such as blocking services and warnings of frozen membership, while public police prefer to use the criminal justice system and procedures such as fines and imprisonment.

Clearly, largely dissimilar interests motivate them to claim ownership of policing so that tension is unavoidable between the private and public sector. For the private sector, it is important to protect company assets and customers from any fraudulent activity. For the public sector, it is important to protect taxpayers' assets and citizens from any harmful online activity. However, too many things overlap between these interests. Most private interest is for the public good so that it is difficult to distinguish between the two interests (Swanton, 1993).

Other factors, such as insufficient information sharing between the two sectors have also demoted effective policing activity for internet fraud. Each sector has a different purpose of policing thus some information cannot be shared between the sectors. Sometimes, legal restraints, such as the Data Protection Act in the UK and Personal Information Protection Act in Korea, hinder their sharing of information. Besides, an asymmetric information flow is another problem promoting the ineffective policing of internet fraud. It has been suggested that there should be a balanced two-way communication between the two sectors.

Contrary to general belief, the public police play a small part in policing cybercrime (Sommer, 2004) since they have insufficient resources and knowledge to respond to criminals. Internet fraud is different from other cybercrimes so in many ways it is more appropriate to use a private model of policing. While public police cannot deal with incidents that involve the loss of small values, such as auction fraud (Chua and Wareham, 2004), private security can deal with any case if it is necessary or beneficial.

In terms of loss control and prevention, many private companies such as the telecommunication and financial services industry, employ large number of IT security experts to protect themselves and their customers (EURIM,

2006). They spend more money on policing cyberspace, including internet fraud, than a small nation's annual budget because they have recognized that the potential risk may significantly harm their business activity.

It also appears that the tension between criminal justice and intelligence is not the consequence of a power struggle for the ownership of policing rather different interests and aims carry the tension within the intelligence network (De lint; O'Connor and Cotter, 2007).

3.9.1.2 Tensions within the public sector

Tensions within the public model of policing hinder the development of inter sector cooperation in response to internet fraud. Actually, a study of tensions within the public model of policing internet fraud is a difficult topic to deal with. Without working inside an agency or having special connections to access agency data, it is hard to obtain reliable data. Congressional audit and media reports have often addressed tensions that negatively influence the cooperation of public policing bodies. However, these tensions are only discussed by those within the public sector. Due to the political sensitivity of the issue and potential denial of agencies, third parties tend not to be involved in research on this topic.

As a result, it is even more difficult to reveal tensions concerning the policing of internet fraud within the public sector. Instead, we can `borrow` some tensions within the terrestrial level of policing that are likely to also affect the policing of internet fraud. Among the tensions within the public sector, the most common are overlapping jurisdictions, lack of information sharing and competency.

In cyberspace, there are no clear borders so it is difficult to claim the scope of jurisdiction. Local, state and federal law enforcement agencies have often separately policed and investigated the same crime without recognizing others' involvement. Particularly, internet fraud has been targeted by many public agencies including state funded police and state funded non-police agencies. Extraordinary characteristics of internet fraud have required various policing bodies to respond to it. Unless there is a special law to

assign different jurisdictions and the role of each agency. overlapping jurisdictions problems will continue. It seems that cyberspace is a place with no traffic lights. When every agency wants to claim its cyber jurisdiction, a chaotic situation occurs.

Lack of information sharing has been found among public agencies whether they are state funded police or non-police agencies. Each agency is reluctant to share any merit for the successful policing or investigation while equally. no agency wants to take entire liability. Effective partnership policing cannot be expected if there is no sharing of information within the public sector. Since cybercrime travels over jurisdictions and national borders. the sharing of information is vital to remove internet fraud. As cybercrime has become a transnational problem, establishment of an international information sharing system is imperative.

Lack of competency is 'where cases are passed on from lower to higher levels if it is felt the lower level is not competent to resolve the issue' (Wall, 2002: 202). As long as the transfer case from a lower level to higher-level agency occurs based on mutual trust and respect, it could be considered a good sign of inter-sector cooperation. However, a lower level agency would be discontented if a higher-level agency took over the case without consent, using agency power. This has happened to many centralized national police system nations.

As illustrated above, it appears that different interests and aims of the private and public sectors create tensions and these hinder the development of effective partnership policing between and within sectors. Fundamentally, major tensions are created due to lack of trust, sharing of information and lack of competency. Other tensions also discourage the positive partnership effort between and within two sectors. However, it is assumed that some tensions may become useful motivations for making an effective policing partnership for the prevention of internet fraud.

Positive and negative perspective of tension

Tensions between private and public sectors and tensions within the public sector appear to be quite different from each other. Tensions between private and public sectors are produced mainly due to different interests while tensions within the public sector are produced mainly due to inter-sector competition. Tensions are not always seen as negative factors hindering the development of effective partnership policing. Some tensions are necessary to promote partnership policing between private and public sectors. For example, lack of resources and knowledge of IT within the public sector can be a good reason to invoke the cooperation of the private sector. In particular, investigation of financial fraud cannot be handled by the public sector alone. Cooperation in the investigation by credit card companies and banks is imperative given the complicated nature of the fraud. Therefore, these tensions appear to be very useful factors to invoke partnership policing for internet fraud.

In contrast, some tensions, such as negative publicity and adverse impact on stock value, are good examples of negative tension that can promote partnership policing for internet fraud. These tensions tend to discourage fraud incident reporting by the private sector because these tensions are directly related to the success of their business. Many companies have been disappointed when news of police investigations have exposed their weaknesses to the market and eventually ruined their brand image and company reputation. Actually, negative publicity and adverse impact on stock value are closely related to the downgrading of business reputation. The impact of media sensitization is far beyond our imagination.

Paradoxically, some tensions are useful stimuli to invoke the promotion of partnership policing while others deter their optimistic efforts. It seems that tension contains more negative characteristics than positive. Only some positive tensions described above are considered good stimuli for partnership policing of internet fraud. Thus, both tensions work as a 'check and balance' function in policing internet fraud. However, it appears that there is little evidence to support this assumption. Broadly speaking,

tensions are products of negative relationships. In order to develop a more logical connection between two tensions, the cause and effect of each tension has to be studied in relation to the development of partnership policing for internet fraud.

To summarize, tensions tend to contain more negative than positive characteristics that prevent both sectors from building a positive partnership police for internet fraud. Now, it is necessary to examine how criminological theory and the policing of internet fraud are academically related in order to explain the creation of the new phenomenon of internet fraud as a cybercrime.

3.10 Conclusion

There are three critical reasons why the policing of internet fraud by the public police has been challenged and questioned. Firstly, internet fraud is not an easy problem for the public police to tackle because they lack the requisite knowledge and resources. However, in many countries, the general public tend to think of the public police as the emergency service to deal with all problems. Secondly, the cultural claim by the public police to a greater ownership of policing cyberspace does not square with the fact that the public police only do a small part of that work compared to other networks (Wall 2006: 9). This claim to ownership stems from the traditional Peelian paradigm of the police, which has not only defined the local-police-public mandate but also shaped the organizational and professional priorities of the police whilst framing their 'constitutional' position in the broader framework of policing society (Wall 2006: 11). Thirdly, the primary function of the public police is to police for the public interest, but internet fraud largely takes place in a private domain covered by private interest so corporations tend to want to pursue a private model of justice in order to secure their strength and maintain confidence in the market. This incentive to self-police as determined by 'private interest' is viewed as being in the best interests of the public, despite creating a tension between public and private policing (Wall, 2006).

Tensions between private and public sectors in policing cyberspace are raised due to the different interests each sector has to pursue. Tensions between the private and public sector of policing bodies deter and impede the building of positive relationships. Security experts believe that lack of trust; information sharing, different investigative philosophies, negative publicity, and adverse impact on stock are the most common tensions between two sectors. In addition, Wall (2005: 87) argued that the most affecting examples of tension are 'low levels of prosecution and low levels of recorded Internet fraud'.

Tensions within the public model of policing hinder the development of inter-sector responses to internet fraud. The most common tensions are overlapping jurisdictions, lack of information sharing and competency. Since cybercrimes travel across national borders and jurisdictions, it is imperative to establish close partnerships among agencies internationally. Lack of competency underline the importance of inter-sector cooperation through mutual trust and respect. These tensions illustrated within the sector are the same as tensions between sectors in that cooperation or partnership policing is imperative to respond to rapidly growing rates of cybercrime.

Chapter 4: Policing internet fraud in US Research

4.1 Introduction

Internet fraud is not a major concern for the local and state police agencies since lack of resources and the borderless nature of internet fraud deter them from participating in effective policing. However, federal level agencies are well prepared for the response of internet fraud under full congressional financial support. The toughening up of national security after the 9/11 terrorist incidents make it easier to develop responses to internet fraud on behalf of integrated security systems.

4.2 Who polices internet fraud in the US?

Compared to South Korea and the UK, the policing of internet fraud in the US appears more advanced and well organized. However, the US model of policing depends too much on the public sector. It may be influenced by the law enforcement focused crime prevention programme and anti-terrorism focused national security policy. For the response to internet fraud, IC3 and NW3C are enthusiastically performing their best efforts. Particularly, the US government and Congress provide sufficient budgets to achieve their aims for the prevention and control of internet fraud. It is also important to see how other policing actors in the US practice policing activities for internet fraud. Like other nations, Wall's (2007) 'the internet's order maintenance assemblage' model is also seen in the US.

Internet users and user groups

Internet user and user groups perform similar actions in any jurisdiction against internet fraud because they do not have legal authority and mechanism to respond to it. Like other nations' internet users, most internet users take individual action to report their victimizations to appropriate agencies such as NCL's fraud centre, the Internet Crime Complaint Center (IC3) and National White Collar Crime Complaint Center (NW3C). They directly report serious case to the police. Most cases were found to be online auction and shopping related frauds.

Online virtual environment managers

Online virtual environment managers are 'emerging as a new stratum of behavior governors' (Wall, 2007) and hired to police the behaviour of their virtual environment. My Space, Facebook and Chat Friendz are good examples that show how people monitor the unusual behaviour of their online community. Like other nations' moderators, they use the sanction of 'time out' and 'removal of access' in order to maintain the community norm and rule (Wall, 2007). While more people are using the internet and joining the virtual community, their community has to be policed by these moderators in order to maintain their community value.

Non-government, non-police hybrids

NGOs (non-government organizations) and non-police hybrids are not publically known to us for participation in the policing of internet fraud. It seems that an NGO is in too difficult a position between corporate and government sectors. Generally, private and public sector security systems in the United States respond well to cybercrimes so there is less space for NGOs to take part in policing internet fraud.

Internet Service Providers (ISPs)

Microsoft, Yahoo and AOL are major Internet Service Providers in the US. They have their own security teams to monitor unethical behaviour on their websites. They control online behaviour through 'contractual governance' (Crawford, 2003; Vincent-Jones, 2000). ISP's terms and conditions control behaviour of internet users to represent ISP's interests. Compared to other policing actors, ISPs prefer to excise self-regulation without any governmental intervention. Since ISPs are profit-oriented companies, their policing activities toward customers seem negligible to government agencies.

State-funded non-police groups

The US Securities and Exchange Commission (SEC) is an independent, non-partisan and quasi-judicial regulatory agency with responsibility for administering federal security laws. The mission of the SEC is 'to protect

investors, maintain fair, orderly and efficient markets, and facilitate capital information' (SEC, 2008). The SEC has many divisions for the commission including 'Division of Enforcement'. It is a law enforcement function. This division conducts investigations into violations of securities law. This division recommends the commission to take civil action to the federal court or administrative judge. Criminal cases are often referred to other law enforcement agencies by this division. These days, this division closely monitors fraudulent activity online because investors use the internet as a primary tool for transactions.

The US Financial Crimes Enforcement Network (FinCEN) was established in 1990 by the US Treasury Department to fight against financial crime under the BSA (Bank Secret Act), especially drug money laundering. Actually, FinCEN does not directly relate to internet fraud. However, BSA's requires recordkeeping and 'to establish financial trail for investigators to follow as they track criminals, their activities and their assets' (FinCEN, 2008). Though its database, FinCEN supports all kinds of financial investigation. Recently, its scope has been expanded to internet fraud because financial related frauds are committed over the internet.

The Federal Trade Commission's Bureau of Consumer Protection works for the prevention of fraud, deception and unfair business practice in the market place, it takes online complaints from victims of internet fraud, provides useful information to avoid internet fraud, and enforces federal laws to protect consumers (FTC, 2008).

The Internet Crime Complaint Center (IC3) provides a central referral service to the law enforcement and regulatory agencies at local, state, federal and international levels. IC3 has a partnership with the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C) and the Bureau of Justice Assistance (BJA).

For the response to internet fraud, IC3 has provided an easy to use reporting system for victims (IC3, 2008). IC3 is a hub of internet crime response. Below Figure 4-1 shows how to file a complaint with IC3.

Figure 4-1: IC3 complaint manual

Filing a Complaint with IC3

IC3 accepts online Internet crime complaints from either the person who believes they were defrauded or from a third party to the complainant. We can best process your complaint if we receive accurate and complete information from you. Therefore, we request that you provide the following information when filing a complaint:

- Your name
- Your mailing address
- Your telephone number
- The name, address, telephone number, and Web address, if available, of the individual or organization you believe defrauded you.
- Specific details on how, why, and when you believe you were defrauded.
- Any other relevant information you believe is necessary to support your complaint.

File a Complaint >>

(Source: http://.ic3.gov/default.aspx\)

NW3C is a congressional funded, non profit corporation that supports the law enforcement agencies and prosecution offices at local, state and federal levels. It does not have any investigative authority but its main role is to help other law enforcement agencies to fight against economic and high tech crimes. For the response to internet fraud, NW3C provides analytical services to other agencies such as the Internet Crime Complaint Center (IC3) and White Collar Crime Research Consortium (WCCRC) in order to increase public awareness (NW3C, 2008). Thus, the policing of internet fraud by the NW3C cannot be seen by internet users. It is only recognized by the law enforcement agencies and regulatory bodies.

State-funded police

The United States Department of Justice website introduces appropriate law enforcement agencies that will respond to internet fraud: FBI local office. The US Secret Service (Financial Crimes Division). The FBI has local

stations in major cities. Those local stations receive complaints directly from victims or local police departments. Since internet fraud is a borderless crime, local offices report to the headquarters for a nationwide response.

The US Secret Service's financial division is well known for counterfeit and other economic crime investigation. Along with the growth of e-commerce and internet fraud, Secret Service has expanded its policing activity to internet fraud. With the financial division, the Electronic Crimes Task Force (ECTF) prioritizes to conduct investigations about e-crimes that significantly affect the community (US Secret Service, 2008).

Corporate security

US corporate organizations have advanced security systems in domestic and international offices to protect their assets and interests. Internationally renowned telecommunications firms, banks and credit card companies police their websites to prevent any possible threats from fraudsters or other criminals. They are: IBM, Yahoo, Apple, Oracle, Bank of America, Wells Fargo, VISA and Master Card Company. Their policing activities involve risk management software and other technological methods. However, their detailed activities are not publically introduced because corporate organizations tend not to disclose their special know-how to others. Large corporations have practiced two different ways to police their virtual spaces: in-house security and contract-out security. For internal security, they tend not to hire outsiders to police their intranet.

4.3 Internet fraud law in the US

Internet fraud is covered by the Fraud law in the US, which is the area of state and federal law that defines fraudulent acts, provides a means to prosecute fraudsters, and describes the type of punishment that guilty fraud criminals may confront. Fraud is defined generally as a deceptive illegal act committed in order to secure unfair or unlawful financial gain at the expense of others. Fraud law is also commonly referred to as white collar crime law (Freidrichs, 1996). Sub-categories of fraud law outline and enforce statutes based on specific types of fraudulent activity. Fraud law covers fraudulent

acts carried out through the internet such as phishing. pharming and voice phishing.

Originally, fraud law was enacted in order to protect consumers and other victims from the serious damages that can be caused by fraudulent actions. Both federal and state governments have enacted fraud law and have assigned various agencies to help enforce fraud law. Either a civil or criminal law can be applied, depending on the circumstances and the severity of the crime. Punishment for fraud law violation can range from fines to imprisonment. Punishments for fraud law violation are often much harsher for corporations than for individuals. For example. the Enron scandal in 2002 resulted in the demise of Arthur Anderson, which was internationally the largest accounting firm. However, shredding of Enron working papers and communications led to a conviction on the grounds of obstruction of justice (Cornwell, 2002).

Fraud law also provides consumers and victims of fraudulent acts with legal remedies so that they may be able to seek compensation for their losses. Although fraud law specifics vary by state and circumstance, most fraud law has a statute of limitations which provides for the amount of time in which a fraud lawsuit can be filed. Many government and regulatory agencies have complaint departments, such as IC3 and NW3C, where you are able to file a fraud law violation.

The US CODE: Title 18, 1030

For internet fraud, the US CODE: Title 18, 1030 describes fraud and related activity in connection with computers.

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or

to the advantage of any foreign nation wilfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or wilfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any non-public computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5) (A)

(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety; or

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States;

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is—

(1)

(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)

(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if—

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)

(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)

(A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and

(5)

(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and

(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.

Hardening of cyber security/ Patriot Act

After 9/11, the US government enacted the PATRIOT Act that allows federal law enforcement agencies to look up any e-mail and electronic message for the protection of the national security purposes (Golden. 2004). Private companies and ISPs must comply with their requests to provide all necessary information. It is not an exaggeration to say that all American internet users are under surveillance. The American Civil Liberty Group argued that the Patriot Act violates rights to free speech and due process (Golden, 2004). The partnership between private and public has never been better than now. This hardening of national security due to terrorist activity has brought a chain effect to all areas of security in the United States (Conrades, 2004). In this case, under the special circumstances caused by breach of national security, internet users' rights have been significantly limited. It seems that there has been a potential conflict between cyber-rights and anti-terrorism initiative (Cameron and Vaile, 2006).

In the light of cyber-rights. the US Patriot Act has had a significant impact on internet users regardless of the national security matter. This shows that

internet users and governments have to choose the correct balance between cyber-rights and cybersecurity for the national interest. The American case could be used as reference for making other nations' cybersecurity laws and policies since the American's 'war on terrorism' policy and practice has rapidly affected many other nations in many aspects. for example. enhancement of international airport security reflects how other nations have been affected by the American 'war on terror' (Enders, 2002). In this sense, there is a possibility that hardening of cybersecurity law may extend to other nations that do not have serious terrorist threats. Amoore and Goede (2005) reported importance of risk management in 'war on terror' because terrorism has given a chilling effect to every business, from border control to international financial transactions that are directly related to internet fraud.

To illustrate how the policing of internet fraud works, Kozlovski's cyberpolicing model will be used to explain the transformation of policing from law enforcement to cyberpolicing. This model will help us to understand the transformation of policing as it occurs through the emergence of the internet.

4.4 How do public and private sectors police internet fraud in the US?

Policing internet fraud by the public sector

In response to internet fraud, NW3C and the FBI created the Internet Fraud Complaint Center (IFCC) (Grazioli and Jarvenpaa, 2003). Later, the IFCC changed its name to the IC3[5] and it has become a leading anti-fraud response centre that has strong partnerships with NW3C and the FBI.

Another large federal agency, the National White Collar Crime Center (NW3C) is a congressionally funded organization that provides a

---

[5] The Internet Fraud Complaint Center (IFCC) was established by the Department of Justice in 2000. For the law enforcement agencies, IFCC provides the Information referral service. Later, the IFCC was later renamed the Internet Crime Complaint Center (IC3) in October 2003 in order to respond to rapidly expanding area of cybercrime and it has a partnership with the FBI and NW3C (http://www.ic3.gov).

nationwide support system to law enforcement agencies for preventing, investigating, and prosecuting economic and high tech crimes (NW3C, 2008).

Other federal agencies that are not directly related to the response of internet crime such as the Fair Trade Commission (FTC) and the Food and Drug Administration (FDA) have proactively participated in policing internet pharmacies related fraud. They have focused on drug and healthcare related fraud. For example, they warned a website operator who had a misleading and deceptive website about SARS (Severe Acute Respiratory Syndrome) to remove the false information. Fraudulent information gathered through the FTC surfing the internet is coordinated with the help of the FDA and the Ontario Ministry of Consumer and Business Services. These kinds of fraudulent activities have resulted in large numbers of victims and monetary damage (FTC, 2003). It is said that 'firms or individuals who violate the FTC Act could be subject to a federal district court injunction, enforceable through civil or criminal contempt proceedings, or an administrative cease and desist order, enforceable through civil penalties of up to $11,000 per violation' (FTC, 2003). As approximately 100 million Americans use the internet to find health information, the need for enforcement is greater than ever since the fraudster can create a bogus website whenever necessary.

The Federal Bureau Investigation (FBI) is a main investigative authority in the federal case although it does not stand at the frontline of fighting internet fraud. The FBI has a partnership with the Internet Crime Complaint Center (IC3) and National White Collar Crime Complaint Center (NW3C) and receives serious cases from them for further investigation. The FBI usually intervenes when IC3 or NW3C refer cases that involve criminal matters. Due to the restriction of human rights and privacy, its proactive cyber policing is limited to the hacking of national infrastructure and communication systems (FBI, 2008).

Policing internet fraud by the private sector

For the private sector, many companies have their own security measures for dealing with internet fraud. There is no unified model of policing internet fraud known to the public. Each company and sector has different concerns and vulnerable points for the fraudster and other criminals because of different products and services they provide to their customers. Usually, private companies have hired in-house IT security teams or contracted-out IT security services to protect their valuable assets and customer information from possible threats (Bartley, 2001).

Internet Service Providers have their own security measures and reporting systems to deal with internet fraud. However, their activities are limited to their networks. They usually involve preventive modes of security measures such as filtering systems, firewalls and anti-virus software. Customer reporting is particularly important to help the ISP respond to internet fraud. Without support from individual users, the ISP does not properly respond to it as a non-police entity. Like a terrestrial level of policing, community support through reporting crime is a key factor for successful and effective control and prevention of internet fraud.

4.5 Relationship between law enforcement agencies and private security

The current partnership for internet fraud is seen as the 'Ad-Hoc partnership model' which was introduced by Sarre and Prenzler (2000). This model entails private and public sectors working together whenever necessary. There is no regular basis for joint work, but for the response to internet fraud good working partnerships have been emphasized. However, the private sector tends not to report to law enforcement due to lack of trust, negative publicity and fall of stock value. In order to resolve these issues, IC3 (Internet Crime Complaint Center) and NW3C (National White Collar Crime Center) were established with the support of the FBI (Federal Investigation Agency) and the congressional fund. These agencies have become buffers between private and public sectors in order to reduce their concerns. Private security firms usually do not want to contact law

enforcement agencies unless there is an imminent threat. In this sense. IC3 and NW3C are very useful channels through which private companies can report internet fraud. These agencies are likely to solve problems by themselves and report to the law enforcement agency depending on the seriousness of the incident (IC3, 2008).

4.6 Transformation of policing cybercrime

Kozlovski's (2005) 'paradigm shift in policing from law enforcement to cyberpolicing' introduces the appropriate policing model for the response of internet fraud. Kozlovski (2005) argued that the law enforcement strategy does not appropriately respond to the quickly developing cybercrime. According to Kozlovski, existing assumptions about law enforcement are out of date in terms of deterrence effect, jurisdiction and successful investigation and prosecution. More precisely, lack of investigative knowledge, low levels of prosecution, geocentric policing and punishment expectancy within the public model of policing were criticized. In the meantime, a social preference for private policing was also emphasized. Cost of crime prevention, protection of privacy and prevention of lawful activity were considered. In addition, private interest was also an important factor to consider the paradigm shift from law enforcement to cyberpolicing.

Kozlovski (2005) summarized the characteristics of the policing strategy (see Table 4-1). The cyberpolicing strategy reveals a very different approach for dealing with cybercrime. Overall, it tends to depend more on preventive measures based on proactive tactics and is intelligence focused. while the law enforcement model depends on reactive and evidence-based investigation. The cyberpolicing strategy is more appropriate for internet fraud because most cybercrimes are not crime but harms. Therefore. regulation through code, non-discretionary and non-judicial sanctions fit them better. Besides, active victimization is different from the terrestrial level of crime.

Table 4-1: Policing strategy

Law Enforcement	**Cyberpolicing**
Reactive	Proactive tactics
Evidence based investigation	Intelligence focused
Law as primary regulator	Regulation through Code
Discretionary enforcement	Automated, non discretionary
Deferred judicial sanction	Present non-judicial sanctions
Passive victim	Active victim
Criminal focused	Intermediaries focused

Source: http://crypto.stanford.edu/portia/talks/online_policing_model.ppt

As presented in Table 4-1, law enforcement structures indicate a totally different structure from that of the cyberpolicing model. It appears that the law enforcement structure is similar to a military structure. Compared to cyberpolicing, the overall structure of law enforcement is quite simple and centralized. Its policing activity is limited to the geocentric and terrestrial level. It tends to limit delegation of policing power and individual use of force.

However, the organizational structure chart by Kozlovski indicates (see Table 4-2) that cyberpolicing has a more complicated, decentralized and internationalized structure than that of law enforcement. In contrast to the law enforcement structure, delegation of policing function and empowerment of the individual are more widely admitted. These characteristics are similar to the multi-tiered governance structure suggested by Wall (2001).

Table 4-2: Organizational structure

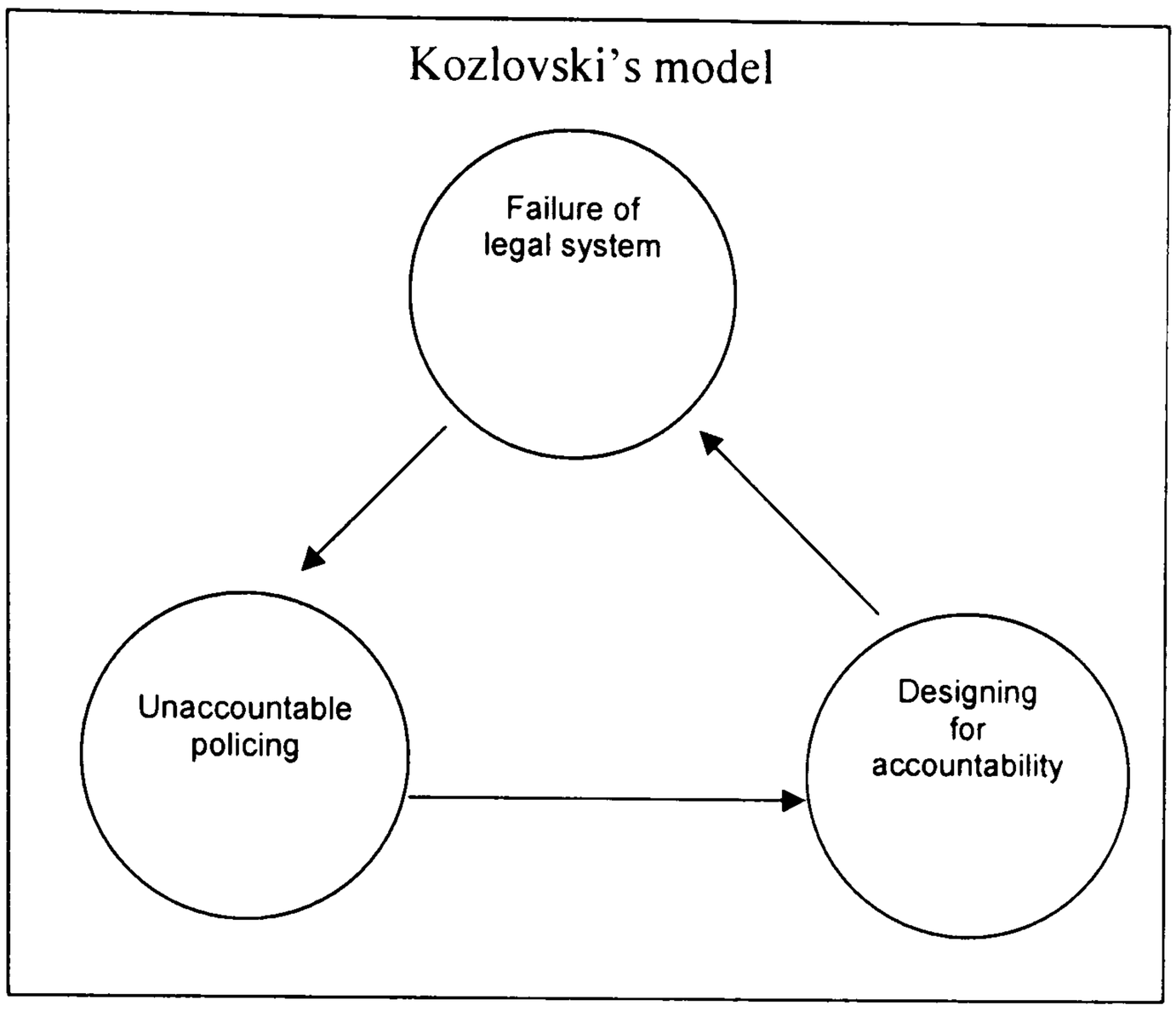
Law Enforcement	**Cyberpolicing**
Public officials	Multiplex organizational structures
Central command	Decentralized
Territorial	Non territorial. internationalized
Limits on delegation of policing power	Delegation of policing function
Limits on individual's use of force	Empowerment of the individual (self help)

Source: http://crypto.stanford.edu/portia/talks/online_policing_model.ppt

The significance of Kozlovski's model is in explaining why law enforcement structures do not appropriately respond to cybercrime. While American law enforcement enhanced its federal law enforcement power after 9/11, the shift from law enforcement to cyberpolicing structure could generate the misconception of diffusion of policing power. However. Kozlovski's model innovatively demonstrates how the policing of cyberspace has to be changed. In particular, participation of the individual user is emphasized. This is the most important aspect of cyberpolicing. Wall (1998: 205-206) stated that 'the Internet is renowned for "voluntary policing" of the activity of users'.

Kozlovski's model (see figure 4-2) proposed three main research questions that are relevant to this thesis concerning reduction of tensions. The configuration of figure 4-2 is based on comparison contents in Tables 4-1 and 4-2. Figure 4-2 indicates the three main concerns that the current criminal justice system has to deal with. The first concern is 'the failure of the current legal system to control cyberpolicing'; this is public official and reactive model focused. The second concern is 'unaccountable policing' which considers the lack of set rules, policing policies and actual enforcement. The third concern is 'designing for accountability' and refers to the fact that 'legal, institutional, and technological settings of conventional law enforcement are based on the conditions of physical crime scenes and fail to transfer smoothly to the online [environment]' (Kozlovski, 2007: 108).

Figure 4-2: Kozlovski's major concerns in the current criminal justice system



The emerging cyberpolicing is different from offline policing: 'it is mainly preventive, highly decentralized, a hybrid of public and private enforcement, and highly automated'. It 'calls for the ubiquitous policing of online activities to monitor, control, deter, deflect, detect, prevent, or pre-empt risky and potentially malicious activities' (Kozlovski, 2007: 107). It requires the establishment of new laws to embrace this cyberpolicing model. For example, the Fraud Act 2006 in the UK supports the policing of cybercrime by including 'phishing' as a crime.

In order to enhance a safe online environment, 'it is imperative to design an accountable policing model' (Kozlovski, 2007: 108). This model could be a 'multi-tiered policing model' and relate to 'The Internet's order-maintenance assemblage' suggested by Wall (2007).

Kozlovski (2007) stated that new technology requires new institutions to supervise policing, and value-driven design now demands legal procedures that are better shaped to support policing to be accountable. Policing internet fraud may require the establishment of new institutions to supervise its policing activity, such as SOCA in the UK.

Kozlovski's (2007) 'designing accountable online policing' emphasized the transformation of policing for cybercrimes. A shift from law enforcement to a cyberpolicing model is imperative to provide an effective policing service to the public. Cyberpolicing aims to prevent and pre-empt crime rather than to prosecute. This policing model relies on non-legal restraints such as technology, network, and social construction of particular users of computers. The new policing is a hybrid form and tends to rely more on the private sector. The hybrid architecture of cyberpolicing takes advantage from optimizing the allocation of responsibilities between the centre (centralized) and the edge (decentralized). The regulation of victims and third parties becomes important. The notion of open intelligence establishes a new information sharing architecture. While a self-help sanction is widely adopted by the individual user. For example, use of upfront exclusion and virtual imprisonment. Online identification processes have become important to cyberpolicing since the internet is the anonymous users' heaven. Cyberpolicing relies heavily on non-content data such as traffic data and automated system logs for the investigation of cybercrime. Overall, it appears to be very similar to David Wall's 'transformation thesis' (Wall, 2007: 4).

Fundamental to this analysis, the policing of internet fraud is a newly emergent form of policing cybercrimes. Whether Kozlovski's cyberpolicing model is satisfactorily adopted for policing internet fraud or not, this model introduces a different approach to policing strategy that is more appropriate for the response to internet fraud.

4.7 Development of multi-sector agency partnership

After the 9/11 terrorist incident, the US government enhanced the national security by establishing the DHS (Department of Homeland Security). The DHS uses resources within federal, state, and local governments to coordinate 'the transition of multiple agencies and programmes into a single, integrated agency focused on protecting the American people and their homeland. More than 87,000 different governmental jurisdictions at the

federal, state, and local level have homeland security responsibilities.' The DHS believes that 'partnership between the public and private sectors is essential, in part because the private sector owns and operates approximately 85% of the nation's critical infrastructure' (DHS, 2008).

For the protection of critical infrastructure, CIPAC (Critical Infrastructure Partnership Advisory Council) 'provides the operational mechanism for carrying out the sector partnership structure. The CIPAC provides the framework for owner and operator members of Sector Coordinating Councils (SCC) and members of Government Coordinating Councils (GCC) to engage in intra-government and public-private cooperation, information sharing, and engagement across the entire range of critical infrastructure protection activities'(DHS, 2008). Although CIPAC shows an effective operational mechanism for the partnership structure, it does not aim to respond to internet fraud. Therefore, it is necessary to establish a separate partnership model for the multi-sector agency.

In order to promote the partnership, an understanding of the 4Cs (Communication, cooperation, coordination, and collaboration) is essential: communication emphasizes the sharing of information; cooperation emphasizes the joint operation and sharing of personnel; coordination emphasizes the common goal of crime prevention; collaboration emphasizes the understanding of partner's 'mission overlap and adopt policies and projects designed to share resources, achieve common goals, and strengthen the partners' (BJA, 2005: 5).

The Bureau of Justice Assistance (2005: 5) reported that there are 12 components to promoting successful law enforcement and private security partnership.

- Common goals
- Common tasks
- Knowledge of participating agencies' capabilities and missions
- Well-defined projected outcomes
- A timetable

- Education for all involved
- A tangible purpose
- Clearly identified leaders
- Operational planning
- Agreement by all partners as to how the partnership will proceed
- Mutual commitment to providing necessary resources
- Assessment and reporting.

The US Department of Homeland Security (DHS) recommended nine guidelines for law enforcement agencies that seek to improve collaboration with their private partners (BJA, 2005:6). These nine guidelines can be applied to law enforcement agencies and government regulatory bodies participating in policing internet fraud.

- Recognize the need for prevention.
- Establish a system, centre, or task force to serve as a clearinghouse for all potentially relevant domestically generated terrorism information.
- Ensure timely interpretation and assessment of information.
- Prepare Memorandums of Understanding (MOUs) and formal coordination agreements between public and private agencies. MOUs should describe mechanisms for exchanging information about vulnerabilities and risks, coordination of responses and processes to facilitate information sharing and multijurisdictional pre-emption of terrorist acts.
- Use community policing initiatives, strategies, and tactics to identify suspicious activities related to terrorism.
- Explicitly develop 'social capital' through collaboration among the private sector, law enforcement, and other partners so that data, information, assistance, and 'best practices' may be shared and collaborative processes developed.
- Coordinate federal, state, and local information, plans, and actions for assessments, prevention procedures, infrastructure protection, and funding priorities to address prevention.

- Establish a regional prevention information command centre and coordinate the flow of information regarding infrastructure.
- Include prevention and collaboration measures in exercises.

These nine guidelines are also evoked with a complex network for policing internet fraud to promote partnership policing from the perspective of the private sector. In contrast to the public sector, the diversity of profit organizations makes it difficult to create guidelines for the private sector. Fortunately, relationships between private and public sectors in the US have been developed to achieve common goals for crime prevention and avoidance of terrorism, meanwhile the policing of internet fraud resides within them.

4.8 Barriers to policing internet fraud

There appears to be no academic data or literature showing the kind of factors which negatively impact upon the policing of internet fraud. However, it is believed that in many ways it retains great similarity with the policing of cybercrime, because internet fraud shares many points with the characteristics of cybercrime: lack of trust, negative publicity and adverse impact on stock value (Wall, 2007). Compared with other cybercrime, internet fraud is more pertinent to economic crime. Therefore, the private sector tends not to report to the police unless they cannot directly handle the case.

At the operational level, the two sectors do not cooperate with each other. Too many different interests create conflict between the two sectors, while victims want to recover their loss as soon as possible. The absence of mandatory reporting law is accredited for discouraging the partnership policing of internet fraud (Smith, 2005). Although there are a few non-police channels to report incidents, private companies tend to solve problems within their organizations. eBay and other auction companies directly receive complaints from their customers and hold victims until they find a solution. Fraudsters are aware of the complaint procedure and thus take advantage of delayed investigation due to lack of cooperation. This

suggests that the best way to deal with this is to establish partnership for policing internet fraud.

4.9 Tensions between private and public sectors in policing internet fraud in the United States

Only a few academic literatures have introduced tensions that are produced between private and public sectors in policing. It is believed that tensions are generally created due to lack of trust and sharing of information, different investigative philosophies, negative publicity, and adverse impact on stock (Shearing, 1992; Greene, Seamon and Levy, 1995; Connors, Cunningham and Ohlhausen, 1999; Rigakos, 2002; Crawford, Lister and Wall, 2003; Delint, 2005; Joh, 2004; Bhanu and Stone, 2004: Ferret, 2004). It is assumed that tensions between private and public sectors in policing internet fraud in the US are somewhat different from that of the United Kingdom. As introduced in the earlier section, NW3C and IC3 have become hubs for reporting internet fraud. They have created buffers to reduce tensions between the two sectors, although large corporations tend to solve problems internally. Tensions are created where private and public interests are too different. Large global corporations would like to avoid any potential threat that may cause negative publicity and adverse impact on stock value. Since they are profit organizations, protection of their assets is the highest priority. In order to protect their assets and personnel allocated worldwide. they have well equipped security systems. Some global corporations, such as IBM, HP and Microsoft, spend huge amounts on security. costs which are in excess of a small nation's annual security cost.

Global corporations would like to handle security breaches themselves in order to protect their brand image. During the initial stage of investigation, the public police are temporary excluded. Unless public intervention is obligatory, global corporations tend not to ask for help from the public sector. Since they often hire former federal law enforcement agents and national intelligence experts, their policing and investigative capabilities are way ahead of local or regional law enforcement agencies. As indicated earlier in Chapter 3, the FACI (Forensic Accounting and Corporate

Investigation) industry has enabled great advances in the capabilities of financial crime investigation.

As illustrated above, lack of trust between the two sectors has created hostile working environments when responding to internet fraud. Lack of trust has also created other tensions. If the two sectors trusted each other, other tensions would disappear. However, the fact that the two sectors pursue different interests means they cannot completely resolve this problem: the private sector's interest focuses on maximizing its profit while the public sector focuses on maintaining law and order. Their reasons for policing and investigation are totally different, while the mutual goal of crime prevention has to be maintained. Thus, it is felt that building trust is the most important factor for working together.

Lack of sharing information is considered another serious tension between the two sectors. Information is a very valuable asset in the digital era so no one provides it without reward. It is more seriously considered in the business and political environment. Sharing of information usually occurs to obtain mutual benefit for all parties involved. Through exchanging useful information, both sectors are enabled to perform effectively in policing internet fraud. When a law enforcement agency provides warning signs for possible threats, such as phishing and pharming, private companies prepare for the threat and educate their customers for prevention. This kind of information can be provided to achieve the goal of public interest. It shows that information flows from the public to private sector appear to be routine activities in terms of public service. When information flows from the private sector to the public sector, it shows a slightly different trend. It seems that the private sector is more concerned about their information going to the public sector. Particularly since some information contains very sensitive company secrets or business know-how, this could provide knowledge to the public through which it might be possible to attack the company, financially or with a business scandal. Private companies believe that the police do not properly protect their information and often leak to the media or outsiders. For these reasons, private companies tend not to report incidents to the police or other law enforcement agencies.

Different investigative philosophy is another tension between the private and public sector security. As explained in Chapter 3, each aim of policing is different since each sector has a different interest. Private companies police internet fraud for crime prevention and loss control, while public police and regulatory bodies police internet fraud for the maintaining of law and order and for public safety. Accordingly, private companies want to retrieve their loss in case of internet fraud investigation. At the same time, they would like to conduct investigations confidentially. They worry about any negative publicity occurring if news of incidents is released to the public. On the contrary, public police and other law enforcement agencies have to achieve the goal of public safety and the maintaining of law and order. Since their policing activity and investigation is funded by public taxes, they work for the public's interest. Therefore, public police would not provide any favour while conducting an investigation.

Negative publicity is another reason why private companies tend not to report incidents to the police. When news of an incident is publicized, a private company may suffer a knock to its good reputation and brand image. Although a law enforcement agency may promise to keep confidentiality in the investigation, it is difficult to keep the promise. The private sector recognizes the potential threat due to negative publicity. Unless there is a law to promise a confidential investigation, many companies hesitate before reporting an incident to a law enforcement agency. Realistically, it is difficult to enact the law while promising confidentiality in the investigation. Some private interests are also public interests. Imagine that personal information stored in Facebook or My Space is hacked by someone. This kind of incident not only damages the private interest but also public interest. It has become more difficult to distinguish between private and public interest. The information society and digital technology have integrated these interests into one. Since virtual space can not belong to one sector, an overlap of interest always exists between the two sectors. Besides, it is difficult to find any justification for protecting confidentiality and private interest while spending public taxes doing the investigation. Therefore,

negative publicity cannot be removed unless there is a law which will promise the protection of private interest.

Finally, adverse impact on stock value is another tension existing between the private and public sectors. This tension is closely related to negative publicity since it could adversely affect stock value. Private companies have always attempted to maximize their profit and protect their assets through in-house security or contract-out security services. Private companies are afraid of adverse impacts on stock value which can occur upon disclosure of an incident. Sometimes, massive amounts of negative publicity surrounding a company may result in the collapse of a company. A similar incident occurred in the 'Enrol Scandal' of 2001[6]. Enron shares dropped from over US $90 to less than 50cent. Also, e-commerce is facing more risky situations than other business types. In order to remove this tension, special law needs to evolve to secure stock prices while law enforcement conducts investigation into internet fraud incidents (WIKIPEDIA, 2008).

4.10 Conclusion

The policing of internet fraud in the United States is mainly carried out by federal law enforcement agencies, government regulatory bodies and the corporate sector security. Compared with the United Kingdom, the US internet fraud policing model does not really assign much importance to non-government, non-police hybrids. This may be attributed to the

---

[6] The Enron scandal was a financial scandal involving the Enron Corporation (former NYSE ticker symbol: ENE) and its accounting firm Arthur Andersen, that was revealed in late 2001. After a series of revelations involving irregular accounting procedures conducted throughout the 1990s, Enron was on the verge of bankruptcy by November of 2001. A white knight rescue attempt by a similar, smaller energy company, Dynegy, was not viable. Enron filed for bankruptcy on December 2, 2001.

As the scandal was revealed, Enron shares dropped from over US$90.00 to less than 50¢. As Enron had been considered a blue chip stock, this was an unprecedented and disastrous event in the financial world. Enron's plunge occurred after it was revealed that much of its profits and revenue were the result of deals with special purpose entities (limited partnerships which it controlled). The result was that many of Enron's debts and the losses that it suffered were not reported in its financial statements.

dichotomy of policing internet fraud still taking place in the United States. There is no coverage for NGOs actively taking part in policing internet fraud. From the optimistic point of view, US law enforcement agencies and government regulatory bodies are well prepared to respond to internet fraud. As Kozlovski (2007) suggested. the traditional law enforcement model for cybercrime has been transformed to the cyberpolicing model. It emphasizes ubiquitous policing and individual participation of cyberpolicing. With the transformation of the policing of cybercrime, multi-sector agency partnership has been enhanced through government policy and forums such as CIPAC (Critical Infrastructure Partnership Advisory Council). Sector Coordinating Councils (SCC) and members of Government Coordinating Councils (GCC) promote intra-government and public-private sectors cooperation. However, CIPAC does not exist for the development of multi-sector agency partnership policing of internet fraud. Thus, it is imperative to establish an independent council or organization for coordinating a multi-sector agency for responding to internet fraud.

Chapter 5: Policing internet fraud in South Korea

5.1 Introduction

'Policing internet fraud' is becoming a very important task for both the public and private sectors since rapidly growing levels of cybercrime are costing individuals and businesses billions of dollars across the international jurisdictions. For effective policing, a cooperative effort between the public and private sector is essential. However, inherited structural barriers of the public sector and legal and political barriers of the private sector tend to hinder the development of policing cybercrime.

As briefly introduced in Chapter 3, David Wall (2007) has clearly classified seven different groups who currently police cyberspace. His internet order maintenance assemblage table is well defined in relation to each entity's role and sanction. Among the seven tiers the 'online virtual environment and security' tier (see Table 3.1) is the most recent addition. This updated assemblage emphasizes the importance of self-regulation of ISPs, is to be discussed later in this section.

The internet user and user groups are the smallest policing actors in the networks and nodes of security within cyberspace, but are the most numerous. They exercise significant power to control the online behaviour through criticism of some events or crimes (Wall, 2007). Individual users employ a wide range of software solutions such as firewalls, spam-filters and anti-virus vaccines to prevent themselves from victimization of cybercrime. 'Working on a self-appointed mandate, the Internet users are simultaneously auspices and providers of governance' (Wall, 2007: 167).

Diverse and self-appointed memberships often lack formal mechanisms of accountability for their action. Sometimes, internet users commit illicit and illegal acts before they realize it. Fortunately, there are many socially beneficial user groups working for the public interest such as anti-spam, anti-phishing and anti-pornography groups. For the individual user's level

of policing, eBay's online auction trading partner profile rating system is a good example of peer-policing (Haywood, 2006, Wall, 2007).

Online virtual environment managers and security managers are people who 'police the behaviour of their online community' (Wall, 2007: 169). They have to ensure that norms and rules are maintained in their virtual community. If any breaches occur, sanctions might be imposed to the violators. Sanctions vary from temporarily freezing accessibility to permanent exclusion from the community, depending on the seriousness of violation.

ISPs (Internet Service Providers) are important policing groups since they work as 'gatekeepers' of cyberspace through 'contractual governance' (Crawford, 2003; Vincent-Jones, 2000). They use 'terms and conditions of contract' as a tool to control the behaviour of their client, the internet users. According to Wall (2007), market, law and the interest of the ISP form those terms and conditions. In terms of service providers, ISPs are also subject to contractual governance through the terms and conditions laid down in individual contracts between each telecommunications provider. ISPs also have to provide necessary online security services for their customers. Recently, ISPs have suffered from much litigation, which has exerted a 'chilling effect'. ISPs have to respond to numerous demands, ranging from individuals to the police, to remove offensive material whether obscene or not. According to Wall (2007: 171), 'ISPs tend to organize themselves both within specific jurisdictions and across them with a further level of transnational organizations, for example the Commercial Internet exchange, the Pan-European Internet Service Provider's Association: EuroISPA and Internet Providers' Consortium (mainly US)'. In addition, under the oversight of ICANN (the Internet Corporation for Assigned Names and Numbers), ISPs are domain name registries (EuroISPA, 2008)

Corporate organizations exercise their contractual governance over both employees and clients and any other outsiders in order to protect their corporate interest (Wall, 2007). Contractual terms and conditions warn of cancellation of services or civil and criminal litigation in case of serious

violation. As e-commerce developed, corporate security organizations became major players of policing cyberspace. However, their policing activity is not exposed to the public since they have to protect the confidentiality of their private interest. They also tend to pursue the 'private model of justice' since the criminal justice model does not reflect what private companies want to do (Wall, 2001). Corporate security organizations tend to work independently in order to achieve their corporate interest although there is less support from the public sector.

Non-governmental, non-police organizations 'contribute to the order maintenance assemblage by acting as gatekeepers to the other level of governance, but also contributing towards cybercrime prevention' (Wall, 2007: 172). Internationally, many NGO groups provide governance of cyberspace under the auspices of mandates from governments. The Internet Watch Foundation (IWF) in the United Kingdom and Computer Emergency Response Team (CERT) in the United States are good examples of non-governmental/non-police organizations. However, according to Wall (2007: 173-174), 'they tend to lack the formal structure of accountability normally associated with public organizations and sometimes find themselves the subject of public concern'.

Governmental non-police organizations 'provide governance under the auspices of regulations, rules and law through charges, fines and the threat of prosecution' (Wall, 2007: 174). For example, KISA (Korea Information Security Agency) indirectly controls internet users through government-controlled ISPs. By law, all Korean ISPs have to report any significant incident to the KISA.

In the United Kingdom, CPNI (Centre for the Protection of National Infrastructure) was formed in February 2007 out of the merger of the National Infrastructure Security Co-ordination Centre (NISCC) with the National Security Advice Centre (NSAC - part of MI5). CPNI provides integrated (combining information, personnel and physical) security advice to the businesses and organisations which make up the national infrastructure' (CPNI. 2008). Like KISA, UNIRAS (The Unified Incident

Reporting and Alert Scheme) receives IT security incidents in government departments and agencies in the UK. Similar to KISA and UNIRAS. the National Infrastructure Protection Center (NIPC) in the US is responsible for the protection of the national critical infrastructures (Wall, 2007).

Public police organizations are known to provide a small portion of policing of cyberspace in Western countries. However, policing capabilities vary from simple investigation to the international cooperation of cybercrime prevention. In contrast to local police, federal and national police organizations provide more effective policing. In the US, the FBI and US Secret Service are the main bodies of policing cybercrime. They are responsible for investigating crimes related to multi-jurisdiction crime and federal law violation. In the UK. SOCA (Serious Organized Crime Agency) took over the National High Tech Crime Unit (NHTCU) as a SOCA's e-crime unit in 2006. SOCA is a UK version of FBI or US Secret Service. Compared to other Western countries, Korea's National Police Agency has unique capabilities to respond to cybercrimes. More than 230 local police departments have almost the same capacity as the headquarters (Cyber Terrorism Response Center) in terms of investigation competence. CTRC is linked with the all-local police forces so that there is no technological gap between headquarter and branches.

5.2 Who polices internet fraud in South Korea?

Both the private and public models of policing have dealt with policing internet fraud in South Korea since the negative impact of internet crime significantly affects both groups' interests. However, the importance of the private sector policing internet fraud has not been discussed in Korea. This is due to the perceptions of 'policing' as related to the police and other law enforcement agencies. Therefore, it is unthinkable for the private sector to use the word 'policing'. The private sector uses the terminology 'private security' to replace the negatively stigmatized term 'private policing', although they in fact participate in the same 'policing' activities. Thus, the concept of policing internet fraud by the private sector in Korea is inertly

limited to preventive IT security activities by financial institutions, such as banks, credit-card-companies and stock companies.

Only a few criminal justice academics and security experts are aware of the terminology 'policing' and there is an even greater lack of general public awareness regarding the concepts of 'plural policing' (Loader, 2000; Crawford and Lister, 2004; Newburn, 2006), 'multi-lateralization of policing' (Bayley and Shearing, 2001), and 'multi-tiered policing' (Wall, 2001). These concepts are very important to illustrate how cyberspace is policed by various levels of policing actors. The policing of internet fraud in South Korea is thus seen as very similar to 'the internet's order maintenance assemblage' model. The following sections introduce how the system resembles it.

Internet users and user groups

Internet users and user groups police cyberspace voluntarily. Whether they are aware or not, they are the most powerful police force in cyberspace. They are motivated by various personal reasons or factors that stimulate their participation of policing cyberspace, such as higher moral standards, community service minds and unpleasant past experiences. It is difficult to define or to clarify internet user activity into a certain category since this tiered system consists of too many people who have different socio-economic and political backgrounds. Like a terrestrial level of policing, some internet users want to implement tough or strict counter-measures while others want to implement softer counter-measures against cybercrime. Nevertheless, user groups are different from the individual user level due to the fact that they represent their group interest in order to accomplish the goals of the group they represent through their collective activities. Recently, the emergence of the personal blog "naver.com", "daum.net" and mini homepages "cyworld.com" has encouraged more users and user groups to participate in policing cyberspace. Recently, victims of internet fraud have created their own community websites "thecheat.co.kr" and catchall.or.kr" to track down fraudsters and warn the innocent public about fraudulent activities. The Cheat and Catchall were founded in 2006, as not-for-profit community websites to act as response agents to internet fraud. Both sites

are sponsored by the internet user for their operation, with their major activities involving the sharing of fraud information and the introduction of anti-fraud measures. Although they only demonstrate a basic level of fraud prevention measures, these models are still beneficial for the policing of internet fraud in the private sector. The reporting of fraud incidents collated and analyzed by the private sector is not an easy task and has yet to be attempted by any public agency.

Online virtual environment managers

'Online virtual environment managers and security-for online role playing/game playing, chat rooms, discussion lists, e-auction rooms, cyber worlds' are using 'removal of access rights, exclusion from the environment to regulate their virtual space when community norms or laws are transgressed' (Wall, 2007: 168). This category has wider range of interest groups because there is countless number of online communities existing, for example, "social reform" and "cyworld". As government requires more strict self regulation of the internet community, security staff members that monitor their service sites pay more attention to unusual activity. Naver is a largest portal site that increased its monitoring staff from 270 in 2007 to 430 in 2008 in order to respond to any illegal and unethical activities. Daum, second largest portal site, also increased its monitoring staff from 200 in 2007 to 300 in 2008 (Sports Seoul, 2008). Recent news reported that fraudsters hacked messenger IDs and passwords to deceive friends online. By using messenger, they asked friends for money for an emergency.

Non-government, non-police hybrids

Non-government, non-police hybrids are motivated by socio-political influences and they have insisted that there is only one pure way to prevent cybercrimes. Recently, NGOs (non-governmental organizations) represented general internet users in Korean society who, individually, did not believe themselves to be opinion leaders. But, collectively, their activities eventually created public consensus, which pressed government to establish laws that reflected their demands. The implementation of an 'Opt – In System' is a good example of their achievement. Peoplepower21, Jinbonet, Citizen Action, Lawyers for a Democratic Society and Intellectual

Property Left are the most powerful NGOs that advocate the safety and freedom of the internet in Korea. There is a very unique group called 'CONCERT' which is positioned between the NGO and corporate security. Consortium of CERT was founded in June 2005 as an organization of security power, merging public and private security for collective benefit, consisting predominantly of private companies related to internet security that are involved in IT businesses. These companies include Samsung SDS, SK Telecom, LG CNS, KT, Naver, Daum, KTF, Shinhan Bank, SIEMENS, SK C&C, LG Telecom, POSCO, Korea Amway, Dacom, Koscom,[7] and other private companies. CONCERT's major objective is to share information and to respond to any threatening attempts to penetrate the Korean telecommunication infrastructure.

Internet Service Providers (ISPs)

Internet Service Providers (ISPs) are motivated by both governmental intervention and management interests. Firstly, governmental intervention has been made by recommending the establishment of the self-regulation of ISPs in order to prevent harmful contents or pornography. However, self-regulation cannot punish those who create harmful content or pornography. Public awareness programmes, education programmes and hotlines to respond against immediate threats should support it. If ISPs do not impose any action against risky activities, they will result in inviting legal intervention by the government that could damage ISPs' reputations. Secondarily, management interests are motivated to involve vigorous cyber policing activities in order to protect corporate assets, to avoid any liability and to provide hassle-free internet service to their clients. KT, SK Networks, KFT, Samsung Networks, Onse Telecom and Hanaro Telecom are the most popular ISPs in Korea and are acting members of the Korea Internet Infrastructure Promotion Association.

---

[7] These company names are original, not abbreviations.

State-funded non-police groups

State-funded non-police groups consist of several governmental agencies that each have formal authority over the supervision of internet activities. Thus, each agency has different motivations for their participation in the governance of cyberspace. Depending on the agency. jurisdictions are varied from pure IT related issues to financial issues. For example. the Korea Spam Response Center focuses on overflowed spam mail problems by receiving complaints from internet users and by developing anti-spam software to protect inboxes from the overwhelming amount of spam mail and mail that may contain scams (KSRC, 2003). KrCERT monitors unusual activity on the internet (KISC, 2004). The Korea Consumer Protection Board is also making an effort to protect consumers' rights through monitoring commercial internet transactions.

The FSA (Financial Security Agency) was founded by the FSS (Financial Supervisory Service. The major functions of the FSS include the supervision, examination, investigation of and enforcement over financial institutions. along with other matters delegated by the Financial Supervisory Commission (FSC) and the Securities and Futures Commission (SFC) in May 2005, which is a special research institution that works to produce preventive measures for financial transactions. The FSA is major public policing body for internet fraud. The FSA established a KFCERT and Phishing Incident Report Center in Jan 29, 2007 (Lee, 2007). The FSA primarily runs the One Time Password (OTP) centre to protect internet banking transactions. The FSA not only does research work but it also does quasi-policing activity. The FSA is seeking to implement more proactive policing activities (Lee, 2007), yet at this time there could be a possible conflict of interest with the Korea Financial Telecommunications and Clearing Institute (KFTC) that is under the control of the Ministry of Finance and Economy (MFE). Both the FSS and the MFE have operated quasi-policing bodies under the title of 'research institute' (the Korean equivalent of the FSA name includes 'research institute'). It seems that the FSS and the MFE have had concerns about the possible opposition for the establishment of those subsidiary agencies since they said they were going to involve more policing activity.

The Korea Financial Telecommunications and Clearing Institute (KFTC) is another public policing body for internet fraud under the control of the Ministry of Finance and Economy (MFE). Its primary activity is to secure and to maintain safe financial transactions for membership banks and customers (Digital Certification Center, 2006).

KISA (the Korea Information Security Agency) is another public-funded cyber policing agency, which is an affiliated agency of the Ministry of Information and Communication, established by *The Information Facilitation Act No. 14* in April 1996 (KISA, 2003). KISA was founded to respond to emerging problems in the digital era such as the leaking of personal information, misuse of IT systems, and to handle worldwide computer hacking at a national level. KISA's main role is to oversee the overall activity of membership organizations, which are defined under *the Acts on Promotion of Telecommunications Network Utilization.* Membership organizations number between 300 and 400 and are limited to ISPs (Internet Service Providers), internet security service companies and vaccine production companies. Membership organizations must report all accidents to KISA; this is not a voluntarily provision, it is a legal requirement. This also differs from the presidential direction, which is being used by the NCSC (National Cyber Security Center). KISA also has a liability to keep the secrecy of incident information that KISA receives from membership organizations.

The Korea Spam Response Center is a subsidiary unit within KISA that provides services to prevent illegal, unwanted mail. The KRSC ensures a clean and dependable cyber world through performing a variety of campaigns to prevent spam-related damage: by generating technical measures such as the creation and distribution of free anti-spam software, and by implementing policies and studies to improve laws and systems restricting spam activities. Another important measure is the participation in anti-spam activities by moving forward towards international cooperation with foreign countries, anti-spam organizations and international organizations (KSRC. 2003).

PRIVACYNET is a subsidiary unit within KISA that has endeavoured to prevent personal information infringements and their expansion. Too much personal information has been given away from ISPs and web-based business companies to small venture businesses and even individuals for various purposes. Its Secretariat monitors whether businesses comply with the personal information protection laws on a regular basis. If businesses violate the laws, the Secretariat recommends them to correct themselves voluntarily or to refer the facts to the related agencies. Its primary function is to represent the internet user (KISA, 2004).

KrCERT/CC (The Korea Information Security Center) is a subsidiary unit within KISA that prevents infringement cases and minimizes damage from the internet in Korea. It plays an important role in improving the technical capability for the protection of the Critical Network Infrastructure Internet communication network and for the reinforcement of prediction and alarm systems. Sometimes fraudsters illegally penetrate the internet communication network to search for or disguise potential victims, and it is therefore important to block such attempts. KrCERT has established international cooperation with many nations' CERT and IT security related offices to share necessary information and to be able to respond at an international level (KISC, 2004).

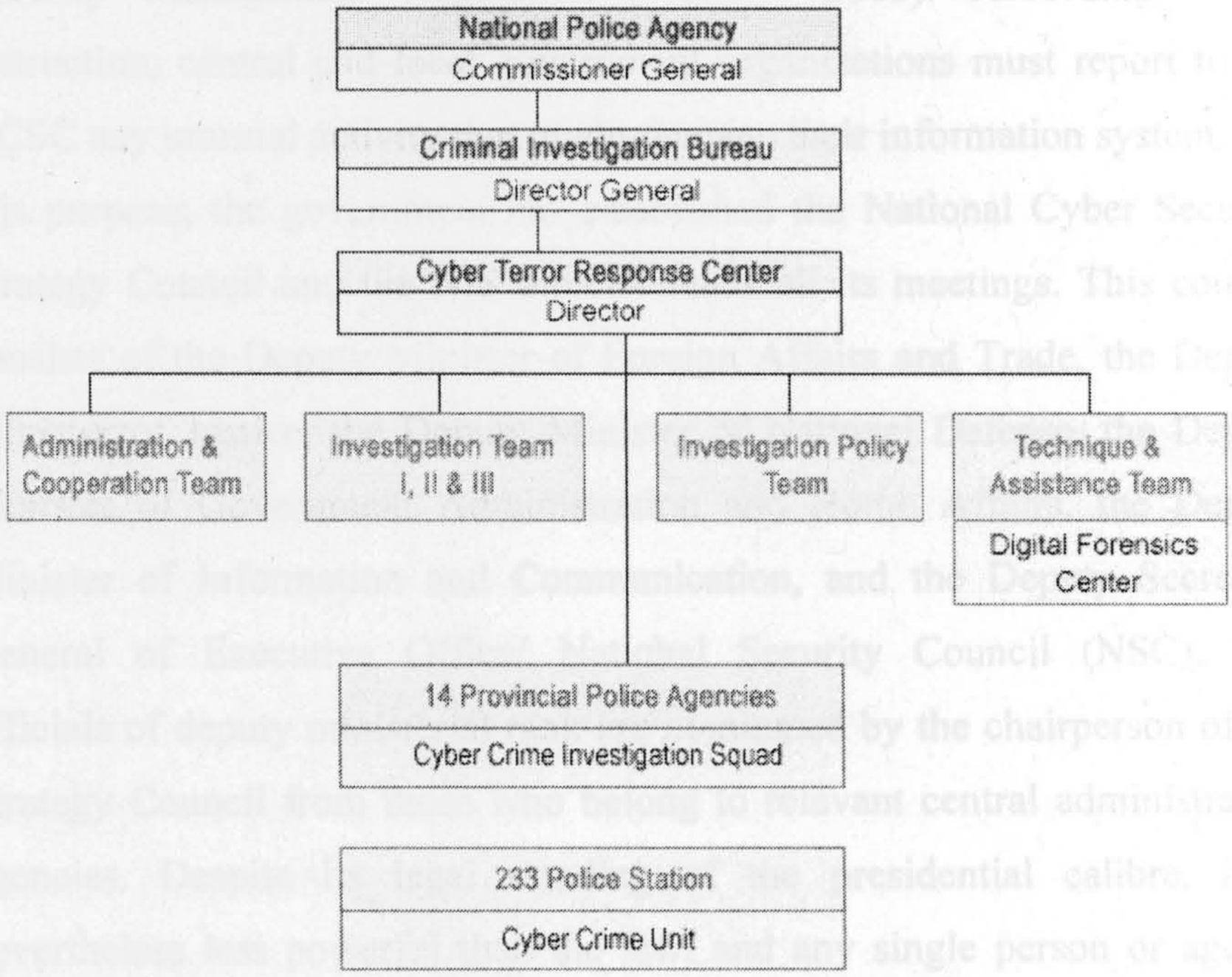
State-funded police

State-funded police are motivated mainly by their duty to protect and to serve their communities. Their motivations are based on the public interest to contrast with private security services, which are based on profit, market-oriented services and private interest. Their policing services widely range from small districts to large metropolitan areas of jurisdiction. Sometimes, the national police system mandates them to take a responsibility to police the whole country. The Korea National Police Agency operates the CTRC (Cyber Terror Response Center), which is the headquarters for all cybercrime units. The CTRC coordinates nationally deployed cybercrime units in the police force (CTRC, 2005).

Compared to other nations' public policing models for internet fraud. South Korean law enforcement agencies and regulatory agencies have given little attention to internet fraud. Since public sector agencies do not see it as a serious threat to the majority of internet users and the national information infrastructure system, occurrence of internet fraud has silently increased. In spite of continuous growth, policing of internet fraud in the public sector needs to establish specialized response units in law enforcement agencies and regulatory agencies. Korean public sector agencies (see Table 3-2) do not have any specialized response units for internet fraud such as those found in the US and the UK. Although Korean agencies do not specialize in responding to internet fraud, their routine activities do involve the prevention of internet fraud.

The Korean National Police (NPA) established the Cyber Terror Response Center (CTRC), originally named the 'Hacker Investigation Squad', in 1995. It has developed alongside the growth of Korean IT businesses and an increasing population of internet users. The CTRC's policing work mainly focuses on copyright violations, illegal websites, defamation and sexual assaults, hacking, internet fraud and the distribution of viruses. These crimes are described in the Korean Criminal Law Article 41, in which internet fraud is the subject of Article 347. The NPA is the pioneer of policing cyberspace and handling internet crime investigations in Korea. It is not an exaggeration to state that CTRC is the one of the best cyber police forces in the world, and many Western police agencies have signed up for the MOU (Memorandum of Understanding) with the KNPA (CTRC, 2005).

Figure 5-1: The National Police Agency



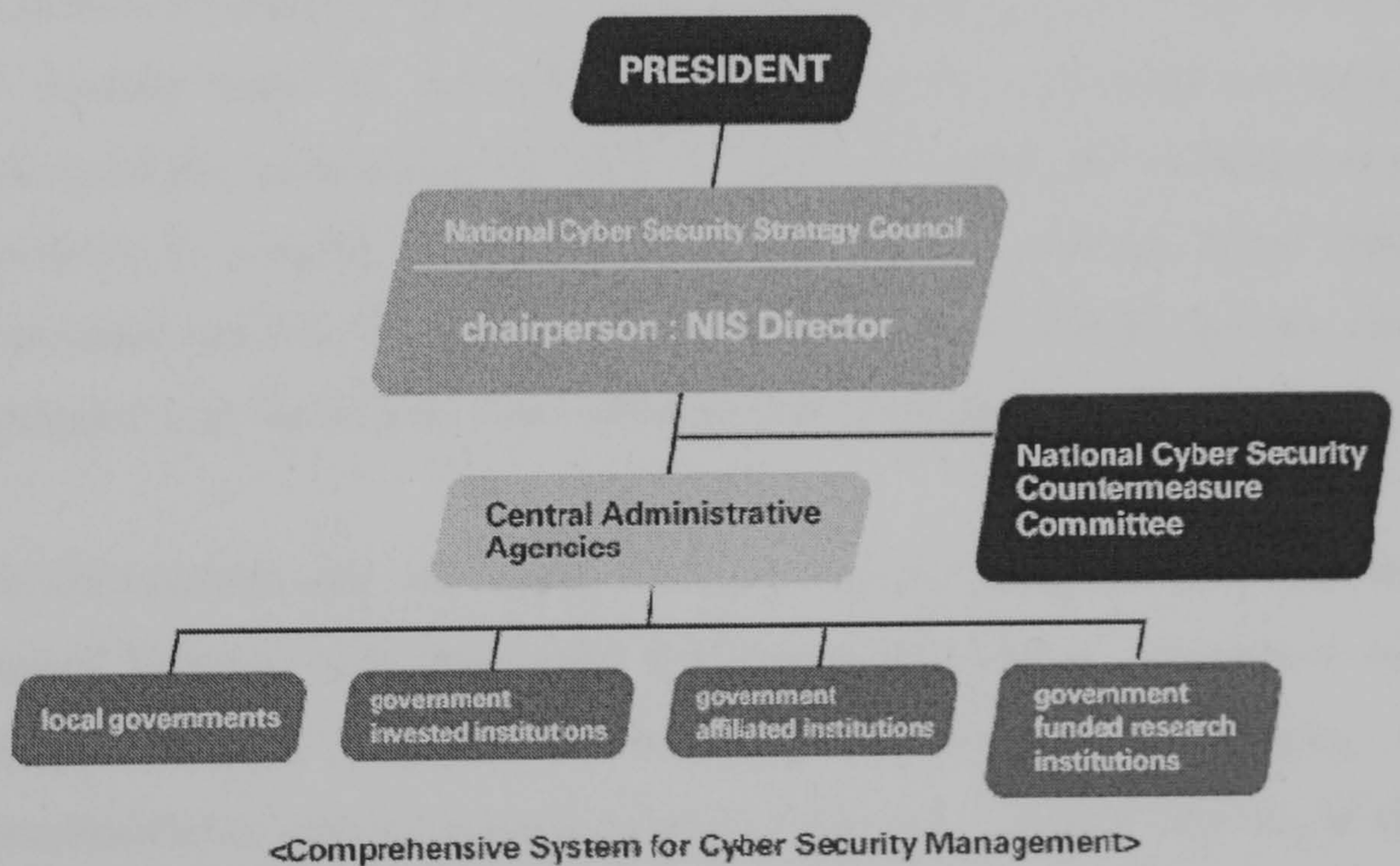
(Source: www.ctrc.go.kr)

The Supreme Prosecutors' Office (SPO) operates the Computer Investigation division, while the Seoul District Central Prosecutors' Office (DPO) operates its Computer Investigation department, which is the only actual computer investigation office in the SPO. However, prosecutors who work at the Computer Investigation department are not in permanent positions because they regularly transfer to other departments or to different district offices (at least every two years) in order to prevent corruption issues. As a result of transfers, new prosecutors and staff members have to be constantly trained and organized to effectively perform law enforcement activity (SPO, 2005).

The National Cyber Security Center (NCSC) is the central point of government for identifying, preventing and responding to cyberattacks and threats in Korea. It was founded in 2003 in order to protect the critical national infrastructure in Korea. The National Cyber Security Center (NCSC) is under the command of the National Intelligence Service (NIS is the Korean equivalent of MI6). Its major cybersecurity activities are defined

and enacted by The Presidential Direction Number 141-National Cyber Security Management Regulation (January, 2005). According to its instruction, central and local government organizations must report to the NCSC any unusual activity that might damage their information system. For this purpose, the government has established the National Cyber Security Strategy Council and the NIS director leads all its meetings. This council consists of the Deputy Minister of Foreign Affairs and Trade, the Deputy Minister of Justice, the Deputy Minister of National Defense, the Deputy Minister of Government Administration and Home Affairs, the Deputy Minister of Information and Communication, and the Deputy Secretary General of Executive Office/ National Security Council (NSC). The officials of deputy ministerial rank are nominated by the chairperson of the Strategy Council from those who belong to relevant central administrative agencies. Despite its legal standing of the presidential calibre, it is nevertheless less powerful than the law, and any single person or agency will argue that the NCSC has a superior power over cybersecurity. The NCSC also works with the private sector and the military to improve warning and response time (NCSC, 2005).

Figure 5-2: The National Cyber Security Strategy Council



<Comprehensive System for Cyber Security Management>

(Source: www.ncsc.go.kr)

In 2006, the National Cyber Security Center (NCSC) launched the Korean National CERT council with nine government agencies (*National Intelligence Service, National Police Agency, The Supreme Prosecutors' Office, Korea Information Security Agency, Korea Financial Telecommunications and Clearings Institute, Defense Security Command, Ministry of Information and Communications, Ministry of Science and Technology,* and *Ministry of Government Administration and Home Affairs*) as a functional group that shares intelligence services within the public sector concerning current vulnerabilities, threats and the status of counter-measures regarding cyber threat and terrorism.

Corporate security

Corporate security is motivated thoroughly by the profit and market-oriented philosophy of each firm. Their motivations vary depending on products, local culture, and laws that frame the status of the corporation. This part of security or policing of cyberspace is not well known to outside societies. However, through globalization and transnational functions of businesses security, agencies now require the most sophisticated technology and strategies to be used in order to protect their valuable assets deployed worldwide. Corporate security is divided by 'in-house security' and 'contract-out security' services. Large corporations have their own 'in-house IT security team' to police their networks, while mid-sized companies outsource the 'contract-out IT security' service or adopt the combination of 'in-house IT security' and 'contract-out IT security' services. Many small companies are vulnerably exposed to cyber threats and risks, but are only equipped with feeble anti-virus software and firewalls.

Ahnlab Coconut was founded by AhnLab, Dacom, Enterprise Networks and Hansol Telecom with their joint investment, technology, know-how and capital. AhnLab Coconut is Korea's first company specializing in comprehensive internet security services. AhnLab Coconut introduced the concept of internet security service in the Korean market, offering 'ongoing security consulting' in oriented, comprehensive security services that follow the steps of diagnosis-design-building-management in their monitoring and operations (Ahnlab, 2007). For IT security people, policing internet fraud is

not their primary role and is often a voluntary by-product of their ordinary occupations when their assistance is requested by the police.

KOSCOM, a private company, operates the Financial ISAC (Information Sharing and Analysis Center), which is approved by the Ministry of Finance and Economy in order to protect financial trading information. KOSCOM/ISAC is a security centre for collecting and analyzing cyber terrorism and hacking threats, and is also used for formulating hacking countermeasures. KOSCOM/ISAC provides real-time detection of cyberterror, such as hacking and viruses, in cooperation with the computer systems of member institutions and other financial and public institutions. Their system provides immediate warnings for clients if an intrusion is detected; it then finds the security vulnerabilities and quickly devises measures to protect the system. KOSCOM/ISAC also provides a cyber incident database, vulnerabilities database, patch information database and online security information. KOSCOM/ISAC has operated an ESM (Enterprise Security Management) system, a CERT team, a real-time analysis and a process of response for when cyberattack occurs (KOSCOM/ISAC, 2005).

The BC Card Company has independently operated fraud prevention measures, installing special monitoring software into their server to detect any unusual events occurring to the accounts or credit cards of their customers. These companies use Experian's risk management programme to monitor customer's behaviour, such as excessive withdrawals of cash or excessive use of credit cards. They have enhanced their risk management capabilities in order to satisfy the Basel II requirements; financial institutes must have their own risk management systems, which are to be supervised by the National Financial Agency (BC Card, 2005).

Auction.co.kr is an affiliation of eBay international. It has maintained almost the same system as that of eBay. Through operating a safety centre, customers can obtain necessary information about buyers and sellers. In case of default of transaction, the safety centre becomes actively involved to solve the problem. If serious fraud occurs, the safety centre reports it to the

police so they can investigate the case. In addition, it has many useful safety tips to customers for preventing fraud.

The NHN has a security team that consists of a security analysis team, a security service team and a customer information protection team. Naver.com is one of the largest and most popular Internet searching portal service companies operated by the NHN Corporation. As a popular searching portal company, there are continuous problems existing between companies and customers in terms of internet fraud. Although most incidents should be reported for civil and regulatory action rather than criminal investigation, there is still a need for intervention by the police. Therefore, the NHN security team has maintained a strong relationship with the police through hiring former police high rank officer (Choi, 2006).

Overall, the reactive and auxiliary role of the private sector has facilitated more fraudulent activities in cyberspace. Although most fraudulent activities have occurred in the private domain, private industry has looked on without doing anything until the public policing bodies have become officially involved, whether voluntarily or involuntarily. Most fraudulent incidents have not been reported to the public police due to lack of trust, different investigation philosophies, negative publicity, and adverse impacts on stocks. Simply put, the private sector does not believe that the public police appropriately protect their private interests. This predisposition of public policing has been noticed by many previous incidents. The public police tend to be involved when criminal activities occur that considerably harm public interests, which must be protected by the law. Recently, private and public sectors of policing have realized that they have to cooperate with each other in response to increasing fraud incidents in cyberspace.

Before examining the reform of public policing in South Korea, it is important to take a look at current internet fraud law in the country. therefore this will be reviewed in the following section.

5.3 Internet fraud law in South Korea

Korean criminal law was amended in 1995 in order to cope with new crimes in the age of information. It regulates computer-involved crimes such as fraud, forgery, interference of business, embezzlement and privacy interruption through computers and destruction of electronic records and documents. Internet fraud is a subject of criminal law, which includes the Acts on Promotion of Telecommunications Network Utilization and the Telecommunication Business Law (Lee, 2000).

Under *Korean criminal law*:

- Article 347-1: a person, if convicted for fraud, could face a maximum of 10 years in prison or a fine of up to 20 million Won.
- Article 347-2: Illegal use of a computer to process false information or incorrectly attempt to make money could face a maximum of 10 years in prison or a fine of up to 20 million Won.

For example, a total of 274,638 people were booked for the charge of fraud (Article 347-1.2) by the police and they were reported to the Prosecutors` Office. Among them, 55,618 were finally prosecuted in 2005. The percentage of prosecution is relatively low for fraud cases because it is difficult to prove without concrete evidence (CTRC, 2005).

Under the *Acts on Promotion of Telecommunications Network Utilization*:

- Article 48-3, Article 62-5: a person who sends excessive signals or processes illegal commands in order to interrupt the stability of a telecommunications network could face a maximum of 5 years in prison or a fine of up to 50 million Won.

For example, a total of 4,019 people were booked to face charges for the violation of this act (Article 48-3, 62-5) by the police and they were reported to the Prosecutors' Office. Among them, 2,032 people were finally prosecuted in 2005 (CTRC, 2005).

Under the *Telecommunication Business Law*:

- Article 53: Fraudulent activity can be prohibited and punished by this law although many people and parties ignore this administrative order administered by the Minister of Information and Communications and by the Korea Internet Safety Commission. Violation of this law could face a maximum of 2 years in prison or a fine of up to 100 million Won.

For example, a total of 156 people were booked to face charges for the violation of this act (Article 53) by the police and they were reported to the Prosecutors' Office. Among them, 88 people were finally prosecuted in 2005 (CTRC, 2005).

The conviction rate for the above examples is not available, but it is alleged that the prosecution rate and the conviction rate are almost the same in Korea. The Korean criminal court rarely overturns prosecuted cases because the court often accepts offenders' guilty statements presented to prosecutors as evidence of non-involvement.

However, many expert respondents in this research criticized the fact that these laws are not able to catch up with the speed of technology and culture. Criminals are always a step ahead of the law enforcement agency, resulting in growing demands upon public policing bodies. As a result of numerous professional meetings, the government has decided to revise current laws governing the internet and cyberspace. Revision of the Act was implemented in 2007 after passing the community hearing and the legislation procedure.

The revision of *the Act on Promotion of Telecommunications Network Utilization and Information Protection* in 2007 mandates (MGL, 2007):

- ISPs (Internet Service Providers) and Media with more than 300,000 and 200,000 visitors per day must implement the limited 'Real Name' system.
- The ISP and Media must confirm the name and contact number of their bulletin board and keep that information for at least 6 months. If the ISP does not implement 'Real Name' confirmation, the MIC

(Ministry of Information and Communications) can order for their correction, and a 30,000,000 Won fine will be imposed if they do not comply.

- When personal information transfers abroad, the ISP must notify the name of the country and recipient, method of transfer, aim of use of the user and finally they must obtain permission from the user to transfer their information.
- In cases of infringement of privacy and defamation, victims can submit the offender's name, address and contact number to the Office of Mediation of Defamation in order to initiate a lawsuit against the person who committed the crime. Five lawyers are then appointed by the Information and Communication Ethics Committee to handle the case.
- In cases of transfers of personal information due to the mergence and acquisition of a company, it must be notified wholly via e-mail, letter and by telephone to the user. If there is no contact information for the user, this information must be informed on the company's website for 30 days.

The revision of this Act focuses more on the responsibilities of ISPs in terms of protection of personal information. This Act has been modified in 2008 in order to enhance the responsibility of ISPs so that number of portal site and news site visitors changed from 300, 000 (portal site) and 200, 000 (news site) to 100, 000 visitors (Kim, 2008). It will become more difficult to trade personal information between or within commercial markets internationally. Meanwhile, ISPs will have to perform more policing activities in cyberspace in order to fulfil the revision of the Act. It is quite contradictory that self-regulation has been considered the more preferred form of internet control worldwide. Korean laws could be more realistic than other countries' laws since Korea has more than 70% internet user population and has become one of the strongest IT nations. Events in Korea suggest that the international community are very likely to confront similar occurrences. Korean laws could thus be used as international guidelines in the future.

However, the government faces many challenges from liberal cyber community groups to abolish the revision of these acts. They are concerned that this revision of law will violate human rights and infringe on the privacy of internet user, arguing that the 'big brother' is online to oversee them. The Korean government has argued that the balance between safe and risky cyberspace must be considered a very serious matter.

The National Internet Development Agency of Korea reported that about 75 percent (32,570,000) of Koreans use the internet, with about 35 percent of the population using internet banking (June, 2006). Therefore, it is fundamental to have greater internet security, despite strong opposition from internet user groups, such as the Korea Information Security Agency (KISA).

5.4 How do public and private sectors police internet fraud in Korea?

In the public sector, there is no public agency solely focusing on internet fraud. Since internet fraud is considered a cybercrime, it is embedded with general cybercrime. The police do not police internet fraud separately. Therefore, most internet frauds are reported by victims. When internet fraud occurs, the victim has to go to the police department to make an official report. Initially, police were taking reports through an internet site but too many false reports were received. As a result of abundant false reports, the police changed their policy and now take reports directly from victims. This direct reporting policy has reduced false reports by victims dissatisfied with internet shopping. After changing the reporting policy, only serious internet frauds have been reported and prosecuted by law enforcement agencies.

In the private sector, a few organizations, such as 'Catchall' and 'The Cheaters' respond to internet fraud. Groups are voluntarily organized by victims and managed with a small amount of support from them. Through their websites, they receive internet fraud reports from victims. As the media has introduced their activities and websites, more victims have joined in order to catch fraudsters by exchanging useful information, such as tricks

and methods that were used by them. However, their policing activities are causing concern for law enforcement agencies. The police ask victims to report it when they locate fraudsters rather than taking action themselves.

Corporate victims are likely to recover their losses through their security measures. They are concerned with the impact of negative publicity and negative impact on stock value so they sometimes absorb their loss as 'cost' rather than officially respond to it. If their loss is considerably large, they tend to report to the police. Compared to foreign companies, fraud investigation and prevention methods are rarely used. Although it may cause significant loss, Korean companies are unlikely to spend money on preventing possible threats or risks.

Internet Service Providers police internet fraud through their security staff, but they have a lack of staff available to monitor complicated fraudulent activities. Their security staff members spend most of their time watching for defamation comments and replies in membership cafes. Recently, the subject of defamation comments and replies has become a very serious social issue in South Korea. In particular, politicians and entertainment celebrities are the main targets. Some entertainment celebrities have committed suicide because of malicious words. This situation needs a greater response.

5.5 Relationship between the public and private sectors

In contrast to other Western countries, the relationship between private and public sectors is not receptive. Historically, authoritarian governments have ruled Korean society for more than five decades. The government used to treat private companies as subordinates although not in their chain of command. Through regulation and policy, the government has tightly controlled the private sector. This hostile relationship has gradually disappeared with the process of democracy. However, lack of trust between the two sectors has remained. This relationship has acerbated the need for cooperative behaviour for information and knowledge exchange.

Government agencies used to obtain the necessary information from the private sector without formal request. However, this kind of practice is not acceptable these days. The vertical relationship has slowly changed to a horizontal relationship. Each sector has realized that partnership policing is important in responding to internet fraud. In order to establish an effective partnership, more precise law has to define the necessary relationships. Lack of appropriate law has meant their relationship has remained indifferent. They do not exactly know how to improve their relationship in terms of policing internet fraud.

5.6 Development of policing cybercrime in South Korea

History of Cyber Terror Response Center

The Korean National Police Agency established the first computer crime investigation team within the International Criminal Affairs Division in 1992 in order to respond to computer related crime. Later, this team became a Hacker Investigation Unit in October 1995; it consists of four staff: two investigators and two analysts. Since the breakdown of the Nowcom network in May 1997, this team has belonged to the Investigation Bureau and has more staff members and equipment; it was renamed the Computer Crime Investigation Team in August 1997. As cybercrime has increased throughout the nation, the Korean National Police Agency (KNPA) established the Cyber Crime Investigation Team in 16 provincial police agencies in January 2000. At the national level, KNPA's Cyber Terror Counteraction Plan was submitted in February 2000. This plan emphasized the national level of response to cybercrime. The Ministry of Public Administration and Security approved the establishment of the Cyber Terror Response Center (CTRC) with 80 staff members and an annual budget of 10 billion won in April 2000. Eventually, CTRC opened in July 2000 (CTRC, 2005).

Reform of the criminal justice system

The Korean criminal justice system is different from other Western countries' systems in that there are two law enforcement agencies

competing for investigation authority; The Supreme Prosecutors' Office and the National Police Agency. In the Korean Criminal Prosecutors' Law, only the prosecutor can conduct a criminal investigation and has the right to close the case. The public police are defined as assistants to the Prosecutors' Office. However, the police agency has attempted to attain an 'independent investigation right', by freeing itself from the control of the prosecution, as part of democratic reforms in the early 1990s. This effort gained impetus when the incumbent administration started an extensive judicial reform programme covering all areas of law enforcement, ranging from the training of lawyers to the operation of criminal trials.

When the Presidential Commission on Judicial Reform released a draft proposal in April 2005 for the revision of the Criminal Procedures Law with a provision granting independent investigative power to police, the Prosecutors' Office was notably embarrassed. Moreover, the commission would not allow prosecutors to use defendants' statements in their interrogation as evidence in criminal trials. Prosecutors, in alliance with other legal professionals, went on a counterattack, primarily inquiring about police awareness for the protection of human rights (Korea Herald, 2006).

There is currently a political environment whereby the public police are struggling to obtain independent investigation power whilst the Prosecutors' Office is strongly defending its ownership of investigation authority.

According to Bhanu and Stone (2004), it needs external as well as internal support for police reform to succeed. Without leadership committed to improvement within a police organization, external calls for reform will rarely penetrate the daily delivery of police services on the front lines. But without external support for reform, even the most committed police leadership will lose the political backing and resources necessary to sustain a successful reform process. However, it seems that this reform of policing is not easily implemented as the Korean National Police have barriers both inside and outside of the agency.

Most Korean police officers believe that the Commissioner General is not willing to stand on the front line of a war to achieve independent investigation power, and that the position of the Commissioner General is not the final career position. After one office term, the Commissioner General could be promoted to the Deputy Director of the NIS, Director of Presidential Secret Service, or the Minister of Government administration and Home affairs. Sometimes, they could directly join as a member of National Congress with support by the ruling party. Because of these reasons, it is believed that the Commissioner General will not sacrifice his career for such a difficult political challenge.

Furthermore, the congressional legal committee consists of a former judge and prosecutor, making it impossible to pass the revised criminal procedure without support from public citizens. Fortunately, there is a growing consensus about the revision of the criminal procedure and legal system, which is comparable to the US legal system. However, this faces powerful opposition from legal professionals who do not want to give up their vested rights.

The only hope lies in public awareness in that they are customers of police services, and the public's consideration of what kind of policing system serves to benefit them in providing improved public accountability. Policing reformations must consider the public interest, not only the agency's interests.

However, the public still regards the competition between the police and prosecutor as a fight to obtain their own investigation power, not as a battle for the promotion of human rights. As a result of their negative public image, policing reforms have come to a lull.

For the public police, this reform is a challenge to their independent investigation power to perform at full capacity to police cybercrime without any intervention by the Supreme Prosecutors' Office. The CTRC is a pioneer of cybercrime policing, but its investigation is still subject to prosecutorial supervision by the law.

5.7 Partnership policing for the response to internet fraud in South Korea

In view of the growing tendency toward internet fraud, it is imperative to establish more specialized internet fraud policing units in the private and public sectors in South Korea. Through establishing specialized policing units for internet fraud, both sectors could achieve mutual goals for crime prevention while pursuing their different interests. Whether those units work together or separately, more specialized policing units in both sectors would discourage the development of internet fraud and would promote safe e-commerce activities.

In spite of various preventive strategies being adopted by the private sector, partnership with the public sector is crucial to prevent and to respond appropriately to internet fraud. However, it is argued that discussion of partnership policing should take place after establishing specialized internet fraud policing units in both sectors. Although there are a few volunteer groups' websites such as The Cheaters and Catchall, it is difficult to say that they work together with the police. These groups report to the police when they locate fraudsters who defrauded their members. Online auction and internet shopping mall companies have monitored fraudulent activities, but their policing capabilities show minimum results. They mainly deal with complaints received from their customers.

For the development of partnership policing, it is suggested that more attention must be given to internet fraud by both sectors. In order to perform in full partnership, the establishment of an information clearing house has to be prioritized. This information clearing house would store useful data such as victim, offender and method. Without an information clearing house, neither sector has a platform through which to share information. Unfortunately, there has been no discussion about establishing an information clearing house for internet fraud.

5.8 Barriers of policing internet fraud by the police in South Korea

There are four main barriers to policing internet fraud in Korea. First, a lack of understanding of the impact of internet fraud by the public sector could be the most serious barrier in policing internet fraud. The public sector has given little attention to internet fraud compared to other cybercrimes. This may be attributed to the complicated process inherent in proving criminality. Fraudsters usually deny their criminal behaviour and avoid their liability. Subsequently, it costs more money to prove criminality than to recover losses.

Second, lack of investigative skill of the police deters victims from reporting incidents. Not many people report their losses or damage to the police because they believe that the police do not properly deal with internet fraud. Since police do not have sufficient experts at the local level, complicated incidents have to be dealt with by the computer crime unit at the regional or national headquarter level. CTRC (Cyber Terror Response Center) has developed more sophisticated methods and tools for responding to cybercrime, but it does not relate specifically to internet fraud.

Third, lack of budget discourages people from reporting internet fraud to the police. Since internet fraud is not a high priority for the police, budget allocation for it is small. Investigation of internet fraud requires substantial cost and time since many sophisticated tricks are involved. However, there is no separate budget for internet fraud investigation. Internet fraud is considered to be a part of general cybercrime, as classified by the KNPA. This discourages the investigation of internet fraud.

Fourth, lack of human resources makes it difficult to police internet fraud. Although KNPA (Korean National Police Agency) has trained and hired more cyber-cops, there are still insufficient personnel to respond to internet fraud. The rapidly growing threat of internet fraud needs more personnel to respond to it. Hiring more personnel costs less money than the total loss of e-commerce due to internet fraud.

In the next section, the tensions in both sectors are examined with particular regard to the similarities and differences of current partnership policing of internet fraud.

5.9 Tensions between private and public sectors in policing Internet fraud

Similar to those reported in Chapter 3 (United Kingdom) and Chapter 4 (United States), tensions are also found in South Korea. They are lack of trust, lack of knowledge and under-reporting. Different cultural, social and political environments produce slightly different types of tensions. Compared to the UK and US, policing internet fraud in South Korea is less developed, because there is no independent government agency policing internet fraud, and there is a low level of public awareness of internet fraud. This environment offers less tight control of internet fraud by both sectors.

The first tension is a 'lack of trust' between private and public sectors in policing internet fraud. This tension is also found in the United Kingdom and the United States. It is a fundamental tension that subsequently affects other tensions. Like other nations, private and public sectors do not trust each other. Historically, the public police lost their reputation while they protected the authority of the military government. Authoritarian style policing worsened the relationship between the private and public sectors. Although the police have changed with democracy, old traditions are still embedded and public relations tend to lack in building partnerships with the private sector. Recently, private and public sectors have talked through various communication channels such as conferences, seminars and roundtables. However, there have been some criticisms in that the meetings have not discussed sensitive issues. When the government agency organized a conference, most participants were pro-government scholars and companies. Thus, almost the same participants are seen at different conferences organized by other government agencies. For better communication, the public sector has to listen more to the private sector. Lack of trust can be solved if the two sectors truly communicate with each other. Through this communication, mutual respect and cooperation can be achieved.

The second tension is 'lack of knowledge' between private and public sectors in policing internet fraud. Although the two sectors have approached internet fraud in terms of crime prevention and law enforcement, their knowledge about internet fraud is insufficient. Not many people who monitor internet fraud understand the skills and methods used by fraudsters. As mentioned earlier, social engineering is a common method used to deceive victims, but few people know how to protect from it. For internet fraud prevention, the private sector has greater knowledge than the public sector, since they have to protect their assets. Compared to the private sector, public police and other regulatory agencies show less interest in the prevention of internet fraud. Practically, famous portal site companies, online auction companies and financial institutions have much greater knowledge with regard to internet fraud control. Therefore, private sector security experts tend to look down on the capabilities of the police in terms of their response to internet fraud.

The third tension is 'under-reporting' between private and public sectors in policing internet fraud. This tension is found more at the individual victim level. Comparatively, a small amount of loss makes a victim more hesitant to report the incident to the police. Small amounts of loss will eventually become large amounts of loss if ignored by victims and law enforcement agencies. Fraudsters take advantage of the fact that victims of small amounts of loss tend not to report to the police, therefore they deceive innocent internet users with minor deceptions by selling low-priced items and game money. These items attract people to pay small amounts of money without suspicion. At the corporate level, private companies have low expectations for successful investigations by the police because they do not believe that the police have sufficient capabilities to deal with internet fraud investigation.

5.10 Conclusion

A range of tensions in policing internet fraud between the two sectors has interrupted the motivation for partnership policing: they are lack of trust, lack of knowledge and under-reporting. Although different cultural, political and social backgrounds are evident, lack of trust is the most common tension found in all three nations, including South Korea. Interagency conflict, bureaucratic conflict and technological intervention have also been found to be negative factors for adapting effective public policing, whereas, political and legal barriers interrupt the active participation of policing cybercrime by the private sector, particularly in South Korea. In order to establish effective partnership policing for internet fraud, mutual needs for the successful partnership have to be prioritized. To do that specialized internet policing units in private and public sectors have to be established. In order to provide more effective policing, establishment of an information clearing house is also necessary. Without recognizing its imperativeness, effective policing of internet fraud cannot take place in South Korea.

Chapter 6: Analysis of Findings

This chapter will consider, in three parts, the most serious tensions affecting the policing of internet fraud, both between the private and public sectors, and within the public sector. It will also suggest resolutions for tensions and outlines expected forms that a proposed model for partnership policing could take. The current condition of policing Internet fraud in South Korea is outlined based on comments from private and public sector experts. Through the process of analyzing interviews, the conceptual framework and research expectations of the study will be used as a theoretical framework for the comparison and interpretation of the findings. Through analytical comparison of the data collected from the interviews, an effort will be made to identify factors that are readily apparent from the data.

6.1 Part I: Most serious tensions affecting the policing of Internet fraud

This part gives context to the question of tensions between the private and public sectors of policing internet fraud by exploring current practices and issues that negatively affect partnership policing.

The most serious tensions between the public and private sectors

*Interviewees were asked to explain the **three most serious tensions** they perceived to have an affect on policing of internet fraud in Korea. Based on respondents' answers those that responded negatively to influences on policing internet fraud were used to structure the first part of this chapter:*

Tensions between the private and public sectors (see Table 6-1)

- Lack of trust between the private and public sector (both)
- Different investigation philosophies (both)
- Lack of legal perception (public)
- Negative publicity (private)
- Adverse impacts on stock value (private).

Table 6-1: Tensions between the private and public sectors

Sectors	What are the three most serious tensions between the sectors?	What are other serious tensions between the sectors?	What is the most serious tension?	Why do you believe that is the most serious tension between the sectors?	Why are those tensions produced?	How do those tensions influence your working practices for response?	Why are there tensions still existing while the government has encouraged the use of private policing?
Public	Lack of trust Different investigation philosophy Lack of legal perception	Lack of sharing information Lack of convincing material Lack of communication	Lack of trust	Cooperation of policing internet fraud is impossible without trust.	Self- interest Public vs. Private	Deception of evidence from the private sector Failure of prosecution	Cannot ever be removed

Private	Lack of trust Negative publicity Adverse impact on stock value	Politically influenced	Lack of trust	Private sector will not report fraud cases to the police if there is no accountability.	Self- interest Public vs. Private Power struggling	Use of private connection for police investigation Report only serious incidents	Limited delegation of power

The three most serious tensions between the private and the public sectors vary across different companies and agencies; however, respondents report that 'lack of trust' overlaps the two sectors. Along with this tension, different investigation philosophies and lack of legal perception were chosen as the three most serious tensions by the public sector. Negative publicity and adverse impact on stock values were chosen among the three most serious tensions by the private sector.

6.1.1.1 Lack of trust

The lack of trust is heightened by the belief that law enforcement fails to investigate internet fraud and other non-internet related crimes by the private sector. Previously, during the military regime, policing was exclusively owned by the state. The emergence of private security is a recent event coinciding with the democratization of Korea. Since the early 90s, Korean society has developed and demanded a more international standard of policing mechanisms. As a result, terrestrial levels of policing that are shared with the private sector have increased. For terrestrial policing, it is relatively easy to make a distinction between the public and private in terms of jurisdiction. Terrestrial policing activity is obviously seen and monitored by many interested parties.

However, the policing of internet fraud is highly indistinguishable because there is no physical boundary in cyberspace (Post, 1996; Richman, 1996) and there is no specified law to define the ownership of policing cyberspace because physical boundaries have characteristically outlined legal boundaries (Logan, 1999). This uncertain situation makes policing internet fraud more complicated than the terrestrial level of policing.

The respondents interviewed in this study expressed their opinion based on this uncertainty. The respondents in both sectors provided the same answer, but each sector had different grounds to explain why 'lack of trust' was chosen by each sector in answer to this research question.

The respondents of the public sector including the National Police Agency (CTRC: Cyber Terror Response Center), The Supreme Prosecutors' Office

(ICIC: Internet Crime Investigation Center), the National Intelligence Service (NCSC: National Cyber Security Center), the Financial Supervisory Service (FSA: Financial Security Service), the Korea Information Security Agency (KSRC: Korea Spam Response Center and PRIVACYNET) and KrCERT/CC (Korea Information Security Center) provided their professional perspectives to why lack of trust is included as one of the three most serious tensions.

The public sector respondents who were interviewed conveyed a belief that cooperation and assistance from telecommunications providers and Internet Service Providers are essential in dealing with internet fraud because most of the national information infrastructure is owned and operated by private corporations (Cordeiro and Hawamdeh, 2001). This information infrastructure contains digital evidence, which may prove wrongdoings. however, private corporations do not usually cooperate with an investigation in the absence of a Court warrant. What follows are two examples of this:

> Upon urgent requests for cooperation to investigate and examine their log-file and copies of e-mail communication documents, private companies tend to pay no heed to our request. When this happens, we obtain an official warrant from the Court and levy on their property before those documents can be damaged or destroyed (#1). In the instance that evidence is compromised, they may be charged for civil liability (#2).

> It seems very strange to us that private companies would hesitate to aid our investigation as we have no intention to cause harm. We investigate only the incident and do not seek to interrupt their private business. We assume that the negative relationship has been exacerbated by previous police activities against ISPs that occurred between 7-8 years ago when we cracked down on a few companies for copyright violations. Consequently, they are resistant to cooperation (#5, #6).

Non-police respondents in the regulatory authority who control internet fraud through monitoring ISPs provided slightly different points of view to interpret the current situation. They want to be differentiated from the law enforcement agency, however, they are still considered public agencies by

the private sector, whether they have law enforcement authority or not (#5, #6):

> Private companies do not cooperate with us although we are not a law enforcement agency. For their eyes, all public agencies are the same as law enforcement agencies. Because of this reason, they don't trust us. Besides, there are some rumours about our information leaking to the law enforcement and intelligent agency (#5).

In this study, the respondents from the private sector, including Ahnlab Coconut, KOSCOM/ISAC (Koscom), CONCERT, Auction, BC Card. Daum, GCN (National Council of the Green Consumer`s Network in Korea) and the YMCA (National Council of YMCA`s of Korea), expressed an uncomfortable relationship with the police and criticized the partnership policing against internet fraud.

Most business enterprises in Korea have experienced uncomfortable relationships with the police because the police are recognized as a notorious agency. The police lost their accountability as public servants for long periods during the modern political history of Korea when military dictators ruled former governments (Lee, 2004). During this period of military dictatorship, the Korean public police served as puppets for dictators to protect their political regimes (Lee, 2005). Although the Korean political environment has significantly changed during the last decade with the adoption of a democratic system, the image of the Korean public police agency still remains an undependable organization in the eyes of the private sector. Because of their negative reputation, the private sector still prefers to maintain some distance from the public sector (#9).

Most respondents from the private sector believe the police do not focus on the case reported by them. They explain:

> When we report the incident to the police, they do not focus on the incident itself. They always look for other information about our business and company. They are sniffing us! Like a hunting dog! They were not asked to collect other information about us. They have still kept the old image of the police. We feel uncomfortable with their

> interventions in our investigation. There is also lack of feedback from the police about the progress of the investigation. This leads us not to expect any cooperation from the police with respect to the investigation (#9).

However, police respondents criticized the fact that private companies tend to hide information when they report incidents so that it is often necessary to look up other related information to find what they did not disclose. Sometimes that information can be an important tip for the investigation. Too many different views create the gap between two sectors.

Meanwhile, NGO (Non Government Organization) respondents argued that the police do not immediately respond to internet frauds that involve small amounts of monetary loss (#10). As an advocate for the citizens, NGOs often represent victims of internet fraud and other cybercrimes. NGOs have more sympathy with the victimization of internet fraud than the police, so many individual victims have reported issues to such NGOs. They have worked for the benefit and right of citizens so their activities have often conflicted with the public sector:

> It takes a long time to commence the official investigation by the police. Police do not like to investigate fraud cases since it is difficult to prove their criminality and intentions. Police don't like our involvement in the investigation of internet fraud (#11).

However, respondents from the police refuted the fact that the delay of investigation was usually caused due to insufficient evidence and falsity provided by victims. The respondents also said that it takes at least a few weeks to hold a cross interrogation for parties involved in a case.

> We can prove only about 10% of all cases reported to the police and prosecutor's office. Since fraudsters and victims have known for a certain period, it is difficult to prove the criminal intention of an accused person (#2).

6.1.1.2 Different investigation philosophy

Different investigation philosophy is also believed to be one of the most serious tensions by the both sectors, indicating a critical difference between the two sectors. Divergent goals with respect to investigations are often a cause of conflict, which too often results in the nullification of cases (#1, #2, #3). Whilst the private sector conducts an investigation for the recovery of loss, discovery of weak points and termination of the activity (Davis, Lundman and Martinez, 1991), the police conduct their investigation with the goal of achieving criminal justice; this often results in the modification of policies and implemented regulations in order to prevent future offences:

> We have observed many cases that were legally nullified due to damaged evidence and illegal procedure; actions that were intended to reduce losses incurred to the private sector. The private sector has dealt with many fraud cases independently, eventually compromising the case in a manner that makes it impossible for the public security sector to recover any conclusive evidence. Therefore, we have sometimes felt unmoved to assist with cases already handled by the private sector (#2).

Contrary to the police, the private sector maintains a completely different point of view upon conducting their investigations:

> In the face of huge amounts of economic loss, sometimes we have to conceal an internet fraud case in order to protect indiscernible assets, such as our brand name, reputation and e-marketing. Should details of an incident leak, the public will not want to use our site for purchasing merchandise, so we have to maintain the confidentiality of an occurrence for the sake of safe marketing. When bad news leaks to the market, sales will be significantly hindered and the company may fall into a deep slump. Although we know that we have to punish those fraudsters, it may be at the expense of financial damage to our e-business (#10).

The respondents in the private sector reported that they focus more on business outcomes while the public sector focuses more on legal issues. The private sector has often used an investigation process as a fraud control strategy (#12). If fraudsters know that investigation has taken place, they may not continue their criminal activities. As described earlier, each sector has different interests to pursue in order to achieve their aims and objectives.

For the private sector, the goal of criminal justice does not fit their aims and objectives. Private Justice focuses more on loss prevention and risk management. Deterrence and prevention of fraudulent activity is better for the private sector than the arrest of offenders.

> Arrests of criminals and successful prosecutions are important to accomplish the goal of the public security and criminal justice. However, private companies prefer not to involve the formal investigation. It costs more money than what we have lost (#11).

The private sector prefers to handle Internet fraud through their corporate expertise while they maintain the reputation of having safe business environments. They believe that the news of a fraud incident would cause more forfeiture than the internal make up of loss due to Internet fraud (#11). Corporate security departments are usually under the supervision of corporate legal office, but some of them work independently depending on corporate structure. Corporate lawyers often advise the security department on how to deal with serious fraud cases. Private companies tend to solve problems discreetly because it is usually not worth reporting to the police because of cost and outcome (#12).

6.1.1.3 Lack of legal perception

Lack of legal perception is believed to be another of the three most serious tensions between the two sectors, as chosen by the public sector respondents. Since the private sector tends to lack sufficient legal knowledge, they often break the law without intention. However, regardless of whether or not they do have the intention of breaking the law, legal infringements will nonetheless be punished (#2):

> Because of the internet's relatively short history, people often do not know what may be deemed as a violation of law. Due to this lack of awareness surrounding security laws, ISP provided personal information without the permission of user, and thus unknowingly committed an illegal act. In order to avoid future prosecution due to the violation of IT related laws, they must educate themselves on these laws and maintain awareness of them! It does not work to say 'we did not know' (#2). In practice, almost every ISP has had to pay fines for the absence of

> provisions in their service at some point in the past. How ridiculous! They have interest in making money but did not know how to prevent any potential liability they might face (#2).

Sometimes, private security departments have overreacted during investigations and have embarrassed the police and related prosecutors. Tracking down and hacking a private person's computer is still an illegal act in Korea. The best thing they can do is to report the incident or location of offender to the police. Without reporting an incident to the police, loss of fraud cannot be recovered by the insurance. The private security sector should have enough legal knowledge before they conduct their own investigation. Breaching of the criminal procedure will eventually lose a case and the offender (#1).

> Protection of private information law prohibits any person to look up the private information without permission of the person. Many private sector investigators have ignored and broken this law for their investigation. ·It will cause the loss of the case due to illegal acquisition of private information (#2).

IT security staff in the private sector do not have sufficient legal study background so they have often ignored how to respond to fraud incidents. Their decision making processes often cause them to make mistakes in terms of legal procedure. Sometimes, they do not know whether it is a civil or criminal matter. Despite this, the private sector is well equipped with high technology; humans are the main actor of the decision-making process (#2).

There is growing concern about the legal education of IT company's employees with the development of Information Technology. The law is always one-step behind technological development. As technology advances, criminals are getting smarter and crimes are getting more complicated. Providing legal education to security staff must come first in order to respond to those smart fraudsters. Some fraudsters who commit large scale fraud have better legal knowledge than security staff members (#2). Recently, the internet has become a good communication tool for exchanging useful fraud skills among criminals. Fraudsters have a forum for

exchanging criminal information and updated scams for possible projects (#10).

> Fraudsters are very smart. Smarter than you think! They are well aware of laws. However, IT security staffs or ISP staffs are engineers. They are not really true private security experts in other Western countries. They do not have a legal mind, which security experts must have. Basic legal education and regular workshops are probably needed to improve the quality of security staff (#2).

It has been advised that participating in workshops, seminars and conferences for the introduction of updated laws can improve the lack of legal perception of the private sector employees. Employment of experienced workers who have a legal background would improve the staffing of an IT company and is believed to be another way to solve this tension. However, IT companies have rarely recruited in-house legal counsel. They usually outsource legal service for the protection of intellectual property and patent related works. Respondents from the public sector in this study reported that providing regular sessions of basic legal education gradually improves the legal perception of employees:

> Only a few Korean companies have provided legal education for the employee while IBM, Microsoft and other large IT companies have provided legal education for their employees in order to protect their valuable assets and prevent any legal liability. In Korea, more private companies have been recommended to prepare legal education programmes by regulatory agencies (#3).

As Korean companies depend on more lawsuits and litigations for protecting their intellectual property and assets, more legal education should be provided to their employees and customers in order to avoid any serious liability from unawareness or ignorance of related laws (#2).

6.1.1.4 Negative publicity

Negative publicity has been noted as another serious tension by the private sector. According to Jones, 'many companies are afraid to report fraud incidents because of the potential for negative publicity, and loss of goodwill' (Jones, 2006). The private sector tends to be hesitant to report

cases to the police out of fear for their brand image, which is any company's most valuable asset. Wall (2001: 174) argued that use of 'the public criminal justice process may expose their weakness to their commercial competitors.' Through the internet, negative publicity spreads by a mere click of the mouse, and can cause a wide variety of undesirable effects. Negative publicity on the Internet is unfair and can damage any company significantly. According to a PWC (Price Waterhouse and Coopers, 2001) survey, 39% of UK companies did not report incidents to the authorities. 80% of companies who have been victims of fraud remain confident of their control systems, despite the high incidence of overall fraud rates and the apparent ineffectiveness of existing anti-fraud procedures (Out-Law, 2001).

Private companies believe that the police cannot protect them from negative publicity (#10):

> Well, I don't like to say this, but it is true that the police do not consider how important it is to maintain confidentiality of a company's profile with regards to an internet fraud case. They often disclose information to reporters, and hence, embarrass us. For this reason, we usually find someone who can better trust the police and then report the incident through our reliable channel (#10). The police are much too bureaucratic in their political organization. They do not consider our situation in the competitive market (#10). Their bureaucratic culture does not reflect our needs. It will take a long time for the police to understand that the private sector's interest is also the public's interest (#11).

Many companies believe that it takes quite a long time to recover from the loss of negative publicity. The value of breached firms could be damaged. Customers tend to avoid using incident prone ISP services and have looked for more secure business transaction methods. The recovery time for a good reputation and brand loyalty could consume more time and money than private companies have, and so they have overlooked or unreported incidents to the police (#12):

> We believe that it takes too much time to catch up the loss of negative publicity. Once a company's reputation goes bad, a negative image of the company will stay for long time. Rein over the good reputation of company is more difficult than to make a brand new one. Look at the

> Hanhwa scandal; the misconduct of its CEO has critically ruined his company's reputation (#13).

The respondent of the public sector in this study reported that Internet fraudsters have continuously penetrated the private sector where they deceive someone to steal from private companies and their customers. Internet fraudsters know that private companies tend not to disclose their victimization and have used this vulnerability for continuous attacks. The fear of negative publicity has frightened private companies and has discouraged them from reporting all incidents. Because of this reason, both sectors' respondents have suggested a mandatory reporting policy (#1, #2, #10, #11).

> Negative publicity can be prevented if companies announce their damage or loss caused by fraudulent activity as soon as company recognizes it. Insurance will pay for its damage to their customers. They don't need to hesitate to inform their victimization. If they attempt to conceal their incident to protect for their brand image and customer loyalty, it will cost more than they had to pay for it. Negative publicity that is made from the incident that happened is less than the negative publicity that is made from the dishonest act done to their customers and the public (#1).

Insurance investigators report on company staff and clients of any doubt, and give vital independent corroboration of the company position without exposing it to the negative publicity a police inquiry might generate.

6.1.1.5 Adverse impact on stock value

Adverse impact on stock value is believed by individuals in the private sector to be another source of serious tension in their sector. This has a causal relationship to negative publicity. When an author or a newspaper editor posts an article with the intent to influence a stock value, its value could be changed. Practically speaking, the stock market is very sensitive and unpredictable, and when a police investigation is made known to the public, falling stock value may cause the company to collapse, even if the company is not necessarily at fault.

It was previously suggested that private companies should announce the incident before any negative news is broadcasted. The official announcement of an incident may direct the public to consider it not as serious as the actual damage is, which could positively affect the stock value. However, no one can guarantee how the general public would react after he or she heard about the incident. Therefore, at this point in time private companies cannot easily decide whether they wish to publicize incidents of fraud or not (#13).

> The rise and fall of stock value cannot reflect how much a company is honest or not. Investors would like to maximize their investments so that they do not give any credit for the incident reporting. Whether an incident happened or not, companies have to maintain that their stock value has continuously ascended (#10).

Avoidance of adverse impact on stock value cannot be guaranteed although there is a confidential investigation and embargo of media reporting. The stock market has its own intelligence network to exchange necessary information. Compared to other private companies, stock market intelligence is very accurate and reliable. Usually, intelligence is produced among stock analysts and fund managers through IR (Investor Relations) among the major stock companies. This intelligence is not shared outside of their network and it is meanwhile preserved for them only, however, alarming news goes out quickly and it significantly influences stock value.

> We have to consider the balance between stability of business and justice. If we could prevent adverse impacts on stock value with a reasonable amount of money, it would be much better to pay for the loss without reporting to the police. Once an incident report goes to the public, we have to pay more money than was our loss caused by fraud (#10).

Efficiency in police investigations and conviction rate when combined with the revision of the *Acts on Promotion of Telecommunications Network Utilization and Information Protection* in 2007 would reduce loss from internet fraud.

Other serious tensions

Interviewees were asked to consider ***other serious tensions*** *they perceived to have an effect on the policing of internet fraud in Korea. Based on respondents' answers, the perceived negative influences on policing internet fraud were used to structure the second part of this chapter:*

Tensions between the private and public sectors (see Table 6-1)

- Lack of sharing information
- Lack of convincing material
- Lack of communication
- Political influence.

6.1.1.6 Lack of sharing information

The respondents from the public sector reported that they shared limited information with other sectors such as crime reports and security levels of networks. Other important information sharing has been done through human relationships between people who have previously worked together or have otherwise known each other. One of the respondents from the public sector reported that there is too much competition among public agencies for them to become major partners of cyberpolicing with the private sector. Recently, the NCSC (National Cyber Security Center) signed a MOU (Memorandum of Understanding) with many private companies to develop internet security software together and share the updated information. Because of this support from the private sector, the public sector has expected a more cooperative environment toward a partnership to police internet fraud together. According to McKenzie (2006: 271), 'partnership meant information sharing.'

> We, the police, have put a lot of effort to develop a better relationship with the private sector. However, the private sector has confused which agencies to share their information with because many public agencies have participated in policing internet fraud. It also needs an establishment of information sharing system within the public sector (#1).

The respondent in the private sector argued that the public sector asks more confidential information from the private sector while they provide the

general public with information that they can find on the internet. An asymmetrical flow of information creates more tension between two sectors and a hostile relationship. However, public sector respondents reported that symmetric information sharing is impossible since the public sector has too much information that is protected by the protection of personal information law.

> I believe that the protection of personal information law has promoted the problem of asymmetric information flow. In order to promote a better information and communication process, another law to support effective communication between the two sectors must be established (#2).

The respondents in both sectors reported that more interchange of information, knowledge and other resources would help to understand each sector's upfront issue. Personnel interchange between sectors was considered the most effective way to do this; however, it has been implemented in only limited areas of business with the government agency. Close cooperation between private and public sectors of security is considered an important factor to improve the overall capacity of policing internet fraud; however, each sector has not prepared to disclose its own weakness to their major competitors.

6.1.1.7 Lack of convincing material

The respondents in the public sector have often felt that their activities were misunderstood by the private sector although the public sector has had good intentions to do them. Unfortunately, there is no convincing material to explain what they are doing and how it is beneficial for them. Convincing material is a tool of communication for the private sector by having the advantage of boasting volumes of readers and the capacity to preserve materials. However, the production of convincing material costs money and professional effort. Therefore, many public agencies have not carried this out (#2):

> Our work has often been misunderstood by the private sector since we cannot provide any material that explains our purpose of work. So we

> have to provide more convincing materials and public awareness programmes for the general public (#2).

Distribution of convincing material to the private sector will improve their relationship and prevent possible disagreements in future projects. However, organizational culture and budgetary restrictions have impeded the production of convincing material and have caused some tensions between the two sectors.

NCSC/NIS as a part of the intelligence agency has distributed much convincing material to the private sector in order to receive more support to become a central player in cybersecurity while other law enforcement agencies have not yet attempted it due to insufficient budgets and administrative procedures.

> You can see that the National Cyber Security Center Brochure to public and private organizations is a good example of the distribution of convincing material which other public agencies have not attempted due to substantial cost (#1).

The respondent also reported that convincing material is different from PR material in terms of promotion of partnership policing internet fraud. It should have a good explanation of partnership policing and guidelines to partnership policing so that the private sector is able to carry out all necessary functions.

6.1.1.8 Lack of communication

The respondents in the public sector argued that lack of communication was created by the self-centeredness of the private sector. Although some efforts have been made by both sectors such as co-hosting conferences and workshops, they are still in the beginning stages of creating a partnership and they need more efforts to develop the appropriate communication system to link the two sectors together for effective partnership policing (#2).

CONCERT (consortium of KrCERT) is a good example of a communication venue for the purpose of exchanging and sharing

information in order to protect our information network systems. More than 300 private security units and government agencies are sharing information through CONCERT's communication channel. CONCERT members are able to send real time messages and any inquiry can be distributed all members to obtain their expert opinion:

> I think that it is the fastest way to get help when any incident occurs online. Our members are very cooperative and reliable so I feel very safe as if I have my own back-up troop. CONCERT emergency alarm system runs for 24 hours per day, 365 days per year (#11).

The respondents in the private sector criticized that the lack of communication was a product of the former authoritarian governments. During the authoritarian regime, only one-way communication was really practiced by the public sector. Even though Korea's authoritarian government has been overturned, its conservative culture has still remained in some parts of the public sector and their communication practices have not satisfied the private sector:

> Well... [there have been] a lot of changes in the public sector. They now know how to communicate with the private sector. And, they have to put more effort into establishing a better communication channel with us. It is however necessary to appoint a communication or liaison officer who is to maintain a regular communication channel (#13).

The respondent from the public sector reported that a personal relationship rather than an official communication channel has made the most communication headway. The respondents reported that the official title of 'Information Officer' (IO, NCSC) and 'Liaison Officer' (NPA) sometimes hinders increased communication with the private sector.

> When we go out the field, we want to be called by first name or brother. We do not want to be called by our official rank such as 'Inspector' or 'Superintendent'. Those call-names create a gap between the informants and us (#1).

6.1.1.9 Political influence

Political influence that deters the growth of private policing has been found to be another tension between the private and public sectors. According to Napoli (2001), communication policies and regulations are products of institutional power dynamics and struggles and have social, cultural and political influences. Generally, authority and wealth cannot be given to one single party in Korean society. Because of this deep-rooted principle, the private sector was given limited power to participate in policing cyberspace. This is also likely to further exacerbate existing political and competitive tensions between the two sectors.

Abrahamsen and Williams (2005: 13) said this is where 'policing ends and private security begins.' However, contrary to Western nations, Korean society has not prepared to adopt the full package of private policing which has perceived the private sector as a formal partner to policing cyberspace. Private policing is still seen as auxiliary to public policing (#1, #2). Many large private companies want to expand their security business' capabilities to be entitled to police cyberspace but the government has not given any sign of approval for their active participation because their participation may disregard the public sector's position in the policing of cyberspace (#11).

The public sector does not allow the full ownership of policing internet fraud whether the private sector has better knowledge and technology or not (#13).

> As a profit organization, we are not supposed to participate in policing internet fraud without an official letter of support from the public sector for our cooperation in an investigation. We provide only secondary work although we have professional knowledge (#11).

A recent announcement declared that the Presidential Commission on Judicial Reform made a decision that judicial reform will be carried out which may encourage development in the privatization of Internet policing in Korea. Beginning in 2012, the current Korean Bar Exam will be abolished and it will be substituted with a law school system. As a result of

this judicial reform, the Korean criminal justice system will be changed, mimicking the US system, and will hence need more support from the private sector.

From a private policing perspective, this is a very good opportunity to implement a more effective and efficient policing system in Korea. To date, judicial reform has halted the reformation of the policing system due to criminal procedure law. Independent police investigations will be implemented if the current criminal procedural law also changes. Privatization of policing will also develop at a fast pace, as police reform will take place. Eventually, policing internet fraud by the private sector will not be affected by any political influence.

The most serious tension of all

Internet fraud experts in the private and public sectors interviewed for this study reported that ***lack of trust*** is the most serious tension, which as a consequence deters the efficacy and efficiency of policing internet fraud. As reported, this tension is caused by mutual scepticism by both sectors. Both sectors reported lack of trust to be the most serious tension between them, however, each sector had a different rationale for this belief.

For the public sector, it was believed that the lack of trust between the sectors is a fundamental demoting factor for the cooperation between sectors to police internet fraud.

> Private companies and NGOs do not trust us so we have a hard time dealing with internet fraud. In fact, we have lost many cases that had been compromised due to the inadequate investigation by the private sector. They must know that the police are not working for the clean up of ruined investigations by the private sector (#1).

The private sector believes that the lack of trust is a critical factor in deciding whether or not the private sector will report a fraud incident. It seems that the private sector recognizes the lack of trust in terms of police accountability. The difference in responses suggests that the public sector is more concerned with the mechanism of policing, whilst the private sector is more concerned with the outcome of policing internet fraud.

We have been disappointed to see how the police handled internet fraud cases. In order to prove any criminal intentions in a fraud case, an agency needs to be prepared from the initial stage of investigation and if they fail to be so, they will inevitably release the criminals. However, the police have dealt with internet fraud as the same as conventional crime. Even at the terrestrial level of fraud, cases require a lot of effort to prove their intentions; internet fraud has to be dealt with special expertise (#11).

Too many different perceptions of tension between the two sectors make it even more difficult to reconcile their peace talks. Neither of them would like to give up their current position even to pursue their own interest. Although both of them are aware of an overlap of interest with the other sector, their cross-sector power game does not allow them to provide any ground to surrender their advantaged positions.

6.1.1.10 Rational of selection

Why do you believe that is the most serious tension between the sectors?

Respondents in both sectors interviewed in this study reported that lack of trust is the most serious tension since public and private sector security cannot effectively control internet fraud while criminals are getting smarter and crimes are getting more complicated. Tensions between the two sectors may create a blind spot that will not allow each sector to reach their ideal policing authority level. However, it is necessary to make sure there are no dark corners where internet fraud can occur (#1, #2, #3, #10, #11, #12, #13):

> We have to draw a clear line of jurisdiction in order to avoid overlapping or missing place in cyberspace. Too much check and balance between two sectors makes blind spots so that criminals are acting in the vulnerable areas (#2).

From the public sector's perspective, lack of trust has negatively affected their partnership with the private sector in terms of police accountability. Although they have tried to overcome the shortcomings, long-time distrust cannot be easily removed. It needs more time to change.

> For the successful investigation and prosecution, trust between the private and public sector is an essential tool to link each sector. Without trust, each sector has to waste energy on psychological warfare in order to get more power to police internet fraud (#1, #2).

From the private sector's perspective, lack of trust has negatively affected partnership with the public sector in terms of a policing division of labour. Pluralization and multi-lateralization of policing is an international trend, however it has been believed that Korean law enforcement agencies and other related public sectors do not want to break up and give their cyberpolicing area to the private sector.

> As you know that the policing of internet fraud by the police is very limited since the police do not have sufficient know-how to investigate cases. However, the police do not want to be treated as a partner of the private sector. Despite the horizontal relationship between the two sectors, the public sector always wants to control the private sector (#11).

Origins of tension

Why are those tensions produced?

Respondents in both sectors in this study reported that the self-interest of each sector has created those tensions in order to take an initiative of policing internet fraud. The private and public sectors separately 'seek to establish monopoly control over areas which are currently in the public domain of cyberspace' (Wall 2001: 169). Policing internet fraud is not done solely by the public sector. Most Internet fraud occurs in the private domain so the private sector naturally has a better know-how to respond to the fraud incident. In particular, financial fraud requires great professional expertise for the investigation. There has to be someone who knows the banking system well enough to track down the criminal. However, the private sector does not have any legal authority to investigate that type of criminal activity. Thus, fraud incidents should be reported to the police for formal investigation. Because of this complicated nature of internet fraud investigation, the two sectors have to assist each other to perform to their full capacity of investigation with the expertise they can both contribute. Therefore, policing internet fraud cannot be owned by any one sector.

> Monopoly of ownership of policing internet fraud or cybercrime is impossible because cyberspace cannot be owned by any one sector. Cyberspace is a new arena for all sectors so it does not allow any exclusive ownership of its territory. It is a land of freedom (#9).

The private sector respondent argued that the public sector investigators tend not to share the merits of successful investigation with the private sector. However, the respondent said that they would like to share the liability of any malfunction of policing or investigation with the other sector. This contradiction has exacerbated the public sector's view of its relationship with the private sector. It has been claimed that there will be no true partnership policing until the public sector truly realizes the importance of the private sector.

> The public sector does not know our capability and potential power. They just think us as an 'extra side dish' of policing. Without our assistance, they cannot respond to internet fraud. Internet fraud requires a more advanced level of investigation, which is obtained from the private sector's support (#12).

The third party experts reported that tensions were created due to power struggles between sectors. Each sector has attempted to obtain the hegemony of cyberspace and to draw a line around their jurisdiction in cyberspace. There is no mechanism to manage this situation and there is a need for more appropriate laws to define what kind of act can be done by each sector. Clear responsibility of each sector would remove tensions (#1, #2, #9, #10):

> Simply, cyberspace is a ground where the competition has not been finished. No one knows who is going to win. It appears that one sector cannot compete alone. Anyway, competition surrounding the ownership of policing internet fraud by two sectors will contribute to crime prevention in cyberspace if they have good intensions for it (#13).

Influence of tension

How have those tensions influenced your working practices for response?

The respondents in the public sector reported that those tensions have significantly influenced working practices in two ways: deception of evidence from the private sector and failure of prosecution. The deception of evidence from the private sector has often occurred due to the understood tensions: lack of trust, lack of legal perception and different philosophy of investigation. Because of those tensions, the police and Prosecutors' Office tend not to trust evidence from the private sector and they confirm many facts before commencing the formal investigation. They list what they receive from the private sector. The private sector has often been confused whether an incident is civil or criminal, due to lack of legal perception. Sometimes, fraud incidents have been reported and in the end are found as minor civil cases which exhaust police and further stiffen tensions.

> Fraud incidents must be passed to the police quickly without any contamination of evidence. However, the private sector tests so many things until they find that they cannot properly handle these cases. Because of tainted evidence, we have lost many of these cases (#1).

In order to accomplish a successful prosecution, there must be good collaboration between sectors for the investigation, thoughtful preparedness of legal procedure and purpose of justice attainment. Without support of these conditions, successful prosecution cannot be achieved. From the initial stage of investigation to the litigation, the private and public sectors should perform good cooperation in order to beat criminals (#1).

> Perfect condition of criminal investigation would bring out successful prosecution. If any insufficient conditions exist, failure of prosecution may result and criminals will be released without any legal action (#2).

The respondents in the private sector of this study reported that those tensions have been significantly influenced by working practices in two ways: private sector use of private connections for police investigations and by reporting only serious incidents to the police.

In cases of internet fraud, private sector investigators contact an acquaintance in the police to solve the problem. They do not want to report to unknown people in the police force who may not help them with the

result of the investigation. If the investigation result goes to the public. negative publicity of their company's network system may result and have an adverse impact on stock value and decrease in sales. For this reason. private companies hire former high-ranking police officers as security managers who could influence the direction of police investigation.

Private companies prefer to handle incidents internally as long as they do not find any significant difficulties in their investigation. If they do find difficulties they find serious legal breaches. Confidentiality of investigation and non-legal solutions have been preferred by senior staff of companies and so, private sector investigators reluctantly report only serious incidents to the police. The selection of serious incidents that require reporting to the police depends on the volume of victimization. If many victims are involved, confidentiality of the internal investigation with the private sector is impossible.

> We would like to handle the incident internally if there are only a small number of victims involved. However, phishing and pharming involve too many victims so that it is better to report those cases to the police. Redemption of loss from those incidents is almost impossible. Since offender, server and wired money are all physically located in different places it takes a long time to investigate those incidents (#13).

Most serious tensions within the public sector

*Interviewees were asked to explain the **three most serious tensions within the public sector** that they perceived to have the most effect on policing internet fraud in Korea. Based on respondents' answers those that responded negatively to influences on policing internet fraud were used to structure the following part of this chapter.*

Tensions within the public sector (CTRC, NCSC, ICIC, FSA, KISA. KTFE, KrCERT, KSRC):

- Lack of trust
- Control of investigation results
- Lack of appropriate laws
- Accountability

- Different aims
- Role play
- Different levels of power
- Special law enforcement powers

Table 6-2: Tensions within the public sector

Public agency	What are the three most serious tensions?	Why those tensions are produced?	How do those tensions influence your work in terms of your working practices for response?
CTRC/NPA	*Lack of trust, control of investigation results, and lack of appropriate laws*	Monopolization of investigations	Depression of occupation
ICIC/SPO	*Lack of trust, control of investigation results, and lack of appropriate laws*	Challenge to the criminal procedural law	Repetitive investigation
NCSC/NIS	*Different aim, role play, lack of appropriate laws*	Lack of understanding of our mission	More efforts to convince others
FSA/FSS	*Lack of accountability, appropriate laws, special law enforcement powers*	Special knowledge	Heavy work load
KFTC/MFE	*Lack of accountability, role play and appropriate laws*	Organizational power game	Heavy work load
KISA KrCERT KSRC	*Role play, different level of power, lack of appropriate laws*	Ambiguous status between the public and private sectors	Limited power without law enforcement

6.1.1.11 Lack of trust within the public sector

The three serious tensions within the public sector vary across different agencies. The respondents in the National Police Agency (NPA) and the Supreme Prosecutors' Office (SPO) reported lack of trust, control of investigation result and absence of appropriate laws to be the three most serious tensions. These tensions overlap between the two agencies. Lack of trust was also found between the private and public sectors. Simply put,

policing bodies do not trust each other in terms of cyber-hegemony. There is currently a war 'without sounds of shooting within the public sector' (#1, #2, #3).

The respondents interviewed in this study reported that the characteristic of 'lack of trust' within the public sector is different from the characteristics of lack of trust between the private and public sectors. While the lack of trust between private and public sectors have been found due to a hostile relationship between sectors, the lack of trust within the public sector has been found due to a competitive relationship within the sector.

Policing internet fraud as a part of the governance of cyberspace is considered a most important activity by many public agencies in the information age. The internet has been used as a great force to craft many things although it can also be misused as a criminal tool. The control of the use of the internet is a key factor to obtain the political power that involves policing activity (#2).

> Now, policing cyberspace has become a major issue among all law enforcement agencies. Every agency wants exclusively to obtain the power to control the internet and its users. Internet will continuously be used as a great force for human society although it will also be used as a criminal tool. Internet will ceaselessly shape our society (#2).

Digital government is a popular term used by the government in Korea. This implies that public organizations transform through digital technologies. From local governments to the central government, digital technologies have connected all agencies within the public sector. For example, the police share useful criminal information with local police forces across the country. 'Most wanted' criminals are online and Interpol's 'red notice' can be seen on the Interpol website to be publicized. Patrolling police officers can confirm anybody's identification through hand-held mobile equipment. The Prosecutors' Office can see the progress of the police investigation through the internet. The Court receives important legal files from the Prosecutors' Office through the internet. Thus, all important

criminal justice information is being processed through the internet today (#1, #2, #3).

> The concept of e-government, digital government and cyber government has been used by many nations. Without talking about information technology, public administration seems outdated and inefficient. We have invested huge amounts of money to transform our system to a digitalized one because it will build a true competitive power for the nation (#3).

However, some criminal information is not shared among agencies due to its high value for the particular agency. This self-interest of organization further generates the lack of trust within the public sector. Many respondents in the public sector reported that important information is not shared by other agencies although some cases require strong cooperation with other agencies. Nevertheless, each agency wants to achieve the merit of performing successful investigations. Ownership of policing cyberspace is another factor that promotes a more competitive working environment among public agencies. Policing internet fraud has attracted many public agencies to take part since police or non-police agencies can respond to internet fraud. Every agency wants to become a major actor of policing cyberspace since there are no qualifications yet defined (#1, #2, #3, #4, #5, #6, #7).

> It is impossible to give up our policing activity in cyberspace since it is a new opportunity for developing our agency to govern the new territory of the future. Competition for the ownership of policing is a very natural phenomenon (#2).

The respondents interviewed in this study uniformly reported that lack of trust can be removed within the public sector if there is no competition among the public agencies. However, it is practically impossible as long as multiple policing bodies exist. The majority of respondents believed that the establishment of clear jurisdictions and duties for each agency would relieve the competitive environment. Without establishing strict regulations or laws, each agency will continuously compete for the ownership of policing internet fraud (#2, #12):

> This boiling competitive environment produces a lack of trust among agencies to compete for the ownership of policing internet fraud. Until we find out who is the winner of the game, competition and lack of trust will not disappear (#1).

6.1.1.12 Control of investigation results

The control of investigation result is one of the most serious tensions within the public sector. Particularly, this tension between the prosecutor and the police has been known as the most serious one. The results of an investigation can be different depending upon the main agent of investigation. The current Korean criminal justice system has two main investigation bodies, the prosecutor and the police. In general, the police conduct most criminal cases. According to the criminal procedure law, the police begin and end an investigation under the supervision of the Prosecutors' Office. Generally, 90% of cases investigated by the police have been accepted by the Prosecutors' Office without any significant changes. The prosecutor only conducts the investigation when the internet fraud case has been directly reported to them or when some serious case was detected by the Prosecutor's intelligence. If a directly reported case is not serious enough, the case will be sent to the police for them to conduct the investigation. As a subordinated agency, the police have often found that their investigation results change at the Prosecutor's Office.

The police often feel enervated when prosecutors change investigation results without reasonable explanation. Because of the right of arraignment from the prosecutor, offenders tend to confess more crime facts to the prosecutor. Although Korean criminal justice procedures do not allow a plea bargain, offenders believe that their punishment can be reduced at the Prosecutor's Office if they confess or provide more important crime information (#1):

> Career criminals know that their punishment will be reduced if they provide more criminal information before the prosecutor so that they tend not to disclose all information at the police department (#1).

From the prosecutor's perspective, the police are the gatekeepers of the criminal justice system because offenders are arrested and booked by the police. Some prosecutors believe that the police sometimes do not pass what they find from their investigation to the prosecutor for many reasons (#2):

> We had to investigate many cases that were not completely investigated by the police due to complaints from victims. It is a waste of time and money for taxpayers. Because of this reason, we are strongly opposed to the independent investigation of the police (#2).

Similar tension has also been found between the police and non-police public agencies. Non-police public agencies have an authority over private companies through administrative sanctions to restrict their business activities. The non-police agencies concern is the police or prosecutors who have too much power whereby they are not able to have control over the results of investigations. Sometimes, similar offences result in totally different outcomes. Law enforcement agencies, for example, have a greater understanding of public interest and criminal justice, whilst non-law enforcement agencies have more socio-economic or political considerations for Chaebol (business conglomerate):

> Law enforcement agencies always solve their problems as criminal matter so private companies have maintained some distance with the police and the prosecutor. They do not know the soft way to handle their cases. According to our experience, many cases can be solved by non-criminal justice procedures (#7).

The respondents in the non-police agencies reported that inconsistency of investigation results diminish the reputation of the law enforcement agencies whereas consistent investigation results would help to build the accountability of the related law enforcement agencies. It would also remove tension within the public sector.

> For the same case, investigations completed by police and prosecutors are sometimes too different. How we can understand this happening? More harmonization is needed between the police and the prosecutor's investigations (#6, #7).

6.1.1.13 Lack of appropriate law

An absence of appropriate law is selected as another serious tension within the public sector. This lack of legal foundation has caused a chaotic environment of policing internet fraud, as each agency does not know when they have to be involved in their investigations. This confusion has also negatively affected the private sector in that they do not know which agency is to be the main investigator of the incident:

> Too many agencies put their spoons on the same table! It is ridiculous that no one knows how much food each can eat (#2).

The public sector is concerned that the current law does not precisely describe their activities and does not clearly define each agency's role and responsibilities. For this reason, potential conflicts exist within the public sector in terms of competition for jurisdiction (#1, #2, #3):

> I believe that the current Internet related laws are like stopgaps that contain many blind spots. They do not fully cover what they are supposed to do. We did not have the sufficient knowledge and vision to see into the future when we made the laws. Law professors, a computer science professor and telecommunications experts made them; however, no single person understood everything as a whole. Laws were made to include various concerns but they are not consistently linked each other so we have gradually revised them and now many problems have become evident to us (#10).

Like other public sector respondents, the respondent from NCSC/NIS criticized that there is no appropriate law to define which public agency has to deal with internet fraud as the main actor of investigation. The current *Criminal Law* and *The Acts on Promotion of Telecommunications Network Utilization* do not precisely describe what constitutes Internet fraud and where incidents should be reported. Many respondents of this study reported that internet fraud should be policed by both sectors and the law must preserve the investigation authority for the private sector.

The respondent from the FSA in this study had also seen it as a serious tension because this anarchic situation forces public agencies into confusion. There are many questions raised about who is the main actor of

investigation of internet fraud. The existing law does not prescribe internet fraud as a single category of crime. It can be punished by the current *Criminal law* (Article 347-1, 347-2) and *The Acts on Promotion of Telecommunications Network Utilization* (Article 48-3, Article 62-5). The making of internet fraud law has been debated by many scholars.

KISA and its subsidiary agencies: KrCERT and KSRC found that existing laws cannot appropriately control the use of the internet. *Criminal law* (Article 347-1, 347-2) and *The Acts on Promotion of Telecommunications Network Utilization* (Article 48-3, Article 62-5) have been used to deal with internet fraud and other internet crimes. However, this law and acts cannot completely cover all internet fraud. Internet fraud is distinct from conventional fraud in that it occurs in cyberspace. A different model of policing and law should respond to it. However, there has been a lack of study with regard to this subject, and so making appropriate laws is not an easy task. More efforts to make laws from both sectors will solve this problem.

6.1.1.14 Different aim

The respondent of the NCSC argued that other public agencies do not need to compete for the ownership of policing internet fraud with the NCSC. Since the NCSC has a different aim of policing cyberspace, its activity cannot be compared with other public agencies. As an intelligence agency, there are many clandestine operations for national security, and no matter what they cannot disclose their original intentions. Secrecy of the agency has always amplified their surreptitious power and has kept away other agencies and organizations. However, the NCSC has strongly persuaded other groups that policing cyberspace or internet fraud is not a major activity of the NCSC. What the NCSC has focused on in the matter of policing cyberspace is the control and coordination of the security network among government agencies.

> As you know, we are not on the same ground that other public agencies compete for. According to the National Cyber Security Regulation, Presidential Direction No. 141, we protect the national infrastructure system of telecommunications and networks. As you know, we do not

> have any law enforcement power except for espionage. If we find any criminal information, we pass it to the police or the prosecutor to handle it (#3).

Other public agencies have been blamed for participating with the NCSC/NIS in policing cyberspace. The NIS participation in policing cyberspace has shrunk the power of other policing agencies. The NCSC has stepped into policing cyberspace after other public agencies spent more than 10 years in the field. The NCSC revealed their superior budget and power of agency and have taken over the first place in policing cyberspace although they have a different aim for policing cyberspace. Their allegations still have not convinced other public agencies in terms of participation of policing cyberspace.

However, third party experts argued that the establishment of the NCSC/NIS has contributed to the protection of the national information infrastructure and network system. The respondents also argued that their security activities are not the same as the police provide in terms of policing cyberspace. Therefore, other agencies do not need to compete for the ownership of policing cyberspace with the NCSC/NIS.

> I know that other agencies have concerns about the NIS cybersecurity activities in relation with the establishment of a special terrorism act. Some people also argue that the NIS will eventually take over the ownership of policing cyberspace. There had been exaggerated anxieties about this since the NIS had a notorious image of using their resources for illegal eavesdropping. I can say that NIS cybersecurity activities do not focus on policing activity but that it does focus on the protection of the national information infrastructure and network system (#11).

6.1.1.15 <u>Role-play</u>

The respondent of the NCSC/NIS criticized the fact that there is no clear role play defined for each agency within the public sector. Each agency should concentrate on its original role in policing cyberspace. For example, the NPA focuses on the prevention of crime, the FSA focuses on financial security and KISA focuses on the response of internet incidents. However, these agencies have acted outside of their original role and have

transgressed others' jurisdictions. It suggests that the policing of cyberspace is very attractive to all public agencies.

Among the public agencies, KISA has a dual role to play in terms of official standing. KISA was established to support private sector companies. However, private companies consider KISA to be a part of a government agency so they do not fully trust KISA as an ally. The respondents from KISA blame the public sector for their ambiguous role within the public since it confuses others of KISA's characteristics. KISA's central position between the public and private sectors prevent it from carrying out more effective policing activity.

> We work for the private sector but private companies do not trust us because we are under the supervision of the Ministry of Information and Communication (MIC). Although KISA is a subordinate agency of MIC, we were established to support the network security of the private sector. However, many private companies misunderstand why we exist and what we do (#7).

Despite KISA's claims that they have supported the private sector for a long time, there are still rumours going around about the composition of executive members of KISA. Because there are few former NIS agents appointed as executive members, it has been continuously questioned whether KISA has provided to legally protect information from the NCSC/NIS or not. The respondent of KISA answered that they only provided the volume of internet incident data to the NCSC/NIS and it did not include detailed information. Since KISA has worked for the internet security of private companies, government agencies and other research institutes have often contacted KISA in order to obtain private companies' related information.

The respondent from the NCSC/NIS argued that other public agencies have to understand the difference between 'national security' and 'crime prevention'. Policing cyberspace through the NCSC/NIS is not for crime prevention but is more focused on information security. The NIS does not have an investigation authority over cybercrime while the police officially

has. Although the NIS does not have investigation authority over cybercrime, they can directly report to the Prosecutors' Office without passing by the police. Because of this reason, police agencies have felt that their policing authority has been challenged by the NCSC/NIS. Actually, many high tech crime and industrial espionage cases have been informally investigated by the NCSC/NIS and passed to the Prosecutors' Office for further investigation and prosecution.

> We have passed many industrial espionage cases to the Prosecutor's Office with concrete evidence for the perfect prosecution. Compared to the police, we have more intelligence networks to collect criminal intelligence worldwide and more advanced technology to pursue criminals. Our know-how and resources have been built up for the counter-intelligence purpose so that it is much more sophisticated than you think (#3).

6.1.1.16 Lack of accountability

The respondent of the FSA believes that other agencies cannot fully conduct an independent investigation due to lack of expertise in a financial background. Therefore, they have often been called by the Prosecutors' Office for their assistance regarding financial investigation when cases of a serious calibre occur. Whether they would like to do so or not, the FSA has to cooperate with the Prosecutor's investigation. The FSA does not like to work as a secondary investigation agency as they have special knowledge to uncover financial fraud. For that reason, the FSA would like to have its own independent investigation power, but there was strong opposition by other law enforcement agencies. An SPO respondent argued that financial fraud is a criminal justice matter, not a subject of financial matter. The SPO respondent said that financial knowledge is an important part for the investigation, but it is not the only factor needed for the whole investigation. The SPO respondent believed that financial investigation must be done by the law enforcement agency. However, the respondent from the FSA in this study believed that delegation of policing power based on professional expertise of each agency would improve the prevention of financial fraud in cyberspace:

> Let's see...Financial fraud in cyberspace should be policed by the FSA. Since we protect internet banking transactions, it is a more effective way to prevent and investigate financial fraud compared to other law enforcement agencies. The FSA would be able to save time and cost when getting a response to a financial related crime (#4).

Lack of accountability of the police was also mentioned by the Prosecutors' Office since there have been some mistakes made by the police. Prosecutors believe that insufficient legal training of police officers has often ruined criminal cases. Consequently, those mistakes made by the police have often resulted in the failure of prosecution:

> Well.... they did not follow the appropriate legal procedure so we lost the case in court. As you know the Court does not admit any illegal interrogation occurred by the police or prosecutor so it is important to follow the appropriate procedures. Reforms to the criminal justice system should mainly concern the human rights issue in the investigation process (#2).

6.1.1.17 Different level of power

Different level of power was reported by the respondents of KISA and its subsidiary agencies (KrCERT and KSRC) as one of most serious tensions within the public sector. There is practically no chain of command among public agencies unless an office is a subsidiary agency or office. However, non-police agencies and the general public have perceived that the NPA, the SPO and the NIS to be powerful authorities within the public sector. For the same case, the outcome can be different depending on whether the police or the prosecutor investigates it. It seems that the level of power is decided by whether the involved agency has law enforcement authority or not.

As a regulatory agency, KISA has not received the same support that other law enforcement agencies have received from other agencies or private companies. Therefore, KISA has often felt that they need a more powerful position in the government for the effective response of Internet crime incidents:

> People know that we are not a law enforcement agency so they are not afraid of KISA's actions. Administration restraint is not enough to scare

> them to follow our regulation. Many people break the law and simply pay the fine. They do not think of it as a big deal! For them, it is like a parking ticket (#7).

Some respondents in the non-police agencies have also argued that their agencies do not have the same power as the prosecutor and police do in terms of control of internet fraud. They are not afraid of a regulatory agency since it does not have any law enforcement authority. As a result, fraudsters have often not corresponded to their regulatory requirements. If a violation is serious, a regulatory agency has to accompany the law enforcement officer in order to carry out the Court order.

The respondent from KISA reported that the cooperation of private companies is essential in order to respond to an Internet-related incident. However, some companies do not comply with the regulation:

> Private companies and ISPs have to report to us when an incident occurs. However, 80-90% of companies have shown a negative attitude toward incident reporting although we mutually signed for the protection of information. They continue to think that KISA is not able to provide necessary action against internet incidents. For this reason, they prefer to report to the police or the prosecutor who has law enforcement power. Without law enforcement authority, KISA's status is like a 'soldier without a sword'. Use of administration order and freezing licenses does not effectively control private companies and organizations because there are many ways to continue their businesses such as new licensing with other names or appealing to the court for taking more time (#7).

6.1.1.18 Special law enforcement power

The respondent from the FSA reported that they wanted to have special law enforcement power for financial crime investigations. They wanted to become an agency like a Secret Service or ATF under the Department of Treasury in the United States. In order to obtain this special law enforcement authority, it would be necessary to make a special law to approve their law enforcement authority. However, the process of law making and the implementation of new policy are not simple tasks.

According to the respondent, it is not desirable to have to call the Prosecutor for assistance with their investigations. It makes the FSA feel as though they are a subordinate agency of the Prosecutors' Office while the FSA has many elite staff members within the government organization. It has been argued that the policing of internet fraud seems to be more appropriately investigated by the FSA than by other agencies since it causes a lot of monetary loss for financial institutions or their members.

> Given the special law enforcement power, the FSA would be a more effective help regarding the policing of Internet fraud. We can see many Western countries' financial agencies have special law enforcement power. We have heard that the police and prosecutors strongly oppose the implementation of special law enforcement powers for other agencies (#4).

The Ministry of Information and Communication (MIC) also demanded special law enforcement power. The MIC is a main government body, which governs the national infrastructure system of information and communication. However, prosecutors and the police have not been allied with the body due to strong opposition. They do not allow in any other agencies that are capable of law enforcement authority. The failure of special law enforcement authority by the MIC shows why other agencies have not attempted to apply for special law enforcement power.

As described earlier, the Congressional legal committee members consist of former prosecutors and judges. It seems that they will not allow law that permits special law enforcement by other public agencies. It is practically impossible to obtain special law enforcement power unless the structure of the committee membership changes:

> I think that the appointment of the Congressional legal committee member should be changed and its candidate should be tested if they have any predisposition about the legislation. For a long time, legal committees have supported the interests of the Court and the Prosecutors' Office. No agency can challenge their privilege in Korea. Too much power is given to them and there is no mechanism to control them (#1, #4).

However, the recent discussion of the reform of the Korean criminal justice system implies the possibility of expansion of special law enforcement power since this reform of the criminal justice system imitates the American criminal justice system where policing is fragmented and decentralized. Despite strong opposition by the Prosecutors' Office and the police to give special law enforcement power to other non-police agencies nothing has deterred this provision of reform. Overall changes in the criminal justice system will make it possible for this provision to be implemented in order to maintain harmony with other non-law enforcement agencies.

6.2 Part II: Resolution of tensions

Interviewees were asked to consider the possibilities for resolution of tensions in the policing of internet fraud. Three main questions were asked: *Can government do anything to reduce these tensions? Can any other organizations get involved?* and *What is the best solution?* Based on the interviewees' answers those which were relevant to the possibilities of resolution between tensions in policing internet fraud were used to structure this part of this paper. The responses to the three questions are listed as follows:

- Easy access to public information
- Confidentiality of investigation
- Sharing technological knowledge
- Cross-sector meeting at the low-levels of staff
- Establishment of appropriate laws.

Table 6-3: Resolution of tension (tensions between the private and public sectors)

	Can government do anything to reduce these tensions?	Can your organization do anything to reduce these tensions?	Can any other organizations get involved?	What is the best solution?
Public Sector	Allow easy access to the public information	Share technological knowledge	NA	Establishment of appropriate laws
Private Sector	Confidentiality of investigation	Hold cross-sector meetings at low-levels of staff	NA	Establishment of appropriate laws

Can government do anything to reduce these tensions?

6.2.1.1 Easy access to public information

Easy access to public information could reduce tensions between private and public sectors as reported by the majority of interviewees in the public sector. They believe that the security threshold of public information is still too high to be accessed by the private sector. Although there are many formal channels to access public information, procedures to obtain the permission to do so from the government is still seen as 'a very complicated process'. Since the emergence of the internet, the confidential lifespan of new information has become shorter than before. Today's important information could become unworthy public news tomorrow. The respondents admitted that the monopoly over information that the public sector has appears to be a very old-fashioned style of administration. Although there is a growing concern about the disclosure of sensitive public information, it is imperative for the public sector to provide easy access to public information in order to remove tensions.

> Due to the difficult access to public information, tensions between the private and public sectors are not disappearing. I think that the much-complicated process to access public information discourages the use of public information by the private sector. Therefore, people in the private

> sector tend to use unofficial communication channels or personal relationships to obtain the necessary public information (#9).

Easy access to public information appears to be related to the lack of sharing information in terms of the use of information. Both sectors reported that sharing information is the most important factor for building an effective partnership in policing. And easy access to public information could be the first step to developing the mutual trust needed for sharing information.

> How can we share information? It is not just 'sharing' tangible goods! We need some methods to do it. Easy accessibility is a key factor to sharing information. Then there will be more steps to get closer to the sensitive information (#11).

6.2.1.2 Confidentiality of investigation

Private companies tend not to report cybercrime incidents since they have to consider the side effects of negative publicity and the subsequent adverse impacts. When the police release information from an incident, it could negatively affect their reputation, brand image and stock value. Therefore, many private companies tend to make deals regarding the confidentiality of investigation before they report to the police. Without promising confidentiality of investigation, private companies never report their incidents. Although the police recognize their incidents, private companies often do not cooperate with the police. It is important for the police to keep the confidentiality of investigation in order to save their relationships with private companies.

> As long as we can promise to keep the confidentiality of investigation, many private companies will report their incidents without hesitation. However, it is very difficult to keep this promise. As you know, reporters come to the police department everyday to collect information on various investigations. It is almost impossible to guarantee the confidentiality of investigation. To do that, we need to get cooperation from the media; however, investigation information sometimes still goes out to the public despite having any agreements with the media. With the competition among newspaper companies and TV companies, reporters often break their promises for the embargo. Regardless of this type of situation, tensions would be reduced if we could promise the confidentiality of investigations (#9).

Can your organization do anything to reduce these tensions?

6.2.1.3 Sharing technological knowledge

The public sector interviewees reported that sharing technological knowledge with the public sector would reduce tensions between the two sectors. Generally, the private sector has a better capability to update its level of technology and knowledge. Public sector activities are restrained by definite budgets and strict regulations while the private sector has more financial resources and flexible rules. Today's hackers are well equipped with high technology and advanced knowledge. In order to respond to fast-developing cybercrimes, the public sector has to keep updating technological knowledge. Sharing of technological knowledge is not only for the benefit of the public sector but also for the benefit of the private sector. Although private entities do not have any law enforcement authority, the police could use the updated technology learned from the private sector to respond to cybercrimes.

> Too many Internet security-related companies are inventing new technologies everyday. Although we have developed our own technology for internet security, it is far beyond the private sector's technology due to a limited budget and limited resources. Sharing technological knowledge is very beneficial for us. Ultimately, sharing technological information is good for the private sector as well. Private companies could test their knowledge with the help of the police (#1).

However, some interviewees in the private sector argued that original research intentions could become dull due to sharing technological knowledge between private and public sectors. The interviewees said that some know-how should be kept and used for their business purposes only.

> If we provide everything to the public sector, the public sector would depend on us continuously. There are also some blurred distinctions between what we can share and what we cannot share with the public sector. Sometimes, our technological knowledge could be used for attacking another private company's tools (#9).

6.2.1.4 Cross-sector meeting at low-levels of staff

The private sector interviewees reported that the establishment of regular meeting sessions would help to reduce tensions between the two sectors. Although there are already some regular meetings established within the sectors where other sector staff members are invited as guests, active cross-sector meetings are not available. It has been criticized that the participants of these meetings are high-ranking officers, agents and executives, while low-level staff members are actually the people working at the front line of Internet security and crime prevention. Fortunately, there have been some efforts to develop the partnership between the two sectors through CONCERT (the consortium of CERT) but this partnership is still dominated by private entities. Recently, the NCSC/NIS (National Cyber Security Center/ National Intelligence Service) has organized regular cross-sector meetings and conferences to help build a stronger partnership with the private sector. However, these meetings are not private-driven and so participants cannot always fully address their concerns. Therefore, organizing cross-sector meetings is mandated by the private sector to address their concerns.

> Well, CONCERT is a good organization used to meet and share information between the two sectors. However, we always see the same people from both sectors. In particular, government officials are rarely changed. It could be attributed to the nature of their work or their position in the agency as they are usually high ranking government officials. Maybe this shows that they can best readdress the suggestions gathered from their sector meetings to the policy making? However, at the operational level, we do not know who actually responds to incidents or to investigations in the law enforcement agencies. For an effective partnership, we have to see people at the same level as us who are responsible for crime prevention (# 11).

What is the best solution?

6.2.1.5 Establishment of appropriate laws

Interviewees in both sectors reported a lack of appropriate law to be used as a mechanism for removing tensions. From the private sector's perspective, current law does not protect private companies from negative publicity and

adverse impacts on stock values when they report incidents to the police. From the public sector's perspective, current law does not provide them with sufficient law enforcement power to police cyberspace. Interviewees provided the same answer to the research question: *What is the best solution?* although they gave different reasons for their answers. Both sectors' interviewees believed that tensions would be reduced if there were appropriate laws established to protect their interests and to encourage their cooperative efforts.

The public sector interviewees reported that the law restrains their activities. They rarely excise police discretion while they investigate cybercrime. They admitted that current laws do not have any special consideration for the protection of private interest while they investigate the private sector's incidents. In order to promote a partnership in the policing of cybercrime or internet fraud, it is imperative to establish clear laws to describe each sector's role, legal power and scope of operation. Current laws are mainly concerned with public interest although the private sector's role in policing internet fraud has become more important. As a result of inadequate legal bases, tensions have not been reducing between the two sectors. Establishing more 'cyberpolicing-oriented' laws would reduce tensions between the two sectors and maintain a good balance between the two policing models.

> We can only work within the law that specifies our activity. Personally, I understand all of the issues surrounding policing cybercrime but I cannot do anything beyond the law. As you know, the law and other regulations restrain our activities. Not much flexibility is available for the field officer to excise police discretion. Conducting an investigation is then followed by criminal procedure, which guides our professional conduct. Too many people from the private sector ask us to give favours. However, we do not have much capability to provide what they want to receive from us. Prosecutors may have more flexibility to give them favours for confidentiality and other secrecy. Unless the law clearly defines our additional power to protect the private interest, we cannot arbitrarily do any favours for them (#1).

The private sector interviewees reported that the best solution to reduce tensions between two sectors is to make an appropriate law to promote partnership policing. They argued that current laws discourage the private sector from reporting their incidents to the police while internet fraud is increasing in their domain. As stated in Chapter 2, internet fraud has special characteristics and requires cooperative efforts to respond to it. However, Korean law ignores the private sector in the investigation process even though private companies prefer to monitor all processes (because their incidents are directly related to any negative publicity and adverse impacts on stock values). The interviewees suggested that an updated-internet fraud law should include the provision of the protection of private interest.

> We want to build a good relationship with the public sector. However, current laws appear to hinder rather than promote the cooperation between the two sectors. Police and law enforcement agencies ask us to provide substantial amounts of personal information without a court warrant. When we refuse to provide it without a warrant, they deem us uncooperative. In the past, we used to provide noticeable amounts of personal information to the police and other law enforcement agencies, for investigation purposes, through unofficial channels. These days, congressional auditing activities have been enhanced in order to protect human rights and privacy. Anyway, we did many things for the public sector although many acts were not legally protected. However, the public sector has not worked for our interest. They only take advantages for themselves. I think...this kind of situation creates tension between two sectors. Establishment of appropriate laws and regulations for policing Internet fraud would define the clear role of each sector and scope of work and would eventually reduce some levels of tension (#14).

Plural policing models?

Interviewees were asked to answer questions concerning the concept of plural policing models in the way of policing internet fraud.

Table 6-4: Plural policing models

	When is it more appropriate to involve private rather than public policing mechanisms?	When is it more appropriate to involve public rather than private policing mechanisms?	How do you work with the other sector?	How often do you work with the other sector?
Public Sector	Minor fraud within the private domain	Serious fraud that threatens public security	Formally and informally	Very often
Private Sector	As long as private policing handles properly	Outside of private policing authority	Formally and informally	Often but

6.2.1.6 When is it more appropriate to involve private rather than public policing mechanisms?

The public sector interviewees reported that it is more appropriate to involve private models of policing when an offence is not serious and the process of the private justice system can compensate victimization. Since public policing is limited by definite resource and legal restraints, private police could more effectively treat minor offences. As explained earlier, the private sector has more profound resources to be able to police cyberspace than the public sector does. However, the range of minor offences is not clearly defined yet. Generally, they include auctions, internet shopping malls and game-money related frauds. Sometimes minor offences could become serious offences that result in significant impacts and large volumes of victimization. As mentioned in Chapter 2, fraudulent activity through phishing and pharming are good examples. However, some interviewees argued that private companies should keep incident records so that public police can review them whenever necessary. Sometimes, minor incident records can be used as very useful evidence for tracking fraudsters in future investigations. The interviewees in this study were united in expressing a general perception of plural policing that, to them, delegating the policing of cybercrime to the private sector is a big challenge. However, the interviewees recognized that policing cyberspace through the private sector would help to reduce overall cybercrime and would save the public the cost of the crime prevention.

> I think that minor offenses committed in the private domain and which are related to the private interest should be responded to by private

policing. It could be a more effective and efficient way of controlling minor offences. We do not have enough resources and time to respond to minor offences that are usually committed by non-career criminals. What we can do is maybe...impose a small fine for the offender if we pursue the case. It is futile to spend time and money for us. However, private companies have pursued different goals. They have to avoid net financial loss and they need to stop illegal activities so that they can more actively respond to lesser serious and minor offences (#1).

In later interviews, non-police government agencies expressed little concern about proactive policing by the private sector. Giving more police authority to the private sector of security may take away the policing functions of non-police government agencies. Overlapping of cyber-jurisdiction would occur between them.

> Although private policing would help overall cybersecurity issues, there is no clear distinction between non-police government agencies in terms of use of authority. Previously, we were in the middle of continuum but we will soon be the same with the private sector (#6).

In general, delegation of policing cyberspace authority to the private sector is an unavoidable step in plural policing which has now become widely accepted on the terrestrial level of policing.

> Look at other countries - their policing is fragmented and decentralized. Korean policing is too centralized and monopolized by the government. For the prevention and response of internet fraud, a plural form of policing would be a more effective policing model. Policing internet fraud is not traditional police work (#9).

The interviewees from the private sector agreed that minor offences should be responded to by the private security whenever they detect them. They also agreed that the concept of plural policing should be implemented in policing internet fraud. Moreover, they said they would like to have more independent police power to control minor fraudulent cases in their domain. They believe that the private model of policing more effectively control minor offences. Because these minor offences occur in the private domain, they are in direct relation to their business activities. Private companies have experienced many harmful activities against their companies and

customers through internet websites. They have argued that the public model of policing cannot cover minor offences. However, for private companies, these harmful activities are potential threats that may develop into serious cases in the future. Auction companies have been particularly concerned about minor fraudulent activities that have occurred on their websites. Too many complaints have been reported stating buyers do not receive their items although they paid for them.

> See what kind of results you can get from reporting minor fraud cases to the police. Actually, you will be asked to take legal action against the offender however, its process can give you even more stress than what you had when initially victimized. Although the cases can be successfully resolved with legal procedure, you only receive a small amount of redemption (#12).

From the customer's perspective, recovery of loss is more important than any other solution. Private models of policing mainly focus on the reinstitution of loss so that their customers do not need to take legal action individually or collectively. Besides this, private models of policing are usually integrated with insurance companies for the recovery of costs from losses and other damages. It shows that a private model of policing provides more customer-oriented service to the customers in their domain.

6.2.1.7 When is it more appropriate to involve public rather than private policing mechanisms?

The interviewees in the public sector reported that it is more appropriate to involve a public model of policing when an offence is serious and recovery of loss cannot be achieved without public intervention. Public intervention achieves a deterrent effect for future crime. Contrary to the private model of policing, public models of policing have pursued the goal of attaining public security so that it strictly applies the law to respond to internet fraud. Serious fraud cases usually involve multiple numbers of victims and huge amounts of monetary loss. Often, offences have to be dealt with by more than two jurisdictions. The location of the offender, server and victims are different in most cases. They are internationally dispersed so that international cooperation is essential to respond to serious fraud. However,

international cooperation in the private sector has worked through each nation's CERT without law enforcement power.

The interviewees in the private sector agreed that serious fraud has to be responded to by the public model of policing. Since private security does not have law enforcement authority, it cannot effectively respond to serious fraud. However, private security nevertheless wants to observe the process of investigation as a way to increase their ability to prevent future occurrences.

> As long as we can retrieve our losses from such incidents, it is much better to report to the police in order for them to commence a speedy investigation. However, it is very difficult to distinguish between minor and serious offences due to the nature of internet fraud. Unless fraudsters leave concrete evidence, it takes a lot of time to piece together the whole picture. Therefore, we'd like to participate in the fraud investigation from the beginning stages (#13).

In spite of its effectiveness in the ability to respond to serious Internet fraud, the public model of policing has a disadvantage, which is that it does not have any flexibility in investigations. Private companies are not able to control the process and result of an investigation. Sometimes, negative publicity and adverse impacts on the stock values are unavoidable so private companies have to consider whether they report incidents to law enforcement agencies or not.

6.2.1.8 <u>How do you work with the other sector?</u>

The interviewees in the public sector reported that cooperation with the private sector has sometimes been made through an official letter of cooperation made by the head of each office or department. Most cooperation is made through law enforcement agencies that oversee personal information such as log-in data or e-mail accounts. However, the enactment of the Personal Information Protection Act prohibits any informal access to personal information. Unless there is an emergency situation, law enforcement agencies have to obtain a court warrant to look up any personal information.

For a response to Internet fraud or cybercrime, the use of informal channels of cooperation is more prevalent between public and private security personnel. The use of informal channels of cooperation is very effective in terms of speedy responses therefore both sectors' experts use informal channels of cooperation as long as it does not negatively affect their investigations.

> There is no time to follow formal procedures to get the necessary information. We have to respond to such incidents immediately. It's time fight! (#1).

Some interviewees in both sectors were concerned that the use of informal channels of cooperation may in the end nullify a fraud incident.

> Because criminals become very smart they know how to escape from legal procedures. If they find out someone looked at their data or record without warrant, they would make a complaint about it (#9).

It appears that law enforcement, government agencies and private companies' security experts routinely exchange information through messenger and e-mail. Recently, mobile communication makes it more convenient to exchange necessary information whenever they need useful information.

6.2.1.9 How often do you work with the other sector?

The majority of interviewees in the public sector reported that they frequently work with the other sector. Prior to making a formal legal action or commencing an investigation, public agency staff or police investigators collect primary information about an incident and the offender and they contact the IT security team or CSO (Chief Security Officer) in the ISP or private company. Depending on the seriousness of the offence, they have to decide whether to take formal action or not.

> As you know internet fraud and other cybercrimes are occurring continuously we have to work closely with the private sector. They are like our 2nd division! Without cooperation from the private sector, it will cost more money for the response to internet fraud (#1).

Like the public sector interviewees, the private sector interviewees reported that they have often worked with the public sector. They criticized that they have to work for the public sector as an auxiliary unit. It appeared that more inquiries came from the public sector.

> Our position is very passive although we work together very often. It seems very unfair that inquiries that come from the public have to always be taken care of. Our requests have often been ignored (#14).

Throughout the interviews, it was revealed that the frequency of cooperative work does not give any credit for the real meaning of cooperation in policing internet fraud. More efforts to understand what the other sector would like to achieve have to be seriously considered by each sector. Thus, as yet, the concept of plural policing has not been fully implemented for an internet policing model for internet fraud in South Korea.

6.3 Part III: Partnership policing for internet fraud

Interviewees were asked to consider the meaning of partnership policing with regard to policing internet fraud.

Table 6-5: Partnership policing

	Do you believe that a partnership created to help police Internet fraud is either necessary or helpful?	**What would the ideal partnership look like?**	**How would you promote the partnership?**	**How would ideal policing look at local, national and international levels?**
Public Sector	Yes	Mutual respect	Formalize a contract or law	Protection of private and public interest
Private Sector	Yes	The sharing of liability	Make appropriate laws	Protection of individual and commercial victims

Do you believe that a partnership created to help police internet fraud is either necessary or helpful?

The interviewees from both sectors were assured that partnership policing is imperative and inevitable for an effective response to internet fraud. However, the operative meaning of partnership is slightly different in each sector. What the public sector wants is to have a pro-government partnership while the private sector wants a pro-business partnership.

> We hope that private companies show more respect and trust in our investigations. Hostile relationships could contribute to the creation of a dark corner in policing internet fraud (#1).

Not surprisingly, the interviewees in the private sector indicated a completely different point of view.

> As you know, authoritarian-conservatism has been rooted for a long time in the public sector. Public agencies have to change their thoughts and attitudes in order to develop our nation. However, we have not seen any significant change in them throughout our modern history. Despite private companies constantly changing their structure and policies for the their betterment, the public sector still wants to be on top of the private sector controlling it. Without a change in the make-up of the public sector, no true meaning of partnership will ever be implemented (#9).

It is advised that both sectors have to re-consider what style of policing would be best for the most effective policing of internet fraud. If partnership is the answer, both sectors have to offer some capitulates to create the forthcoming environment.

What would the ideal partnership look like?

The interviewees in the public sector believed that the ideal partnership should be built on mutual respect. The majority of interviewees also said that negative sympathy is prevalent between the two sectors and unethical practice by both sectors has created more gaps between the private and public sectors of security. The interviewees in the public sector humbly admitted that they have not fully attempted to develop an effective partnership.

> The main point is we do not respect each other. Traditionally we look down on the private sector and treat them as our secondary division. Maybe that makes them annoyed. We feel it is kind of late to build a good relationship through spoken dialogue. There should be a special momentum to change both sectors. Mutual respect means having a horizontal relationship as opposed to the current vertical relationship we have in terms of policing structure (#1).

Contrary to the public sector, the majority of interviewees in the private sector reported that an ideal partnership meant sharing liability when an investigation goes bad. They said that the private sector couldn't solely be responsible for the failure of a joint investigation. Partnership policing must be based on a mutual agreement and so blame has to be shared by both sectors.

> What we want to do is, 'live and die together with the public sector'. But, whenever joint-investigations go bad, we become a target for the blame. The public sector silently escapes from liability. How we can trust them if similar situations continuously occur? Merit and responsibility cannot be separated. The result of a joint-investigation has to be shared by both sectors (#11).

In spite of slightly different answers, both sectors mentioned organizational behaviour related issues. They both believed that mutual respect and sharing of liability are their priorities in order to contour an ideal policing partnership. This crucially implies that the respondents in both sectors perceived organizational behaviour to be the most influential factor for forming an ideal partnership; more than any other external factor, such as the criminal justice system or laws.

How would you promote the partnership?

The interviewees in the public sector believed that the promotion of a partnership would not be achieved through informal agreements or working practices between sectors. They believed that a partnership should be formalized through a contract or law.

> As you know, we have failed to establish a truthful partnership through informal efforts such as the sharing of information and holding

> conferences and meetings. These are not secure methods to promote partnership. I believe that a formalized contract or law could promote a policing partnership (#2).

Some of the interviewees disagreed with the idea that a formalized contract or law would promote partnership. They believed that a formalized contract or law may limit the full capacity of a partnership through prescribed contents.

> Once we make a contract or law, we have to work within the boundary of that contract or law. That's another factor toward the hindrance of the promotion of partnership policing (#6).

Similar to the public sector, the interviewees in the private sector reported that the making of appropriate laws to promote partnership policing has to come first. The absence of related laws makes both sectors uncomfortable to initiate a joint-investigation. They advocated that the promotion of partnership policing would happen if there were appropriate laws to support the private sector's legitimate involvement in the investigation of Internet fraud.

The answers provided by the interviewees in both sectors indicate that their perception concerning partnership policing is not significantly different. Interviewees in this study seemingly share similar values and perceptions about current policing of internet fraud regardless of their membership.

How would ideal policing look at local, national and international levels?

The interviewees in the public sector agreed that the ideal model of policing internet fraud should maintain good partnership between public and private sectors at the local, national and international levels. However, they did not know what exactly would make it an ideal model for policing internet fraud. Since the Korean public policing system is a centralized national police system, distinctions between local and national were blurred.

> Our police are not fragmented like the USA and UK. The National Police Agency supervises more than 250 police departments. When CTRC (Cyber Terror Response Center) receives a fraud report, CTRC passes to the local police department where the victim or offender resides. If fraud victimization is nation-wide, CTRC directly investigates the case with the support of the local police department (#1).

Recently, police stopped taking online internet fraud reports due to excessive false reporting. Therefore, victims of internet fraud have to visit the police to report the incident in person. This procedure has deterred third party private intervention, such as *The Cheat* and *Catchall*. A lack of anonymity in crime reporting makes it even more difficult for victims to report fraud to the police.

> As you know that police officers treat victims like another criminal when they conduct the interrogation so that we do not want to report minor cases to the police unless we know someone in the police (#15).

The majority of private sector experts complained that police do not care about minor Internet fraud victims and do not target Internet fraud as a police priority. Individual victims of internet fraud, especially minor fraud victims, actually have few places available to help. In this regard, the emergence of *The Cheat* and *Catchall* became beneficial for minor internet fraud victims and for potential victims. However, some concerns are arising in that those involved in private policing internet fraud may position themselves in the wrong place within the larger context of policing internet fraud in Korea. At the same time, local police departments have gradually given up on the policing of internet fraud in their original police work. If the current situation persists, the policing of internet fraud will be left untouched by the public police and this would damage our criminal justice system in terms of internet fraud control.

Since local police departments and individual victims have to interact to deal with internet fraud in the first place, easier reporting and rapid investigation are important when creating an ideal model for policing internet fraud at the local level. Many internet fraud victims argue that obtain the police assistant is not easy. Each police department has a different

capability for policing internet fraud therefore it is necessary to establish standardized internet fraud investigation procedures.

Although most internet fraud incidents reported by individuals are relatively minor in comparison to fraud incidents reported by the commercial sector, partnership is still vital to succeed with investigation. User group websites such as *The Cheat* and *Catchall* may receive more information than a police website since many people feel more comfortable discussing their cases on the user group website.

> Internet users feel uncomfortable registering their real name on the police website in order to discuss or to report fraud information. As you know citizens and police are not close each other. They prefer to use private channels to exchange information about internet fraud (#16).

To maintain ownership of the policing of internet fraud, local police departments should not overlook minor internet fraud cases. In order to give more attention to the minor fraud case, easier reporting systems have to be established. False reporting problems can be solved if the police work together with Internet user groups. The internet user groups could filter internet fraud incidents that require formal police investigation.

> It is a win-win strategy to beat the fraudster! Through our filtering of incident cases, police could save a lot of time and labour while they achieve the goal of criminal justice. Actually, police have to pay for our labour (#15).

The public sector interviewees expressed concern that overload from minor internet fraud investigations might paralyze other cybercrime priorities. They emphasized that the ideal model of policing internet fraud would have to consider the protection of private and public interest. Therefore, it would be imperative to establish the priority of the investigation on behalf of the protection of private and public interest. This consideration may conflict with the rights of the individual victim of internet fraud.

> For the protection of public interest, individual victimization of internet fraud may be neglected due to lack of police labour and resources.

> Between the private and public interest, public interest always has a priority to be protected (#2).

Interviewees of *GCN* and *YMCA* refuted the fact that protection of the individual victim should be treated as equally as protection of the public interest. They believed that the protection of the individual victim is the protection of the public interest and a small unit of victimization eventually threatens public security.

However, it is questionable as to what kind of law would support their online community policing activity. How could private internet user groups or organizations represent victims of internet fraud? Who would be responsible for the result if the investigation went poorly? The private sector interviewees criticized the protection of the individual and felt that the commercial victim needs more attention from the local police even when minor losses occur, while the public sector interviewees were concerned with protection of the private and public interest.

At the national level, both sectors' experts recommended that the establishment of a central reporting agency like an IC3 in the US would be necessary in order to perform successful partnership policing. They believed that establishment of a central reporting agency would contribute to the development of policing internet fraud in Korea. Particularly, this agency would be able to collect and analyze incidents for the prevention of possible online fraud activity. The absence of a central reporting agency has hindered the laws and regulations for policing internet fraud in Korea. Without reliable internet fraud incident data, some felt it was not worth discussing partnership policing of internet fraud.

> As you know that we do not have any public agency to respond to internet fraud so we do not exactly know what is happening. We only have officially reported fraud data complied by the police and prosecutor but these cannot represent the real occurrence of internet fraud. Without reliable data, it is difficult to determine the correct balance of policing (#9).

From the perspective of the public sector, internet fraud is not seen as a major threat for national cybersecurity. However, this may be attributed to the absence of reliable data showing exactly how it can create damage. Other nations' law enforcement agencies are well aware of the significance of internet fraud and have thus founded special units in national and federal law enforcement agencies, such SFO (Serious Fraud Office) and FBI's IC3 (Internet Crime Complaint Center). The interviewees agreed that their data is unreliable.

> You know that the current police and prosecutor's office data do not completely reflect the real level of internet fraud since reported fraud incidents are a small part of the total number of internet fraud incidents. Uncountable numbers of minor internet fraud have not been reported to the law enforcement agency (#1).

The interviewees in both sectors suggested that the establishment of a central reporting agency like an IC3 in the US would form part of an ideal model for policing internet fraud. However, management of this central reporting agency is another issue. Making it a subsidiary of each agency would enhance the power of policing internet fraud. Therefore, NPA (National Police Agency), NIS (National Intelligence Service) and SPO (Supreme Prosecutor's Office) would compete to host this central reporting agency, if the government did decide to build it. The private sector does not have any choice in being able to do anything until the government decides upon its establishment.

Currently, the most similar agency to IC3 in Korea is the NCSC (National Cyber Security Center) of the NIS (National Intelligence Service). Although it was not founded to respond to internet fraud, it could provide a good model for a central reporting agency. In order to establish a central reporting agency, political decision by the President or Congressional approval would be essential. For example, *The Presidential Direction Number 141 - National Cyber Security Management Regulation* (January, 2005) founded the NCSC. In addition, enactment of special law for the establishment of a central reporting agency and its activity would be needed.

At the international level, both sector interviewees agreed that partnership policing has to be enhanced but few people knew how international cooperation could be practiced. Although the Korean government regularly hosts international cybercrime conferences and forums, local participants are always high ranking government officials and scholars so working level investigators do not get the chance to build knowledge about the international level of partnership policing.

Since many of the reported internet fraud incidents indicate that offenders are living in other nations, Korean police do not have any legal responsibility to perform any appropriate action for those victims. Many victims experience problems after using internet shopping malls or auction sites abroad. If they have not used reliable payment methods to purchase their items, such as PayPal, recovery of their loss is almost impossible. Especially for minor fraud incidents, police are unable to obtain any international law enforcement assistance.

The private sector experts said that partnership policing is more effectively practiced among private entities such as banks, credit card and insurance companies. These financial institutions are using the private model of policing to protect their assets and customers from any possible threats. It was advised that benchmarking of the private model of policing Internet fraud could be very useful for the aspect of prevention and control. Historically, financial institutions have used the most advanced security methods to control fraudulent activities. As indicated in Chapter 2, CAPA (Confederation of Asian and Pacific Accountants), NeIBA (The Internet International Business Authority) and FACI (Forensic Accounting and Corporation Investigation) are good examples demonstrating the international level of the private model of policing.

One of the interviewees from a law enforcement agency said that the establishment of an Asian Police Agency is essential in order to link Europol's ENISA (European Network and Information Security Agency) and the Interpol at the same level. Since ENISA and Interpol's activities focus on Europe and American regions, an equivalent international level of

agency should be founded in Asia. It was alleged that the foundation of an Asian Police Agency would help successful international cross-sector partnership.

> We have experienced how international cooperation of police investigation is difficult at the terrestrial level. How many cases are cleared through Interpol? How long do we have to wait for criminal repatriation? Even offline partnership proves extremely difficult! So how we can expect online cooperation! Partnership policing with the private sector has to be discussed after we successfully link with Interpol and Europol through an Asian Police Agency (#1).

Overall, partnership policing between the private and public sectors at the international level would be very beneficial for internet users worldwide. However, there are many prerequisites that would have to be discussed and solved. In contrast to other levels of partnership policing, international partnership policing includes numerous issues, such as international law, jurisdiction and cost of policing. Efforts are being made to consider these factors, as can be seen from the 7th International Conference on Cybercrime which addressed the issues of organizing more training sessions and joint efforts by all the multilateral agencies for working out a comprehensive International convention (Patil, 2007).

Chapter 7: Towards an ideal model for policing Internet fraud

7.1 Introduction

The main objective of this study has been to determine the correct balance of policing models by analyzing and examining tensions; both between the private and public models and within the public models of policing fraudulent activities in cyberspace, with special reference to the Korean context. The primary research material used in the study was the result of a series of semi-structured qualitative interviews with 16 internet fraud investigators in the private and public sectors. To achieve its objective of a theoretical explanation of policing internet fraud, the study employed a conceptual framework, the primary assumptions of which have been that:

- the governance of internet fraud/cybercrime is characterized by a complex 'assemblage' of networked nodes of security that shape virtual behaviour (Wall, 1997; 2001: 171; 2002: 192; Walker and Akdeniz, 1998:8; Newman and Clarke, 2003: 160)
- 'much policing is now taking place beyond the auspices' of the public police (Crawford and Lister, 2004: 426)

Based on this conceptual framework, the study sought to provide a structured and systematic description of the component elements that are involved in the policing of internet fraud, and to formulate research expectations that can guide and direct the work of the research.

Throughout this research, the 'internet's order maintenance assemblage model' by David Wall (2007) was used to compare three nations' policing practices for internet fraud. As a result, it was possible to find out the similarities and differences among three nations. Seven different groups of policing actors were also found in the three nations. Although there are minor differences in policing among three nations' policing actors, overall the practices are very similar. Governance providers and sanctions in the three different nations are seen as almost same, although there are small

differences in the scope of sanctions. In contrast to the United States and the United Kingdom, South Korea does not have any specialized internet fraud policing bodies in both private and public sectors. While NW3C and IC3 are working in response to internet fraud in the United States, and the SFO and NFRC[8] are dealing with online and offline fruad in the United Kingdom. It suggests that more specialized internet fraud policing bodies are necessary in South Korea.

In this chapter, promotion of efficient policing of internet fraud, consideration of the required balance between private and public models and ideal models of policing internet fraud were discussed based on Wall's (2007) 'internet's order-maintenance assemblage' model introduced in Chapter 3 and Kozlovski's (2005) 'cyberpolicing' model in Chapter 4. A combination of the two models provides very useful information regarding aspects that this research attempted to tackle. The aims of this final chapter are threefold:

- to uncover constructive factors that may promote the policing of internet fraud by analyzing and examining the tensions between private and public and within public sector models of policing;
- to determine the correct balance of policing models by analyzing and examining tensions between private and public sectors;
- to present a conceptual framework developed for the study as an 'ideal policing model' that can be applied in future studies, to better understand and analyze the policing of internet fraud.

Attention will also be given to the larger implications of the study, including its relevance to the field of cyberspace crime, its limitations, and suggestions for future research.

---

[8] UK government will establish the National Fraud Reporting Centre (NFRC) by 2009.

7.2 Promotion of effective partnership policing of internet fraud in South Korea

Tensions between the private and public sectors

Chapter 3 outlined the tensions that reside between private and public models of policing internet fraud, which may affect the effectiveness of policing by two sectors. Later, those tensions confirmed though interviews in Chapter 6 led us to suggest the implementation of a successful partnership for policing internet fraud. Interviews with public and private sector experts indicated that most tensions in this study were also found in previous studies relating to policing e-crime or cybercrime, although some of the tensions were less emphasized due to different political and cultural environments.

In order to achieve the first objective of this study (to reveal constructive factors to promote the policing of internet fraud by analyzing and examining the tensions between private and public and within the public sector models of policing), interviewees were asked questions such as: *What are the three most serious tensions between the sectors? Can government do anything to reduce these tensions? Can your organization do anything to reduce these tensions? What is the best solution?*

Interviewees in both sectors reported that tensions should be removed in order to promote effective partnership policing of internet fraud. Although some tensions could be positive stimuli, most tensions hinder the promotion of effective policing. According to interviewees, lack of trust remains the most serious tension between the two sectors and this tension negatively affects the desire for building a partnership. However, lack of trust cannot be easily overcome unless the surrounding environment and conditions are changed since it is not a factor that can be fixed by systematic efforts.

The findings suggest that information sharing is one of the most effective operational factors to promote cooperation between the private and public sectors. Sharing of information is an important routine activity which would facilitate effective policing by two sectors. However, their hostile

relationship hinders the bi-directional sharing of information. Analysis shows that each sector does not want to share its important information with the other sector since the majority of investigators deemed possession of more information to be possession of power.

Interviewees in the public sector argued that the protection of 'personal information law' restricts the disclosure of information to the private sector. However, private sector interviewees believed that the police just do not want to share their information with the other sector. It is unlikely that more information sharing will follow in the absence of appropriate laws to secure the legitimate transaction.

The majority of public sector interviewees recommended that easier access to police information could promote effective partnership policing. This is also relevant to the sharing of information. However, an interviewee in the law enforcement agency argued that the personal information of the victim and offender should be protected. Alternatively, police could charge for the use of police information by the private sector, in addition to an agreement of confidentiality. This would introduce a new police role as an information brokering service, as mentioned by Ericson and Haggerty (1997).

Among various tensions, negative publicity and adverse-impact on stock value were the most serious tensions chosen by the private sector as they were believed to cause harm to the reputation of private companies. For a serious case, a company may have to close the business due to those tensions. The interviewees suggested that confidentiality of police investigations must be kept and the process of investigation should be reported to the victimized party. However, these cannot be guaranteed by informal agreements between the two sectors. The absence of protection of 'business secrecy law' or any provision of criminal procedure has created more tensions in the private sector.

These tensions are also relevant to the under-reporting of incidents to the police. Since private companies do not trust the confidentiality of investigation by the police, they tend not to report these incidents. To

receive compensation of insurance premiums they have to report their incidents to the police. It appears that the involvement of an insurance company as a third party facilitates mandatory incident reporting to the police whether private companies like it or not. This shows that the insurance company is to some extent participating in the policing of internet fraud. It seems that insurance policy may be a more powerful tool to control human behaviour. This implies the participation of the insurance company as a formal partner in policing internet fraud.

Cross sector meetings at the working-level of staff was suggested as one of the most effective methods to promote partnership policing of internet fraud. What investigators expect is to share their investigation experience with other sector investigators. However, there is not much opportunity to meet other sectors' investigators at the working level. Most meetings are held at the management level of staff, such as directors and deputy-directors because the position of public relations officer tends to be assigned to high ranking officials. Particularly, public agencies tend to control the communication channel only through the high level office so that working level staff members do not have enough voice to discuss with private sector investigators.

Considering that working-level staff conduct most investigations, regular meetings for the exchange of criminal information and investigation methodologies should be held at the working-level. Forums such as conferences, round-tables and regular meetings were suggested as useful means for sharing information. Some interviewees recommended that cyber-forums could be used for the sharing of information which would mean that investigators could remain in the workplace. Interviewees believed that information technology would make it possible to establish cyber-forums without any difficulty. Currently, CONCERT (Consortium of CERT) operates online communication channels, but its participants are limited to membership companies who pay an annual fee.

Interviewees of the public sector expressed concern about a lack of legal perception from private sector employees. What the public sector suggested

was to licence the private investigator. In order to obtain an official licence, they would have to study and pass an exam. Currently, South Korea does not have any licences for internet fraud or cybercrime investigation. Therefore, police do not believe that the private sector has sufficient capability to conduct proper investigations. Although some private sector employees have CISA (Certified Information Systems Auditor), CISSP (Certified Information System Security Professional) and SIS (endorsed by KISA), these licences are not for the investigation of Internet fraud. For terrestrial level fraud investigation, CFE (Certified Fraud Examiner) is internationally renowned. However, its training programme does offer a course for Internet fraud investigation.

In order to perform to their full capacity in an investigation, private investigators should be trained to the same standard as police investigators. However, there is no mechanism for providing cross-sector training services. Practically, cross-sector training is not easy; therefore, licensing of internet fraud or cybercrime investigators was suggested. However, it is highly political. Since Korean law does not permit private investigation, the birth of the licensed private investigator has been left pending. Unlike other Western nations, Korean society appears to be far from ready to implement the licensing of private investigators, both online and offline.

As mentioned in Chapter 6, the government exclusively 'owns' policing so the licensing of a private investigator could prove very challenging. However, the successful reform of public policing would allow the licensing of private investigators. Private sector investigators advocate the fact that licensing of the private investigator will eventually be beneficial to the police and the retired police. However, police do not recognize its necessity in Korea. Along with the wait for licensing of the private investigator, licensing of internet fraud or cybercrime investigation has become a less important issue.

One of the interviewees in the public sector recommended that production of convincing material would help people to understand what the public sector is doing and aiming to achieve. It is well known that public sector

people tend not to mention what they are going to do. The passive role of private companies has depreciated their relationship. Misunderstandings between the two sectors due to miscommunication could be reduced if there was convincing material, such as regular e-mail news or monthly publications provided to the private sector. In contrast to law enforcement agencies, non-police government agencies have produced many public relation materials that explain their action plans and programmes to the private sector. However, law enforcement interviewees said that they couldn't provide such materials due to limited budgets and the nature of their work. Now, they believe that providing public relation materials would help to recover the mutual trust between the two sectors.

Finally, the interviewees were asked how they would promote the partnership. The public sector interviewees suggested that making a formal contract or law would promote partnership policing. They believed that an informal partnership does not secure the process and outcome of the investigation. Under this circumstance, each sector could blame the other sector in case of failure of the investigation or lack of prosecution. Although some official MOUs (memorandums of understanding) were made at the individual agency level, no detailed operational provisions were included. Besides, their MOUs were usually about the exchange of technological information but did not relate to partnership policing. MOUs thus become a mere scrap of paper. Similar to the public sector, private sector interviewees suggested that the creation of appropriate law could promote their relationship with the public sector. What private sector interviewees said was not much different from the public sector. They believed that the current legal system does not support partnership policing of Internet fraud.

Tensions within the public sector

In Chapter 6, public sector interviewees provided controversial views of tensions within the public sector. It is not usual to report any conflict within the public sector. They revealed that serious tensions exist between and among government agencies over the policing of cyberspace. The majority of interviewees believed that ownership of policing cyberspace is considered a possession of power in the digital era. Taking over the policing

of cyberspace is directly related to the police interest while other government regulatory bodies have attempted to take away their initiative from the police. At the very least, other government agencies would like to share policing authority with the police. Unlike tensions between the private and public sectors, tensions within the public sector are seen as more politically vulnerable.

Particularly, tensions between the police and Prosecutors' Office are the most serious. As indicated earlier (Chapter 5), the police criticized the fact that the Prosecutors' Office often over-turned what the police believed to have been perfectly investigated. However, the police have to follow what the Prosecutors' Office says and decides according to criminal procedure law in Korea. There is no distinction between online and offline criminal procedure. Although the District Prosecutors' Office has a small-sized unit, criminal procedure law makes it possible for them to supervise how the police control the policing of cybercrime.

Police believed that the prosecutor could control their investigation outcome whenever they felt it necessary, while the prosecutor believed that rejection of police investigations wouldn't happen if the police provided concrete digital evidence. However, the police did not believe that the prosecutor's rejection was due to the lack of evidence or tainted evidence, although it would be difficult to prove the police's argument.

The findings suggest that a transparent process of prosecution is necessary to remove any suspicion due to control of the police investigation outcome by the prosecutor. By implementing a clear process of prosecution, the police could see how the prosecutor has reviewed their investigation. The police could accept reasonable objection even if they did not expect it.

However, this suggestion is unlikely to be accepted by the prosecutor. The prosecutor would like to maintain the doctrine of convenient prosecution in criminal procedure. This means that the prosecutor flexibly decides whether to prosecute or not depending on his or her willingness. According to this doctrine, the prosecutor can stop and close the case whenever necessary.

From the prosecutor's perspective, there is no reason why they should have to convince the police of why they have rejected the outcome of a police investigation.

Moreover, political influence was attributed to the rejection of police investigations. Hostile relations between the police and the prosecutor due to the mandate of independent police investigation power could be one of the reasons. This problem appears to have formed a foundation for conflict between the police and the prosecutor. In contrast to other Western countries, the Korean criminal justice system places the police under the supervision of the prosecutor. Lack of trust between the two sectors arises from this politically and legally controversial issue. The previous Roh, the Moo-Hyun administration, attempted to reform the provision of police investigation in the criminal procedure law, but it failed due to extreme disparity between the two sectors. It appears that the provision of police independent investigation will not change until public consensus mandates its change.

Interviewees in the non-police public agencies suggested that empowerment of special law enforcement for them is imperative to promote the policing of internet fraud and other cybercrime. As indicated in Chapters 2 and 4, police alone cannot prevent and investigate internet fraud therefore division of policing labour has to be implemented. The Financial Security Agency (FSA), the Ministry of Information and Communication (MIC) and Korea Information Security Agency (KISA) have sufficient aptitude to exercise law enforcement power. Compared to the police, they have more knowledge and technical capability to carry out their mission to protect citizens and public assets.

Increasing numbers of law enforcement agencies for policing internet fraud would reduce tensions due to different levels of agency power in the public sector. With the empowerment of special law enforcement to the public agencies, the concept of partnership policing would settle down in the Korean criminal justice system. Partnership policing for internet fraud could be a good example since internet fraud tends to occur more in the private

domain. If special law enforcement power is not provided to those public agencies, a complete version of partnership policing cannot be expected.

Analyses suggest that lack of appropriate law promotes a more chaotic situation for policing internet fraud within the public sector. At a first glance, it is very confused as to which government agency should have the primary jurisdiction over internet fraud. Ultimately, it seems that joint investigation is a key factor to succeed and be effective and efficient. But which agency should become a central coordinator for the investigation of internet fraud? How should the agency coordinate among other agencies? Is it necessary to enact a special law to do this? Some suggestions were made from the Department of Homeland Security model. It will be discussed in the later part of this chapter.

7.3 Balancing the private and public models of policing Internet fraud

Chapter 3 introduced the balance of policing internet fraud between the public and private models in nations that appear to have a more advanced form of policing than that currently practiced in South Korea. Partnership policing of internet fraud does not formally exist in Korea because policing activity by the private sector is not legally permitted. Therefore, it is difficult to determine what a correct balance between the two sectors should be.

In order to achieve the second objective of this study (to determine the correct balance of policing models by analyzing and examining tensions between the private and public), questions such as *When is it more appropriate to involve private rather than public policing mechanisms?* and *When is it more appropriate to involve public rather than private policing mechanisms?* were asked to both private and public sector experts.

This study suggested how the disproportional policing of Internet fraud between private and public models could be balanced. Currently, the policing of internet fraud attaches too much work to the public sector.

whereas it should be reasonably distributed between the two sectors. As indicated in Chapter 2, most fraud incidents occur in the private domain so it is more appropriate to use private policing in the response to Internet fraud.

Through the interviews, it was initially discovered that 'seriousness of the offence' was a standard through which it was decided who would investigate: the police or private. The public sector interviewees suggested that the public police or regulatory agencies should investigate serious fraud cases while private sector people could conduct relatively minor fraud cases. They believed that the public model of policing rather than the private model should respond to serious fraud cases since most serious fraud cases were subject to criminal laws. However, this criterion is not clear because minor fraud cases can be also subject to criminal laws. The distinction between serious and minor fraud is also very blurred. What interviewees mentioned was a very abstract concept of classification. Therefore, more objectively acceptable measures or standards should be made in order to distinguish between serious and minor frauds. For example, felony and misdemeanour cases are distinguished based on the length of imprisonment: i.e. over a year or less than a year, in many jurisdictions in the United States. Korean Criminal Law does not have a concept of felony and misdemeanour or distinguish them based on the length of sentence. As indicated in Chapter 5, fraud is considered a very serious offence in Korea.

- Article 347-1: a person, if convicted for fraud, could face a maximum of 10 years in prison or a fine of up to 20 million Won.
- Article 347-2: Illegal use of a computer to process false information or incorrectly attempt to make money could face a maximum of 10 years in prison or a fine of up to 20 million Won.

As indicated above, fraud is not categorized as misdemeanour under Korean Criminal Law. Because of this reason, classification between serious and minor fraud cases is difficult. In Chapter 6, the public and private interviewees indicated that recovery of loss and attainment of public security are important factors for choosing between the public and private

models of policing. For minor fraud, rapid recovery of loss is more important than any other factor because victims would like to reclaim their losses as soon as possible since their losses are relatively small. For serious fraud, achieving the goal of public security and deterrent effects are predominant issues. This suggests that the balancing of policing between the two sectors is not only affected by efficiency (fast recovery), but also effectiveness (deterrence) of policing.

According to private security experts, public police have rarely responded to minor fraud cases due to constraint of budget and human resources. However, private securities, both in-house and contract-out, have to perform their duties to protect their customers and assets. The majority of public security suggested that minor fraud occurring in the private domain has to be dealt with by the private model of policing. Although private interest is public interest, insufficient resources and human personnel of the public sector meant they would not be able to pay attention to minor fraud cases that tend to occur in the private domain. Like terrestrial policing, a clear boundary of policing has to be defined by the law. Particularly, who pays for the police service is important issue. The public sector interviewees argued that taxpayers' money should not be used for the protection of private company assets or their customers. However, Internet fraud does not equally occur in both sectors so it is difficult to determine the correct balance of policing. It is not clear what standard has to be used for deciding the correct balance of policing. There were some examples of standards introduced, such as frequency of incident, amount of loss and numbers of victims. These standards can be used as important factors to decide which policing model is more suitable in the response to internet fraud.

Higher incident rate, monetary loss and victims in a certain sector should not be pivotal criteria to decide which policing model would be more appropriate in the response to internet fraud. It was already mentioned that most internet fraud incidents occur in the private domain. As suggested earlier, effectiveness and efficiency of policing models have to be considered in order to decide upon more appropriate policing models.

It was advised that minor fraud that occurred in the private domain such as internet shopping malls and auction sites could be policed by the private model of policing since their policing is more effective and efficient than public policing in terms of cost of fraud prevention and recovery of loss. If minor fraud is reported to the police, it takes too long to commence the formal investigation due to the heavy workload of the police and the lack of priority of the investigation. However, private companies would not ignore minor internet fraud because it directly relates to the reputation of their company and the sale of their products. Therefore, private companies would be more likely to rapidly respond to internet fraud to retrieve their customers' losses. Sometimes, they have to spend more money to retrieve their loss. For the long term, it involves risk-management strategy to protect their potential assets and customers.

Like a minor fraud case, the private model of policing could be also used for a serious fraud case. However, the private entity does not have any legal authority to punish the offender. Their sanctions are limited to frozen or cancelled membership and referral to the police. If they continue the investigation, the obtaining of evidence is the last stage for them. For the serious fraud case, the court may require police reinvestigation in order to prove the reliability of evidence. In consideration of efficiency, redundancy of investigation by both sectors is an abuse of cost, time and labour.

The handover of policing minor internet fraud to the private sector is not a simple task since the Korean policing system has maintained a centralized national police force. Generally, policing is 'owned' by the sovereign state, thus the government has a duty to provide a police service for public safety. Since the Korean public policing system is not fragmented, handover of policing internet fraud to the private sector would involve an innovative restructure of policing division of labour. If the police officially handover minor fraud cases to the private sector, it could be seen as a privatization of policing for internet fraud. Therefore, the majority of public sector experts were still hesitant to support the private model of policing internet fraud even though they recognized its efficiency and effectiveness.

However, the private model of policing internet fraud would have to be legally implemented in order to respond to the widespread nature of internet fraud. As Bayley argued (1994: 3), 'The police do not prevent crime'. Policing division of labour is an unavoidable issue in policing cyberspace crime. Ownership of policing internet fraud should not be claimed for a part that the police cannot actually accomplish. Balance between the private and public models of policing internet fraud would protect the symbolic power of the police as a public service agency. If the police do not handover minor fraud investigation to the private sector, efficiency and effectiveness of the policing of internet fraud will continuously decline.

Experts suggested that establishment of a central reporting agency, whether sponsored by a private or public fund would help to determine the correct balance of policing internet fraud. Similar to an IC3 (Internet Crime Complaint Center) in the United States, which is a good example. If a neutral agency recorded the statistics of incidents with detailed information it could be used for guidelines to determine the correct balance of policing internet fraud between the private and public sectors. This central reporting agency would recommend the reported frauds to the appropriate model of policing to respond to them.

In order to adjust the balance in policing internet fraud, mandatory incident reporting law has to be implemented. Without implementing mandatory incident reporting law, no reliable data will be available to detect trends and patterns of internet fraud and it will not be possible to classify which cases have to be passed to the private or public sectors. The collected data should contain volumes of incidents, types of frauds, amount of loss, demographic factors of victims and other useful information. These collected data could be reviewed by both sectors whenever they wanted to see them. This agency should also have a reviewing board so that unsolved cases could be passed to the other sector to investigate. Over the period of operation, the correct balance of policing between the private and public models of policing would be established so that efficiency and effectiveness could be accomplished.

7.4 Ideal model of policing internet fraud

Chapter 4 introduced Kozlovski's (2005) 'cyberpolicing' and Wall's (2007) 'Internet's order-maintenance assemblage' models. These two models suggested how policing cybercrime should be done and considered what kind of policing models should be implemented in order to create an ideal policing model. Based on these two models, an ideal model for policing internet fraud in South Korea will be suggested.

In order to achieve the third objective of this study (to present the conceptual framework developed for the study as an 'ideal policing model' that can be applied in future studies, to better understand and analyze policing internet fraud), questions such as: *Do you believe that a partnership created to help policing internet fraud is either necessary or helpful? What would the ideal partnership look like? How would you promote the partnership? How would ideal policing look at local, national and international levels?* were asked to both private and public sector experts.

This study now suggests how an ideal policing model could be constructed. Since there has been insufficient partnership policing of internet fraud practiced in Korea, but existing studies and the current research showed that partnership policing is the most appropriate model for internet fraud control, this study will help to guide the establishment of an ideal model of policing internet fraud.

For the third research objective, three different levels of policing are now discussed: local, national and international.

Local level

Interviewees in both sectors suggested that the establishment of partnership policing between the private and public sectors is most important since the local police department has an investigation authority over most internet fraud cases, while serious internet fraud cases are investigated by the CTRC (Cyber Terror Response Center) at the National Police Agency.

At the local level, easier reporting by the individual victim is the most important priority to be solved for the development of partnership policing, because at the moment victims of internet fraud do not know how to deal with the incident when they are victimized. It was also believed that the police do not pay attention to minor fraud cases. Victims of minor internet fraud said that they were not able to obtain the necessary support from the public sector. Therefore, victims of minor internet fraud established internet fraud monitoring groups such as *The Cheat* and *Catchall* to exchange critical information to detect and catch fraudsters in Korea. However, those victims' policing activities are very restricted due to legal constraints, so they have to depend on the information that other victims publicize. These groups control internet fraud using 'moral censure, cold-shouldering, lobbying, reporting, hacktivism' (Wall, 2007). For extension of the interest groups, online virtual environment managers and security 'for online role playing/game playing, chat-rooms, discussion lists, e-auction rooms, cyberworlds' (Wall, 2007: see also Table 5.1) are good participants of policing internet fraud. In Korea, 'cyworld', 'naver-blog' and 'auction' are good models for this category. They can help to control the level of internet fraud using 'removal of access rights and exclusion from the environment' (Wall, 2007: see Table 5.1).

Analyses in Chapter 6 suggested that partnership with internet user groups would enable the assimilation of previously unrecorded minor internet fraud incidents. The study found that individual victims tend not to report to the police and they prefer to get assistance from internet user groups. The primary advantage of partnership with internet user groups is to save costs and labour of the police, because the internet user groups will filter reported incidents and only pass on cases that need formal police investigation.

As Kozlowski proposed in Chapter 4 (see Table 4-1), the policing cybercrime structure has to be transformed from a law enforcement model to a cyberpolicing model, which has a multiplex organizational structure, decentralized command, is non-territorial, and involves delegation of policing function and empowerment of individual users (self help). This organizational structure can be applied to the local level of policing internet

fraud. Particularly, participation of the individual user is emphasized. Wall (1998: 205-206) proposed the importance of individual cyberpolicing in his early work where he is quoted as saying that the internet is well-known for 'voluntary policing' of the activity of users.

According to Wall (2007: 188-189), 'Internet users and user groups exert a very potential influence upon online behaviour through censure, usually after the occurrence of signal event', which are behaviours that may not necessarily constitute a major infraction of criminal law, but 'nonetheless disrupt the sense of social order' (Innes, 2004: 151). This statement shows that the individual user is the smallest unit for the policing of cybercrime. Therefore, local level policing of internet fraud has to promote partnerships between internet users and user groups. For the police to be most effective in policing cyberspace, they will have to take on new ideas and accept other networks of communication. Forging new relationships with other 'nodes' (Wall, 2007) will enable transformations to take place in the basic structure of the current model of policing for internet fraud and will enhance effectiveness, efficiency and legitimacy.

National level

Throughout this research, the findings have shown that the establishment of a central reporting agency (the so called 'National Internet Fraud Reporting Center') is a high priority for internet fraud control in order to perform partnership policing in Korea. The absence of reliable data and a neutral agency is the main factor aggravating the chaotic situation of policing internet fraud in Korea.

Yar reported (2006: 93) that the IC3 (Internet Crime Complaint Center) in the USA could be a good model for institutional innovation. The IC3 model presents a dual benefit. First, IC3 is a centralized national contact point for complaints and IC3 passes Internet fraud cases to the most appropriate law enforcement agency for investigation and action. Second, IC3 records incidents and uses the data for the future crime detection. Yar argued that 'where national Internet crime agencies have already established, online

fraud may not necessarily be included within their present remit (as in the case of the UK's National Hi-Tech Crime Unit (NHTCU). which does not deal with fraud complaints' (2006: 93).

According to IC3's mission statement, 'significant and supplemental to partnering with law enforcement and regulatory agencies. it will remain a priority objective of the IC3 to establish effective alliances with industry'. IC3 links the private and public sectors and works for the benefit of the public. Although IC3 is co-sponsored by the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NWC3). it performs as a neutral agency that does not show bias to the public sector. Simply. it looks like any other public-funded fraud-reporting centre.

The IC3 model is very similar to the NCSC (National Cyber Security Center) of the NIS (National Intelligence Service) since it is funded and operated by the NIS. However, NCSC does not deal with Internet fraud rather it deals with the protection of the information infrastructure and networks in Korea. The establishment of the NCSC shows how the Korean government could launch a central reporting agency for the response to internet fraud.

The Korean criminal justice system does not have a secondary law enforcement agency such as SFO (Serious Fraud Office) and SOCA (Serious Organised Crime Agency) in the United Kingdom. Under the supervision of the Prosecutors' Office, the Korean police exclusively deal with internet fraud. Other regulatory bodies have participated in policing internet fraud, but they are not law enforcement agencies. Therefore, partnership policing with the private sector is a very important task for the police. However, the competitive political situation with other public agencies deters the development of partnership policing. Therefore. establishment of a central reporting agency is essential, but it first requires a presidential decision (as when the NCSC was founded in 2005).

Taken together the analyses show that the policing of Internet fraud needs a quick response and data preservation so it is imperative to establish a central reporting agency. Since the policing of cybercrime is not fragmented in

Korea, operation of a central reporting agency would provides the foundation for partnership policing of internet fraud. It could remove the issue of the monopoly of policing cyberspace by the police.

International level

For the public sector, the 'most prevalent and formal mechanism of the policing of the internet fraud can be through diplomatic missions making use of the multilateral and bilateral instrument of cooperation' (Patil, 2007). For overall cybercrime, 'three multilateral organizations are currently involved in shaping high tech crime policy: the European Union (EU), the Council of Europe (COE) and the G8. Other organizations, such as the Organization for Economic Cooperation (OECD), the United Nations, Interpol and Europol have been involved to a lesser extent' (Williams, 2005: 3-4).

In terms of law enforcement, Europol's ENISA and Interpol are the most renowned law enforcement agencies to deal with cybercrime. However, they have not fully focused on partnership policing with the private sector since their partnership between national level agencies is still dormant (Yar, 2006). Meanwhile, it was suggested that the establishment of an Asian Police Agency, equivalent to Europol and Interpol, would be beneficial. Like ENISA of Europol, an internet fraud investigation office to be built within an Asian Police Agency was suggested. Some concerns about international cooperation focus too much on the European and American regions. Current international cooperation through Interpol has shown its effectiveness for the investigation of major hacking and child pornography, but not necessarily for internet fraud.

In contrast to the public model of policing, the private model of policing has performed better in terms of international cooperation through private networks such as CAPA (Confederation of Asian and Pacific Accountants) and NeIBA (The Internet International Business Authority). These agencies have maintained good communication among member companies and have produced useful solutions for internet fraud. International banking, credit cards and stock exchanges need the highest levels of online security since

they deal with huge amounts of money on a daily basis. These financial institutes have used their own in-house security and contract out high-end security services. Whenever they need to investigate serious breaches, they hire the FACI (Forensic Accounting and Corporation Investigation).

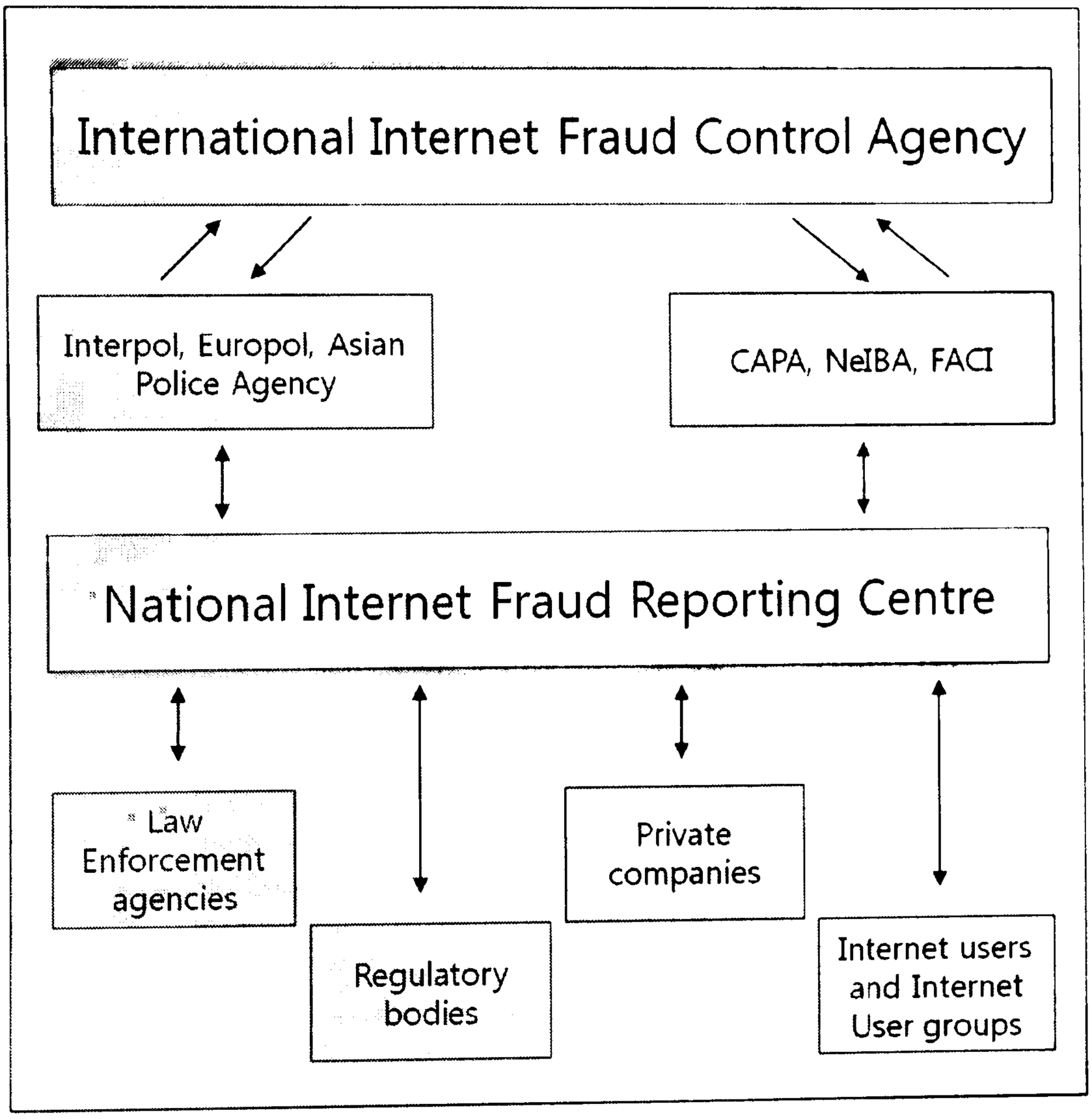
Analyses show that international cooperation between private and public models of policing is essential in order to respond to Internet fraud effectively and efficiently. These days, international shopping and trade is commonplace via the internet, consequently hardening and enhancement of online security has occurred. Therefore, security measures of global corporations are much more advanced than those of some nations. Meanwhile, private companies have also hosted many conferences and offered training programmes. For example, VISA card and HSBC offer regular sessions in anti fraud programmes for their employees.

International cross-sector partnership policing of internet fraud between private and public sectors should have more effective and efficient procedures for intra agency and industry cooperation and coordination. This could be accomplished through the establishment of a neutral non-profit international agency that links the two sectors worldwide. It could have a similar function to the IC3 model at the national level, but a much more advanced capability to monitor international online fraud activity. It could be called 'The International Internet Fraud Control Agency' (see Figure 7-1).

The International Internet Fraud Control Agency (IIFCA) would coordinate the national and transnational level of policing internet fraud. As illustrated in Figure 7-1, internet fraud incident reports would be collected from the local, national and international levels. The National Internet Fraud Reporting Centre (NIFRC) would collect the information from internet users/user groups, private companies, regulatory bodies and law enforcement agencies. These data would be available to the international level public and private agencies to review and to take necessary action in response to internet fraud. This model is an extensive structure of the internet's order-maintenance assemblage in Chapter 3 (see Table 5-1) by Wall (2007). The operation chart below shows that 'Internet order

maintenance assemblage' has been converted to focus more on internet fraud control than overall cybercrimes. It indicates that various actors at the local level report directly to the National Internet Fraud Centre (NIFC) and then filtered information report to the international level private/public agencies such as CAPA and Interpol. Finally, these agencies report to the International Internet Fraud Control Agency for the further analysis and reference. Since international response should focus on macro-transnational fraud activities, IIFCA would not directly deal with individual or local level agencies.

Figure 7-1: Operation chart of the international fraud control agency



7.5 Conclusion

Internet fraud is a serious problem in Korea, especially taking into account its rapidly growing occurrence and the degree of negative impact on e-commerce and online customers. Private and public policing agencies

involved in policing cybercrime have little experience in crime reduction programmes aimed at internet fraud. It is, therefore, suggested that the present study could make a valuable contribution to the development of policing internet fraud initiatives in Korea. The study offers possibilities for resolution of tensions and suggestions for maintaining a good balance. This could be implemented through establishment of an information clearinghouse and creation of mandatory reporting law which would together reduce the level of internet fraud. In addition, this thesis proposed an ideal model for policing internet fraud at the three levels: local, national and international in order to introduce the idea of how the policing of internet fraud ought to be organized. Designing these models is important in order to develop effective policing strategies for the future. Partnership policing efforts to reduce the incidence of Internet fraud and to minimize monetary loss of those victimized are unlikely to succeed unless they are fully aware of the way in which tensions could be removed. Moreover, a visual example of the way a cooperative structure could work may help to alleviate current tensions as it would be a completely new structure which would inhibit the struggle for power between and within sectors.

7.6 Contribution to the field of policing internet fraud

In the study, the main focus throughout was to determine the correct balance of policing models by analyzing and examining tensions between the private and public, and within the public models of policing fraudulent activities in cyberspace. The study aimed to also find an appropriate model for policing internet fraud by analyzing and examining the tensions. These matters are of great interest to criminologists who are concerned with internet fraud, rather than with theories of white-collar crime. Internet fraud does not conveniently fit into any category of crime. It is therefore forcefully classified as a part of white-collar crime since there is a preconception that the internet is only used by well-educated groups of people. However, although it shares a minimum part of its characteristics, internet fraud does not fit into the category of white-collar crime.

According to Wall (2007), policing cybercrime offers an approach to the study of policing cyberspace which is concerned less with theories of crime. than with tensions, strategy and structure of policing models: the focus thus being on the ideal policing model, rather than on internet fraud. In the consideration of tensions between private and public models of policing internet fraud as a serious problem needing a solution, it is proposed that this study makes a contribution to the field of policing internet fraud: and that it does so conceptually and methodologically.

In conjunction with the following characteristics the study could be identified as being particularly significant and relevant. Firstly, the study provides a systematic explanation of tensions affecting the policing of internet fraud; and in so doing it emphasizes cross-sector cooperation and coordination at local, national and international levels in terms of partnership policing of internet fraud. Secondly, the study was designed within the paradigm of qualitative research (although quantitative techniques were also used), and in compliance with a realist approach to research. With this philosophical basis, qualitative interviewing of the study subjects provided an appropriate methodology for the research conducted in the study, research in which factors affecting the policing of internet fraud could be directly explained by the experience of experts in policing cybercrime and internet fraud.

7.7 Recommendations for further research

The study was based on semi-structured interviews conducted with experts of policing internet fraud in private and public sectors; and on secondary data sources that were used to verify the conceptual framework. An inherent limitation of this approach was that the findings of the study allowed for analytical generalizations that related to the research expectations of the study, which in turn were based on the conceptual framework. Although this study has wider application value in terms of its capacity to conceptualize the appropriate model of policing internet fraud, and to determine the correct balance of policing, the characteristics exhibited by these factors are not necessarily valid for other nations.

To increase the reliability and validity of the study and, in turn, allow for broader generalizations with respect to both the correct balance of policing internet fraud between private and public sectors and the development of an ideal policing model of internet fraud, it would be appropriate to apply the conceptual framework in further related studies that would engage with other nations' contexts and situations. Undertaking such further studies would result in a more representative overall picture of policing internet fraud.

Future research should also incorporate cultural factors affecting the policing of internet fraud and the environment in which such tensions are produced, which were held constant in this study. That incorporation would allow a more comprehensive investigation and analysis of tensions between private and public models of policing internet fraud. Such factors could include variation in the reported tensions, to include, for instance, not only political conflict, but also legal constraints.

Policing internet fraud is a new area of study in the field of criminal justice and criminology. Although progress has been made with regard to policy guidelines in respect to policing internet fraud, there is still a need for substantive and in-depth research to support these efforts; and there is a need to monitor and evaluate the success or failure of partnership policing of internet fraud, including those concerned with tensions. The opportunity, thus, exists to initiate policing model-specific research that aims to support defined policing internet fraud initiatives and to monitor and evaluate the progress of a partnership policing model of internet fraud, over a sufficient period of time.

Bibliography

Abrahamsen, R. and Williams, M. (2005). Country Report: Kenya. *The Globalisation of Private Security*. [online]. [Accessed 12th November 2006]. Available from World Wide Web:< http://www.aber.ac.uk/interpol/en/staff/abrahamsenpub.htm >

Abrahamsen, R. and Williams, M. (2005). Country Report: Nigeria. *The Globalisation of Private Security*. [online]. [Accessed 12th November 2006]. Available from World Wide Web:<http://users.aber.ac.uk/rbh/privatesecurity/country%20report-nigeria.pdf.>

Adamski, A. (2004). *Legal guidelines for private and public partnership in combating cyber crime*. [online]. [Accessed 25th April 2005]. Available from World Wide Web:<http://www.lefis.org/meetings/workshops/2004/rovaniemi/presentaciones/legal_guidelines_for_private_public_partnership_in_combating_cybercrime.ppt>

Adler, M. and Ziglio, E. (1996). *Gazing into the oracle.* Bristol: PA, Jessica Kingsley Publishers.

Ahnlab (2007). *Ahnlab-Service*. [online]. [Accessed 11th November 2007]. Available from World Wide Web:< http://www.coconut.co.kr/>

Allen, M. (2006). Social Engineering: A means to violate a computer system. *SANS Institute*. June 2006. [online]. [Accessed 30th May 2008]. Available from World Wide Web: <http://www.sans.org/reading_room/whitepapers/engineering/>

American Institute of Certified Professional Accountants (2004). [online]. [Accessed 28th June 2005]. Available from World Wide Web http://www.aicpa.org/webtrust/index.htm.

American Institute of Certified Professional Accountants. (2004). [online]. [Accessed 06th May 2005]. Available from World Wide Web : <http://www.aicpa.org/webtrust/index.htm>

American Library Online (April 7 2003). Homeland security agents pull Ohio libraries' ha-mat document.

Amoore, L. and Goede, M. (2005). Governance, risk and dataveilance in the war on terror. *Crime, Law and Social Change*. 43 (2-3). pp. 149-173.

Andrews, R. (2007). Consumer Goods, Public Sector. Shopping. Security, Online Fraud, UK Fraud. *Econsultancy*. 26 March 2007. [online]. [Accessed 20th May 2007]. Available from World Wide Web:< www.econsultancy.com>

Anderson, C. (2007). Wired: The Miraculous Power of Scale. 16 November 2008. *Chris Anderson: Blog* [online]. [Accessed 11th July 2008]. Available from World Wide Web: <http://www.longtail.com/the_long_tail/2008/11/the-miraculous.html>

APACS (2004). *Card fraud: the facts 2004*. [online]. [Accessed 8th December 2008]. Available from World Wide Web:< http://www.cardwatch.org.uk/pdf_files/cardfraudfacts2004.pdf.>

APACS (2005a). *The UK Payment Industry: A Review of 2004*. London: APACS. [online]. [Accessed 10th October 2006]. Available from World Wide Web: <www.apacs.org.uk/downloads/Annual Review 2004.pdf>

APACS (2005b). *UK card fraud losses reach £ 504.8m: criminals increases their efforts as chip and PIN starts to make its mark*. APACS press release. 8 March. London: APACS. [online]. [Accessed 10th

October 2006]. Available from World Wide Web: <www.apacs.org.uk/downloads/cardfraudfigures%20national&regional %20-%208mar05.pdf.>

APACS (2005c). *Card Fraud The Facts 2005.* [online]. [Accessed 10th October 2006]. Available from World Wide Web: <www.cardwatch.org.uk/pdf_files/cardfraudfacts2005.pdf.>

APACS (2006). *Fraud: The Facts 2006.* [online]. [Accessed 13th May 2007]. Available from World Wide Web: <www.apacs.org.uk/resources_publications/documents/FraudtheFacts20 06.pdf.>

APACS (2008). About APACS. [online]. [Accessed 18th November 2008]. Available from World Wide Web: <http://www.apacs.org.uk/>

APWG (2004). *Phishing Attack Trends Report 2004.* [online]. [Accessed 01st December 2005]. Available from World Wide Web:< http://www.antiphishing.org/APWG Phishing Attack Report-May 2005.pdf.>

APWG (2005). *Phishing Activity Trends Report.* April. [online]. [Accessed 10th October 2006]. Available from World Wide Web: <http://antiphishing.org/APWG_Phishing_Activity_Report_April_pdf.>

APWG (2008). *Anti-Phishing Working Group.* [online]. [Accessed 11th April 2008]. Available from World Wide Web:< ttp://www.antiphishing.org/index.html>

Ashenfelter, D. (2002). Law firm out of $2.1 million in African fraud. *Detroit Free Press.* 21 September 2002. [online]. [Accessed 10th March 2005]. Available from World Wide Web : < http://www.lettersfromlagos.com/Facts.htm >

Attaran, M. (1999). Internet-based business opportunities: buyers beware of scams. *Information Management and Computer Security.* 7 (4). pp. 176-178.

Avivah, L. (2004). Phishing Attack Victims Likely Targets for Identity Theft. *Gartner.* 04 May.

Baek, M. and Lee, S. (2008). Internet Shopping Mall Fraud. *Naeil.com.* 26 February 2008. [online]. [Accessed 16th May 2008]. Available from World Wide Web:< http://www.naeil.com/News/politics/ViewNews.asp?nnum=387129&sid=E&tid=0>

Baker, R. (2002). Crime, Fraud and Deceit on the Internet: Is there hyper reality in cyberspace? *Critical Perspectives on Accounting.* 13. pp. 1-15.

Balsmeier, P., Bergiel, B. and Charles Viosca, R. (2004). Internet Fraud: A Global Perspective. *Journal of E-business.* 4 (1), pp. 1-12.

Barlow, J. (1994). The economy of ideas: a framework for rethinking patents and copyrights in the digital age (Everything you know about intellectual property is wrong). *Wired.* [online]. 2(3), [Accessed 22nd January 2007], p.84. Available from World Wide Web: <www.ifla.org>

Barrett, N. (1997). Social Engineering: Hacking the weakest link. *Information Security Technical Report.* 8 (4), pp. 56-64.

Barrett, N. (1997). *Digital Crime: Policing the Cybernation.* London: Kogan Page.

Bartley, R. (2001). *Corporate Information Security Strategy - how to avoid giving free information to attackers.* [online]. [Accessed 11th October 2007]. Available from World Wide Web:< http://www.securityfocus.com/guest/5144#5_15_pr>

Bayley, D. and Shearing, D. (2001). *New Structure of Policing: Description, Conceptualization, and Research Agenda.* Rockville: National Institute of Justice.

Bayley, D. (1994). *Police for the Future.* New York: Oxford University Press USA.

Barratt, D. (2007). Crime risk warning to users of social networking sites. *The independent on Sunday*, 12 November 2007. [online]. [Accessed 27th November 2008]. Available from World Wide Web:< http://www.independent.co.uk/news/uk/crime/crime-risk-warning-to-users-of-social-networking-sites-400062.html>

BBC (2006). Free speech online 'under threat'. *BBC News Online*, 27 October 2006. [online]. [Accessed 27th October 2006]. Available from World Wide Web: < http://news.bbc.co.uk/2/hi/technology/6090448.stm>

BC Card (2005). *Risk Management.* [online]. [Accessed 28th March 2006]. Available from World Wide Web:<http://www.bccard.com>

Beebe, M. (2005). Sweepstake Prize Could Be More Unwanted Phone Calls. *Consumer affairs.com. 8 August 2005.* [online]. [Accessed 14th April 2006]. Available from World Wide Web: <http://www.consumeraffairs.com/news04/2005/ar_sweepstakes.html>

Berg, Al. (1995). Cracking a Social Engineer. *LAN Times. 6* Nov 1995. [online]. [Accessed 26th March 2006]. Available from World Wide Web: <http://packetstorm.decepticons.org/docs/social-engineering/soc_eng2.html>

Berg, B. (2001). *Qualitative Research Methods for the Social Science.* Neeham Heights. MA: Allyn and Bacon.

Bhanu, C. and Stone, C. (2004). Public-Private Partnerships for Police Reform. *Crime and Justice*. pp. 1-9.

Bilek, A.J. (1977). *Private Security Standards and Goals* (The Report of the Official Private Security Task Force). Cincinatti OH: Anderson Publishing Co.

Birkenstock, G.E. (1992). The Foreign Intelligence Surveillance Act and Standards of probable cause: An alternative analysis. *Georgetown Law Journal*. 80, pp. 843-871.

Bottoms, A. (2000). The Relationship between Theory and Research in Criminology in King, R & Wincup. E (eds). *Doing Research on Crime and Justice*, Oxford University Press. Oxford.

Bradley, A.A. (2002). Extremism in the defence of liberty? The Foreign Intelligence Surveillance Act and the significance of the U.S.A. Patriot Act. *Tulane Law Review*. 77, pp. 465-493.

Braithwaite, J. and Drahos, P. (2000). *Global Business Regulation*. Cambridge: Cambridge University Press.

Brenner, S. (2004). Distributes Security: Moving Away from Reactive Law Enforcement. *International Journal of Communications Law and Policy*. Spring 2005. 9, pp. 1-50.

Brewer, J. (1994). *Black and Blue: Policing in South Africa*. Oxford: Oxford University Press.

British Society of Criminology (2005). *Code of Research Ethics*. [online]. [Accessed 12th April 2005]. Available from World Wide Web:<http://www.britsoccri m.org/ethics.htm>

British Sociological Association (2002). *Statement of Ethical Practice for the British Sociological Association*. [online]. [Accessed 15th April 2005]. Available from World Wide Web: < http://www.britsoc.co.uk/Library/Ethicsguidelines2002.doc>

Broadhurst, R. (2005). *11th UN Congress on Crime Prevention and Criminal Justice, Workshop 6: Measures to combat Computer Related Crime*. 18-25 April 2005, Thailand, pp. 1-2.

Brodeur, J. (1995) Le controle social: Privatisation et technocratie. *Deviance et Societe*. 19 (2), pp. 127-147.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management*. 29 (3), pp. 408-433.

Broadhurst, R. and Chantler, A. (2007). Future of High Tech Crime. *Australian Institute of Criminology*. January 2007.

Broersma, M. (2006). Phishers catch on to the Net's long tail. *CNET News*.12 September. [online]. [Accessed 11th November 2006]. Available from World Wide Web:<www.cnet.com>

Bureau of Justice Assistance (2005). *Engaging the Private Sector to Promote Homeland Security*. September 2005.

Buchanan, J. and Grant, A. (2001). Investigating and prosecuting Nigerian fraud. *United States Attorneys' Bulletin*. November, pp. 39-47.

Button, M., Johnston, L., Frimpong, K. and Smith, G. (2007). New direction in policing fraud: The emergence of the counter fraud specialist in the United Kingdom. *International Journal of the Sociology of Law*. 35 (4). pp. 192-208.

Button, M. (2002). *Private Policing* . Devon: Willan Publishing.

Button, M. (2003). Private security and the policing of quasi-public space. *International Journal of the Sociology of Law*. 31, pp. 227-237.

Burns, R. and Whitworth, K. (2002). Internet fraud: Law enforcement resources, collaboration, control and prevention. *Report Submitted to the National White Collar Crime Center Research Contract Program.* Fort Worth, TX.

Burns, R., Whitworth, K., and Thompson, C. (2004). Assessing law enforcement preparedness to address Internet fraud. *Journal of Criminal Justice*. 32, pp. 477-493.

Byassee, W. (1997). Jurisdiction of cyberspace: applying real world precedent to the virtual community. *Wake Forest Review*. 30, pp. 205.

Bywell, C. and Oppenheim, C. (2001). Fraud on Internet auctions. *Aslib Proceedings*. 53(7), pp. 265-272.

Caden, M. and Lucas, S. (1996). Accidents on the Information Superhighway: on-line liability and regulation. *Richmond Journal of Law and Technology*. [online]. 2(1), [Accessed 4th January 2006]. Available from World Wide Web: <www.richmond.edu/~jolt/v2il/caden_lucas.html >

Calomiris, C. (1990). Is deposit insurance necessary?:A historical perspective. *Journal of Economic History*. 50 (2), pp. 283-295.

Cameron, J. and Vail, D. (2006). The Impact of Security Concerns on Cyber Liberties. *The Information Society:Emerging Landscapes*. 195. pp. 153-167.

Carroll, R. (2005). *The Skeptic's Dictionary: Pyramid schemes, chain letters and ponzi schemes*. [online]. [Accessed 12th February 2006]. Available from World Wide Web: <http://skeptic.com/pyramid.html>

Castelan, G.. (2000). Its buyer beware in cyberspace: 1999-2000 Credit Card Survey. *Consumer Action News*. 1 March 2000. [online]. [Accessed 10th July 2006]. Available from World Wide Web:

<http://www.consumer-
action.org/news/articles/2000_credit_card_survey#Topic_12>

Canadian Better Business Bureau (2005). [online]. [Accessed 25th August 2007]. Available from World Wide Web:<http://www.ccbbb.ca/>

Centeno, C. (2002). *Building Security and Consumer Trust in Internet Payments: The potential of "Soft" measures.* Background Paper No.7. Electronic Payment Systems Obervatory (ePSO). May 2002.

Centre for the Protection of National Infrastructure (2008). [online]. [Accessed 23rd October 2008]. Available from World Wide Web: <http://www.cpni.gov.uk/about.aspx/>

Charney, S. (2005). Combating Cyber Crime: A Public-Private Strategy in the Digital Environment. *Microsoft Corporation.* 31 May 2005.

Chau,D., Pandit, S., and Faloutsos, C. (2006). Detecting Fraudulent Personalities in Networks of Online Auctioneers. *Lecture Notes in Computer Science.* 4213, pp. 103-114.

Choi, Y. (2006). Cybercop. 14 March 2006. [online]. [Accessed 20th June 2007]. Available from World Wide Web:< http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=105&oid=038&aid=0000321721>

Chua, C. and Wareham, J. (2002). Self-Regulation for online auctions: An analysis. *Proceedings of the International Conference on Information.* [online]. [Accessed 22nd April 2005]. Available from World Wide Web: <http://wareham.eci.gsu.edu/Resume/Papers/wicis5bib.pdf>

Chua, C. and Wareham, J. (2004). Fighting Internet Auction Fraud: An Assessment and Proposal. *IEEE Computer Society.* 37(10), pp. 31-37.

Charlton, K. and Taylor, N. (2004). *Online Credit Card Fraud against Small Businesses.* Australia Institute of Criminology.

Chat Friendz. (2008). [online]. [Accessed 27th October 2008]. Available from World Wide Web: <http://www.usachatrooms.co.cc/>

Chung, T. (1999). GIS: An Effective Technological Intervention for Proactive Policing. *Master Program Thesis*. Michigan State University.

Clarke, M. (1989). Insurance Fraud. *British Journal of Criminology*. 29 (1), pp. 1-20.

Clarke, M. (1990). *Business Crime: Its Nature and Control.* Cambridge: Polity Press.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM.* 42 (2), pp. 60-67.

Clark, E. Dugdale, A. and Sathye, M. (2004). *Fraud in E-Government Transactions: Risks and Remedies.* [online]. [Accessed 22nd March 2005]. Available from World Wide Web: < http://www.finance.gov.au/publications/future-challenges-for-egovernment/docs/AGIMO-FC-no14.pdf>

Clarke, M and Harrington, C. (1994). Insurance Fraud. *British Journal of Criminology*. 29, pp. 1-20.

Cohen, F. (2001). Corporate Security Intelligence: An Oxymoron? *Network Security*. 3, pp.12-17.

Cohen, F. (2002). Computer fraud scenarios-Robbing the rich to feed the poor. *Computer fraud and Security*. 1, pp. 5-6.

Coleman, C. (2003). Cyberspace security. *Computer law and security Report.* 19 (2), pp. 131-136.

Committed to wiping out Internet scams and fraud (2008). [online]. [Accessed 23rd November 2008]. Available from World Wide Web: <http://www.apwg.org/>

Confederation of Asian and Pacific Accountants (2001). *Controlling Fraud on the Internet: A CAPA Perspective.* 13 July 2001. [online]. [Accessed 11th May 2005]. Available from World Wide Web:< http://www.capa.com.my/article.cfm?id=1 >

Connors, E., Cunningham, W., and Ohlhausen. P. (1999). *Operation Cooperation: A Literature Review.* ILJ and Hallcrest Division of SAIC.

Consumer Direct Provides clear, practical ,consumer advice (2008). [online]. [Accessed 18th November 2008]. Available from World Wide Web: <http://www.consumerdirect.gov.uk/>

Conrades, G. (2004). Hardening the Internet. *National Infrastructure Advisory Council.* [online]. [Accessed 29th October 2007]. Available from World Wide Web: <http://www.dhs.gov/xlibrary/assets/niac/NIAC_HardeningInternetPaper_Jan05.pdf>

Corbett, P. (2006). Prosecuting the Internet fraud case without going broke. *HeinOnline.* [online]. 76:841, [Accessed 30th September 2007]. Available from World Wide Web: <www.heinonline.org>

Cordeiro, C. and Hawamdeh, S. (2001). National Information Infrastructure and the realization of Singapore IT 2000 initiative. *Information Research.* [online]. 6(2), [Accessed 23rd June 2007]. Available from World Wide Web: <http://informationr.net/ir/6-2/paper96.html>

Cornwell, R. (2002). US indicts Andersen for shredding Enron papers. *The Independent.* 15 March.

Crawford, A. and Lister, S. (2003). Contractual governance of deviant behaviour. *Journal of Law and Society.* 30 (4), pp. 479-505.

Crawford, A. and Lister, S. (2004). The Patchwork future of reassurance policing in England & Wales: integrated local security quilts or frayed, fragmented and fragile tangled webs? *Policing: An International Journal of Police Strategies & Management.* 27 (3), pp. 413-430.

Crawford, A., Lister, S., Blackburn, S. and Burnett, J. (2005). *The mixed economy of visible patrols in England and Wales.* Bristol: Policy Press.

Crimestoppers (2008). Card Fraud losses up by 14 percent. 1 October 2008. [online]. [Accessed 25th November 2008]. Available from World Wide Web:< http://www.crimestoppers-uk.org/media-centre/crime-in-the-news/october-2008--crime-in-the-news/card-fraud-losses-up-by-14-per-cent>

Cunningham, W. and Taylor, T. (1985). *Private Security and Police in America* (The Hallcrest Report). Portland OR: Chancellor Press.

Cyber Terror Response Center (2005). [online]. [Accessed 17th February 2005]. Available from World Wide Web : < http://www.ctrc.go.kr/english/index.j >

Davis, P. (2005). Cyber security and implications for national infrastructure. *Security of Distributed Control Systems.* [online]. [Accessed 2nd Nov. 2005],pp.1-12. Available form World Wide Web:< http://ieeexplore.ieee.org/Xplore/login.jsp?url=/iel5/10377/32979/01545622.pdf?tp=&isnumber=&arnumber=1545622>

Davis, M., Lundman, R. and Martinez, R. (1991). Private Corporate Justice: Store Police, Shoplifters, and Civil Recovery. *Social Problem.* 38 (3), pp. 395-411.

Deleuze , G. and Guattari, F. (2004). *A Thousand Plateaus:Capitalism and Schizophrenia.* Minneapolis: University of Minnesota Press.

De lint, W. (2005). Public Order Policing: A tough act to follow. *International Journal of the Sociology of Law.* 31. pp. 179-199.

De lint, W., O'Connor, D. and Cotter, R. (2007). Controlling the flow: Security, Exclusivity, and Criminal Intelligence in Ontario. *International Journal of the Sociology of Law*. 35, pp. 41-58.

Dennehy, M. (2000). eBay motors breakdown? *AuctionWatch.com*. 23 June. [online]. [Accessed 22nd May 2006]. Available from World Wide Web:<http:// www.auctionwatch.com/awdaily/dailynews/june00/1-062300.html >

Denning, D. (1999). *Information Warfare and Security*. London: Pearson Books.

Department of Homeland Security (2005). [online]. [Accessed 14th August 2007]. Available from World Wide Web: <http://www.dhs.gov>

Department of Homeland Security (2005). [online]. [Accessed 19th December 2007]. Available from World Wide Web: <http://www.dhs.gov/xprevprot/editorial_0206>

Digital Certification Center (2006). Yes sign Service Provision. [online]. [Accessed 12th December 2007]. Available from World Wide Web:< http://www.yessign.or.kr/english/cps.htm>

Draper, H. (1978). *Private Police*. London: Penguin Books.

Drinkhall, J. (1997). Internet fraud. *Journal of Financial Crime*. 4, pp. 242.

Duh, R., Jamal, K. and Sunder, S. (2002). Control and Assurance in E-commerce: Privacy, Integrity, and Security at eBay. *Taiwan Accounting Review*. 3 (1), pp. 1-27.

Dupont, B. (2004). Security in the age of networks. *Policing and Society*. 14 (1), pp. 76-91.

Dupont, B. (2007). The nodal structure of international police cooperation: an exploration of translational security networks. *Global Governance*. 13 (3), pp. 347-364.

Edelman, B. (2008). Deterring Online Advertising Fraud through Optimal Payment in Arrears. *Harvard Business School*. [online]. [Accessed 14th December 2008]. Available from World Wide Web:< http://www.hbs.edu/research/pdf/08-072.pdf>

Emery, D. (2002). The Nigerian e-mail hoax. *SFGate.com*. 14 March. [online]. [Accessed 18th February 2006]. Available from World Wide Web:< http://www.sfgate.com .>

Emling, S. (2001). Dot.cons. Atlanta *Journal Constitution*. 28 January. pp. P1-P4.

Emsley, C. (1996). *The English Police: A political and Social History* (2nd eds). London: Longman.

European Network and Information Security Agency (2005). [online]. [Accessed 24th July 2005]. Available from World Wide Web: < http://www.enisa.eu.int>

EPIC (1996). Silencing the Net: The threat to freedom of expression on-line. *Human Rights Watch*. [online]. 8(2): G., [Accessed 19th June 2001]. Available from World Wide Web: <www.epic.org/free_speech/intl/hrw_report_5_96.html >

Ericson, R. and Haggerty, K.D. (1997). *Policing the Risk Society*. Oxford: Clarendon Press.

Ericson, R. (1994). The Division of Expert Knowledge in Policing and Security. *British Journal of Sociology*. 45 (2). pp. 149-175.

Ericson, R., Doyle, A. and Barry, D. (2003). *Insurance as Governance*. Toronto: University of Toronto Press.

Euractiv (2004). *Cyber crime*. [online]. [Accessed 12th December 2007]. Available from World Wide Web:< http://www.euractiv.com/en/infosociety/cybercrime/article-117465>

EURIM (2006). *Information Society Alliance*. [online]. [Accessed 11th January 2007]. Available from World Wide Web:< http://www.eurim.org.uk/>

EuroISPA (2008). [online]. [Accessed 28th July 2007]. Available from World Wide Web:< http://www.euroispa.org/>

Facebook (2004). [online]. [Accessed 26th November 2008]. Available from World Wide Web: <http://ko-kr.facebook.com/>

Federal Bureau of Investigation (2005). [online]. [Accessed 24th July 2005]. Available from World Wide Web:<www.fbi.gov/cyberinvest/cyberhome.htm>

Federal Trade Commission (1998). *Fighting consumer fraud: New tools of the trade*. Report dated April 1998. [online]. [Accessed 20th April 2007]. Available from World Wide Web:< http://www.ftc.gov/reports/fraud97/index.shtml>

Federal Trade Commission (2003). *The CAN-SPAM Act of 2003: Requirements for Commercial Emailers*. [online]. [Accessed 26th November 2007]. Available from World Wide Web:<. http://www.ftc.gov/bcp/edu/pubs/business/ecommerce/bus61.shtml>

Federal Trade Commission (2003). *FTC and FDA Crackdown on Internet Marketers of Bogus SARS Prevention Products*. Press release, issued 9 May 2003. [online]. [Accessed 20th April 2008]. Available from World

Wide Web:< http://www.fda.gov/bbs/topics/NEWS/2003/NEW00904.html>

Federal Trade Commission (2004). *National and State Trends in fraud and identity theft* . [online]. [Accessed 22nd February 2005]. Available from World Wide Web: <http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf>

Federal Trade Commission (2005). *The truth of advance fee loan scams.* [online]. [Accessed 23rd August 2006]. Available from World Wide Web: <http://www.ftc.gov/bcp/conline/pubs/tmarkg/loans.htm>

Ferret, J. (2004). The State, policing and "Old Continental Europe": managing the local/national tension. *Policing and Society*. 14 (1). pp. 49-65.

Financial Service Authority (2008). [online]. [Accessed 21st November 2008]. Available from World Wide Web: <http://www.fsa.gov.uk/>

Fisse, B. and Braithwaite, J. (1983). *The Impact of Publicity on Corporate Offenders.* New York: SUNY Press.

Fleming, J. (2006). *The challenge of partnership policing and security network.* Sydney: University of South Wales Press.

Foremski, T. (2008). Will the burden of the long tail kill Internet commerce? *ZDNet news.* 22 March. *Tom Foremski: Blog* [online]. [Accessed 12th March 2008]. Available from World Wide Web: < http://updates.zdnet.com/tags/Tom+Foremski.html>

Forst, B. and Manning, P. (1999). *The privatization of policing: Two views.* Washington, DC: Georgetown University Press.

Fowles, J. (1978). *Handbook of Future Research.* Connecticut: Greenwood Press.

Fraud Review (2006). *Final report*. [online]. [Accessed 22nd June 2008]. Available from World Wide Web:< http://www.attorneygeneral.gov.uk/Fraud%20Review/Fraud%20Review%20Final%20Report%20July%202006.pdf>

Fried, R. (2003). Cyber Scam Artists: A new kind of .con. *SANS Institute*. [online]. [Accessed 28th June 2005]. Available from World Wide Web:< http://www.sans.org/rr/whitepapers/threats/482.php>

Friedrichs, D. (1992). White collar crime and the definitional quagmire: A provisional solution. *Critical Criminology*. 3 (2), pp. 5-21.

Friedrichs, D. (1996). *Trusted criminals*. Belmont CA: Wadsworth Publishing.

Garlik (2008). *The Online Identity Experts*. [online]. [Accessed 24th July 2008]. Available from World Wide Web:<http://www.garlik.com/press/garlik_uk_cybercrime_report.pdf/>

*Gartner. (*2007). *Gartner survey shows phishing Attacks escalated in 2007; More than $3 billion lost to these attacks*. [online]. [Accessed 17th March 2008]. Available from World Wide Web: < http://www.gartner.com/it/page.jsp?id=565125>

Gelsthorpe, L. , Tarling, R., and Wall, D. (1999). Code of Ethics for Researchers in the field of criminology. *British Society of Criminology*.

Get Safe Online (2007). [online]. [Accessed 24th July 2008]. Available from World Wide Web: < http://www.getsafeonline.org>

Gibbons, S. (1996). Private Function. *Police Review*. 9 February.

Gibbons, P. (2001). Mouse clicks and dirty tricks. *Platypus magazine*. 72. pp. 33-34.

Gill, M. and Hart, J. (1997). Exploring Investigative Policing: A study of private detectives in Britain. *British Journal of Criminology*. 37. pp. 549-67.

Glaessner, T., Kellermann, T. and McNevin, V. (2004). *Electronic Security: Risk Mitigation in Financial Transactions Public Policy Issues*. [online]. [Accessed 22nd September 2006]. Available from World Wide Web: < http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.19.1957>

Glink, I. (2005). Travel Scam. *WGN-TV*. [online]. [Accessed 08th June 2006]. Available from World Wide Web:< http://www.thinkglink.com/Travel_Scams.htm >

Golsby, M. (1998). Formalizing cooperation in crime prevention: police and security sectors working together. *Security Journal*. 10 (2). pp. 121-29.

Goodin, Dan. (2008). *Man accused of siphoning $50, 000 in micro-payments from Schweb E-trade*. [online]. [Accessed 20th August 2008]. Available from World Wide Web: < http://www.theregister.co.uk/2008/05/28/micro_payment_indictment/>

Grabosky, P. (2000). Computer Crime: A criminological Overview. Conference Paper Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. 15 April. Vienna. [online]. [Accessed 20th April 2005]. Available from World Wide Web: <http://www.aic.gov.au/conferences/other/compcrime/index.html >

Grabosky, P. and Smith, R. (2001). Telecommunication fraud in the digital age: The convergence of technologies. *In*: Wall, D. eds. *Crime and the Internet*. London: Rutledge.

Gragg, D. (2002). A multi-level defence against social engineering. *SANS Institute*. [online]. [Accessed 22nd November 2007]. Available from

World Wide Web: <http://www.sans.org/reading_room/whitepapers/engineering/>

Gragg, D. (2003). A multi-level defence against social engineering. Whitepaper. San Diego: SANS Institute.

Granger, S. (2001). *Social Engineering Fundamentals, Part I Hacker Tactics.* [online]. [Accessed 15th May 2005]. Available from World Wide Web: <www.securityfocus.com >

Gray, K. and Gray, S. (1999). Civil rights, civil wrongs and quasi-public space. *EHRLR.* 1, pp. 46-102.

Graycar, A. and Smith, R. (2002). Identifying and responding to electronic fraud risks. *In: 30th Australian Registrars' Conference, 13 November, Canberra.* Canberra: Australian Institute of Criminology. pp. 1-10.

Grazioli, S. and Jarvenpaa, S. (2003). Consumer and Business Deception on the Internet: Content Analysis of Documentary Evidence. *International Journal of Electronic Commerce*. 7 (4), pp. 93-118.

Greene, J., Seamon, T., and Levy, P. (1995). Merging public and private security for collective benefit. *American Journal of Police.* 14 (2), pp. 3-20.

Green, T. (2001). *Biometric Security-Practical and Affordable!* [online]. [Accessed 17th January] Available from World Wide Web :<http://www.moreilly.com/CISSP/Dom3-2-biometric_security.pdf .>

Guenther, M. (2001). *Social Engineering-Security Awareness Series: Information Warfare Site U.K.* [online]. [Accessed 27th May 2007]. Available from world Wide Web: <http://www.iwar.org.uk/comsec/resources/sa-tools/social-engineering.pdf>

Guidera. J. (2000). *Dow Jones Newswires: FTC investigating Smith Kline's Top-Selling Paxil.* [online]. [Accessed 15th April 2007]. Available from Worldwide Web:< http://lists.essential.org/pipermail/ip-health/2000-December/000688.html>

Hart, G. (2001). Here's a Better Way to Be Secure. *Time*. 8 October. p. 33.

Harreld, H. (1998). GSA: Protect Web users' privacy. *Federal Computer Week*. 13 July.

Haggerty, K. and Ericson, R. (2000). The surveillant assemblage. *British Journal of Sociology*. 51(4), pp. 605-622.

Haywood, A. (2006). *Online Auctions: User Experience Insights from eBay*. April (No.2006-10). [online]. [Accessed 29th November 2008]. Available from World Wide Web:< http://www.essex.ac.uk/chimera/content/Pubs/wps/CWP-2006-10%20eBay-User-Experience-Insights.pdf>

Henry, K. (2001). Is Security at Risk from the IT Downturn? *Computer Fraud & Security*. 7, pp. 10-12.

Henry, S. (1983). *Private Justice: Towards Integrated Theorizing in the Sociology of law*. Boston. MA: Routledge.

Henry, S. (1987). Private Justice and the Policing of Labor: The Dialectics of Industrial Discipline' *In:* C . Shearing and C. Stenning. Eds. *Private Policing*. Newbury Park, CA: Sage. pp. 45-71.

High Tech Crime Consortium (2008). [online]. [Accessed 29th November 2008]. Available from World Wide Web:< http://www.hightechcrimecops.org/HTCC_minibroc07.pdf>

Hynds, L. (2003). *Policing Cyberspace.* 17 April. [online]. [Accessed 8th May 2006]. Available from World Wide Web: < http://www.computerweekly.com/Articles/2003/04/17/193926/policing-cyberspace.htm>

Huberman, M and Miles, M. (1994). *Data management and analysis methods. In*: N. Denzen &Y.S. Lincoln. eds. Handbook of Qualitative Research. Thousand Oaks.CA: Sage.

Independent Banking Advisory Service (2008). [online]. [Accessed 16th November 2008]. Available from World Wide Web: <http://www.ibas.co.uk/>

Intenet Crime Complaint Center (2008). [online]. [Accessed 13th September 2008]. Available from World Wide Web: <http://www.ic3.gov/about/default.aspx>

Internet fraud: A growing threat to online retailers (2001). [online]. [Accessed 5th March 2005]. Available from World Wide Web:< http://www.experian.co.uk/downloads/business/internetfraud.pdf>

Innes, M. (2004). Reinventing tradition? Reassurance, neighbourhood security and policing. *Criminal Justice.* 4 (2), pp. 151-171.

Internet Fraud Complaint Center (2000). *Six Month Data Trends Report : May-November 2000.* [online]. [Accessed 15th March 2005]. Available from World Wide Web: <http:www.ifccfbi.gov/>

Internet Fraud Complaint Center (2005). [online]. [Accessed 10th April 2005]. Available from World Wide Web:< http://www.fbi.gov/hq/cid/fc/ifcc/about/about_ifcc.htm>

Internet Fraud Watch (2002). *2001 Internet fraud statistics.* [online]. [Accessed 23th May 2005]. Available from World Wide Web:< http://www.fraud.org/internet/2001 stats.htm >

Internet Fraud Watch (2005). *2005 Internet fraud statistics.* [online]. [Accessed 20th July 2005]. Available from World Wide Web: <http://www.fraud.org/internet/intset.htm >

IOP Press (2003). Legal Manual for Combating Cybercrime. *Digest of Electronic Commerce Policy and Regulation.* 26. pp. 137-141.

Jacobson, P. (2001). Regulating health care: From self-regulation to self regulation? *Journal of Health, Politics, Policy and Law.* 26 (5). pp. 1164-1177.

Jewkes, Y. (2004). Policing Cybercrime. *In*: T. Newburn et al. eds. *Handbook of Policing* (2nd edn). Devon. UK: Willan Publishing. pp. 501-523.

Joh, E. (2004). The paradox of private policing. *Journal of Criminal Law and Criminology*. 95, pp. 45-99.

Jones, T. and Newburn, T. (1998). *Private Security and Public Policing.* Oxford: Oxford University Press.

Jones, T. and Newburn, T. (1999). Urban Change and Policing: Mass Private Property Re-considered. *European Journal on Criminal Policy and Research.* 7 (2), pp. 225-244.

Joh, E. (2004). The Paradox of Private Policing. *Journal of Criminal Law and Criminology.* 95 (1).

Joh, E. (2005). Conceptualizing the Private Police. *Utah Law Review.* 3 February.

Johnson, J and Lim, Y. (2002). Money laundering: has the Financial Action Task Force made a difference? *Journal of Financial Crime.* 10, pp. 7-22.

Johnston, L. (1992). *The Rebirth of Private Polcing.* London: Routledge.

Johnston, L. (1999). Private policing in context. *European Journal of Criminal Policy and Research.* 7 (2), pp. 175-196.

Johnston, L. (1996). *Policing diversity: the impact of the public-private complex in policing. In*: Leishman, F., Loveday, B. and Savage, S. eds. Core Issues in Policing, 1st edition. London: Longman. pp. 54-70.

Johnston, L. and Shearing, C. (2003). *Governing security: explorations in policing and justice.* London: Routledge.

Jones, K. (2006). Cyber Crime High on FBI priority list, help wanted. *Techweb.* 24 October. [online]. [Accessed 15th June 2007]. Available from World Wide Web: < http://techsearch.cmp.com/search.jhtml?queryText=negative+publicity+jones+2006&personality=category>

Jordan, T. (1999). *Cyberspace and the Internet.* London: Routledge.

Justchat (2008). [online]. [Accessed 20th November 2008]. Available from World Wide Web: <http://www.justchat.co.uk/>

Kaiser, L. and Kaiser, M. (2000). *The Official eBay Guide, New York.* NY: Simon & Schuster.

Kaleewoun, P. (2001). *An overview of corporate computer user policy.* 27 December [online]. [Accessed 7th April 2007]. Available from World Wide Web: <www.sans.org>

Kauffman, R. and Wood, C. (2003). Why does reserve price shilling occur in online auctions? *In: Preceedings of the 2003 International Conference on Electronic Commerce. Pittsburg.*

Kirshner, J. (2003). Bitten Bidders. *US News and World Report*. 16 June. 134, pp. 21.

Kennedy, D. (2000). A web of crime. *Sydney morning herald*. 11 July.

Kempa, M, Stennig, P and Wood, J. (2004). Policing Communal Space. *British Journal of Criminology*. 44 (4), pp. 562-581.

Kempa, M. et al. (1999). Reflections on the evolving concept of private policing. *European Journal on Criminal Policy and Research*. 7. pp. 197-223.

Kiernan, P. (2005). Role and Responsibilities of the Serious Fraud Office in Fighting Fraud Within the United Kingdom (From Annual Report for 2004 and Resource Material Series No. 66, P 91-98. 2005. Simon Cornell, ed. -- See NCJ-213348). Tokyo: Japan.

Kim, H. (2008). Real name conformation on Internet. *ZDNet Korea*. 3 December 2008. [online]. [Accessed 16th December 2008]. Available from World Wide Web:< http://www.zdnet.co.kr/news/internet/etc/0,39031281,39175939,00.htm >

Kim, K. (2008). KNPU invites foreign police forces for cybercrime training. 18 June 2008. *Newsis*. [online]. [Accessed 28th October 2008]. Available from World Wide Web:< http://www.newsis.com/article/view.htm?cID=&ar_id=NISX20080618_0008003122>

Knights, M. (2008). *Card fraud abroad up claims. APACS*. 30 December. [online]. [Accessed 27th July 2008]. Available from World Wide Web: < http://www.itpro.co.uk/177357/card-fraud-abroad-up-claims-apacs>

Korea Information Security Agency (2003). The Information Facilitation Act No. 14. April 1996. [online]. [Accessed 12th April 2005]. Available from World Wide Web:< http://www.kisa.or.kr/index.jsp>

Korea Information Security Agency (2004). *Privacynet*. [online]. [Accessed 22nd October 2005]. Available from World Wide Web:<https://www.kisa.or.kr/kisae/privacy/jsp/privacy_02_02.jsp>

Korea Internet Security Center (2004). *KrCERT/CC: Vision*. [online]. [Accessed 28th May 2005]. Available from World Wide Web:< http://www.krcert.or.kr/index.jsp>

Korea National Statistical Office (2007). *Cyber Shopping Mall*. [online]. [Accessed 27th May 2008]. Availalble from World Wide Web:< http://www.kosis.kr/>

Korea Spam Response Center (2003). *Background of establishment*. [online]. [Accessed 23rd August 2005]. Available from World Wide Web:< http://www.kisa.or.kr/kisae/ksrc/jsp/ksrc_02_01.jsp>

KOSCOM/ISAC (2005). *About ISAC*. [online]. [Accessed 24th September 2005]. Available from World Wide Web:< http://www.koscomisac.com/front/eng/mainEng.html>

Kozlovski, N. (2005). *A Paradigm shift in Policing from law enforcement to cyberpolicing. PORTIA Project.* Yale University. [online]. [Accessed 29th May 2007]. Available from World Wide Web: <http://crypto.stanford.edu/portia/talks/online_policing_model.ppt>

Kozlovski, N. (2007). Designing Accountable Online Policing. *In*: J.M. Balkin.ed. *Cybercrime: Digital Cops in a Networked Environment*. New York University Press. pp. 107-134.

Krawetz, N. (2004). Anti-spam solutions and security. *Security Focus*. [online]. [Accessed 2nd April 2005]. Available from World Wide Web: < http://www.securityfocus.com/infocus/1763 >

Kroll,Inc. [online]. [Accessed 27th August 2006]. Available from World Wide Web : <www.krollworldwide.com/service>

Lang, P. (1999).How to beat credit card fraud. *Sell it!* 20 March. [online]. [Accessed 29th March 2005]. Available from World Wide Web: < http://sellitontheweb.com/ezine/howto004.html>

Lee, C. (2004). Accounting for rapid growth of private policing in South Korea. *Journal of Criminal Justice*. 32 (2), pp. 113-122.

Lee, C. (2005). The Historical Development of Private policing in Korea during the Pre-Modern Era. *Asian Policing*. 3 (1), pp. 37-50.

Lee, J. (2000). Law Enforcement Officers step up efforts to tame cybercrime. *The Korea Herald,* 17 November 2000. [online]. [Accessed 19th June 2005]. Available from World Wide Web:<www.koreaherald.com>

Lee, S. (2008). Online Game Ring Smuggling out $38 million to China. *Donga Daily*, 22 October 2008. [online]. [Accessed 13th November 2008]. Available from World Wide Web:< http://english.donga.com/srv/service.php3?bicode=040000&biid=20081 02291528>

Lee, Y. (2007). FSA established KFCERT. *Digital Daily,* 30 January 2007. [online].[Accessed 23rd September 2008]. Available from World Wide Web:< http://www.ddaily.co.kr/news/news_view.php?uid=20301>

Leggart, H. (2007). *Biz Report: Low and Regulation.* [online]. [Accessed 22nd February 2008]. Available from World Wide Web: < http://www.bizreport.com/>

Leland, H. (1979). Quacks, Lemons, and Licensing: A theory of minimum standards. *The journal of political economy*. 87 (6). pp. 1328-1346.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Lessig, L. (1999). The Law of the Horse (Judge Frank Easterbrook) vs. The Law of Cyberspace (Professor Lawrence Lessig). *Harvard Law Review*. 113, pp. 501-549.

Lessig, L. (2001). Code and other Laws of cyberspace. *Canadian Journal of Communication*. 26 (1), pp. 179-180.

Levi, M. (1991). Regulating Money Laundering: The death of bank secrecy in the UK. *The British Journal of Criminology*. 31. pp. 109-125.

Levi, M. (1992). White-Collar Crime Victimization. *In*: K. Schlegel and D. Weisburd. eds. *White-Collar Crime Reconsidered*. Boston. MA: Northeastern University Press. pp. 169-192. ____ (1993).White-Collar Crime: The British Scene. *Annals of the American Academy of Political and Social Science*. 525, pp. 71-82.

Levi, M. (2002). Suite justice or sweet charity?: Some explorations of shaming and incapacitating business fraudsters. *Punishment & Society*. 4 (2), pp. 147-163.

Levin, H. (1985). Principles of data storage and retrieval for use in qualitative evaluation. *Educational Evaluation and Policy Analysis*. 7 (2), pp. 169-186.

Levy, S. and Stone, B. (1998). Risky Business: You can get anything you want on the auction site eBay. But proceed with caution. *Newsweek* . 21 December. [online].[Accessed 10th May 2007] Available from World

Wide Web: <http://www.newsweek.com:80 nw-srv/printed/us/st/tc0125_1.htm>

Leyden, J. (2005). *Reformed UK fraud law to tackle phishing attacks.* 27 May [online]. [Accessed 28th July 2006]. Available from World Wide Web: < http://www.theregister.co.uk/2005/05/27/fraud_law_reform/>

Leyden, J. (2007). Security fears stymy online sales. *The Register.* 17 December. [online]. [Accessed 17th March 2008]. Available from World Wide Web:.< http://www.theregister.co.uk/2007/12/17/e_commerce_security_fears/>

Leyden, J. (2007). Bank and mortgage scam nets ID crooks thousands. *The Register*. 30 October. [online]. [Accessed 27th December 2007]. Available from World Wide Web:.< http://www.theregister.co.uk/2007/10/30/bank_mortgage_scam/>

Leyden, J. (2008). Hidden card fraud taxes UK.biz. *The Register.* 23 April. [online].[Accessed 22nd July 2008]. Available from World Wide Web:.< http://www.theregister.co.uk/2008/04/23/hidden_card_fraud/>

Leyden, J. (2008). *SOCA socks up asset recovery agency: More powers to seize ill-gotten gains for 'UK's 'FBI'.* 1 April. [online]. [Accessed 19th July 2008]. Available from World Wide Web: < http://www.theregister.co.uk/2008/04/01/soca_gets_asset_recovery_powers/>

Leyden, J. (2008). *US cybercrime losses reach $240m: Auction fraud means record high.* 4 April [online]. [Accessed 27th June 2008]. Available from World Wide Web: < http://www.theregister.co.uk/2008/04/04/cybercrime_losses/>

Lincoln, Y. and Guba, E. (1985). *Naturalistic Inquiry*. London: Sage Publications, Inc.

Lister, S., Wall, D. and Crawford, A. (2003). *Great Expectations: Contracted Community Policing in New Earswick.* York: Joseph Rowntree Foundation.

Litan, A. (2004). Phishing attack victims likely targets for identity theft. *Gartner.* 4 May. [online] [Accessed 10th June 2005]. Available from World Wide Web: <www.gartner.com >

Loader, I. (2000). Plural Policing and Democratic Governance. *social and legal studies.*9 (3), pp. 323-345.

Loader, I. And Walker, N. (2001). Policing as a Public good: Reconstituting the Connections between Policing and the State. *Theoretical Criminology.* 5 (1), pp. 9-35.

Loader, I. (1997). Thinking Normative about Private Security. *Journal of Law and Society.* 24 (3), pp. 377-394.

Logan, R. (1999). REACHING INTO CYBERSPACE WITH MAINE'S LONG-ARM STATUTE. *Maine Bar Journal.*

Malakedsuwan, P. and Stevens, K. (2003). Model of e-fraud. *7th Conference on Information Systems*. July 2003. Adelaide: South Australia. pp. 10-13.

Mandel, R. (2002). *Armies Without States: The Privatization of Security.* Colorado: Lynne Rienner Publishers.

Martino, J. (1983). *Technological Forecasting for Decision Making.* New York: North-Holland.

.

Marx, G.. (1987). *The interweaving of public and private police in undercover work.* Private Policing. Beverly Hills: Sage.

Matthews, R. and Cote, R. (2004). Understanding aboriginal policing in a social capital context. *Thematic Policy Studies, Police Research Initiative Conference.* 13-15 December.

Matusic, K. (2001). Be aware of Internet Appeals. *Reuters Limited.* 19 September.

Mawby, R. (1999). *Policing across the world.* London: Routledge.

Mawby, R. (2000). Core policing: the seductive myth. in F. Leishman et al. eds. *Core Issues in Policing* (2nd edn). London: Longman. pp. 107-23.

Merseyside Police. (2008). Crime Prevention: Business Advice. *Long-firm fraud.* [online]. [Accessed 13th November 2008]. Available from World Wide Web:< http://www.merseyside.police.uk/html/crimeprevention/business/fraud/long-firm.htm>

Millersmiles (2003). [online]. [Accessed 28th November 2008]. Available from World Wide Web: <http://www.millersmiles.co.uk/>

Ministry of Government Legislation (2006). *Korean criminal law* Article 347-1, 347-2 (Translated). [online]. [Accessed 10th April 2006]. Available from World Wide Web:< http://www.moleg.go.kr/index.mo>

Ministry of Government Legislation (2006). *The Acts on Promotion of Telecommunications Network Utilization* Article 48-3, Article 62-5 (Translated). [online]. [Accessed 11th April 2006]. Available from World Wide Web:< http://www.moleg.go.kr/index.mo>

Ministry of Government Legislation (2006). *The Telecommunication Business Law* Article 53 (Translated). [online]. [Accessed 11th April 2006]. Available from World Wide Web:< http://www.moleg.go.kr/index.mo>

Ministry of Government Legislation (2007). *The Act on Promotion of Telecommunications Network Utilization and Information Protection* (Translated). [online]. [Accessed 20th December 2007]. Available from World Wide Web:< http://www.moleg.go.kr/index.mo>

Mitnick, K. (2001). Click me: Social Engineering in Malware. *My First RSA conference*. [online]. [Accessed 11th October 2006]. Available from World Wide Web: <http://www.securifocus.com.news/199 14>

Mitrakas, A. and Zaitch, D. (2006). Law, Cybercrime and digital forensics: Trailing Digital Suspects. *In*: Kanellis, P, eds. *Digital crime and forensic science in cyberspace*. London: idea group inc. pp. 267-290.

McKenzie, S. (2005). Cyber Criminals on Trial (Review). *UMPA Postgraduate review*. 2 (1), pp. 29-30.

McKenzie, S. (2006). Partnership policing of electronic crime: an evaluation of public and private police investigation relationships. Ph.D. thesis, University of Melbourne.

Mcshane, M. and Williams, F. (1992). Radical Victimology: A critique of the concept of victim in traditional victimology. *Crime and Delinquency*. 38, pp. 258-271.

Morphy, E. (2007). E-Commerce Fraudsters' Haul May Reach $3.6B in 2007. *E-Commerce Times,* 19 November. [online]. [Accessed 22nd March 2008]. Available from World Wide Web:< http://www.ecommercetimes.com/story/60394.html>

Murphy, D. and Murphy, R. (2007). Phishing, Pharming, and Vishing: Fraud in the Internet Age. The Telecommunication Review. pp. 37-45

Murray, J. (2005). Policing Terrorism: A threat to community policing or just a shift in priorities?. *Police Practice and Research*. 6 (4), pp. 347-361.

Myers, M. (1997). Qualitative research in information systems. *MIS Quarterly archive*. 21 (2), pp. 241-242.

Myspace (2003). *About Myspace*. [online]. [Accessed 20th November 2008]. Available from World Wide Web: <http://www.myspace.com/>

Nalla, M. and Hummer, D. (1996). Relations between police officers and security professionals: a study of perception. *Security Journal*. 12. pp. 31-40.

Nalla, M. and Hummer, D. (1999). Assessing strategies for improving law enforcement/ security relationships: Implications for community policing. *International Journal of Comparative and Applied Criminal Justice*. 23 (2), pp. 227-239.

Nalla, M. and Morash, M. (2002). Assessing the Scope of Corporate Security: Common Practices and Relationships with Other Business Functions. *Security Journal*. 15 (3), pp. 7-19.

Napoli, R.M. (2001). *Foundations of Communications Policy*. Creskill. NJ: Hampton Press.

National Anti-Fraud Network (2008). *About NAFN*. [online]. [Accessed 21st November 2008]. Available from World Wide Web: <http://www.nafn.gov.uk/>

National Association of Insurance Commissioners (2005). About the NAIC. [online]. [Accessed 14th May 2005]. Available from World Wide Web: < http://www.naic.org>

National Conference of State Legislatures (2008). About NCSL. [online]. [Accessed 11th March 2005]. Available from World Wide Web: < http://www.ncsl.org>

National Consumers League (1999). *Top ten Internet fraud reports charts.* [online]. [Accessed 29th April 2005]. Available from World Wide Web: <http://www.nclnet.org/Internetscamfactsheet.html >

National Consumers League's Fraud Center (2004). *Internet Fraud Watch-Internet Scams Fraud Trends.* [online].[Accessed 16th February 2006]. Available from World Wide Web: <http://www.fraud.org/2004-internet%20scams.pdf>

National Consumers League (2005). *ID Thieves preying on consumers with new phishing scam called pharming: During national cyber security awareness month, groups helping consumers protect themselves.* [online]. [Accessed 29th December 2006]. Available from World Wide Web: < http://www.nclnet.org/news/2005/phishing_10132005.htm>

National Consumers League's Fraud Center (2007). *2007 Top 10 Internet Scams.* [online]. [Accessed 15th April 2008]. Available from World Wide Web: < http://www.fraud.org/internet/2007internet.pdf>

National Consumer's League Internet Fraud Watch (1998). *Consumer Protection in Electronic Commerce. Panel at the public voice in the development of Internet policy conference of the Global Internet Liberty Campaign.* [online]. [Accessed 14th March 1999].Available from World Wide Web: < http://www.fraud.org/internet/9810stat.htm>

National Cyber Security Center (2005). NCSC INFO. [online]. [Accessed 10th July 2005]. Available from World Wide Web:< http://www.ncsc.go.kr/eng/>

National White Collar Crime Center (2002). *IFCC 2001 Internet fraud report.* [online]. [Accessed 15th August 2008]. Available from World Wide Web: < http://www.ic3.gov/media/annualreport/2001_IFCCReport.pdf>

National White Collar Crime Center (2005). *IFCC 2004 Internet fraud report.* [online]. [Accessed 14th May 2005]. Available from World Wide Web: < http://www.ic3.gov/media/annualreport/2004_IFCCReport.pdf>

National White Collar Crime Center (2008). NW3C INFO. [online]. [Accessed 17th September 2008]. Available from World Wide Web: <http://www.nw3c.org/>

NCL's Fraud Center (2008). About NCL. [online]. [Accessed 25th October 2008]. Available from World Wide Web: <http://www.fraud.org/>

Nelson, R. (2004). *Methods of Hacking: Social Engineering, the Institute for Systems Research.* University of Marylan. [online]. [Accessed 20th May 2006]. Available from World Wide Web :< http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html>

Newburn, T. (2001). Urban change and policing: Mass private property re-considered. *European Journal on Criminal Policy and Research.* 7 (2), pp. 225-244.

Newburn, T. (ed). (2006). *Plural Policing.* London: Routledge.

Newman, G. and Clarke, R. (2003). *Superhighway robbery: Preventing e-commerce crime*. Portland: Willian.

NFIC (2005). Internet Scams, Fraud Trends. *National Fraud Information Center. January-December 2005.* [online]. [Accessed 26th May 2006]. Available from World Wide Web:< www.fraud.org/2005_Internet_Fraud_Report.pdf.>

NHTCU (2002). *Hi-Tech Crime: The impact on UK business.* London: National Hi-Tech Crime Unit.

Nhan, J. (2006). Policing Cyberspace: an assessment of criminal justice capacity in two key private industry sectors. *In: the Annual meeting of the American Society of Criminology. Los Angeles.* 1 November, 2006.

NIPC (1998). *Mission Statement*. National Infrastructure Protection Center. [online]. [Accessed 18th June 2005]. Available from World Wide Web: <www.nipc.gov/about/about.html>

Noaks, L. and Wincup. E. (2004). *Criminological research: understanding qualitative methods.* London: Sage.

O'Brien, M. (2005). Clear and Present Danger? Law and the Regulation of the Internet. *Information and Technology Law.* 14 (2). pp. 151-164.

O' Malley, P. (1991). Legal Networks and Domestic Security. *Studies in Law, Politics, and Society.* 11. pp. 171-90.

Oriola, T. (2005). Advance fee fraud on the Internet: Nigeria's regulatory response. *Computer law & Security report.* 21, pp. 237-248.

Out-Law (2001). 70% of UK companies hit by fraud, says PWC. 27 June 2001. [online]. [Accessed 22nd October 2006]. Available from World Wide Web:< http://www.out-law.com/page-1756>

Out-Law (2006). Prison terms for phishing fraudsters. 14 November 2006 [online]. [Accessed 13th February 2007]. Available from World Wide Web:< http://www.theregister.co.uk/2006/11/14/fraud_act_outlaws_phishing/>

Out-Law (2008). eBay sues business partners over alleged cookie stuffing. 4 September 2008. [online]. [Accessed 10th November 2008]. Available from World Wide Web: < http://www.channelregister.co.uk/2008/09/04/ebay_cookie_stuffing_suit />

Overill, R.E. (2001). Information warfare: battles in cyberspace. *Computing & Control Engineering Journal.* 12 (3), pp. 125-128.

Palumbo, J. (2000). Social Engineering: What is it, why is so little said about it and what can be done? *SANS Institute.* [online]. [Accessed 23rd May 2005]. Available from World Wide Web: < http://www.sans.org/infosecFAQ/social/social.htm >

Park, S. (2008). Vices of malicious comments. *Sports-Seoul.* 3 October.

Parker, D. (1980). *White Collar Crime: Theory and Research.* Beverly Hills: Sage.

Patil, S. (2007). *7th International Conference on Cyber-Crime. New Delhi: India.* Interpol. *12 September 2007.* [online]. [Accessed 23rd June 2008]. Available from World Wide Web: < http://www.interpol.com/public/ICPO/speeches/India20070912Minister.asp>

Parliament of Victoria (2002). *Inquiry into fraud and electronic commerce: emerging trends and best practice responses.* Drugs and Crime Prevention Committee. Melbourne: Government Press.

Peel, M. (2006). *Nigeria-Related Financial Crime and Its links with Britain: An African Programme Report*. November 2006. [online]. [Accessed 23rd December 2007]. Available from World Wide Web:< http://www.chathamhouse.org.uk/files/3377_nigeria1106.pdf>

POLCYB (2008). *The Society for the policing of cyberspace*. [online]. [Accessed 10th March 2008]. Available from World Wide Web:< http://www.polcyb.org/>

Post, D. (1996). American Lawyers. Plugged in 1996. *How Shall the Net Be Governed?* [online]. [Accessed 25th June 1997]. Available from World Wide Web: <http://www.temple.edu/lawschool/dpost/governance.html>

Prenzler, T. and Sarre, R. (1998). Regulating Private Security in Australia. *Trends and Issues in Crime and Criminal Justice*. No.98. Australia Institute of Criminology. [online]. [Accessed 26th June 1999]. Available from World Wide Web: <http://www.aic.gov.au/publications/tandi/ti98pdf.>

Punch, M. (1996). *Dirty Business: Exploring Corporate Misconduct Analysis and Cases*. London: Sage.

Rackow, S.H. (2002). How the U.S.A. Patriot Act will permit governmental infringement upon the privacy of American in the name of intelligence investigations. *University of Pennsylvania Law Review*. 150, pp. 1651-1695, 1673.

Radzinowicz, L. (1957). *A History of English Criminal Law and Its Administration from 1750: The Clash between private initiative and public interest in the Enforcement of Law 184*.

Rantala, R. (2004). Cybercrime against businesses. *2001 Computer security survey: Pilot test results*. Bureau of Justice Statistics. Washington, D.C. U.S. Department of Justice.

Ray, T. (2000). Trust in big business. *Smartmoney.com*. 27 June. [online]. [Accessed 28th May 2006] . Available from World Wide Web: < http://www.smartmoney.com>

Reichman, N. (1993). Insider trading. *Crime and Justice: A Review of Research*. 18 (55).

Reiner, R. (1994). *The politics of the police*. 2nd Edition. London: Harvester.

Reiner, R. (1997). *Policing and the police*. *In*: M. Maguire. R. Morgan and R. Reiner. eds. Oxford Handbook of Criminology. Oxford: Oxford University Press.

Reiner, R. (2000). *The Politics of the Police.* 3rd Edition. Oxford: Oxford University Press.

Richardson, T. (1999). UK anti-spam minnow takes on US big fish: Redoubles effort to pursue all spammers through the court. *The Register.* 20 April. 1999. [online]. [Accessed 26th September 2006]. Available from World Wide Web: < http://www.theregister.co.uk/1999/04/20/uk_antispam_minnow_takes>

Richman, S. (1996). Censorship in cyberspace. *The Future of Freedom Foundation.* [online]. [Accessed 23rd June 2007]. Available from World Wide Web: < http://www.fff.org/freedom/0396c.asp>

Rigakos, G. (2004). *The New Parabolic: Risk Markets and Commodified Social Control.* Toronto: University of Toronto Press.

Rip-off-tip-off (2008). [online]. [Accessed 28th November 2008]. Available from World Wide Web: <http://www.ripofftipoff.net/>

Roberg, R., Kuykendall, J. and Novak, K. (2002). *Police Management.* 3rd Edition. Roxbury Publishing Company.

Ross, E. (1907). *The Criminaloid. Chapter 3 in Sin and Society: An analysis of Latter-Day Inquiry.* Boston: Houghton Mifflin Company. pp. 45-71.

Rundle,M. and Laurie,B. (2005). Identity Management as a Cybersecurity Case Study. *Berkman Center Research Publication.* January 2006. [online].[Accessed 29th June 2007]. Available from World Wide Web:< http://ssrn.com/abstract=881107>

Rummel, R. (1981). *Understanding conflict and war.* Beverly Hills: Sage.

Samport (2007). *UK e-shopping boom brings fraud increase.* [online]. [Accessed 20th May 2008]. Available from World Wide Web: <

http://www.samport.com/news/uk-e-shopping-boom-brings-fraud-increase>

Sarre, R. and Prenzler, T. (2000). Relationship between police and private security: Models and future directions. *International Journal of Comparative and Applied Criminal Criminal Justice.*

Savirmuthu, A. and Savirmuthu,J. (2007). Identity Theft and Systems Theory: The Fraud Act 2006 in Perspective. *Scripted.* 4 (4). pp. 436-461.

Sathye, M., Clark, E., and Dugdale. A. (2004). *Fraud in e-government transactions: Risks and remedies.* Information Management Office: Australian Government.

Schlegel, K. and Weisburd, D. (1992). Introduction: White-Collar Crime The Parallax View. *In*: K. Schlegel and D. Weisburd. eds. *White-Collar Crime Reconsidered.* Boston, MA: Northeastern University Press.

Schneier, B. (2001). Managed Security Monitoring: Network Security for the 21st Century. *Computers and Security.* 6 (1). pp. 491-503.

Segell, G. (2007). Reform and Transformation: The UK's Serious Organized Crime Agency. *International Journal of Intelligence and CounterIntelligence.* 20 (2), pp. 217-239.

Selznick, P. (1969). *Law, Society, and Industrial Justice.* New York: Sage.

Sennewald, C. (1998). *Effective security management.* Boston: Butterworth-Heinemann Publishing.

Seoul Electronic Commerce Center (2008). *Internet fraud data in 2007.* [online]. [Accessed 30th September 2008]. Available from World Wide Web:< http://ecc.seoul.go.kr/>

Serious Fraud Office (2008). [online]. [Accessed 22nd October 2008]. Available from World Wide Web: <http://www.sfo.gov.uk/cases/section2.asp>

Serious Organized Crime Agency (2008). [online]. [Accessed 22nd December 2008]. Available from World Wide Web: <http://www.soca.gov.uk/>

Shaker, U and Walker, M. (2001). *A survey of security in online credit card payments.* [online]. [Accessed 8th April 2005]. Available from World Wide Web: <http://www.cs.berkeley.edu/~usshankar/research/ecommerce/credit.doc >

Shankar, U. and Walker, M. (2001). *A survey of security in online credit card payments.* [online]. [Accessed 15th April 2004]. Available from World Wide Web:< http://www.cs.berkeley.edu/~ushankar/ research/ecommerce/credit.htm>

Shaw, R. (2004). Spam: A global challenge in a borderless society. *8/9 September. Busan.* International telecommunication union. pp. 1-21.

Shearing, C. (1996). The Future of Policing. *Law and society review.* 30 (3): 585.

Shearing, C. and Stenning, P. (1981). Modern Private Security: Its Growth and Implications. *In:* M. Tonry and N. Morris .eds. *Crime and Justice: An Annual Review of Research.* 3. Chicago: University of Chicago press. pp. 193-245.

Shearing, C. and Stenning, P. (1983). Private Security: Implications for Social Control. *Social Problems.* 30. pp. 493-506.

Shearing, C. and Stenning, P. (1987). Say "Cheese!": The Disney Order that is not so Mickey Mouse. *Private Policing.* pp. 317, 322.

Shearing, C. and Stenning, P. (1992). Private Security: Implications for Social Control. *In*: K.R.E. McCormick & L.A. Visano eds. *Understanding Policing.* Canadian Scholars Press.

Shearing, C. (1992). The relationship between public and private policing. *Crime and Justice.* 16, pp. 399-434.

Shearing, C. (1992). The relation between public and private policing. *In*: M. Tonry and N. Morris. eds. *Modern Policing, Crime and Justice: A Review of Research.* Chicago: University of Chicago Press. *15.*

Shearing, C. (2004). Thoughts on sovereignty. *Policing & Society.* 14 (1), pp. 5-12.

Shoniregun, C. (2003). The future of Internet Security. [online]. [Accessed 2nd May 2005]. Available from World Wide Web: <www.acm.org/ubiquity>

Simpson, G. (2000). Don't take wooden nickels...on eBay? *ZDNet News.* 12 June. [online]. [Accessed 2nd May 2005]. Available from World Wide Web: <http://www.zdnet.com/zdnn/stories/news/0,4586,2586294,00.html>

Skolnick, J. (1975). Why police behave the way they do. *In:* Skolnick, J. Gray, T. eds. *police in America.* Boston: Little Brown.

Smith, R. (1999). Identity-related economic crime. *Trends and Issues in Crime and Criminal Justice.* No.129. [online]. Canberra: Australian Institute of Criminology. [Accessed 22nd May 2000]. Available from World Wide Web: < http://203.221.207.15/publications/tandi/ti129.pdf>

Smith, R. (2000). Controlling Financial Services Fraud. *Trends and Issues in Crime and Criminal Justice.* No.189. Canberra: Australian Institute of

Criminology. [online]. [Accessed 22nd March 2002]. Available from World Wide Web: < http://203.221.207.15/publications/tandi/ti189.pdf>

Smith, R. (2001). Cross-Border Economic Crime: The Agenda for Reform. *Australian Institute of Criminology*. 202. pp. 1-6.

Smith, R. (2005). *Public Sector Fraud and Corruption*. 28 July 2005. [online]. [Accessed 30th July 2008]. Available from World Wide Web:< http://www.aic.gov.au/conferences/other/smith_russell/2005-07-iir.pdf>

Smith, R., Holmes, M. and Kaufmann,P. (1999). Nigerian Advance Fee Fraud. *Australian. Institute of Criminology*.

Smith, R. and Urbas, G.. (2001). *Controlling Fraud on the Internet: A CAPA Perspective*. Canberra: Australian Institute of Criminology

Snyder, J. (1999). Online Auction Fraud: Are the Auction Houses Doing All They Should or Could Stop Online Fraud. *Federal Communications Law Journal*. 52, pp. 453-463.

Serious Organised Crime Agency (2008). *About SOCA*. [online]. [Accessed 22nd October 2008]. Available from World Wide Web:<http://www.soca.gov.uk>

Solms, B. (2001). Corporate Governance and Information Security. *Computer and Security*. 20, pp. 215-218.

Solms, B. (2005). From information security to...business security? *Computers & Security*. 24, pp. 271-273.

Solms,V. (2001). A Multidimensional Discipline. *Computers& Security*. 20 (6), pp. 504-508.

Sommer, P. (2004). The future for the policing of cubercrime. *Computer Fraud and Securit*. 2004. 1, pp. 8-12.

South, N. (1988). *Policing for profit.* London: Sage Publications.

South Shropshire District Council (2003). Information Technology Service Report. No. 02/03. Scrutiny Committee. report dated June 2003.

Standage, T. (1996). Web access in a tangle as censors have their say. *Electronic Telegraph.*[online]. 475: 10 September. [Accessed 20th June 2005]. Available from World Wide Web: <www.telegraph.co.uk:80/et?ac=005287302314 60&rtmo=3HYABxAM &atmo=rrrrrrq&pg=/et96/9/10/ecsing10.html >

Stephens, P. and Induruwa. (2007).Cybercrime Investigation Training and Specialist Education for the European Union. *Digital Forensics and Incident Analysis.* 27/28 August, pp. 28-37

Sterling, G. (2008). *ISP behavioral targeting test to begin in UK tomorrow.* [online]. [Accessed 11th October 2008]. Available from World Wide Web:< http://searchengineland.com/isp-behavorial-targeting-test-to-begin-in-uk-tomorrow-14840>

Stevens, G. (2001). *Enhancing Defense against Social Engineering.* [online]. CA: SANS Institute. [Accessed 10th October 2002].Available from World Wide Web: <http://www.sans.org/infosecFAQ/social/defense_social.htm>

Stucki, C. (2002). How to begin a No liturgical Forensic Investigation in A.J. Marcella & R.S. Greenfield. Eds. *Cyber Forensics: A field manual for collecting, examining and preserving evidence of computer crimes.* New York: Auerbach Publications.

Supreme Prosecutors'Office (2005). *Organization.* [online]. [Accessed 26th July 2005]. Available from World Wide Web:< http://www.spo.go.kr/user.tdf?a=user.pm.PmApp&seq=1115&chunged =02000000&catmenu=050100&c=2001&catmenu=m05_01>

Sutherland, E. (1949). *White Collar Crime*. New York: Dryden Press.

Sutherland, E. (1983). *The Uncut Version*. New Haven: Yale University Press.

Swanson, C., Territo, L. and Taylor, R. (1998). *Police administration: Structure, processes, and behaviour*. (4th ed.). Prentice-Hall, Inc.. New Jersey: Upper Saddle River.

Swanton, B. (1993). Police and Private Security: Possible Directions. *Trends & issues in crime and criminal justice. Australia Institute of Criminology*. [online]. [Accessed 19th May 2006]. Available from World Wide Web:< http://www.aic.gov.au/publications/tandi/ti42.pdf>

Tappan, P. (1947). *Delinquent Girls in Court: A Study of the Wayward Minor Court of New York*. New York: Columbia University Press.

The Korea Herald (2006). Law enforcement dispute. 24 June 2006. [online]. [Accessed 18th September 2006]. Available from World Wide Web:< http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=108&oid=044&aid=0000051649>

The UK's Fraud Prevention Service (2008). [online]. [Accessed 27th November 2008]. Available from World Wide Web: <http://www.cifas.org.uk/>

The US Department of Consumer Affairs (2004). [online].[Accessed 17th March 2006]. Available from World Wide Web: <http://www.dca.gov>

Tips for safe trading on eBay (2006). [online]. [Accessed 25th October 2008]. Available from World Wide Web: <http://www.ebay.com/>

Tiscali (2008). *About Tiscali*. [online]. [Accessed 18th November 2008]. Available from World Wide Web: <http://www.tiscali.co.uk/>

Tombs, S. and Whyte.D. (2001). Reporting corporate crime out of existence. *Criminal Justice Matters.* 43, pp. 22-23.

United States Secret Service (2008). *Electronic Crimes Task Forces and Working Groups.* [online]. [Accessed 9th September 2008]. Available from World Wide Web: <http://www.secretservice.gov/ectf.shtml>

University of New Haven CJ 625 Course CD: Slide 32/ Profile (2005). [online]. [Accessed 3rd September 2005]. Fraudster. Available from World Wide Web:<www.unh.edu/cj625>

Urbas, G.. (2001). *Cybercrime Legislation in Asia-Pacific Region.* Australian Institute of Criminology.

U.S. Code Title 18: 1030. *US CODE collection* [online]. [Accessed 24th September 2008]. Availble from World Wide Web:< http://www4.law.cornell.edu/uscode/18/1030.html>

U.S. Department of Homeland Security (2008). [online]. [Accessed 16th October 2008]. Available from World Wide Web: < http://www.dhs.gov/xprevprot/partnerships/editorial_0206.shtm >

U.S. Securities and Exchange Commission (2008). [online]. [Accessed 29th October 2008]. Available from World Wide Web: <http://www.sec.gov/about/whatwedo.shtml>

Vassou, A. (2008). *New e-crime unit funding 'ridiculos'.* [online]. [Accessed 8th November 2008]. Available from World Wide Web: < http://www.computing.co.uk/computeractive/news/2227487/police-central-crime-unit>

Vincent-Jones, P. (2000). Contractual Governance: Institutional and Organizational Analysis. Oxford Journal of Legal Studies. 20 (3). pp. 317-351.

Wahap, M. (2004). E-commerce and Internet Auction Fraud: The e-Bay community model. *Computer Crime Research Center*. 29 April 2004. [online]. [Accessed 12th January 2008]. Available from World Wide Web:< http://www.crime-research.org/articles/Wahab1/2>

Wakefield, A. (2003). *Selling Security: The private policing of public space*. Devon: Willian Publishing.

Walker, C. and Akdeniz,Y. (1998). The governance of the Internet in Europe with special reference to illegal and harmful content. *Criminal Law Review Special Edition*. 319 (14), PP. 5-18.

Walker, C. and Akdeniz, Y. (2003). Anti-Terrorism laws and data retention: war is over? *Northern Ireland Legal Quarterly*. 50 (2), pp. 159-182.

Walker, C., Wall, D. and Akdeniz, Y. (2000). The Internet, law and socirty. *In:* Y.Akdeniz, C.P. Walker and D.S. Wall .eds. *The Internet, law and Society*. London: Longman. pp. 3-24.

Wall, D., Davies, P. and Jupp, V. (eds). (1997). *Policing Futures*. London: Macmillan.

Wall, D. (1998). Policing and the regulation of cyberspace. *In*: C. Walker. ed. Crime, Criminal Justice and the Internet. *Criminal Law Review* special edition. London: Sweet and Maxwell.

Wall, D. (2000). Policing the Internet: maintaining order and law on the cyber-beat. *In*:Y. Akdeniz, C.P. Walker and D.S. Wall. eds. *The Internet, Law and Society*. London: Longman.

Wall, D. (2001). Maintaining order and law on the Internet. *In*: Wall, D.S. ed. *Crime and the Internet*. London: Routledge.

Wall, D. (2002). Insecurity and the Policing of Cyberspace. *In* : Crawford, A. ed. *Crime and Insecurity.* Cullompton: Willan. pp. 186- 209.

Wall, D. (2005). The Internet as a conduit for criminal activity. *In*: Pattavina, A.. ed. *Information Technology and the criminal justice system.* London: Sage Publication. pp. 77-98.

Wall, D. (2006). Surveillant Internet technologies and the growth in information capitalism: spams and public trust in the information society. *In*: K. Haggerty and R. Ericson eds. *The New Politics of Surveillance and Visibilit.* University of Toronto Press: Oxford University Press.

Wall, D. (2007). Policing cybercrime: situating the public police in networks of security in cyberspace. *Police practice and Research: An International Journal.* 8 (2), pp. 183-205.

Walsh, W. and Donovan, E. (1989). Private security and community policing: Evaluation and comment. *Journal of Criminal Justice.* 17, pp. 187-197.

WARP (2008). *What is a WARP?* [online]. [Accessed 11th August 2008]. Available from World Wide Web:<http://www.warp.gov.uk/index.htm>

Wasik, M. (1991). *Crime and the computer.* New York: Oxford University Press, Inc.

Westpac (2000). *MasterCard securecode and verified by visa: information pack and enrolment form.* Sydney: Westpac Banking Corporation.

White, G. and Pearson,S. (2001). Controlling corporate e-mail, PC use and computer security. *Information Management & Computer Security.* 9 (2), pp. 88-92.

Wilding, E. (2002). Corporate Computer Fraud — Straight from the Secret Investigators. *Computer Fraud & Security.* 7, pp. 13-16.

WIKIPEDIA. (2008). *Enron Scandal.* [online]. [Accessed 29th July 2008]. Available from World Wide Web:< http://en.wikipedia.org/wiki/Enron_scandal>

William, F. and Edwin, J. (1989). Private security and community policing: Evaluation and Comment. *Journal of Criminal Justice.* 17, pp. 187-197.

Williams, J. (2005). Reflections on the private versus public policing of economic crime. *British Journal of Criminology.* 45, pp. 316-339.

Williams, J. (2007). Governability Matters: The private policing of economic crime and the challenge and the challenge of democratic governance. *Policing and Society.* 15 (2), pp. 187-211.

Williams, M. (2000). Virtually Criminal: Discourse, Deviance and Anxiety Within Virtual Communities. *International Review of Law, Computers & Technology.* 14 (1), pp. 95-104.

Wincup, E. (1997). *Waiting for trial: Living and work in a bail hostel.* Unpublished Ph.D thesis. Cardiff University.

WocChat (2008). About WocChat. [online]. [Accessed 18th November 2008]. Available from World Wide Web: <http://www.wocchat.com/>

Wolfe, R. (1992). *Data Management. In:* M.C. Alkin. ed. Encyclopaedia of Educational Research. New York: Macmillian. 1 (6), pp. 293-299.

Working together for a safer London (2008). *Computer Crime Unit.* [online]. [Accessed 22nd November 2008]. Available from World Wide Web: <http://www.met.police.uk/computercrime/>

Woodward, S. (2005). *Online Auction Fraud.* [online]. [Accessed 27th April 2006]. Available from World Wide Web:< http://searchwarp.com/swa6960.htm>

W3C (2005). *Platform for Internet Content Selection.* [online]. [Accessed 19th August 2005]. Available from World Wide Web: <http://www.w3.org/pics/>

Yar, M. (2006). *Cybercrime and Society.* London: Sage.

Zedner, L. (2003). Too much security? *International Journal of Sociology of Law*. 31, pp. 155-184.

Zhang, Bin. and Zhou, Yi. (2008). *Toward a Comprehensive Model in Internet Auction Fraud Detection.* 7-10th January. *In: Hawaii International Conference on System Sciences, proceedings of the 41st Annual.* Waikoloa, Hi. [online]. [Accessed 6th August 2008]. Available from World Wide Web:< http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4438782>

Appendices

Appendix 1: Interview Schedule

Explanation of study and the Interview Process

This research aim is to identify a projected optimum way to resolve tensions in order to determine the correct balance of policing between the private and public sectors and thereby increase both effectiveness and efficiency.

Through this interview, I would like to obtain a professional opinion based on your experience in order to identify the problems of policing internet fraud by the private and public sector of security.

The results of this study will demonstrate which sector of policing is more appropriate for dealing with internet fraud. Based on these results, we can make a policy, which will be more appropriate to control internet fraud.

I will discreetly handle your responses. Interview results will be used only for the research purpose and your identification will not be released. Digitally recorded interviews will be destroyed after completion of transcript. You may request a copy of the interview transcript if you want to check what has been written.

Throughout the interview, you may ask any questions and stop the interview whenever you feel uncomfortable.

Career Background

I would like to ask about your individual career background if you are eligible to provide necessary answer.

1. What is your role (or job title) in this organization?

2. How many years you have been in your private/ public agency or organization?

3. Do you have any special qualification or training in relation to policing internet fraud?

4. What job did you do previously?

5. What are your usual day to day activities?

6. Have you ever been a member of a law enforcement organization?

7. Could you tell me your own experiences with any fraudulent cases?

8. Approximately how many cases have experienced so far?

9. What type of cases have you experienced so far?

10. Generally speaking, what were the outcomes?

Understanding of terminologies in the interview

The next questions are about your understanding of the policing of internet fraud.

Provide respondents with the definition of cybercrime, internet fraud and tensions:

a. *Cybercrime: is a criminal activity committed on the internet. This broad term describes everything from electronic cracking to denial of service attacks that cause electronic commerce sites to lose money (Computer Crime Research Center).*

b. *Internet fraud: is different from traditional fraud in terms of the use of technology and some characteristics shared with true cybercrimes*

(criminal behaviours transformed or mediated by the internet and distinguishing them from more traditional forms of criminal behaviour) such as spam, phishing and pharming (Wall, 2006).

c. *Tensions: major tensions involved in policing internet fraud surround, for example, ownership of cases, competition for jurisdiction, and monopolization of information by each sector. Ownership of cases and competition for jurisdiction can take place within public policing bodies such as local and national police forces. Monopolization of information can take place between private and public policing bodies. The police are always concerned about the leaking of police information before they arrest criminals. While private companies are always concerned about negative publicity and the adverse impact on stock value. Therefore, they do not want to share their critical information although it would make it easier to police internet fraud. This tension can hinder cooperative efforts between private and public policing bodies in the response to internet fraud (Wall, 2006).*

Tensions between the private and public sector of security

I would like to ask you some questions about any tensions that you have experienced or observed while you have worked in policing internet fraud within your sector.

11. What are the three most serious tensions?

12. Why those tensions are produced?

13. How those tensions influence to your work in terms of your working practices for response?

14. Why there tensions still exist while the government has encouraged the use of private policing?

Tensions within the public sector of security (ask only to members of the public sector).

15. What are the three most serious tensions?

16. Why those tensions are produced?

17. How those tensions influence to your work in terms of your working practices for response?

Tensions within the private sector of security (ask only to members of the private sector)

15. What are the three most serious tensions within the private sector of policing internet fraud?

16. Why those tensions are produced?

17. How those tensions influence to your work in terms of your working practices for response?

Resolution of tensions

Here, I would like to ask questions regarding the resolution of tensions.

19. Can government do anything to reduce these tensions?

20. Can your organization do anything to reduce these tensions?

21. Can any other organizations involved?

22. What is the best solution?

Private and public policing models for internet fraud

Now, I would like to ask your opinion about the concept of a plural policing model with regard to internet fraud.

Provide respondents with the concept of plural policing model: more than a bifurcation of policing in terms of multiple policing actors participates to police in the cyberspace.

23. When is it appropriate to involve (a) private rather than public policing mechanisms (b) public rather than private policing mechanisms?

24. How do you work with other sector investigators?
a) with who?
b) what are the formal procedures?
c) what are the informal procedures?
d) does the link work satisfactorily?
e) if not then how could it be improved?

25. How often?

Provide respondents with the meaning of partnership policing: Assume that everyone not just the police owns and is responsible for tackling the problems that undermine community safety? (Nixon, 2002:118).

26. Do you believe that partnership created to help policing internet fraud is either necessary or helpful?

27. What would the ideal partnership look like? Can you give any examples, either currently existing in policing internet fraud (in Korea or elsewhere) or in other sectors that can be transposed.

28. How would you promote the partnership?

29. Do you have any other comments?

Thank you for your co-operation!

Appendix 2: Introductory Letter

Policing Internet Fraud

I am Tae Jin Chung and am currently pursuing doctoral research in the School of Law at the University of Leeds. The aim of this study is to identify the tensions that surround the policing of internet fraud and have negatively influenced the maintenance of the correct balance between the private and public models of policing internet fraud. Primary objectives of the study are as follows:

- Identification of tensions produced by internet fraud.
- Definition and classification of internet fraud because internet fraud does not fit into the existing category of white-collar crime.
- Identification of correct balance of policing internet fraud.
- Examination of governance of internet fraud.
- Examination of relationship existing between and within the public sector.
- Investigation of major faults and lack of the South Korean policing system in respect to its treatment of internet fraud.
- Analysis of factors that promote and resolve tensions.
- Examination of internet fraud control at the local, national and international level.

.

Most of the information for this study will come from face-to-face interviews and I appreciate your willingness to participate in the study. Participation is voluntary and you can end your participation at any time. The information provided by you will be regarded as anonymous and confidential. Your identity or identifying information will not be gathered in this interview. The interview is being undertaken for academic research purposes only in the hope that the information gained will be useful in helping other offenders. Thus, the results will be personally analysed and no government officials will have access to any of the results. A master copy

and transcripts of these interviews will be kept in a safe and secure location and destroyed upon completion of the study.

The purpose of the interview schedule is to guide both the interviewer and the interviewee in the discussions and to make sure that we cover all the important aspects of the incident. Feel free to share more information on any other aspect if you would like to.

Your cooperation will be greatly appreciated.

Appendix 3: Consent Form

I agree to participate in an interview being conducted by Tae Jin Chung under the supervision of Professor David Wall and Clive Walker of the University of Leeds. I have made this decision based on the information I have read in the information letter. As a participant in this study, I realise that I will be asked to answer various questions and I may decline to answer any question, if I so choose.

All information which I provide will be held in confidence and I will not be identified in any way in the thesis or any subsequent publications. I understand that I may withdraw this consent at any time.

I also understand that I may contact Tae Jin Chung if you have any concerns or comments resulting from my involvement in this research.

Participant's Signature: _____

Participant's Name: _____ (*Please print*)

Date: _____