ECONOMIC AND COMPUTER CRIME IN KOREA

*Choi Joon-Weon**

I. INTRODUCTION

The large scale economic crimes (i. e. Lee and Chang's bank bill fraud case, Myongsung case, Youngdong case) and real estate speculation crimes which took place in the early 1980's made the Korean people aware of the seriousness of economic crime. Since the late 1980's, computer crime has rapidly increased as the users of computers and the Internet have increased.

However economic crimes, including computer-based crimes, are very hard for investigating authoritles to gather evidence on, since such crimes are being committed in an organized and intellectualized way, and the evidence can be easily destroyed. Most investigating authorities are not specialized enough to cope effectively with economic crime. Therefore, it is necessary to develop diversified countermeasures, in accordance with each situation facing economic crimes.

II. REPRESENTATIVE TYPES OF ECONOMIC CRIME AND LEGISLATION IN KOREA

A. Tax and Tariff Evasion

The accusation of the taxation office is a prerequisite to indict for the evasion of tax amounting to less than 50 million won (1 USD $1=1300 won). Because the taxation office punishes most evaders with forfeiture instead of accusation, few evaders have been indicted by prosecution.

B. Monopoly and Unfair Trade

Korea established the Act on Monopoly Regulation and Fair Trade in 1980. In line with the introduction of the Act, the Fair Trade Commission was established. This Commission is committed to removing anti-competitive regulations which act as a stumbling block to free business activities, and to alleviate economic concentration. The main crimes against this law are

(i) anti-competitive aspects
(ii) abusive acts
(iii) undue collaborate acts
(iv) unfair trade acts

C. Infrigement of Intellectual Property

Korean people are not yet familiar with the notion that intellectual property (IP) should be protected as a kind of real property. To spearhead Korea's efforts to eradicate violations of IP, the Joint Investigation Team which specifically handles IP infringement cases was organized at every District Public Prosecutors Office in January 1993. Since then, vigorous crackdowns have been carried out on IP infringements such as illegal copying of computer software and video game cartridges, unauthorized sound recordings and videos, and counterfeited footwear. The result of the nationwide crackdown was remarkable. Public awareness of IP has also been enhanced by the continuous reports of mass media, which is, in some sense, the most crucial countermeasure for effective protection of IP.

D. Insolvent Stock Openings

The Securities Transaction Law of Korea provides that any company, which wants to go public in order to join the stock market, should satisfy the requisite financial conditions achieved by the just examination of a certified public

* Public Prosecutor, Seoul District Prosector's Office, Republic of Korea

accountant (CPA).

If an insolvent enterprise disguises its own financial condition through conspiracy with a CPA, and places its stocks on the market, it may cause damage to the many innocent consumers who subscribed to those stocks. That scheme has no purpose but to defraud consumers. In Korea, this kind of fraud is restrained by the Securities Transaction Law. In 1992, the managing staff of 15 bankrupt corporations were indicted and sentenced because of this type of scheme. The financial damage of defrauded stockholders was presumed to exceed seveval billion won.

The manipulation of stock price is also restrained by the Securities Transaction Law. This is an act conducted by conspired trades, which induces the purchase or sale by others in the stock market, misleading consumers to believe that the trade is in a prosperous condition, and to make a wrong decision.

E. Illegal Cheques

The Illegal Cheques Control Act was establish in 1961 to actively cope with illegal cheques in Korea. Under this Act, issuing an illegal cheque intentionally or accidentally, is one of the primary crimes subject to punishment. On the other hand, the offender of this crime is not punished when the holder does not want to charge the offender. Other types of cheque crimes include forged cheques, false reports, violation of reporting obligations by banks etc.

F. Dishonored Promissory Note

In the commercial transactions of Korea, promissory notes are very widely used as means of payment for goods and services. By issuing or falsifying (faulty) bank bills, that will be obviously dishonored, many offenders are frequently defrauding enterprises of goods or service exchanged for those bills, which causes serious damage to the enterprises receiving the faulty bank bills as payment. Every year, thousands of enterprises in Korea have gone bankrupt by fraud through faulty bank bills.

G. Credit Card Crime

In Korea, credit cards are widely used as a means of payment. The fraud patterns of credit card crime occurring in Korea are as follows:

(i) using a stolen or lost credit card against the card holder's will;
(ii) using a forged credit card;
(iii) using credit cards excessively to settle payments;
(iv) defrauding a credit card company by demanding money with a forged credit card voucher.

H. Pyramid (Multi-level) Sale Schemes

Since the late 1980s in Korea as well as Japan, pyramid selling has negatively impacted society because of its monetary and mental damage to large-scale consumers. Previously, we had tackled the pyramid sale scheme by the provision of fraud in the Criminal Code. However we underwent some difficulty in sentencing pyramid sale scheme parficipants as 'fraud' criminals, and in catagorising the consumer participants as victims of fraud.

Thus in June 1992, the Door-to-Door Sales Law was enacted and came into force to regulate multi-level marketing, namely, pyramid sale schemes. The Law of 1992 was effective enough to curb the proliferation of pyramid sale schemes. Apparently since the Law came into effect, pyramid sale schemes have subsidized in Korea.

I. Fraud, Embezzlement, Breach of Trust

In Korea, there are too many cases of fraud, embezzlement or breach of trust being reported to investigation agencies. Almost all of these cases are reported by the victim's, however, few of these cases are indicted; rate of about 12% in fraud cases and about 23% in both embezzlement and breach of trust cases.

For reference, in 1995 the number of the complaints was 471,702 in Korea, while it was 10,596 in Japan. The number of complaints per 100,000 capita in Korea in 124 times as many as that of Japan. The reason why there are such a great number of complaint cases in Korea is explained by:

(i) The trend that a party concerned chooses to settle the dispute by criminal investigation, even in civil cases such as payment default, on account of time consuming civil procedures.

(ii) The practice of investigating agencies to receive complaints indiscriminately without examinating whether they are worth investigating as criminal cases.

Because of such an excessive number of complaint cases, the problems of violating the rights of the complained, and wasting investigation resourses, are getting worse. Therefore, versatile programs to solve this problem are under consideration.

J. Organizational Structure

(1) Prosecutor's Office
(2) Police
(3) Customs, Office of National Tax Administration
(4) Fair Trade Commission
(5) Security (Insurance, Bank) Supervisory Board

K. Money Laundering and Asset Forfeiture

The Republic of Korea declared the Special Act Against Illicit Drug Trafficking in December 1995. Only money laundering related to drug offenses is criminalized. Korea does not have a special act for money laundering control, as exists in the U.S.A. We do not criminalize money laundering itself. Consequently, we can't punish money laundering if it is not related to a drug offense. Only the assets related to the drug offense and special crimes committed by officers can be forfeited.

In January 1993, concerned authorities in the Korean Government jointly started legislating a new statute for asset forfeiture related to drug offenses. In the middle of 1993, a large-scale local tax evasion case was revealed. The officers who were in charge of local tax collection received bribes and falsified the collection data to disguise and prevent the evaded tax from being collected. In that case, the concerned officers revealed that they accummulated in excess of USD $2 million. However the Government was unable to access the money. As a result of that case, in December 1994 the Korean government made a special statute for asset forfeiture related to special crimes committed by officers.

III. MAIN CASES OF ECONOMIC CRIME IN KOREA

A. Lee & Chang's Case

Lee and Chang's bank bill fraud case took place in May 1982. Lee and Chang defrauded 6 business enterprises, suffering from financial difficulties, of promissory notes equivalent to 164 billion won and put them into circulation. This kind of fraud was possible because Lee and Chang took advantage of their position as the relatives of the President of Korea.

The prosecution indicted 30 people, including Lee and Chang, bank personnel and the public officer involved in the case. This was the largest fraud case during the stage of high economic growth in Korea, and shocked the whole nation. The prosecution suffered from many problems such as leakage of investigation secrets, overlapping or unnecessary investigations, which provided a good lesson for the investigation of large scale fraud cases thereafter.

B. Fraud Sales in Department Stores

In January 1989, a consumers association made a complaint against several department stores on the suspicion that they deceived consumers by attaching a false previous price tag to merchandise to make the consumers believe that the stores were selling the goods at a special price. That is, the department stores attached tags written with "400,000→ 300,000", as if they had been selling merchandise at a special price. The items were scheduled to sell at the price of 300,000 won from the beginning.

Though the sales managers of the 6 department stores were indicted for the fraudulent sale, they were given a sentence of not guilty by both the District and Appellate Court for the reason that they did not cause actual financial loss to consumers. After long-term examination, the Supreme Court reversed the sentence of the Appellate Court, and the sales managers were finally given a guilty sentence.

C. A Large Scale Smuggling Case

In April 1995, the Seoul District Prosecutor's Office indicted 18 people (14 arrested) involved in a ring of gold smuggling disguised as a legal enterprise. They smuggled gold by hiding it in hollow silver bars for camouflage. This was the largest seisure of gold (188kg) confisticated in a single smuggling case.

D. Fraudulent Representation of Coporate Financial Statements

In April 1992, Seoul District Prosecutor's Office indicted 24 people, including the CPAs and the directors of the enterprises, who prepared and audited the financial statements that were fraudulently presented and caused investors to believe the misrepresented financial statement. These enterprises were bankrupt before the investigation began. The investors who believed in the false financial statements suffered huge losses that could not be compensated.

E. Tax Embezzlement Case

In September 1994, the officers who were in charge of local tax collection received bribes for falsely processing collectible tax not recieved from the tax-payers. Furthermore, they embezzled the tax received from taxpayers by forging receipts. This embezzlement was possible because the computer system for the collection of local tax, such as acquisition tax and registration tax, was not set up then. The Inchon District Prosecutors Office indicted 135 people (92 arrested) including taxation officers and the legal affairs office personnel.

F. Manipulation of Stock Price

In May 1998, the Seoul Distric Prosecutor's Office indicted 11 persons (7 arrested) including Mr Woo, fund managers and investment company personnel who helped Mr Woo with the manipulation of the price of a spinning business company. The market price of the company's stock doubled in 5 months after the manipulation. The fraud was conducted by the following methods:

(1) Inducing price rise by purchase orders at the highest price possible.
(2) Placing purchase and sales orders

intentionally at the same time, to show designated stock as very popular.
(3) Disclosure of a false information and new technological developments which might cause price rises in related stock.
(4) The institutional investors maintained the purchase trend for a considerable period of time.

G. Credit Card Fraud Case

In May 1996, the Seoul District Prosecutor's Office indicted 130 entertainment businessmen and members of a bogus credit card company (37 arrested) who evaded sales tax by reporting the sales amount as being less than it was. This fraud was conducted by the following methods:

(1) Opening a bogus credit card membership store by forging business registration certification.
(2) Setting up a credit card identification machine and giving ID numbers of the bogus credit card membership store to an entertainment store (ie. bars. nightclubs etc).
(3) The entertainment store then sells sales receipts at 90% of the real sales purchase price to the bogus credit card company, which causes the tax evasion.
(4) The entertainment store gives bribes to bank managers and credit card company personnel so that they don't cancel the credit card contracts.

H. HanBo Case

This was a representative case which took place in January 1997, showing the connection between politics and the economy in Korea. Mr Jung, President of Hanbo Steel Corporation, bribed some politicians who forced the bank to lend money to his company that seemed to have a very slim chance of profitability and growth.

Unable to repay the loan amount of 3.2 trillion won (about USD $ 2.8 billion), the Hanbo company went bankrupt, causing serious damage to the Korean economy. The Korean citizens became angry at politicians and businessmen. The prosecution arrested and indicted 10 people, including Mr Jung and influential politicians of both the ruling and opposition parties, former ministers, and the president of the bank, most of whom were found quilty and sentenced.

IV. PROBLEMS IN CONTROLLING ECONOMIC CRIME

A. Lack of Specialization

To investigate economic crimes effectively, general investigators should have some specialized knowledge concerning the details of foreign trading procedures, bank finance procedures, tax calculation systems, and analyzing techniques of account records or financial documents, etc. Otherwise, they may often be led astray by the explanation of a suspect.

The lack of the above makes general investigators or policemen depend upon their experience alone. In Korea, both public prosecutors and general investigators go through formal training courses that teach specilized areas to help them investigate economic crimes.

B. Difficulties in Proof-Collection

In most economic crimes, just as it is easy for offenders to eliminate or deform proof, it is very difficult for investigators to detect and prove interference with evidence. Furthermore, judges in Korea who are responsible for criminal trials require strict specification of the content and range of evidence in an indicted case.

C. Name Lending (Concealment of Real Name)

In Korea, many offenders who caused their creditors to be confronted with financial damage due to their bankruptcy or economic offenses, frequently restart their business under the names of their wives or relatives quickly after being punished for their wrongdoings. Furthermore, they even promote cheque transactions with the bank under their wife's or relative's name. Of course, any enterprise or individual that fails to settle a bank cheque is questioneed by the bank, and thereafter restricted from issuing bank cheques for a certain period of time by law. However, if that enterprise or individual tries to restart a business by stealth, under the name of another person, it is difficult to detect the real person. This factor plays an important role in the recurrence of economic crime.

D. Difficulty in Initiating Investigation

The high social influence of some offenders makes it difficult to initiate investigation. Some offenders distribute their illegal proceeds to politicians who have influence or power to appoint or dismiss criminal justice officials and protect the offenders from being punished. Therefore, the criminal justice officials often initiate investigating offenders only after having decisive evidence.

V. COMPUTER CRIME IN KOREA

A. Introduction

1. Drastic Increase of Users of Computers and the Internet

From the late 1980's, inexpensive personal computers were distributed and became widely popular in Korea. Further, communication technology development enabled personal computers to be connected to each other through networks. As a result, the average person, as well as experts, has the opportunity to take advantage of computers and to have easy access to information through computers.

2. Definition of Computer Crime

Computer crime is defined as 'a crime in which a computer is used as a tool of crime or is an object of crime, or a crime related to data or knowledge processed through a computer'. In this context, computers include hardware, software and data. (Some scholars use the terminology of 'Information Crimes' to refer collectively to the crimes with respect to information or information processing machinary; devices including computer crime and computer-related crime).

B. Computer Crime Under Korean Law

1. Regulation Necessity

First, computers create new and various tools for crime. Traditional crimes can be committed in new ways, for example there could be: computer-using fraud; disclosure of personal information of individual; infringement on corporate information; diffusion of obscene materials through communication networks; or defamation by means of commercial networks or electronic mail.

Second, computer-based crime can cause disorder in the basic structure of each sector of society, including, but not limited to, economic damage. The more dependent on computers the society is, the more serious the potential for damage. If a financial network, a resident registration network or land integrated information network, which are already in operation, are victimized by crime, its result will not be limited to economic damage.

Third, computer-based crime is very hard to uncover and prove. Because

computers store volumous data into small spaces such as disks, magnetic tapes and stored data, they have many non-accessible, confidential and invisible characters. Especially in the case of computer programs, there is a peculiar program language and expression or technology unique to each programmer. Thus, even computer experts may have difficulty in fully examining the works of other programmers and in finding errors. Therefore, it is necessary to recognize the importance of the prevention and suppression of computer crimes and to develop competent countermeasures.

2. Korean Law

(i) *Criminal Law*

The amendment of the Criminal Law as of December 31, 1996 added special media records, like electronic records, as an object of crime, into the crimes of: rendering null and void symbols of official secrecy (§140); untrue entry in officially authenticated original deeds (§228); utterance of falsified public document (§229); utterance of falsified private documents (§234); violation of secrecy (§316); obstructing another from exercising his/her rights (§234); robbery by hostage (§336). The amendment also created new provisions of: preparation of false public documents (§227); interference with business (§314 II); fraud by use of computer (§347-2); and added special media records into the object of forfeiture.

(ii) *Special Laws Related to Computer Crime*

- Act for Expanding Distribution and Fostering Usage of Computers
- Act for the Protection of Personal Information in Public Agencies
- Military Secret Protection Act
- Basic Electric Communication Act
- Telecommunication Business Act
- Communication Secrecy Protection Act
- Radio Wave Act
- Election for Public Office and Election Malpractice Prevention Act
- Computer Program Protection Act
- Copyright Act, Patent Act, Trademark Act, Design Act, Utility Model Act,
- Unfair Competition Prevention Act

C. Status of Computer Crime

1. Type of Computer Crime

Computer Crime is composed of each or combined types of computer hacking (which is a typical type of computer crime), eavesdropping or wiretapping of computer communications and telephones, disturbance of telephone systems and phone phreaking, cryptanalysis or code-breaking, computer virus etc.

2. Manipulation of Electronic Records etc.

The misconduct of manipulating computer programs or electronic records is being committed by way of manipulating commercial or financial files such as point-of-sale, electronic funds transfer systems or Trojan Horses, Superzapping Trap Doors, Logic Bombs, and Simulations and Modeling, which are expanding worldwide. Such misconduct has been repeated for a long time and is difficult to uncover.

An international counterfeit ring of credit cards was prosecuted at the end of 1995 in Korea. A woman working in the local post office was under arrest for embezzling about 4.6 billion won by means of falsely recording deposit accounts during the 6 years from 1988 to 1994. In July 1997, it was revealed that personnel in the Choheung Bank conspired with a private lender to unduly loan 65 billion won to him. Bank personnel operated a terminal to make a false deposit to the lender's bank account. In exchange, he recieved bribes totalling 85 million won.

In February 1998, a 23 years old person working in an island post office in Cheonnam province operated the post office terminal to make a deposit of about 8 billion won into 58 non-named or name-borrowed accounts, and withdrew 2.7 billion won in Seoul over two days and disappeared.

3. Information Espionage

Information espionage, which includes industrial espionage, means an act of gathering, or transmitting illegally, confidential information regarding the business of other people, companies or the nation.

In Korea, a certain company transmitted the production methods of high-tech industrial equipment to Eastern European countries in July 1988, attracting public attention. In December 1992 an Australian, who was working (as a technology consultant) in a Korean manufacturing company of speaker products, copied the production technology onto floppy diskettes and sold it to the United States.

In addition, 19 people in organizations as industrial spies were arrested by a prosecutor after they stole, and transmitted to a Taiwanese semi-conductor production company, manufacturing process information of circuit charts for 64 Mega D-Ram of domestic semi-conductor production companies such as Samsung and LG.

4. Information Piracy

While information itself is intangible, a media (device) embodying it can be reproduced. Information piracy is an act to make free use of valuable information by reproducing information that has national, social and economic value, without authorization. Its primary target is computer programs, i.e. software. Illegal reproduction using Writable CD ROM, as well as on-line distribution through computer communication, is prevalent in Korea.

Especially, the Internet is becoming popular. The number of users having application programs which enable multi-media production has been rapidly increasing, and the combination of credit card systems and electric commerce has made possible transactions among individuals in cyber-space. Thus, the Internet, is an exemplary electronic market that could be used as a huge duplicator.

5. Infringement of Privacy

As society is going toward an information era, every organization including national and private business companies are creating databases of personal information of people related to its business, such as residents, customers and patients, using information processing machines (devices). Revealing such data to other people could cause a serious violation of that persons rights.

In 1992, a list of employees who engaged in labor disputes was circulated among employers in Pusan, Korea. Those on the list were rejected to be hired. In 1993, 25 police officers who obtained resident references or criminal records without authorization and distributed them to the delivery service company which gave them bribes, were arrested by the Seoul District Prosecutor's Office. In 1994, department store personnel sold a database about large customers to whomever wanted such information. As a result, those customers became the target of a criminal murder organization called *Jizon-pa*, causing a big sensation nationwide.

Despite such troubles, the fact that materials which are printed out from information processing machines (devices)

detailing bank or business transactions are still being used as wrapping paper in street shops near subway stations, shows a serious problem in security for those who are engaged in computer-related work in Korea.

Under the Credit Information Usage and Protection Act, it is prohibited to illegally gather and investigate particular information such as privacy. To engage in a non-licensed credit information business, and to disclose such information other than for the contemplated purpose, is illegal. Further, the Public Institution's Private Information Protection Act prohibits private information files, gathered and kept by public institutions, from being disclosed without authorization, or being taken advantage of for undue purpose. However, from the fact that private study institutes are sending letters or e-mail to each house promoting out-of-school studies, we may conclude that a lot of personal information about subscribers of computer communication networks are leaking out through illegal channels. Therefore, the protection of privacy seems to be a serious problem in Korea.

6. Cyber-Terror

Cyber-terror is an act to make threats to do harm to an other's life, body or property, through an information processing machine (device), or an information communication network, or to intend to obtain money or something of value by means of such threats. There were two such cases in August 1997 in Korea which were uncovered by the prosecutor's office. One case stopped the function of Internet e-mail via "Hitel", a local internet service company, by way of sending 100,000 e-mails to the same person at the same time. Another made the Internet connection (access) network of "Naunuri", a local Internet service company, out of order by way of sending 20 people a huge file of 450 Mb at the same time.

7. Distribution and Exhibition of Obscene Materials

Obscene sites on the Internet, without any restriction to access, is a problem. In Korea, the people who opened an obscene site on the Internet and sold the visual images, which were combined with pictures of an actress' face, were arrested by prosecutors in April 1998.

Under the Korean Communication Secrecy Protection Act, with regard to the investigation of obscene materials, wiretapping with a warrant is allowed for the investigation of certain crimes. However, on-line wiretapping during communication, which is needed to find out the extent of violence or whether it is obscene or not, is not allowed. Such restriction is creating trouble in investigation practices.

D. Actual Situation of Computer Crime Control in Korea

The investigation results of computer crime (have been provided in tables III and IV of Annexure A.)

1. Main Investigation Cases

- Hacking case in Seoul National University computer system ('96.3)
- Hacking case in Pohang Technology College computer system ('96.5)
- Home Banking Fraud case by means of account transfer through hacking ('96.9)
- Fraud case by manipulating computer networks in the Office of Railroads ('97.3)
- Leaking case of Drafting List in the Office of Military Manpower ('97.4)
- Hitel Computer Business interference case by way of an electronic mail bomb ('97.8)
- Large Amount Withdrawal case by manipulating a terminal in a post

office ('98.2)

2. Establishing Investigation Systems

The Information Crime Investigation Center was set up in the Seoul District Prosecutor's Office in April 1995 and the Information Crime Countermeasure Headquarters was newly established in the Central Investigation Department of the Supreme Prosecutor's Office in June 1996. Some prosecutors were designated to be in charge of Information Crime in each of the 20 local branches of the District Prosecutor's Office on December 20, 1996 and an investigation squad (team) was created in each District Prosecutor's Office in Seoul, Taegu, Pusan and Kwangju on April 25, 1997. Thus a nationwide investigation system of Information Crime was set up.

3. Training of Investigation Experts

To date, there are 48 investigators trained through experts training programs and systems management education programs. Further, it is planned to train 35 investigators each year totaling about 150 investigators by the year 2000.

4. Introduction/Operation of New High Technology Equipment

A full-time investigation team for Information Crime was provided with high technology computer equipment for networking, and Internet exclusive lines for setting-up hacker chasing systems. Further, it created its own internet homepage and is providing Internet connection services through a terminal server.

5. Research/Development of Investigation Techniques

Developing an analysis system of evidence in computer crime was commenced in order to gather and analyze Information Crime-related materials. Such a system is also required for general crime-related evidence that is being inputted into electronic records or computer files.

6. Building up Investigation Support Systems

In light of the trend towards a rapid increase of setting up and using various databases, it is planned to promptly build up a database system for investigation of Information Crime and general crime, and to have a Full-time Information Crime Investigation Team to support any self-initiated ("sua sponte") investigation using databases.

E. Measures to Cope with Computer Crime

1. Diversification of Countermeasures

As the crime organizations impacting national, social and economic values are becoming more organized and sophisticated in their ability to use information, the Information Society faces future trouble. However, if we abopt a policy that only channels provided by the country are allowed for international information communications, and all such communications are subject to censorship in advance (as there is a possibility for international communications to damage the nation's interest), such passive countermeasures will also be an obstacle to the arrival of an Information Society

Accordingly, such passive countermeasures should be the last resort to protect out nation and society. It is necessary to prepare various and general countermeasures from legal, technological and/or social aspects, in order to cope with the challenge from adverse influences in the Information Society.

2. Necessity of Unified Enactments

The Korean law to counter computer crimes is primarily the Criminal Code. It

is our nation's basic law and does not facilitate thorough practical research into real cases of computer crimes. Therefore, some main cases of computer crime could be insufficiently covered by regulations or under no regulations at all. Further, each relevant Ministry enacted its own special law for each type of information crime, which resulted in an unreasonable assessment of cases for punishment/ prosecution.

Typical examples are: the lack of provisions punishing illegal spying or illegal monitoring; lack of regulations on attempt and conspiracy to commit an act causing direct threat to public welfare; an unbalance in punishment between the Criminal Code and special laws; jurisdictional disputes between investigation authorities and judgement authorities, and the warrant requirements as a basic principle of the Criminal Procedure Code.

Therefore, it is urgent to enact a general law, a proposed Computer Crime Regulating Act which includes countermeasures against all adverse impacts of computer crime, resolution of jurisdictional disputes and solves the warrant requirement problem under the Criminal Procedure Code when computer crimes are spread out. In addition, the Act would have to deal with new issues in the Information Society, such as electronic commerce, electronic funds transfer, admissibility and authenticity of electronic evidences, and international cooperation.

3. Practical Measures

Since misconduct in communication networks, such as hacking or phone phreaking, is likely to be directly connected to criminal acts, it is urgently required to develop a Realtime Intrusion Detection System, or any immediate chasing system for such misconduct, as well as a firewall system of blocking such misconduct. Further, we need to develop various and multifunctional security technology and systems e.g:

(i) Abuse/misuse controlling technology for System Security Tools in computer communication networks;
(ii) duplication protection technology;
(iii) connection blocking technology;
(iv) multi-user recognition systems; and
(v) standardization of cryptosystems.

4. Inter-Linked Research by Related Institutions

In Korea, a person or an institute interested in computer crimes independently research each field in the absence of an inter-linked system for general research into computer crimes. However, an Information Society can be secured and settled through general research by investigating authorities, research institutes and business enterprises, and joint research from the natural and social sciences.

5. International Joint Research

The contemplated goals can be attained only if computer crime research and the training and education of investigators are accompanied by international cooperation. Investigating authorities in each country will have to gather, examine and compare information about the extent of regulation and its impact, as well as technical information on information crime in other countries. Further, they should have a joint discussion on the crimes committed in each country and make efforts to cope together with new crime techniques. Without such efforts, developing countries in the computer industry might provide a hotbed for computer crime when crime techniques in developed countries are introduced.

VI. CONCLUSION

Economic crimes are social evils which distort the reasonable distribution of wealth, and harm sound economic development. With the development of transportation and the gradual breaking of tariff barriers, all the countries around the world are now advancing to one market in which all countries are subject to the same economic principles. Thus some kinds of economic crime in one country may cause other countries to be faced with economic damage.

From this standpoint, it is necessary to make all efforts to develop investigation techniques and prevention measures which are suitable for individual countries. When a certain economic crime may cause a bad effect on other countries, or has some relationship with other countries, it is necessary for all related countries to carry out cooperative countermeasures. The control of economic crime must be pursued for the mutual interest of all concerned countries.

APPENDIX A

TABLE I

ECONOMIC CRIME OFFENDERS (NUMBER)

Types	Year	1995	1996	1997
Tax Evasion Punishment Act	Reported	1,006	1,619	2,756
	Indicted (Arrested)	301 (61)	552 (105)	803 (79)
Infringement of Intellectual Property	Reported	13,683	15,166	13,460
	Indicted (Arrested)	13,683 (843)	15,166 (1,106)	13,460 (777)
Illegal Cheques	Reported	109,719	96,347	79,829
	Indicted (Arrested)	23,224 (7,099)	25,427 (7,504)	16,681 (4,144)
Credit Card Act	Reported	2,962	3,434	3,565
	Indicted (Arrested)	1,606 (569)	1,729 (576)	1,614 (398)
Fraud	Reported	294,967	364,970	37,526
	Indicted (Arrested)	31,355 (8,897)	44,514 (11,289)	40,946 (10,035)
Embezzlement & Beach of Trust	Reported	47,997	51,324	47.023
	Indicted (Arrested)	10,852 (1,994)	11,815 (1,990)	10,938 (1,652)

TABLE II

PC & INTERNET USERS (NUMBER)

	1994	1995	1996	1997	1998
PC units (thousands)	4,459	5,349	6,231	7,214	9,000 (Estimated)
Internet Users (thousands)	140	370	730	1,090	2,190

TABLE III

INVESTIGATION RECORDS BY YEAR

Year	No. of Case	No. of Investigated Allegations	(Arrested)
1995(Apr. - Dec.)	21	45	(12)
1996	72	146	(24)
1997(Jan.-Aug.)	47	72	(39)
Total	140	263	(75)

TABLE IV

INVESTIGATION RECORDS BY TYPE

Type	Cases	No. of Investigated allegations	(Arrested)
Forgery/alteration of private electronic records etc.	2	4	(2)
Business interference, such as destruction of computer/eletronic records	6	17	(12)
Home banking fraud	3	3	(3)
Mis-issue of ID/ID usage fraud	6	51	(5)
Terminal mis-usage fraud	10	20	(12)
Commercial communication network fraud	5	5	—
Credit card fraud	4	5	(2)
Computer network protection infringement (Hacking)	10	15	(6)
Computer network processing information damage	3	5	—
Mis-usage of private information by public institute	3	10	(6)
Production/distribution of obscene CDs etc.	9	9	(6)
Others	79	118	(21)
Total	140	263	(75)