THE CRIMINAL JUSTICE RESPONSE TO CYBERCRIME: THAILAND

*Santipatn Prommajul**

I. CYBERCRIME IN THAILAND

A. Current Situation

The transformation of global socio-economic structures along with the worldwide proliferation of new information and communication technologies has given rise to more forms of cybercrime, which pose threats not only to the confidentiality, integrity, or availability of computer systems, but also to the security of critical infrastructure. Furthermore, technological innovation gives rise to distinct patterns of criminal innovation: hence, different threats from cybercrime mirror differences across the spectrum of the so-called "digital divide".

At the same time, recent rapid developments in information and communication technology, the growth of transnational transactions and the diversification of economic activities have all contributed to globalization. Together with these changes, which have created a global economic concern, the *modus operandi* of criminal groups has become more sophisticated and the scale of their activities has increased considerably.

This trend has been accelerated by the rapid proliferation of computers and the considerable increase in the number of Internet users. Advances in computer technology and Internet networks have encouraged Internet users to communicate more rapidly. While innocent users gain huge benefits from such global advancement, criminals have used the same technology to extend their activities and influence. Crimes committed using the Internet easily bypass national borders and criminals fully exploit this. At present, private security is threatened by faceless criminals.

The transnational nature of cybercrime hampers its detection and makes investigation and prosecution more difficult because investigation often requires tracing criminal activity and its effects through a variety of Internet service providers or private companies, sometimes across national borders, which may result in difficult questions of jurisdiction and sovereignty. Accordingly, international and regional co-operation would be an effective approach to assist domestic law enforcement to fight cybercrime.

Cyberspace becomes a newly powerful channel for criminals to commit illegal activities such as on-line fraud, phishing, 419 scams, identity theft, defamation, child pornography, on-line gambling and hacking or cracking. The statistics concerning computer-related offences analysed by the High-Tech Crime Center (HTCC), Royal Thai Police, reveals that from 2006 to 2008, 467 cybercrime cases were prosecuted. A large number of the offences were defamation, on-line fraud and child pornography.

In Thailand, cyber criminals have continuously developed new techniques to escape on-line tracing and police investigation. Rapid communication via the Internet allows criminals to network with transnational syndicates in committing crime in a very short space of time. As a result, techniques for collecting evidence and proving the accusations at trial are obstacles for police and prosecutors.

B. Offences Reported to the Royal Thai Police

The cybercrime cases that were reported to the Royal Thai Police after the Computer-Related Crime Act, B.E.2550 came into effect in July 2007 are categorized below.

* Deputy Superintendent, High Tech Crime Center, Royal Thai Police.

1 Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems

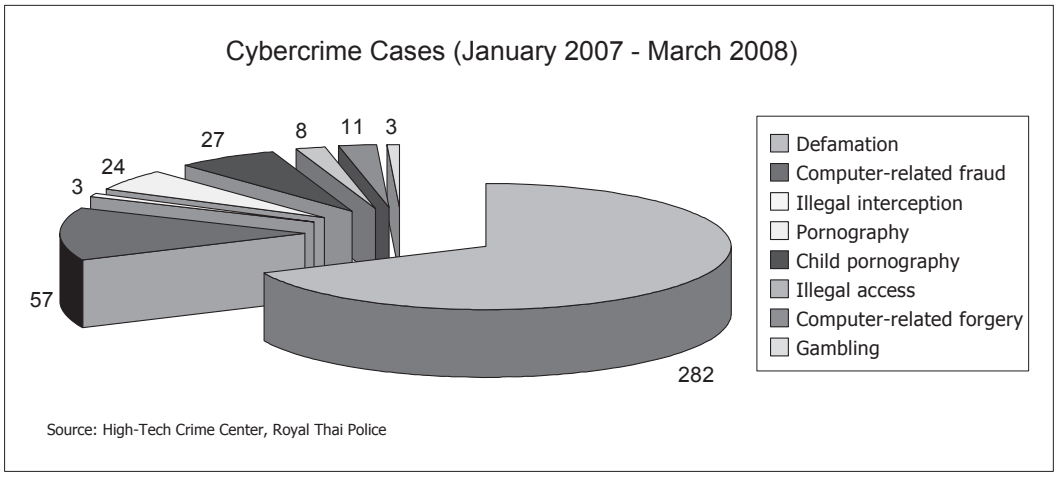
The number of such offences is low but the cost of the damage is high. The criminals employ sophisticated techniques or technology to prevent tracing by the police. Victims of these offences are the customers of Internet banking and online payment services.

2. Computer-Related Forgery and Computer-Related Fraud

These are the most serious category of cybercrime in Thailand. The criminals work mostly in-group and have no sophisticated disguising techniques. At present, there are some criminal groups from West Africa using Internet facilities in Thailand to run scams. The Royal Thai Police has set up a task force to combat these 419 scam groups.

3. Content-Related Offences

Pornographic and child pornographic websites are another category of cybercrime in Thailand. The Royal Thai Police and the Ministry of Culture have set a committee to monitor the content of websites. If they find any websites that contain obscene material or child pornography, the websites must be banned and the operators reported to the Royal Thai Police for prosecution.



II. LEGISLATION

A. Computer-Related Crime Act, B.E.2550 (2007)

The Computer-Related Crime Act, B.E.2550 entered into force in July 2007. The Act sets out the offences against computer-related crime covering hacking, unauthorized access, distributed denial of service, viruses/worms, website defacement, Internet fraud, identity theft, forgery, blackmail, gambling and pornography. It also specifies the authority of competent officials and criminal procedures. The new legislation has become a powerful tool for officers to allege, search, arrest and bring more offenders before court than in the past.

There are two chapters in this Act: Chapter One covers substantive offences; Chapter Two addresses criminal procedure.

Two main offences in Chapter One are enforced. The first are offences against the confidentiality, integrity and availability of computer systems and computer data. The second category is computer-related offences.

Chapter Two enumerates the competent officials who will lay down the procedural provisions for criminal investigations and proceedings.

The Minister of the Information and Communication Technology Ministry shall have charge and control of this Act and shall have the power to issue Ministerial Regulations for the execution of this Act (Section 4).

B. Ministerial Regulations

The Ministerial Regulations that will be issued under this Act are:

1. Ministerial Regulations regarding summonses of seizure or attachment (Section 19) – issued on 30 November 2007.
2. Ministerial Regulations regarding a list of undesirable programmes (Section 21) – not to be issued.
3. Ministerial Regulations regarding a duty of service providers to retain traffic data (Section 26) – enforced on 18 August 2008.
4. Ministerial Regulations regarding qualifications of competent officials (Section 28).
5. Ministerial Regulations regarding the form of the identity card of competent officials (Section 30).
6. Rules on guidelines and procedural methods in arresting, confining, searching, investigating and instituting criminal prosecution against the offender – to be drafted by the working group of the law enforcement agency.

C. Comparison of "Convention on Cybercrime: Council of Europe" and "Computer-Related Crime Act, B.E.2550"

On drafting the Computer-Related Crime Act, B.E.2550, Thailand had studied the Computer Crime Law or Related Law of other countries, including:

- The Electronic Commerce Act 2000 (The Philippines);
- The Computer Crime Act 1997 (Malaysia);
- The Computer Misuse Act (Singapore);
- The Unauthorized Computer Access Law 2000 (Japan);
- The Information Technology Act 2000 (India); and
- The Convention on Cybercrime: Council of Europe.

The following table shows the comparison between the "Convention on Cybercrime: Council of Europe" and the "Computer-Related Crime Act, B.E.2550 (2007)".

Convention on Cybercrime: Council of Europe	**Computer-Related Crime Act, B.E.2550**
Definitions "Computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a programme, performs automatic processing of data.	**Definitions** "Computer system" means a piece of equipment or sets of equipment units, whose function is integrated together, for which sets of instructions and working principles enable it or them to perform the duty of processing data automatically.
"Computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a programme suitable to cause a computer system to perform a function.	"Computer data" means data, statements, or sets of instructions contained in a computer system, the output of which may be processed by a computer system including electronic data, according to the Law of Electronic Transactions.
"Service provider" means: (i) any public or private entity that provides to users of its service the ability to communicate by means of a computer system; and (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service.	"Service provider" shall mean: (1) A person who provides service to the public with respect to access to the Internet or other mutual communication via a computer system, whether on their own behalf, or in the name of, or for the benefit of, another person; (2) A person who provides services with respect to the storage of computer data for the benefit of the other person.

"Traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.	"Computer traffic data" means data related to computer system-based communications showing sources of origin, starting points, destinations, routes, time, dates, volumes, time periods, types of services or others related to that computer system's communications.
Offences **Article 2 – Illegal access** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Section 5** Whoever illegally accesses a computer system that has specific security measures and such security measures are not intended for his use, shall be liable to imprisonment for a term not exceeding six months or to a fine not exceeding ten thousand Baht or to both.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	**Section 8** Whoever illegally makes, by any electronic means, an interception of computer data of another person that is being transmitted in a computer system and such computer data is not for the benefit of the public or is not available for other persons to utilize, shall be liable to imprisonment for a term not exceeding three years or to a fine not exceeding sixty thousand Baht or to both.
Article 4 – Data interference 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Section 9** Whoever illegally acts in a manner that causes damage, impairment, deletion, alteration or addition either in whole or in part of computer data of other person, shall be liable to imprisonment for a term not exceeding five years or to a fine not exceeding one hundred thousand Baht or to both.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	**Section 10** Whoever illegally acts in a manner that causes suspension, deceleration, obstruction or interference of a computer system of another person so that it can not function normally, shall be liable to imprisonment for a term not exceeding five years or to a fine not exceeding one hundred thousand Baht or to both.

Article 6 – Misuse of devices 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: (a) the production, sale, procurement for use, import, distribution or otherwise making available of: (i) a device, including a computer programme, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5; (ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and (b) the possession of an item referred to in paragraphs (a) (i) or (ii) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system. 3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (ii) of this article.	**Section 13** Whoever sells or disseminates sets of instructions developed as a tool used in committing an offence under Section 5, Section 6, Section 7, Section 8, Section 9, Section 10 and Section 11 shall be liable to imprisonment for a term not exceeding one year or to a fine not exceeding twenty thousand Baht or to both.
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Section 14** Whoever commits any offence of the following acts shall be liable to imprisonment for not more than five years or a fine of not more than one hundred thousand baht or both: (1) that involves import to a computer system of forged computer data, either in whole or in part, or false computer data, in a manner that is likely to cause damage to that third party or the public; (2) that involves import to a computer system of false computer data in a manner that is likely to damage the country's security or cause a public panic;

Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: (a) any input, alteration, deletion or suppression of computer data, (b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	(3) that involves import to a computer system of any computer data related with an offence against the Kingdom's security under the Criminal Code; (4) that involves import to a computer system of any computer data of a pornographic nature that is publicly accessible; (5) that involves the dissemination or forwarding of computer data already known to be computer data under (1) (2) (3) or (4).
Article 11 – Attempt and aiding or abetting 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3. Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	The attempt, abetments or aiding is not stipulated in this Act because the Criminal Code can be applied. **Section 15** Any service provider intentionally supporting or consenting to an offence under Section 14 within a computer system under their control shall be subject to the same penalty as that imposed upon a person committing an offence under Section 14.
Article 14 – Scope of procedural provisions 1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2. Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: (a) the criminal offences established in accordance with Articles 2 through 11 of this Convention; (b) other criminal offences committed by means of a computer system; and (c) the collection of evidence in electronic form of a criminal offence. 3. (a) Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of	**Section 18** Within the power of Section 19 and for the benefit of an investigation, if there is reasonable cause to believe that there is the perpetration of an offence under this Act, then a relevant competent official shall have any of the following authorities only as necessary to identify a person who has committed an offence in order to: (1) Issue an inquiry letter to any person related to the commission of an offence under this Act or summon them to give statements, forward written explanations or any other documents, data or evidence in an understandable form; (2) Call for computer traffic data related to communications from a service user via a computer system or from other relevant persons; (3) Instruct a service provider to deliver to a relevant competent official service users-related data that must be stored under Section 26 or that is in the possession or under the control of a service provider; (4) Copy computer data, computer traffic data from a

offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. (b) Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: (i) is being operated for the benefit of a closed group of users; and (ii) does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.	computer system, in which there is a reasonable cause to believe that offences under this Act have been committed if that computer is not yet in the possession of the competent official; (5) Instruct a person who possesses or controls computer data or computer data storage equipment to deliver to the relevant competent official the computer data or the equipment pieces; (6) Inspect or access a computer system, computer data, computer traffic data or computer data storage equipment belonging to any person that is evidence of, or may be used as evidence related to, the commission of an offence or used in identifying a person who has committed an offence, and instruct that person to send the relevant computer data to all necessary extent as well; (7) Decode any person's computer data or instruct any person related to the encryption of computer data to decode the computer data or cooperate with a relevant competent official in such decoding; (8) Seize or attach the suspect computer system for the purpose of obtaining details of an offence and the person who has committed an offence under this Act. **Section 19** The power of authority of the relevant competent official under Section 18 (4), (5), (6), (7) and (8), is given when that competent official files a petition to a court with jurisdiction for an instruction to allow the relevant competent official to take action. However, the petition must identify a reasonable ground to believe that the offender is committing or going to commit an offence under the Act as well as the reason of requesting the authority, including the characteristics of the alleged offence, a description of the equipment used to commit the alleged offensive action and details of the offender, as much as this can be identified. The court should adjudicate urgently such aforementioned petition. When the court approves permission, and before taking any action according to the court's instruction, the relevant competent official shall submit a copy of the reasonable ground memorandum to show that an authorization under Section 18 (4), (5), (6), (7) and (8), must be employed against the owner or possessor of the computer system, as evidence thereof. If there is no owner of such computer thereby, the relevant competent official should submit a copy of said memorandum as soon as possible. In order to take action under Section 18 (4), (5), (6),

	(7) and (8), the senior officer of the relevant competent official shall submit a copy of the memorandum about the description and rationale of the operation to a court with jurisdiction within forty eight (48) hours after the action has been taken as evidence thereof. When copying computer data under Section 18 (4), and given that it may be done only when there is a reasonable ground to believe that there is an offence against the Act, such action must not excessively interfere or obstruct the business operation of the computer data's owner or possessor. Regarding seizure or attachment under Section 18 (8), a relevant competent official must issue a letter of seizure or attachment to the person who owns or possesses that computer system as evidence. This is provided, however, that the seizure or attachment shall not last longer than thirty days. If seizure or attachment requires a longer time period, a petition shall be filed at a court with jurisdiction for the extension of the seizure or attachment time period. The court may allow only one or several time extensions, however altogether for no longer than sixty days. When that seizure or attachment is no longer necessary, or upon its expiry date, the competent official must immediately return the computer system that was seized or withdraw the attachment. The letter of seizure or attachment under paragraph one shall be in accordance with a Ministerial Regulations.
Article 17 – Expedited preservation and partial disclosure of traffic data 1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: (a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and (b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Section 26** A service provider must store computer traffic data for at least ninety days from the date on which the data is input into a computer system. However, if necessary, a relevant competent official may instruct a service provider to store data for a period of longer than ninety days but not exceeding one year on a special case by case basis or on a temporary basis. The service provider must keep the necessary information of the service user in order to be able to identify the service user from the beginning of the service provision, and such information must be kept for a further period not exceeding ninety days after the service agreement has been terminated. The types of service provider to whom the provisions under paragraph one shall apply and the timing of this application shall be established by a Minister and published in the Government Gazette. A service provider who fails to comply with this Section, shall be liable to a fine not exceeding five hundred thousand Baht.

Article 22 – Jurisdiction	**Section 17**
1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: (a) in its territory; or (b) on board a ship flying the flag of that Party; or (c) on board an aircraft registered under the laws of that Party; or (d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	Whoever commits an offence pursuant to this Act outside the Kingdom, whether (1) the offender be a Thai person, and there be a request for punishment by the Government of the country where the offence has occurred or by the injured person ; or (2) the offender be an alien, and the Royal Thai Government or a Thai person be the injured person, and there be a request for punishment by the injured person, shall be punished in the Kingdom.

III. MEASURES

A. Measures to Combat Cybercrime

1. Domestic Approach

(i) Prevention

- Promote public understanding of the cybercrime situation and teach the public how to protect itself from cyber criminals.
- Enlist the co-operation of the private sector and the public in reporting illegal websites, online fraud, etc. and in the investigation process.
- Force the regulations enactment and enforce the Computer-Related Crime Act.

(ii) Suppression

- Provide investigation knowledge for local police, so that they can rapidly respond to cybercrime cases.
- Improve the investigation techniques and the skills of cybercrime investigators to specialist standard and the level accepted by the international law enforcement agencies.

2. International Approach
   - Participate in international activities, meetings, training, etc. to share intelligence and experience.
   - Co-operate with international law enforcement agencies and assist in solving cybercrime cases upon request. At this moment, the Royal Thai Police has assigned officers from High-Tech Crime Center to be contacts for ASEAN 24/7 High-Tech Crime, Cybercrime Technology Information Network System (CTINS) and other law enforcement agencies.

B. Our Vision in Combating Cybercrime

1. Domestic Approach
   - Secure the co-operation of the private sector and public to provide information, advance technology and funding for combating cybercrime.
   - Train police to achieve excellent capability in cybercrime investigation techniques.
   - Develop a knowledge-base and a case management system and provide it to the public and other law enforcement agencies.

2. International Approach
   - Develop co-operation among international law enforcement agencies by supporting international workshops and meetings.
   - Assign a contact person for information exchange among international law enforcement agencies.

IV. ACTUAL CASE

A. 419 Scam

1. Situation

In June 2008, a Thai bank complained to the High-Tech Crime Center, Royal Thai Police, that its logo and a fake name given as its bank manager were used in spam mail. Some customers requested the bank to clarify that mail.

Spam mail informed the receiver that he or she had won US$1,000,000 and the winner must transfer the money for tax payment and service charges including a transfer fee of about US$10,000 to receive this fund. The bank's logo and the fake name of its bank manager were attached in the mail.

2. Investigation

The Royal Thai Police set up a task force to investigate the case led by the Central Investigation Bureau together with the Immigration Bureau, Foreign Affairs Division and High-Tech Crime Center. On investigating, the task force found following facts:

- Three e-mail addresses were used in sending the spam mail;
- The bank manager's name was fake;
- A bank account was opened to receive the transferred money. The owner was a Thai woman.
- The IP address of every spam mail came from the same place. With co-operation from the Internet service provider company, the team found the location at an Internet café in Bangkok.

A surveillance team investigated the owner of the Internet café. He informed them that an African group used his Internet café daily. The team reported that about 30 African people stayed in accommodation around that area, some in the same building as the Internet café.

Covert officers were set to work as staff of the café and manually logged the usage of computers there. The syndicate only used computers to send e-mail, not to surf the Internet.

A court order was issued to do a real time interception of traffic and content data from the Internet café. Log recorders and analysis devices were set at the gateway of the Internet café network.

On viewing the traffic data, the task force compared log records including contents and manual logs to identify the activity of the syndicate. Traffic data proved that syndicates used the café for sending spam mail and committing fraud.

3. Operation

The task force submitted a warrant of arrest for 13 suspects including one Thai woman. The court issued the warrants on 24 July 2008 and the operation was set.

About 200 police officers (uniformed and undercover) were deployed to three target areas. Eighteen suspects (17 Ghanaians and 1 Thai) were arrested.

4. Key to Success

The success of this operation was due to co-operation among the law enforcement agencies and private companies.

The co-operation of police officers from different units caused this operation to succeed. Their intention in combating cybercrime led them to share all information and to learn from each other.

SRAN Security Center provided the log recorders and traffic data analysis at the Internet café free of charge. It caused the task force to prove and present all evidence to the court for the issuing of the warrants of arrest.

Co-operation from Western Union (providing transaction data from the victims to the suspects) led the task force to indentify the location of the group leader.