GROUP 2

CHALLENGES AND BEST PRACTICES IN CYBERCRIME INVESTIGATION

Chairperson	Mr. Elcio Ricardo de Carvalho	(Brazil)
Co-Chairperson	Mr. Mirza Abdullahel Baqui	(Bangladesh)
Rapporteur	Ms. Rita Chun-fa Lam	(Hong Kong)
Co-Rapporteur	Mr. Yoichi Omura	(Japan)
Members	Mr. Hiroyuki Ito	(Japan)
	Mr. Takuya Matsunaga	(Japan)
	Mr. Gilbert Caasi Sosa	(Philippines)
	Mr. Napoleon Bonaparte	(Indonesia)
	Mr. Jesus Rodriguez Almeida	(Mexico)
Visiting Expert	Professor Yunsik Jang	(Korea)
Advisers	Professor Shintaro Naito	(UNAFEI)
	Professor Ryuji Tatsuya	(UNAFEI)
	Professor Tetsuya Sugano	(UNAFEI)
	Professor Koji Yamada	(UNAFEI)
	Professor Haruhiko Higuchi	(UNAFEI)

I. INTRODUCTION

Group 2 started its discussion on 16 September 2008. The group elected, by consensus, Mr. Carvalho as Chairperson, Mr. Mirza Co-chairperson, Ms. Lam as Rapporteur, and Mr. Omura as Co-rapporteur. The Group, following its assignment to discuss "Challenges and Best Practices in Cybercrime Investigation", agreed to conduct the proceedings in accordance with the following agenda:

1. Initial Information Gathering and Undercover Online Investigations;
2. Tracing and Identifying Criminals;
3. Digital Forensic Analysis of Evidence;
4. Cross-Border Investigative Abilities;
5. International Co-operation in Cybercrime Investigations

For the purpose of this document, the term "participating countries" refers only to the countries represented in this group.

II. SUMMARY OF THE DISCUSSIONS

A. Initial Information Gathering and Undercover Online Investigations

As for initial information gathering, all participating countries' law enforcement agencies can directly receive reports about cybercrime from the victims or from third parties, the methods varying from reporting directly to the police stations to web pages and email addresses dedicated to receive the reports through the Internet. Japan, Mexico and the Philippines informed the group that they also conduct active cyber patrols in search of criminal activities on the Internet. In addition, Japan mentioned that the police also receive reports from the Internet Hotline Center.

The group agreed to recommend that the methods of Initial Information Gathering should be improved by:

- Educating the population about cybercrime, aiming to increase the number of reports and to improve the quality of the information contained in those reports;
- Improving the channels of communication with the victims, with training on cybercrime for police officers who receive reports and developing tools to better collect, classify and correlate the reports received from web pages and email addresses; and
- Increasing cyber patrolling activities, being more proactive in monitoring Internet sites in search of illegal activities, observing the legal limitations in each country.

Regarding undercover online investigations, there was a great debate about its definition, methods, limitations and objectives. For the purpose of this group discussion, the concept of undercover online investigation was agreed to be:

"A police officer disguising his or her own identity online or using an assumed identity online for the purpose of gaining the trust of an individual or organization to obtain information and/or evidence, subject to the domestic laws and guidelines of the implementing country and law enforcement agency."

Other aspects which may be included under the concept of implementing undercover online investigation and which were discussed by the group *but were not agreed upon*, given the particularities of each country, were:

- Permission to change legal identity;
- Clearance to pretend to commit a crime, if necessary, when conducting the investigation;
- Ability to use the information obtained while undercover as evidence or just as intelligence information;
- Using an undercover identity to provide to a suspect the opportunity to commit a crime and charge this person for this action;
- In what type of crimes the investigators can use undercover investigation;
- The definition of reasonable grounds for conducting undercover investigation.

The participant from the Philippines asked to make it clear that his country does not allow undercover investigators to commit a crime or to give someone else an incentive to commit a crime.

Having in mind the aforementioned aspects, leaving them open for discussion within each country, respecting their particular traditions and legislation, and considering only the concept the group agreed upon, it is recommended that the participating countries try to improve their undercover online investigation capabilities, which is a very important investigative tool.

B. Tracing and Identifying Criminals

The group reached a consensus that the success of the investigation regarding the identification of the criminal relies upon the availability and the quality of the information provided by Internet service providers and telecommunication providers to law enforcement agencies. Such information can be traffic data, content data and subscriber information. Together they may allow the identification of the individual that performed a given action in a certain time and date. Then the group proceeded to discuss the current situation of the following subtopics in each country:

1. The Relationship between Law Enforcement and ISPs

Data and information held by ISPs and telecoms companies are very important for the investigation of cybercrime. Law enforcement agencies in all the participating countries have contacts with ISPs and telecoms companies in the form of regular meetings and/or inquiries about individual cases.

But no participating countries have laws to force ISPs and telecoms companies to keep data for a certain period of time. The situation varies from agreements, relying solely on the goodwill of the providers to keep the relevant data, to no agreement or regulation whatsoever. Therefore, there is a considerable risk that ISPs' data may no longer be available when investigators request it for an investigation.

2. The Relationship between Law Enforcement and Citizens

Information from citizens is also very important for investigation of cybercrimes. In particular, information from victims can be of high importance at trial.

On the other hand, there are some kinds of cybercrimes, like child pornography, in which we cannot expect information from a victim. In such cases, information provided by citizens using the Internet is very valuable in the early stages of an investigation.

3. The Anonymity of Public Access

The anonymous use of public access points, for example Internet cafés and open wireless networks, is a very serious issue, considering that a crime committed using those infrastructures may be impossible

to trace back to the perpetrator. Our countries do not have effective countermeasures to deal with this issue. Some countries mentioned that video surveillance systems are in use, but it was agreed that the identification of the criminal from such images is still a problem.

As a result of the discussion, we concluded that law enforcement agencies in our countries should have:

- New laws enforcing data retention by ISPs and telecoms providers for an appropriate period of time and restricting the disclosure of this information only to law enforcement agencies conducting an investigation;
- Measures for improvement of the relationship between law enforcement and citizens, for example, education of the population about cybercrime, what is criminalized and how serious cybercrime's influence is;
- Measures to regulate the operation of public access points, forcing administrators of those services to confirm the identification of users.

C. Digital Forensic Analysis of Evidence

The group discussed the following subtopics:

1. Specialized Units for Conducting Cybercrime Investigation/Forensics

All the participating countries either already have a specialized unit or have an organization able to conduct cybercrime investigations. It is desirable that in addition to having specialized units, the countries develop official guidelines for the work of those agencies, especially regarding the collection, preservation, examination and presentation of digital evidence, in order to have standards and procedures compatible with the best practices recognized internationally.

The group agreed that it is of the utmost importance that the countries devote resources to the capacity-building of those specialized units, with investment in personnel, equipment and training.

Considering the functioning of the specialized units, it is also advisable to follow the recommendations contained in the International Review of Criminal Policy (No's 43 and 44): United Nations Manual on the Prevention and Control of Computer-related Crime (1994), articles 198 to 209, in regard to:

1. Administrative and Organizational Security
2. Personnel Security
3. Physical Security
4. Communications-electronic security
5. Hardware and Software Security
6. Operations Security
7. Contingency Planning

2. Availability of Cybercrime Units for other Agencies/Law Enforcement Bodies

In all participating countries the cybercrime units are available to provide assistance or technical advice to other units or organizations within the country. In most countries, this assistance is provided on a case-by-case basis, without an established formal procedure or supervising relationship.

As a recommendation, the group considers that the co-operation among the cybercrime units within a specific country and between them and other governmental agencies should be co-ordinated in such a way so that a main organization could provide assistance to smaller units around the country regarding more advanced or technically demanding investigations. These measures can rationalize the expenditure of setting up forensic laboratories, which is especially important for developing countries.

3. Training

All the participant countries have some kind of training for cybercrime investigations. But the type of the training varies; some countries have only sent officers abroad to receive training, while others have specialized institutions to provide regular training on the subject. Also, most of the countries have received training from private companies. It is recommended to establish a formal and regular technical training course for dealing with digital evidence, at least on the subject of identification, collection, preservation and

presentation of digital evidence.

It is also advisable that the training not be restricted to those who will specialize in cybercrime investigation and forensics. The officers responsible for receiving the first information about the crime or making contact with the victim must also be trained in the basics of cybercrime concepts, in order to properly start the investigation.

As another recommendation, it is important that training activities be included in international co-operation programmes and efforts, improving the sharing of experience and knowledge of cybercrime among the countries.

4. Mechanisms to Exchange Information on Cybercrime

Regarding the mechanisms to exchange information on cybercrime between law enforcement and the private sector and the existence of a specialized organization to facilitate this exchange, the majority of participating countries have those kinds of mechanisms, usually in an informal way. Only a minority have specialized units to assist this exchange.

Although a dedicated organization to facilitate the exchange of information may not be required, the improvement of the relationship between law enforcement agencies and the private sector is critical to combating cybercrime. Regular meetings with the sectors involved, such as financial institutions and ISPs, should be formally established.

5. CERTs

Almost all the participating countries have a Computer Emergency Team. The nature of those CERTs varies; there are completely private CERTs, governmental CERTs and others of a mixed nature.

The group reached a consensus that the existence of a properly equipped CERT is essential for promptly responding to cyber threats, especially attacks on critical infrastructures. It is advisable that government and private sector co-operate closely in the operation of such teams, in order to avoid duplicity of work and difficulties in the communication necessary to cope with the emergency events.

D. Cross-Border Investigative Abilities

The group discussed the following subtopics:

1. Search and Seizure of Computers at the Request of Another Country

The group agreed that this is a very sensitive issue that has deep implications for national sovereignty. In the majority of the participating countries such search and seizure is possible, with some strict conditions, such as:

- Explicit government authorization;
- Criminalization of the act under the requested country's law;
- Enough evidence to open a case under the requested country's law;
- Principle of reciprocity;
- Principle of jurisdiction;
- Use of diplomatic channels for the request, such as Mutual Legal Assistance.

2. Preservation of Computer Data Evidence at the Request of Another Country

Regarding the existence of a preservation law or rule that allows for preservation of computer data evidence at the request of another country, in the majority of participating countries there is no provision for such cases. Nevertheless, in most countries it is possible to informally ask the ISP or telecoms provider in the requested country to preserve the data. The actual delivery of this data to the requesting country may be subject to the restrictions enumerated in the above subtopic.

3. Real-time collecting of Traffic Data at the Request of Another Country

Most of the countries in the group, except for Mexico and Indonesia, do not have the legal capability to engage in real-time collection of traffic data at the request of another country. Japanese investigative agencies do have such authority but have not yet exercised it in response to a request from another country. The implementation of such real-time collection is subject to the same legal requirements listed in the

discussion entitled "Search and seizure of computers at the request of another country", above.

4. Disclosure of Header Information to Another Country

The ability to quickly disclose header information to enable the other country to trace the origin of a communication is available to a majority of the concerned countries, subject to certain legal conditions and on a case-by-case basis.

5. Provision of Secured Electronic Data from ISPs to Another Country

The ability to secure electronic data, such as subscriber information and traffic data, from ISPs or telecoms providers, and then provide it to another country, is possible in the majority of the concerned countries subject to the same legal requirements listed in the discussion of subtopic D.1 above. The provision of content data is subject to even more restrictions, due to privacy issues.

In order to come up with a workable solution to address cross-border investigation, the following are suggested:

- Requests for evidence be made under existing MLAT, MLA and/or Letter Rogatory process;
- The use of 24/7 points of contact (G8, Interpol, Regional organization);
- The utilization of locally based foreign embassies. Most countries have embassies in foreign countries. The representatives of concerned law enforcement agencies who are stationed at the relevant country's embassy must liaise with the host country;
- Use of foreign law enforcement contacts maintained by the cybercrime unit and established through personal contacts and/or workshops, training or seminars.

E. International Co-operation in Cybercrime Investigations

The group agreed to consider the topic of international co-operation in cybercrime investigations as divisible in three dimensions:

1. Legal

2. Operational (Organizational)

3. Technical

The idea is to keep problems with difficult solutions from interfering in the discussion of solutions to problems in other dimensions. For example, the problem of search and seizure of computers in the request of a foreign country is a sensitive issue in the legal dimension. But it should not prevent discussions about how to turn this request into a real operation and how to technically conduct it. Therefore, if at some point a solution for the legal problem is found, a method for implementing the action may have already been established between the parties.

As an example of an idea to improve the operational dimension, the group discussed the establishment of a three-way handshaking protocol for the reception of collaboration requests. The motivation for this is that frequently the requests remain unanswered for some acceptable reason, but the requesting party is never notified of this reason, or some technical difficulty prevents the request from being fulfilled but the parties do not talk about how to overcome it.

A proposal for such a communication protocol, to be run on top of an Integrated Cybercrime Network,[1] would be as follows:

Step 1. The requesting country files a request containing at least the following information:

- Detailed description of the offence being investigated;
- Unit or person responsible for the request issued, to whom a reply should be directed;
- Detailed description of the requested actions.

[1] The definition and implementation details of such Integrated Cybercrime Networks are outside the scope of this document.

Step 2. The requested country, within a previously accorded timeframe, sends a reply containing at least the following information:

- Unit or person responsible for dealing with the request;
- Whether the request is to be answered promptly or demands further analysis;
- Description of legal/operational/technical issues that may arise from the request.

Step 3. The requesting country, within a previously accorded timeframe, sends back a notice acknowledging receipt of the requested country's reply.

As a result of this system, both parties would know that the other end received the message and what issues were involved, allowing for a more efficient and dynamic control of the requests and for a joint effort in overcoming possible problems.

As a suggestion to deal with technical problems, countries could discuss ways to quickly overcome the technical difficulties that arise when there is a difference between the technical capabilities of the countries. For instance, the requested country could generate images of the seized digital evidence and make it available over a secure network for the requesting country.

Another aspect of international co-operation that can happen immediately, in parallel with other legal and operational measures, is the help that developed countries can give to the capacity building of developing countries, creating a baseline for cybercrime investigation units. It would not only help the latter to deal with their internal investigations, but it would also provide for a smoother performance of practical international collaboration when receiving and executing requests from foreign countries.

As general recommendations regarding international co-operation, the group agreed that:

- All countries should implement a 24/7 hi-tech point of contact network (operational dimension);
- All countries should share cybercrime information through Interpol and other regional organizations, like ASEANAPOL (operational dimension);
- Countries should engage in international co-operation on cybercrime investigation (legal, operational and technical dimensions);
- Countries should have a legal framework that allows engagement and joint cybercrime investigation with other countries (legal dimension);
- Countries should not make direct contact to other countries' private sector entities or ISPs, but instead use the established diplomatic/international co-operation channels. But it is acceptable to contact the local office of global ISPs, when available (legal and operational dimensions).

III. CONCLUSION

Although the main theme of this group workshop was "Challenges and Best Practices in Cybercrime Investigation", it is not always possible to discuss such issues without venturing into the debate about legal frameworks, given that most procedural tools designed to overcome the challenges and some implementations of best practices need to be supported by proper legislation within each country.

Nevertheless, the group worked to identify common issues and strived to reach consensus on the recommendations towards the improvement of the fight against the threat of cybercrime. Whenever possible, those recommendations were included in the main body of this document, immediately following the discussion of the respective subject for the sake of clarity and conciseness.