GROUP 2
MEASURES FOR EFFECTIVE INVESTIGATION, PROSECUTION AND ADJUDICATION OF CYBERCRIME CASES

Chairperson	Mr. CHAY Chandaravan	(Cambodia)
Co-Chairperson	Mr. Faatasi PULEIATA	(Samoa)
Rapporteur	Ms. Karla Torres CABEL	(Philippines)
Co-Rapporteur	Ms. URAOKA Naoko	(Japan)
Members	Ms. LAI Thi Thu Ha	(Viet Nam)
	Ms. Judith GOMEZ	(Panama)
	Mr. Thongchai ITTHINITIKUL	(Thailand)
	Mr. Safarbek NURALIEV	(Tajikistan)
	Mr. Arjun Prasad KOIRALA	(Nepal)
	Mr. HOSHI Takashi	(Japan)
Visiting Expert	Dr. Kim-Kwang Raymond Choo	(Australia)
Advisers	Prof. MORIYA Kazukhio	(UNAFEI)
	Prof. YUKAWA Tsuyoshi	(UNAFEI)

I. INTRODUCTION

Group 2 started its discussion on 25 May 2015. On that same date, the group elected Mr. Chay as its chairperson, Mr. Puleiata as its co-chairperson, Ms. Cabel as its rapporteur and Ms. Uraoka as its co-rapporteur. Group 2 conducted its discussion on the topic "Measures for Effective Investigation, Prosecution and Adjudication of Cybercrime Cases" by considering the following: 1) the current practices of the members' respective countries; 2) the challenges to overcome; 3) approaches in improving said current practices and 4) measures that can be implemented to overcome the challenges and improve the current situation.

II. SUMMARY OF DISCUSSIONS

A. Effective Measures for Generating Cybercrime Leads

1. Strengthening Cyberpatrol Systems by Investigative Agencies and Facilitating the Reporting System from the Private Sector and the Public.

During the group discussion, it was observed that a majority of the participants do not have existing cyberpatrol systems in their respective countries. Said countries merely acquire cybercrime-related complaints and information through such reporting systems. However, that same group agreed that the reporting system may not be able to fully monitor and address the prevalence of cybercrime and that a more pro-active stance must be undertaken by the government, with the invaluable assistance of private stakeholders.

Meanwhile, the participants whose respective countries have cyberpatrol systems in place aver that there appears to be reluctance on the part of the private sector to voluntarily submit data records to investigators. This is because doing so may compromise their customers' right to privacy, which would, in turn, affect their businesses. In such cases, a request or preservation order from authorities is required for the release of the information.

Either way, all participants agreed that technical skills and knowhow on the part of the investigators who receive the reports or conduct cyberpatrolling is crucial in cybercrime cases.

After much discussion, the group agreed on the following measures:

- There must be an existing law that requires service providers to furnish necessary information to authorities. Likewise, there must be regulations and measures to protect the right to privacy of the people.

- The public sector, i.e. police and prosecutors which are responsible for cyberpatrolling and/or receiving reports on cybercrime-related incidents, should be properly trained. The private sector should be acquainted with basic cybercrime knowledge, and public awareness on cybercrime should be encouraged.

- A more pro-active stance against cybercrime should be made by the government so that it will not heavily depend on reporting systems; volunteerism should be encouraged.

- Police agencies should be equipped with efficient high-tech tools.

- Cooperation between the public and private sectors should be strengthened.

- Existence of a primary agency (government body) that will monitor cybercrime cases is necessary.

- International cooperation is crucial in strengthening cyberpatrolling, reporting and investigating agencies.

B. Effective Measures for Tracing and Identifying Criminals and Preserving and Collecting Evidence

1. Tracing and Identifying Criminals and Preserving and Collecting Evidence.

A majority of the participants stated that IP addresses are necessary in cybercrime investigations and that they serve as leads in identifying the perpetrator. Some use logs stored in SIM cards and mobile phones in tracing cyber-criminals. On the other hand, tracing cybercriminals using SIM cards becomes a challenge when the cards are not registered.

The group opined that although IP addresses are available, the real challenge is determining the real perpetrator who used the computer associated with a specific IP address. This is because perpetrators currently would exploit proxy servers, TOR onion routers and applications to immediately erase access logs in advancing their malicious intent. Thus, there is a need for authorities to seek other sources of information, which would aid in identifying the perpetrators. This entails following the "money flow" using traditional investigative tools and undercover techniques.

Having discussed the respective situations and challenges encountered by each of the participating group members, the following measures were agreed upon:

- Cybercrime techniques should be regularly updated.

- Government should provide a conducive environment for international cooperation, as well as cooperation between agencies.

- The government should ensure that only specialized and competent officers are allowed to handle cybercrime investigations.

- Minimize dependence on IP addresses and consider other sources of information depending on the type of case, i.e. bank accounts, security cameras, and lease/utilities/infrastructure contracts, open sources in the Internet, etc., and to keep in mind that traditional investigation is also useful in cybercrime cases.

- SIM cards need to be registered to deter cybercriminals from using them with impunity.

- Existing police units should have on-call and available cybercrime experts.

- Authorities should be allowed extensions of time for service providers to save traffic and content data subsequent to proper request or order from responsible authorities/offices.

- Consider criminalizing tipping off suspects under investigation in order to maintain confidentiality.

2. Expedited and Proper Search, Seizure and Preservation of Digital Evidence

A majority of the participants reported that their respective countries do not have specific procedural laws for the search, seizure and preservation of digital evidence. They, however, follow their country's general law on criminal procedure with respect to gathering and preserving digital evidence.

The participants also reported a number of cybercrime challenges which their respective countries need to address. Those challenges include outdated techniques of investigators in collecting digital evidence, inadequate skills on the part of prosecutors and judges handling cybercrime cases, lack of highly skilled digital forensics experts who analyze data, absence of forensic laboratories and storage facilities and inadequate government budgets for cybercrime cases.

Since all the participants observed that there is a need to immediately secure digital data and preserve them for purposes of presenting the same in court, the group agreed on the importance of the following measures:

- Procedural laws which specifically treat digital evidence, i.e. translating digital evidence to physical evidence, should be legislated.
- Officers and investigators should maintain a high level of competency through regular training to ensure correct handling and examination of digital evidence.
- The governments of the participating member-countries should establish forensic laboratories equipped with adequate and updated forensic tools.
- Guidelines and manuals for investigation and seizure of digital evidence must be made available to officers and agents handing digital evidence.
- Informal channels between competent agencies and individuals should be considered in the investigation and prosecution of cybercrimes.
- International cooperation plays a vital role in the expedited search, seizure and preservation of digital evidence since cybercrime is borderless.

3. Cooperation Among Agencies and the Private Sector Dealing with Cybercrime or Cyber-Incident Cases

Most of the participants reported having available anti-virus software and respective computer emergency response teams (CERT) and/or computer security incident response teams (CSIRT) in their respective countries. All have Internet service providers. In this regard, Dr. Kim-Kwang Raymond Choo informed the group about FIRST, the international organization of CERTs.

During the discussion, it was opined by a majority of the members that the service providers in their countries are reluctant to cooperate with authorities and provide assistance in cybercrime investigations. This is especially true in banking institutions victimized by phishing. Similarly, cellphone companies are unwilling to relay subscriber information and mobile data to authorities. Compulsory cooperation is obtained by investigators through preservation orders and/or court orders.

The group agreed on the importance of the following measures:

- Countries without CERTs were recommended to establish an appropriate agency to deal with cybercrime.
- There should be a clear mechanism which would encourage public-private sector cooperation and voluntary cooperation on the part of the private sector, bearing in mind corporate responsibility.
- There is a need to raise public awareness.
- An effective mechanism for network monitoring, which has measures to ensure that the person's right to privacy is not violated, should be in place.

- Government agencies should be updated on cybercrime issues to be able to adequately address the dynamic nature of cybercrime.

- There should be sufficient allotment for up-to-date infrastructure in investigating and combating cybercrime.

4. International Cooperation.

All participants agreed that international cooperation is essential in the investigation, prosecution and adjudication of cybercrime cases. International cooperation between partner states is done through their respective Mutual Legal Assistance Treaties (MLATs) and collaboration with the International Criminal Police Organization (Interpol).

It was further agreed that international cooperation plays a vital role in the exchange of information and technologies and capacity building between nations. Once good rapport between countries has been established, assistance may be provided through informal channels. This is a faster way of securing volatile data vis-à-vis filing formal requests, which takes time to process.

Some of the participants reported that they have neither 24/7 contact points in their respective countries to promptly process international requests for assistance nor a central agency to monitor the same.

The group also remarked that acquisition of digital information from a non-signatory country is made more difficult since what may be considered a crime by the requesting country may not be an offence in another. In this regard, the latter country may refuse to render assistance. Thus, legislative harmonization between nations is strongly encouraged.

After considering the foregoing, the participants agreed on the points enumerated below:

- There is a need to establish a central/primary agency that deals with cybercrime investigations and receives information and requests from foreign states. This agency should also be equipped with a 24/7 contact point mechanism for the expeditious processing of requests.

- Procedures for the processing of requests should be simplified and streamlined.

- Regional and international treaties should be extended and the Convention on Cybercrime should be signed; otherwise, laws treating the collection, investigation, prosecution and adjudication of cybercrime offences should be legislated at the national level.

- International workshops, training programmes and dialogues on cybercrime are necessary.

- Use of informal channels between states is encouraged to expedite the retrieval of digital data.

- Cybercrime legislation and budget should be given priority by the country.

- There is a need for capacity building on the part of the investigators and responsible agencies not only for purposes of dealing with local cybercrime cases, but also in receiving and processing international requests for cybercrime investigations.

C. Effective Measures for Prosecution and Adjudication

1. Measures for Clear Presentation of Digital Evidence, Admissibility of Evidence and the Form of Digital Evidence at Trial

During the discussion, the participants agreed that digital evidence must be presented during trial in a language and manner understood by the presiding judge. Testimonies of expert witnesses are crucial, and prosecutors should have basic knowledge of cybercrime. Moreover, collaboration between the prosecutors and expert witnesses in the trial of cybercrime cases is a must.

Most of the members stated that they have existing laws which treat computer printouts of digital data

as competent/admissible evidence. However, they should be duly authenticated and pass the scrutiny of genuineness and integrity of data. It was also observed that digital evidence is often ruled inadmissible by the court due to lapses in collection and analysis and failure to comply with the mandatory chain of custody procedures. Lack of forensic laboratories also contributes to this dilemma.

A majority of the participants follow their general rules on criminal procedure in presenting digital evidence in court. All agree, however, that the general rules on criminal procedure cannot fully address cybercrime evidence.

Since court hearings in cybercrime cases usually take years to finish, stipulation between the prosecutor and defence, with respect to presentation of expert witnesses, should be considered to expedite the proceedings. It would also help if the country has a specialized team of trained cybercrime investigators, prosecutors and judges/courts which handle cybercrime cases.

After much discussion, the group agreed on the following measures to overcome the above-stated pressing challenges and improve the current situation:

- There must be training programmes for the judiciary, prosecution and police on cybercrime laws and cases.
- Each country should have specialized cybercrime laws and procedures; digital evidence provisions should be included.
- Countries should have highly specialized and trained teams of investigators, prosecutors and courts for cybercrime cases.
- There must be available forensic laboratories, which are able to process and translate digital evidence to visible evidence.
- The trial courts must be properly equipped with projectors, monitors, computers and other facilities to be used in presenting digital evidence.
- Ordinary/traditional methods of evidence gathering and investigation should be considered especially when there is no direct evidence in cybercrime cases.
- Prepare a checklist enumerating the evidence collected and their chain of custody, relative to their collection, examination and safekeeping.
- Prosecution and expert witnesses should collaborate to be able to present digital evidence in a manner understandable by the court; expert witnesses must be able to convince the court that he or she is an expert.
- Consider marathon hearings for cybercrime cases to expedite court proceedings.
- Some of the participants suggested to consider introducing mixed-system trial procedure (inquisitorial and accusatorial/adversarial systems combined), i.e. enabling the judge to see all the evidence before trial, because of highly technical and voluminous pieces of evidence presented in cybercrime cases; while some participants, although opting to maintain their respective criminal laws/procedures, will implement additional measures to expedite court proceedings, before or during trial, of cybercrime cases, i.e. pre-trial conferences, if applicable, stipulation between prosecution and defence.
- Some participants suggested that there should be a legal presumption of guilt against an offender who uses proxy/TOR to conceal the real IP address and refuses to give his or her user name and password to access his or her information in the server. In this case, the burden of proof shifts to the offender to show otherwise.

III. CONCLUSION

Considering the foregoing, Group 2 concluded that there must be an interplay of the following general elements for the successful investigation, prosecution and adjudication of cybercrime cases: 1) capacity building of investigators, prosecutors and judges who handle cybercrime cases, including training on the use of digital forensics; 2) public awareness; 3) public and private partnerships and 4) international cooperation.

Authorities and officials should be properly trained and highly skilled. Investigators and digital forensics experts should have the ability and ingenuity to collect, preserve and process digital data. They should be updated with the latest technologies and forensic tools. Prosecutors and judges need to have specialized skills in dealing with cybercrime for better understanding of digital evidence to maintain proper and efficient investigation and trial of the cases.

On the other hand, the people should be properly briefed and educated on cybercrime law, or other similar laws, to encourage them to immediately report incidents of cybercrime to law enforcement authorities for proper action. The government should provide the public a forum where they can get immediate assistance. This will also prevent the people from falling prey to cybercriminals or being potential cybercriminals, consciously or otherwise.

Public and private partnerships must be encouraged. The government, on its own, will not be able to address the rapid turnover of technologies and pervasive effects of cybercrime. Strategic partnerships with private corporations, such as anti-virus companies, should be fostered.

More importantly, there must be international cooperation between nations. International cooperation entails sharing of best practices in cybercrime investigations, prosecution and adjudication, capacity building and technical assistance in cybercrime investigations.

However, to make international cooperation an effective tool against cybercrime, there must be legislative harmonization among nations so as not to allow cybercriminals to make good on their malicious intent without fear of prosecution to the detriment of the public in general.