GROUP 3

EFFECTIVE MEASURES FOR STRENGTHENING THE SYSTEM FOR SUPPRESSION AND PREVENTION OF CYBERCRIME

Chairperson	Ms. Tetiana Pavliukovets	(Ukraine)
Co-Chairperson	Mr. Takeru Sato	(Japan)
Rapporteur	Ms. Irene Cayetano Cena	(Philippines)
Co-Rapporteurs	Mr. Kunlay Tenzin	(Bhutan)
	Ms. Thi Khanh Nguyen	(Viet Nam)
Members	Mr. Thurain Aung	(Myanmar)
	Mr. Wasawat Chawalitthamrong	(Thailand)
	Mr. Taku Uehara	(Japan)
	Mr. Katsuya Toyama	(Japan)
Visiting Expert	Mr. Yuki Honda	(Interpol)
Adviser	Ms. Ayuko Watanabe	(UNAFEI)

I. INTRODUCTION

Group 3 of the 160th International Training Course commenced its discussion on 25 May 2015, on the topic of "Effective Measures for Strengthening the System for Suppression and Prevention of Cybercrime" . By the consensus of the group, Ms. Tetiana Pavliukovets was elected as the chairperson and Mr. Takeru Sato as the co-chairperson. The rapporteur was Ms. Irene Cayetano Cena and the co-rapporteurs were Mr. Kunlay Tenzin and Ms. Thi Khanh Nguyen. With the assigned topic, the group discussed the following issues: 1) Establishment of special organizations or units against cybercrime and measures of capacity building for criminal justice practitioners; 2) Facilitating international, regional and domestic cooperation among related agencies against cybercrime; and 3) Facilitating public-private partnership against cybercrime.

II. SUMMARY OF THE DISCUSSIONS

A. Establishment of Special Organizations or Units against Cybercrime and Measures of Capacity Building for Criminal Justice Practitioners

Most of the members of the group agreed to the idea that there is a need to establish a special unit that will cater to all cyber-related cases due to the complexity of the issue. The group came to this decision after a thorough study on the advantages and disadvantages of having a separate unit. Some of the members are not yet decided on whether to have a specific unit or not, for they believe that it will bring conflict with the other ministries' duties and functions. Also, they are still uncertain on how this special unit will be managed properly taking into consideration the requirements, such as human resources, logistics, infrastructure, etc., in order to have it operational.

For the capacity-building measures for criminal justice practitioners, the group reached a consensus that there must be two levels of training in dealing with cybercrimes. The first level is the basic knowledge for all cyber-practitioners to have a general overview and common understanding and appreciation of cybercrime, and the second is the specialized training for the experts for the conduct of cybercrime-scene investigation. Also, the group agreed upon the idea to incorporate cyber-related courses upon recruitment of police officers to ensure that new officers, as first responders, at least know the basics on how to handle cybercrime cases and how to preserve the cybercrime scene to make the evidence admissible in courts. For those who want to pursue careers fighting cybercrime, specialized cyber-related training and certifications must be secured to make them experts in their chosen field of specialization.

B. Facilitating International, Regional and Domestic Cooperation among Related Agencies against Cybercrime

Based on brainstorming conducted by the group, there was an understanding that cooperation with investigative or prosecutorial agencies of other countries plays a very important role in the suppression and

prevention of cybercrime. The establishment and utilization of a 24/7 point of contact is a very efficient and effective tool in the fight against cybercrime but this may not be legally binding depending on the nature of existing laws of each country. Instead, the group decided that there must be a hotline center to handle reports of cybercrime on a 24/7 basis in consonance with the Budapest Convention. Also this can be utilized for sharing of information among participating countries. Persons who are designated for this purpose must have a good understanding and appreciation on the complexity of cybercrime and must be familiar with the terminologies and technicalities of cyber-issues and concerns.

On the issue of cooperation between investigative agencies and digital forensic laboratories, all members of the group agreed that this forms part in the fight against cybercrime, whether the investigative agency is the police or the prosecutors or anybody involved in the investigation of cybercrime. Some of the participants deem it necessary to rely on the expertise of private institutions in the investigation of cybercrime cases, especially in the conduct of forensic examination, but some do not agree with this idea because of the issue of the chain of custody of evidence. Some members suggested that the digital forensic examinations be conducted by police officers who are qualified and certified in this aspect, but other members of the group were uncertain on this matter for it may incur additional financial support from the government. They also come up with the idea that these police officers will only make use of their knowledge for their own personal advantage and use it as a means to gain more influence in the government.

C. Facilitating Public–Private Partnership against Cybercrime

On the aspect of cooperation with internet service providers (ISPs), the group agreed that there must be an international regulation for all ISPs to be imposed by the Regional Internet Registry which manages the allocation and registration of internet number resources within a particular region. There must be a strict policy prior to the approval of business permits for these ISPs to comply with certain requirements, to include availability of large storage devices for preservation of information and pertinent data on cyber-related cases. With regard to the preservation of traffic data, the group came up with the recommendation that this information must be preserved not less than 90 days. However, for the data which are deemed necessary in the conduct of investigation on cyber-related cases, the preservation period may be extended depending on the necessity to do so. The group also considered the aspect of cooperation with telephone communication companies (TELCOs), for these entities can also contribute a lot in the suppression and prevention of cybercrime merely because some cyber-related offences are committed through the use of cellular phones. A strict regulation on the purchase and selling of SIM cards by these companies can aid investigators in the identification of perpetrators in cyber-related cases. This may threaten those cyber-offenders so that they cannot hide their real identities, and they cannot easily avoid the consequences of their misconduct in cyberspace; hence they need to think twice before committing cyber-offences.

Even though not all the members of the group have existing cooperation with cybersecurity companies and related agencies regarding the provision of investigation techniques, information and assistance, the group believes that all countries across the world must establish a Computer Emergency Response Team or a Computer Security Incident Response Team as part of the suppression and prevention measures for cybercrimes. Most of the members agreed that the response team for cyber-related cases must be handled by private companies for they have enough resources and facilities to deal with malware attacks. They have established their respective malware laboratories, state of the art equipment and expert personnel to conduct studies pertaining to cybersecurity. Some members of the group suggested that the response team must be taken care of by the government at the cabinet level for the reason that they have the administrative authority and power to handle computer security issues. All the members agree that these organizations should be in close coordination with the investigators and the private companies as well as the government for exchange of information and in depth collaboration.

All the members of the group gave detailed explanations as to the status of cooperation of their respective countries with universities and research institutes. It is worth noting that out of the seven countries represented in this group, only two have no research institutes for cybercrime in place at the moment. Even though these two countries have no existing research institutes to conduct studies on cybercrime, they agree that there is a need for the government to establish rapport with universities and research institutes to work closely and gather information that may support the fight against cybercrime. Information from these institutions may be used as a basis for conducting cybercrime investigations as well as suppression and prevention.

In enhancing public-awareness of the threat of cybercrime, several modes of advocacy were suggested by the group members to include the conduct of cyber-related seminars, training programmes and workshops for all members of the public and private sectors, most especially students who must use the Internet; dissemination of flyers, leaflets and other reference materials pertaining to cybercrime; conducting radio and television interviews with cybersecurity experts for warning the public on the implications of the use of the Internet; production of videos, infographics and manga materials related to cybercrime; conducting cybersecurity summits wherein experts are invited to share their knowledge to prevent cybercrime; regular publication of cybersecurity bulletins; making use of students as junior cyber-patrollers to gather information from the community; morale enhancement through the help of the religious sectors as part of the maintenance of the code of ethics and proper conduct; advertisement in public places with the use of posters and tarpaulins; and information dissemination through SMS from TELCOs and notices from banks and other institutions. The group firmly believes that the government has the greater responsibility in the advocacy and public awareness campaign in terms of cybercrime. But, it must be noted that this issue is not the sole responsibility of the government; each member of the community must contribute and do their share as responsible citizens in order not to become victims of cybercrime. If you want to get rid of becoming a victim of cybercrime, the best defence is to get rid of the use of the Internet and cellular phones.

III. CONCLUSION AND RECOMMENDATIONS

At the end of the discussion and thorough study on the nature and complexity of cybercrime, which is known to be borderless and transnational, the group recommends the following measures for the suppression and prevention of cybercrime:

1. Establishment of a special unit that will handle cybercrime-related matters in aid of investigation and prosecution of cybercriminals; to conduct analyses of digital evidence recovered; and to gather, evaluate and analyse modi operandi of cybercrime cases. Also, on capacity-building measures for criminal justice practitioners, there must be two levels of training: the basic training on cybercrime which aims to give a general overview and common understanding of the subject matter to all cyber-practitioners and the specialized training for the experts for the conduct of crime-scene investigation and enhancement of cybersecurity skills, as well as skills in digital forensics examination. For police officers, basic cyber-related courses should be incorporated in the course upon recruitment to have at least an overview on how to deal and conduct cybercrime-scene investigation for proper identification, seizure and handling of digital evidence, for they are expected to be the first responders. A specialized course must also be undertaken by those who want to pursue a career in cybercrime investigation and secure corresponding certifications needed to become experts not only in digital forensics but also in cybersecurity.

2. Facilitating international, regional and domestic cooperation among related agencies against cybercrime is a must. There should be mutual legal assistance treaties between and among other countries for exchange of information and sharing of intelligence reports relative to cybercrime. Also harmonization of the existing national legislation will also contribute to the fight against cybercrime, to have at least a minimum standard on the issue of dual criminality. In addition, establishment of a hotline center that will be operational 24/7 can also be utilized not only for information sharing but also for collaboration in the conduct of investigations. Informal channels may also be utilized taking into consideration the existing laws and constitutions of respective countries. Also, cooperation between investigative agencies and digital forensic laboratories will contribute in the fight against cybercrime not only in the form of sharing procedures for preservation and collection of digital evidence but also for the procedure and processes to obtain results of analyses.

3. Facilitating public-private partnership is an essential factor to consider in the suppression and prevention of cybercrime. There must be cooperation between internet service providers and the government in order to have a regulation in terms of preservation of all traffic data which should be not less than 90 days with an exception for data which are deemed necessary in the conduct of investigation on cyber-related cases, depending on the necessity of the information. Regarding cellular phones, strict regulation on the purchase and selling of SIM cards must be a prerequisite for proper identification of users, which is a very important tool in cybercrime prevention. Moreover, coopera-

tion with cybersecurity companies and related agencies regarding the provision of investigation techniques, information and assistance will be added factors to prevent the occurrence of cybercrime. All countries across the world must have a Computer Emergency Response Team or a Computer Security Incident Response Team. The responsibility for these teams should be delegated to private companies, for they have enough resources and facilities to handle cyber-related attacks. Cooperation with universities and research institutes are indeed indispensable, for these institutions can contribute to information gathering and sharing and keeping cyber-practitioners up to date in terms of cyber-related issues. And last but not least is the most significant measure in the prevention and suppression of cybercrime—the enhancement of public awareness through conducting cyber-related seminars, training programmes, workshops, cybersecurity summits, etc. for all members of the community, most especially the students who are very exposed in the world of cyberspace; production and dissemination of informative materials and cyber-bulletins in the form of flyers, leaflets, brochures, manga, SMS, notices, posters, tarpaulins, videos, infographics, etc.; conduct of radio and television interviews with experts on cyber-related matters; and conduct of cyber-patrolling to monitor any eventualities within cyberspace.

Cybercrime will persist all over the world, but the battle against it should not and must not only be managed by the governments of every country in the world. Everyone has obligations and roles in the society that can contribute to the fight against cybercrime. Let us all work together to prevent and suppress cybercrime in order to achieve a more secure and productive cyber-environment.