REPORTS OF THE COURSE

GROUP 1
EFFECTIVE CYBERCRIME LEGISLATION FROM THE PERSPECTIVE OF ENFORCEMENT PRACTICES

Chairperson	Mr. Werton Costa	(Brazil)
Co-Chairperson	Mr. Emil Gonzalez	(Panama)
Rapporteur	Mr. Joash Dache	(Kenya)
Co-Rapporteur	Ms. Kawabata Yuko	(Japan)
Members	Mr. Diabate Djakaridja	(Côte d'Ivoire)
	Mr. Ramesh Prasad Gyawali	(Nepal)
	Mr. Vincent Agusave	(Papua New Guinea)
	Mr. Jeffery Jean Baptiste	(Seychelles)
	Mr. Ihor Sekhin	(Ukraine)
	Mr. Sato Hiroyuki	(Japan)
Visiting Expert	Prof. Dr. Marco Gercke	(Germany)
Advisers	Prof. Hirose Yusuke	(UNAFEI)
	Prof. Yukawa Tsuyoshi	(UNAFEI)

I. INTRODUCTION

The First Session of the Group was called to order on 22nd May 2015 at 3:35 p.m in Seminar Group Room 2. It was presided over by Prof. Hirose with Prof. Yukawa in attendance. Mr. Costa of Brazil was nominated and approved by consensus to be Chairperson. Mr. Emil of Panama was nominated and approved as Co-Chair. Mr. Dache of Kenya was nominated and approved as Rapporteur with Ms. Kawabata of Japan as Co-Rapporteur.

After the elections, the Group had its first formal session. Based on the preliminary deliberations, the Group agreed to tackle the second part of its given theme on 'Development of Cybercrime Legislation from the Perspective of Enforcement Practices'. It was further agreed that the Group would conduct its discussions according to the following agenda: (1) a brief summary relating to the current situation of cybercrime legislation in each country; and (2) development of cybercrime legislation from the perspective of enforcement practices. It was agreed by consensus that in canvassing the two main items of the agenda, the Group would rely on the Convention on Cybercrime (Budapest Convention), similar regional approaches where relevant, seminar discussions and jurisdictional experiences as the primary working tools.

II. SUMMARY OF THE DISCUSSIONS

A. Synopsis of the Current Situation of Cybercrime Legislation in the Participating Countries

The Group had 10 members representing 9 countries. In relation to the current situation of cybercrime legislation in each country, it was noted that the circumstances surrounding this matter are different. Of the 9 countries represented, it was only Panama, Papua New Guinea (PNG), Ukraine and Japan which have signed and ratified the Convention on Cybercrime (the Budapest Convention). Panama, PNG and Ukraine—unlike Japan—have not enacted any unified or specific law on cybercrime but have provisions in their domestic Criminal Procedure and Penal Codes and other information and technology-related laws to investigate and prosecute cybercrime.

On the other hand, Brazil, Côte d'Ivoire, Nepal, Seychelles and Kenya have not ratified the Convention on Cybercrime. However, these jurisdictions have domestic legislation covering various aspects of cybercrime. Brazil and Seychelles rely on domestic Criminal Procedure and Penal Codes and a variety of other relevant legislation to investigate and prosecute cybercrime. Kenya has, in addition to its domestic Criminal Procedure and Penal Code, the Information and Communications law in which the substantive law of the Cybercrime Convention is codified. Nepal has enacted the Electronic Transactions Act and attendant regulations which deal with all forms of electronic transactions and digital signatures and make provisions to regulate various computer-based activities and punish cybercrime. Côte d'Ivoire has since 2013 enacted

three relevant pieces of legislation, including a law on cybercrime, which address most of the current issues around cybercrime and related activities in accordance with the recommendations and directives of ECOWAS (a regional body).

The Group recognized that, although a majority of the countries represented have not ratified the Cybercrime Convention, the countries subscribe to other regional bodies under whose auspices there are major initiatives on harmonized regional frameworks on cybercrime. It was, however, noted that despite these fairly recent regional advances and the efforts at enacting and enforcing the relevant domestic laws, almost all the countries represented in the Group still have challenges in the investigation and prosecution of cybercrime. These challenges which are typically systemic, infrastructural and resource-based in nature vary from country to country, although there are generic aspects which may require similar approaches as will be seen later.

B. Development of Cybercrime Legislation from the Perspective of Enforcement Practices

In addressing this broad theme, the Group discussions centered on answering the following specific questions:

1. Whether or Not and How Long to Oblige Internet Service Providers to Preserve Data of Subscriber Information and Traffic Records

It was noted that Articles 16 (Expedited preservation of stored computer data) and 17 (Expedited preservation and partial disclosure of traffic data) of the Cybercrime Convention intentionally do not address the issue of data retention. Instead of an obligation to retain data, the Drafters of the Convention included provisions dealing with expedited preservation. Specifically, the Convention mandates a State Party to adopt such legislative and other measures to enable its competent authorities to order or obtain the expeditious preservation of specified computer data upon request where such data may be particularly vulnerable to loss or modification. It further requires a person in control of such data to preserve and maintain its integrity for up to a maximum of ninety days, which period may be subsequently renewed. The Convention also obliges the custodian of such data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. The exercise of such powers and procedures are subject to Articles 14 and 15.

After discussion, it was agreed that:

(i) Subject to appropriate legal safeguards, there is a need for domestic legislation to provide for a minimum period of one year for retention of subscriber information and traffic records by Internet Service Providers (ISPs) whether or not there is suspicion of a crime. However, in enacting such domestic legislation, the EU directive prescribing a period of data retention which ranges from 6 months to 2 years and the European Court of Justice ruling that such provision would be inimical to human rights, should be borne in mind; and

(ii) The domestic legislation should further provide that in cases of investigation of cybercrime, competent authorities should apply for court orders to require the ISPs to preserve the integrity of the specific data for a period of 90 days which may be extended: (a) once for another 45 days; or (b) indefinitely for 90 days at a time; or (c) until the completion of investigations or indictment of the suspect. Caution should however be exercised in respect of the second and third options, especially if there is likely to be unreasonable delay in the investigation.

2. Whether or Not Digital Evidence is Admissible as Evidence at Trial and Under Which Conditions

The Group recognized that admissibility of electronic evidence is an important issue that should be addressed in domestic legislation as otherwise it would not be possible to effectively prosecute cybercrime in court. The Group appreciated that handling electronic evidence is a fairly challenging affair. The Group subsequently analyzed the Convention to identify provisions dealing with the admissibility of electronic evidence but realized that no such provision existed.

It was noted that the closest the Drafters of the Convention went in this regard are Articles 14 and 15 of the Convention. Specifically, the Convention provides in Article 14 (Scope of procedural provisions) that subject to Article 21, a State Party shall among other issues apply the relevant powers and procedures

referred to in relation to collection of evidence in electronic form of a criminal offence. The Group was of the considered view that this provision does not address admissibility of electronic evidence per se. It was noted that Article 15 on the other hand merely provides for general conditions and safeguards relating to application of procedures and powers which include judicial or other independent supervision, grounds justifying application and limitation of the scope and the duration of such power or procedure.

The Group noted that in 2002, the Commonwealth developed in addition to the Model Law on Computer Crimes, a specific Model Law on Electronic Evidence. The Group also noted a similar approach in the Pacific Model Law, the Caribbean Model Law and the Sub-Saharan Model Law—all of which contain provisions specifically addressing the admissibility of electronic evidence.

Based on this broad analysis, the Group agreed that the conditions for admissibility of digital (electronic) evidence should be captured in special procedures provided for in domestic law. These conditions may include:

(i) Guaranteeing the authenticity, integrity and chain of custody of such evidence, and, with regard to authenticity and integrity, the evidence should where necessary be verified or authenticated by an expert witness or as may be directed by the court;

(ii) Preserving the privacy of the victims and accused person subject to exceptions which may obtain in domestic law; and

(iii) Subjecting such evidence to forensic examination.

3. Whether or Not to Regulate Internet Anonymity and Encryption (Whether or Not to Oblige Internet Users to Disclose and Register Their Identity Whenever They Connect to the Internet); Whether or Not to Oblige Suspects to Disclose Encryption Keys to Investigative Agencies Etc.)

The Group noted that there are two correlated issues at play in this question and canvassed these matters comprehensively because they touch on, among other fundamental rights, the freedom of expression and privacy of the individual. The Council of Europe's Committee of Ministers Declaration on Freedom of Communication on the Internet dated 28th May, 2003 was found by the Group to be persuasive. In Principle 7 (on Anonymity) the Declaration states that: 'In order to ensure against online surveillance and to enhance free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. This does not prevent member states from taking measures and cooperating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the field of justice and the police'.

The Group unanimously agreed that it is not desirable to oblige Internet users to disclose their identity not only on account of the adverse encroachment on the freedom of online expression but also due to the challenges attendant to implementation of such law if enacted. However, domestic legislation may provide for mechanisms through which users of the Internet in registered public places such as internet cafes may be required to provide their identity to the operators of such facilities and eventually to investigative authorities if needed.

On whether or not to oblige suspects to disclose encryption keys to investigative agencies and other state organs, it was observed that:

(i) most constitutions guarantee suspects the fundamental right to remain silent;

(ii) ordinarily, the burden of proof rests on the prosecution; and

(iii) most jurisdictions have laws prohibiting self-incrimination.

Based on these fundamental legal principles, it was therefore unanimously agreed that it would not be advisable to oblige suspects to disclose encryption keys to investigative agencies as encryption is one of the most important technical security aspects of electronic data. The Group was of the view that to address

this complex matter, domestic legislation may authorize law enforcement agencies to use advanced forensic tools (such as key logger) since such a framework would allow internet users to encrypt data and at the same time create the possibility of accessing encryption keys by law enforcement agencies. This approach has been embedded in the Pacific, Caribbean and African Model Laws as a safeguard.

C. Trans-Border Access to Stored Computer Data with Consent or Where Publically Available (Article 32 of the Convention)

It was noted that Article 32 of the Convention addresses the issue of trans-border access to stored computer data as applicable only to State Parties. Specifically, the Article allows a State Party without the authorization of another State Party, to access publicly available information (open source) stored computer data, regardless of where the data is located geographically; or to access or receive, through a computer system in its territory, stored computer data located in another State Party, if the State Party seeking the information, obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data.

It was agreed that sub-article (a) is self-evident and poses no challenge as it relates to information or data which is publicly available (open source). With regard to sub-article (b), however, it was noted that some countries have not ratified the Convention as a consequence of the perceived wide latitude afforded by this provision. This idea is especially prevalent in countries which feel the provision undermines international law as it unduly interferes with the principle of sovereignty of the State.

It was also noted by way of example that some investigative agencies have, despite this provision, experienced inability to access information or data stored in off-shore Google servers due to Google's privacy policy.

In its deliberations, the Group noted the ambiguity inherent in this provision. It was however concluded that sub-article (b) may be interpreted as specifically relating to the release of data by consent of the person who lawfully has control of the data such as owners of off-shore servers (without the requirement of formal consent of the host state). In cases where there is no such consent, the Group recommends that State Parties to the Convention on Cybercrime use the provisions on mutual legal assistance. Countries that are not State Parties may use other international cooperation mechanisms in seeking information. The Group noted the UNTOC framework, which has been signed by over 150 countries, provides similar mechanisms with regard to organized crime and would be preferable in this regard.

D. Other Challenges Relating to Legislation from the Perspective of Enforcement Practices

It was noted that the manner in which the question was framed was capable of different interpretations. The Group, however, identified the following as the key enforcement challenges and suggested measures to address them:

(i) Lack of specialized cybercrime laws in most jurisdictions and, therefore, it would be advisable to enact such laws where non-existent or to adequately amend existing law to address cybercrime and related emerging issues;

(ii) Lack of adequate deterrent sanctions since most cybercrimes are committed by organized criminal gangs whether local or international and therefore there is need for appropriately deterrent penalties for convicted cybercriminals with attention to proportionality of the sanction;

(iii) Non-ratification of the Convention given the international nature of cybercrimes is a challenge, and therefore it is necessary to encourage States to ratify the Convention as it is the current and foremost global framework on cybercrime;

(iv) Lack of proper coordination among key state and non-state actors (such as ISPs) which may hamper investigations and proper prosecutions, and therefore it is important for a domestic legal framework to clarify procedures and arrangements for effective internal cooperation;

(v) Lack of specialized personnel to undertake investigation and prosecution of cybercrime, which therefore calls for continuous capacity building;

(vi) Prohibitive costs relating to investigations of cybercrime (finances, infrastructure, expertise, etc.) due to its trans-border nature, and therefore there is a need to encourage legislative authorities to increase budgetary allocations to government departments and agencies responsible for dealing with cybercrime; and

(vii) Lack of international cooperation frameworks especially where the State Parties have not signed mutual legal assistance treaties, and therefore there is need to encourage States to sign Mutual Legal Assistance Treaties and continued invocation and deepening of other international cooperation mechanisms between states.

(viii) However, there was no complete consensus on the challenge of lack of dedicated courts or special divisions in the existing court structure to determine cybercrime cases. The matter was therefore proposed for consideration and implementation at the country (state) level.

III. CONCLUSION

The Group discussions were conducted in an atmosphere of respect for individual professional opinion and recognition of sovereignty of the countries represented. This enabled robust exchange of ideas and experiences which provided a rich platform for the application of the lessons learned during the lectures. The contributions of the Group Adviser, Prof. Hirose, and Visiting Expert Prof. Dr. Gercke, were invaluable. The Group makes the recommendations contained in this Report (based on the requirements of the Convention on Cybercrime and other regional approaches) in the hope that the proposals will improve state capacity and ability to enhance the fight against cybercrime, which is a dangerous global phenomenon.