GROUP 1

ISSUES AND MEASURES CONCERNING THE LEGAL FRAMEWORK TO COMBAT CYBERCRIME

Chairperson	Mr. Syed Abbas Ahsan	(Pakistan)
Co-Chairperson	Mr. Vijith Kumara Malalgoda	(Sri Lanka)
Rapporteur	Mr. Sergio Gardenghi Suiama	(Brazil)
Co-Rapporteur	Mr. Bafi Nlanda	(Botswana)
Members	Mr. Saleh Mohammad Altawalbeh	(Jordan)
	Mr. Santipatn Prommajul	(Thailand)
	Mr. Koji Sakamoto	(Japan)
	Mr. Nozomu Suzuki	(Japan)
Advisers	Deputy Director Takeshi Seto	(UNAFEI)
	Professor Jun Oshino	(UNAFEI)
	Professor Junichiro Otani	(UNAFEI)
	Professor Tae Sugiyama	(UNAFEI)

I. INTRODUCTION

Group 1 started its discussion on 16 October 2008. The group elected, by consensus, Mr. Ahsan as chairperson, Mr. Malalgoda as co-chairperson, Mr. Suiama as Rapporteur, and Mr. Nlanda as Co-rapporteur. The group, following its assigned topic, "Issues and Measures concerning the Legal Framework to Combat Cybercrime", agreed to conduct the proceedings in accordance with the following agenda:

1. Issues and measures relating to the criminalization of cybercrime;
2. Legal issues relating to the procedural law related to cybercrime, including admissibility of digital evidence;
3. Challenges in combating trans-border cybercrime, including issues of jurisdiction and international co-operation.

II. SUMMARY OF THE DISCUSSIONS

A. Substantive Criminal Law in Respective Countries Concerning Cybercrime, including Evaluation according to the Convention on Cybercrime

The group decided first to identify which offences have been criminalized by the countries as required by the Convention on Cybercrime. The group considered the Convention as a guideline establishing the international standards regarding this issue. Each participant of the Course had received a handout in order to clarify what offences are already included in their respective laws.

According to the participants, the current substantive criminal law of the respective countries regarding cyercrime is shown in the following table:

Country	Illegal access to a computer system	Illegal inter-ception of data	Illegal data inter-ference	Illegal system inter-ference	Illegal production and distribution of devices	Computer -related fraud	Computer related-forgery	Child porno-graphy	Copyright violations
Bangladesh	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Botswana	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Brazil	Partially	Yes	Partially	Partially	No	Yes	Yes	Yes	Yes
Hong Kong	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Indonesia	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Japan	Yes	Yes	Yes	Yes	Partially	Yes	Partially	Yes	Yes
Jordan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mexico	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Pakistan	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Philippines	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes
Sri Lanka	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Thailand	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Country	Identity theft	Illegal gambling	Cyber Terrorism[1]	Spam	Libel and false information	Racism and Hate Speech
Bangladesh	Yes	Yes	Yes	Yes	Yes	Yes
Botswana	Yes	No	No	No	No	Yes
Brazil	No	Yes	No	No	Yes	Yes
Hong Kong	Yes	Yes	Yes	Yes	Yes	Yes
Indonesia	Yes	Yes	Yes	No	Yes	Yes
Japan	No	Yes	No	Yes	Yes	No
Jordan	Yes	Yes	Yes	Yes	Yes	Yes
Mexico	Yes	No	No	No	Yes	No
Pakistan	Yes	Yes	Yes	Yes	Yes	No
Philippines	No	No	No	No	No	No
Sri Lanka	No	No	No	No	No	Yes
Thailand	Yes	No	Yes	Yes	Yes	No

The Chairperson, following the agenda, asked the group to discuss their national legislation regarding cybercrime. From the discussions, it was established that some countries have specific legislation on this subject, but some States do not have a separate legal framework. In such cases, they are using their prevailing legislation with amendments catering for illegal and harmful use of computer systems.

Of all the participating countries, Bangladesh, Botswana, Indonesia, Pakistan, Sri Lanka and Thailand have specific legislation against cybercrime. Brazil, Japan, Jordan, Hong Kong, Mexico and the Philippines do not have a specific legislation on cybercrime.

In Bangladesh, the Information and Communication of Technology Act (2006) covers the offences defined by the Convention on Cybercrime. According to the participant from this country, computer related fraud and forgery could be handled under the provisions of the Penal Code.

In Botswana, most of the offences have been criminalized by a specific act, except the violation of copyright. However, there is another act covering copyright offences, although this act does not mention offences committed on the Internet. The law is silent regarding electronic documents. Child pornography is criminalized (including possession).

In Pakistan, the Prevention of Electronic Crimes Ordinance was enacted to deal with cybercrime and criminalizes all the offences listed in the handout except child pornography and infringement of copyright. However, pornography of all kinds is criminalized in Pakistan through the special law against pornography; therefore, offences related to child pornography defined in the Convention are already covered in the existing legal framework. In addition, Pakistan has criminalized illegal access to computer data as a separate offence. Furthermore, the law does not criminalize copyright infringement as this is covered in a separate law.

In Sri Lanka, almost all offences defined by the Cybercrime Convention, except computer-related fraud and forgery, have been criminalized. Electronic transactions and documents are considered valid according

[1] There is no global consensus about the definition of the term "cyber-terrorism". Therefore, the table has only considered the definition of "terrorism" provided by the national legislations.

to Sri Lankan law. However, the Penal Code already covers the offences of fraud and forgery. In addition, the Evidence Ordinance accepts computer-generated documents as evidence; hence it is possible to prosecute computer-related fraud and forgery as well. Violations of copyright and patents are criminalized and have specific provisions in the law. The Penal Code includes child pornography as a crime, including possession, distribution, sexual abuse and publication. However, there is no specific provision for such crimes when committed on the Internet.

In Thailand, all offences defined in the Cybercrime Convention except child pornography and copyright violations have been criminalized under the Computer Crime Act. Child pornography (possession included) is an offence under Child Protection Act and copyright violations are dealt under the Copyrights Act.

In Brazil, the Penal Code, the Statute of Childhood and Youth and two Federal Acts are sufficiently broad to cover most of the offences defined in the Convention on Cybercrime, except misuse of devices and access and interference in private systems.

In Mexico, the Penal Code covers most of the offences defined in the Convention.

In Indonesia, all the offences defined by the Convention are already criminalized.

In Japan, almost all of the offences are already covered by the Japanese Penal Code or special laws. There is a specific law for copyright offences. Regarding child pornography, the possession of images is not criminalized. Moreover, the production and distribution of computer viruses are not criminalized at present. Misuse of devices is partially covered by national criminal legislation.

In Jordan there are no specific laws, but the Penal Code has been modified to include computer crimes. Moreover, there is a specific law for electronic transactions. Furthermore, draft legislation is under review in the Parliament, aiming at addressing all the offences as defined in the Convention on Cybercrime. Presently, the legal framework is not sufficiently broad to cover all these offences.

In the Philippines, the E-Commerce Act criminalizes only hacking and piracy.

In Hong Kong most of the offences identified under the convention are criminalized under the Crime Ordinance, except child pornography and copyright violations. Child pornography is an offence under Publication of Child Pornography Act and copyright violations are criminalized under the Copyright Ordinance.

After the overview of the respective legal frameworks, the Chairperson proposed a thorough analysis of each article of the Convention, aiming at clarifying any ambiguity regarding the interpretation of the text of the treaty.

Beginning with Article 2, the group debated whether the criminalization of illegal access to a standalone computer (not connected to a network system) should remain optional or be mandatory for the States Parties. Mr. Sakamoto argued that the law in Japan does not consider mere access to a standalone computer a criminal matter, since mere data access is not criminalized under any circumstances. Mr. Ahsan, on the other hand, was of the opinion that the Convention makes it mandatory for all States Parties to criminalize illegal access to standalone computers. Prof. Oshino, while referring to the Convention, explained that Article 2 makes it mandatory to criminalize illegal access to a computer system, connected to a network; however, the Convention differentiates between a computer connected to a network and a standalone computer in the article, and provides an option to the States to criminalize only the first situation. The group agreed to the explanation given by Prof. Oshino, as the wording of the article allows countries to restrict their legislation to computer systems connected to another system through a network.

Professor Oshino inquired about the situation in different countries in respect of offences with the following conditions established by Article 2:

1. Committed by infringing security measures;
2. With the intent of obtaining computer data; and
3. In relation to a computer system that is connected to another computer system.

Mr. Ahsan, Mr. Nlanda, Mr. Saleh and Mr. Malalgoda declared that Pakistan, Botswana, Jordan and Sri Lanka, respectively, do not attach any conditions to the criminalization of illegal access to a computer system. Mr. Prommajul said that in Thailand, the law requires the first condition to be satisfied. Mr. Suiama noted that in Brazil, the second and third conditions have to be established for criminal sanctions. Mr. Suzuki explained that in Japan, the first and third conditions should be satisfied.

The group further discussed criminalizing illegal gambling, cyber-terrorism, spamming, libel, slander, racism and hate speech. The group did not arrive at a definite answer on these issues and decided to take further advice from the Visiting Expert Prof. Marco Gerke. Mr. Ahsan, the Chairperson, concluded on behalf of the group that individual states should be allowed to legislate on these issues according to their own standards of criminal law. This conclusion was also based on the differing constitutional obligations of the states with reference to the rights of their citizens.

B. Visiting Expert's Opinion

To take advantage of the presence of the Visiting Expert, Prof. Marco Gerke, the Chairperson proposed that the session could be dedicated to the discussion of complex issues, on which the group could not come to a definite conclusion. Mr. Ahsan further elaborated that issues thus raised could be put to Prof. Gerke to take his guidance on these questions. The proposal was accepted by the group and the discussion was focused on issues on which the group sought assistance of the Visiting Expert.

Mr. Suiama explained that the most important issue for him was jurisdiction in cybercrime, whereby we can use three approaches:

A. Exercising extra-territorial jurisdiction, but this will raise the problems of sovereignty and breach of international law;

B. International co-operation through mutual legal assistance treaties or multilateral treaties like the Council of Europe Convention on Cybercrime; however, this would require dual criminality and the process will be prone to unnecessary delays;

C. Obliging the local offices of transnational companies to co-operate with the Law Enforcement Agencies.

Seconding the point of Mr. Suiama, Mr. Sakamoto proposed that the following questions should be raised by the group for Prof. Gerke on this issue:

1. Comparing the options of exercising jurisdiction vs. international co-operation; as cybercrime is a borderless crime and transcends international boundaries, how do law enforcement agencies exercise jurisdiction and what is the scope of international co-operation?

2. If the offender is in one country and the victim is in another country, is it possible for the country in which the victim resides to claim jurisdiction? And what if a service based in a country is focused on clients based in other countries?

3. If a service provider's office is located in a country, would it be advisable for the country to oblige such service provider to share data, e.g. the IP address of its users?

The criminalization of spam, libel and false information were also discussed by Mr. Prommajul and Mr. Nlanda, and then referred to the visiting expert as two separate questions:

4. What was the opinion of the Visiting Expert on the criminalization of spam?

5. Should libel and false information be criminalized with reference to cybercrime?

Additionally, Mr. Ahsan suggested that Dr. Gercke be requested to explain issues of criminalization of illegal access to data and to take his opinion on illegal access to standalone computers as well. The group also referred the issue of remote access tools used by law enforcement agencies. To this end the following questions were formulated:

6. Illegal Access to a computer in the convention does not include illegal access to data. The Convention also makes illegal access to a standalone computer an optional offence. What was the opinion of the Expert on these two issues?

7. What was the opinion of the Visiting Expert on the use of remote access tools by Law Enforcement Agencies?

The response of the Visiting Expert Dr. Marco Gercke, in the same order as the questions raised, is as follows:

1. The international co-operation approach is a better option, either directly or through the 24/7 Contact Point. Using the 24/7 Contact Point is a faster mode and the Contact Point will have all the resources and knowledge to reach the relevant person and get the necessary information and evidence at the earliest possible time. This approach has better chances of enforcement, considering that getting evidence from foreign companies, conducting investigations outside its territorial jurisdiction or arresting a suspect in a foreign country may not be easy through other means and may infringe international law. Furthermore, co-operation will not be voluntary and forthcoming to a foreign law enforcement agency but a local law enforcement agency will be better placed to enforce laws in its own jurisdiction.

2. It is possible to establish jurisdiction on the basis of the passive personality principle. Moreover, to resolve issues relating to jurisdiction, it is necessary to establish minimum standards of criminalization for all countries and also to improve international co-operation in these crimes.

3. It would not be very effective to oblige the service provider to share data and information because in some instances the service provider might just decide to close its office and leave the country. It could be more functional to use international co-operation in these matters.

4. The criminalization of spam in general is not advisable. A good example, however, is the law regarding spam in the United States, where only hiding one's identity or using spam for illegal purposes is considered a criminal offence.

5. On the issue of libel, slander and false information, it would be better to look at the general criminal law provisions and follow the same standards, noting however, that it is better to have civil remedies for such acts as applied in many countries.

6. Regarding illegal access to data, it is included in the illegal access to a system. However, as we could see from the Hong Kong example, in which a technician was given a computer to repair and copied information, it might be necessary to criminalize the illegal collection and copying of data. Although it is preferable to criminalize illegal access to standalone computers, in some jurisdictions that is not considered an offence, so a failure to criminalize would not be a serious deficiency in the law.

7. Regarding the use of remote investigative tools, in certain cases the use of such tools may be the only way to investigate a crime; therefore, the use of such tools should not be completely barred. It should be permitted according to the law of a particular jurisdiction defining the limits of the use of such tools.

C. Issues and Challenges faced by Countries concerning Procedural Law, Jurisdiction and International Co-operation

The group briefly looked at the procedural law relating to cybercrime in the participating countries. Procedural laws are available in most countries that support law enforcement agencies to investigate cybercrime, especially the general procedure on search and seizure, expedited preservation, and real time collection and interception of computer data. Most countries do not have any specific procedure on using remote investigation tools, identification requirements for Internet users, disclosure obligations or data retention obligations. The current procedural law of the respective countries regarding cybercrime is shown in the following table:

Country	Expedited preservation of computer data	Search for computer data	Seizure of computer data	Real time collection of traffic data	Real time interception of contents data	Use of remote investigation tools	ID requirement	Disclosure obligations of encryption keys	Data retention obligation
Bangladesh	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes
Botswana	Yes	Yes	Yes	Yes	No	No	No	No	No
Brazil	No	Yes	Yes	No	Yes	No	Partially	No	No
Hong Kong	No	Yes	Yes	Yes	Yes	Yes	No	No	No
Indonesia	Yes	Yes	Yes	Yes	Yes	Yes	Partially	Yes	Partially
Japan	Yes	Yes	Yes	Yes	Yes	No	No	No	No
Jordan	Not clarified	Yes	Yes	No	No	Not clarified	Yes	Not clarified	Yes
Mexico	Yes	Yes	Yes	Yes	Yes	Partially	No	No	No
Pakistan	No	Yes	Yes	Yes	Yes	No	No	Yes	Yes
Philippines	No	No	No	No	No	No	No	No	No
Sri Lanka	Yes	Yes	Yes	Yes	Yes	No	No	No	No
Thailand	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

The group discussion was opened by the Chairman with a question about whether it is possible to investigate and to prosecute a person for illegal content discovered during a search and seizure process which content was not included in the scope of the judicial warrant? After analysing the issue, the group concluded that in fact such a discovery will not be in violation of the warrant, and criminal proceedings can be initiated against the person based on the discovery of incriminating content.

Mr. Ahsan then drew the attention of the group towards the issue of expedited preservation of data. Mr. Saleh stressed the necessity to have specific provisions for search and seizure and preservation of data as such tools are indispensible for cybercrime investigations. Mr. Malalgoda informed the group that Sri Lankan law states that police officers can enforce expedited preservation data for seven days. Mr. Sakamoto added that, in Japan, the process to obtain a search warrant is very expeditious, but it is still advisable to have a provision for the expedited preservation of evidence due to the fluid nature of evidence and data. The group agreed to the importance of the provision for expedited preservation of data and recommended that such a provision should be considered for legislation as evidence in cyberspace can be lost, altered or deleted with much ease.

The Chairman then requested the group members to give their opinion on the issue of admissibility of copied data in the courts and use of data available on websites as evidence. Giving the example of Pakistan, he said that specific changes have been made in the evidence laws in Pakistan to bring electronic evidence in digital format on par with other kinds of evidence; for this the Electronic Transactions Ordinance has established rules and standards of admissibility. Mr. Sakamoto in this regard mentioned that the law in Japan has provisions of search and seizure of hardware, but the law does not stipulate mere copying of digital evidence. Secondly, theoretically, data published on websites can be admissible, but it is advisable that web-based data should be duly verified by the service providers who host such data. Mr. Suiama emphasized that we have to differentiate between published content data available on websites, which can be collected directly by a forensic expert, and traffic data or communication records for which verification can be made mandatory. Mr. Prommajul explained that his experience in prosecuting such cases is that courts require data be made available in printed form where possible. Moreover, in cases involving hackers or malicious code attacks, it is necessary to set up an isolated computer network to show to the court how the crime is committed. He also added that technically it is possible to download the content of a webpage without the assistance of the ISP, but traffic data can only be obtained from an ISP if they retain such data. Summing up the discussion of the group, the Chairman said that digital evidence should be admissible in court and the law should specify a standard for the admissibility of digital evidence. He further added that the group was of the opinion that it is preferable that the standards of collection of digital evidence include certification/verification by the service providers to remove ambiguity and doubt about the evidence collected.

The group next moved to the issue of real time collection of traffic data and interception of content data. Mr. Suiama explained that in Brazil, interception of content data is possible for a maximum period

of 15 days with court orders, but it is possible to extend the time period. According to Mr. Prommajul, in Thailand, interception of content data is possible with court orders and there is no time limitation, but such interception can only be initiated in cybercrimes. Mr Suzuki added that in Japan, apart from the court overview, such methods can be used only in limited offences.

Mr. Ahsan, introducing a new topic, the obligation to retain traffic data, said that in Pakistan, the law states that ISPs must retain traffic data for 90 days. There is a penal sanction of six months for not maintaining traffic data. Mr Suiama added that Brazil has no specific obligation on this matter but the national congress is discussing a minimum mandatory traffic data retention period of two years. Mr. Suzuki, Mr. Malalgoda and Mr. Nlanda also pointed out that their countries do not have specific laws for retention of traffic data. In Thailand, Mr. Prommajul explained, the law states that the ISP must keep traffic data for at least 90 days (and a maximum of one year). If they do not comply with this obligation, they are subject to a fine. The group opined that Article 20 of the Convention supports retention of traffic data and therefore concluded that a legal framework should consider including an obligation for retention of traffic data for a minimum period of six months.

The next topic that came under discussion was the use of remote investigation tools. Mr. Prommajul described that it is possible to search and collect evidence remotely and use different remote access tools to trace criminals. However, over and above the legal issues, it is not possible to assure the integrity of evidence collected through remote means, since the investigators would have full access to the computer of the suspect. It would be difficult to use this data as evidence in a court of law. In terms of interception for the purpose of investigation only to ascertain the commission of an offence or find the location of the offender, use of key loggers and similar tools could be a good, and possibly the only, option. Mr. Suiama raised two issues: first, whether we could use the same rules for normal search and seizure in cases of remote search and seizure; secondly, is this tool a violation of privacy if performed under judicial supervision? The Chairperson was of the opinion that normal search and seizure cannot be compared to remote search and seizure as the suspect is unaware of the whole process. Secondly, if normal search and seizure is possible and the suspect identified, the need for remote search and seizure should not arise. The group agreed that the use of such tools is a controversial issue, but considered that sometimes this tool may be the only option available to the investigators. It was therefore decided that the legal aspects of the use of remote access tools required further in-depth analysis. Nonetheless, the law must define clear limits for the use of such remote access tools and the circumstances in which the use is permitted.

The group then moved to the issue of identification when accessing the Internet through a public terminal. Mr. Ahsan said that in Pakistan, there is no such obligation, and opined that such a system was not useful as the trend is towards liberalizing access to information technology as it is now the major source of knowledge and communication. Many other options are available to offenders and by such measures we will restrict the use of information technology for normal and constructive purposes. Mr. Suiama agreed that it is useless sometimes to oblige cybercafés to identify their users. On one hand, there is an ideal of free access to communication and on the other, there is a challenge in identifying crimes and suspects under difficult circumstances. Mr. Saleh thought it was important to take this measure in order to prevent cybercrime, and identify users at Internet cafés. Mr. Suiama mentioned a possibility of the use of digital identification, but added that it would result in higher costs. The Chairperson recommended encouraging Internet cafés to voluntarily use identification as a social responsibility and good practice. Mr. Suiama and Mr. Sakamoto proposed administrative regulation as another option. The group decided that the use of Internet cafés is different around the world, and although it is better to have a process for identification, the matter is left to countries to take measures suiting their circumstances.

On the issue of disclosure of passwords and encryption keys, Mr. Ahsan said that the law in Pakistan obliges the suspect to provide the password or key but this law is being criticized as a violation of the constitution and against the principle of protection against self incrimination. On the other hand, the supporters of the law argue that any self-incriminating evidence would not be admissible in court and therefore not used, but such measures would be helpful to obtain other evidence. Mr. Prommajul added that in Thailand, there is also a similar obligation, but it demands a judicial request. There is a criminal penalty if the suspect refuses to give the password (a daily fine until he or she complies). Other participants were of the opinion that a law with the possibility of self incrimination would not be possible in their countries.

The final and very important topic discussed by the group was that of jurisdiction and international co-operation. The discussion was opened by the Chairperson who explained the different types of jurisdiction and the issues faced by the international community relating to jurisdiction in cybercrime. Mr. Suiama proposed that it is necessary to go further and try to define some criteria that can be used to define jurisdiction on the Internet. Mr. Malalgoda stated that we must look at the nature of an offence in order to define the jurisdiction. Mr. Ahsan stated that the issues of jurisdiction would best be solved if we establish a proper mechanism of international co-operation. Mr. Suzuki added that there should be some minimum standards of international co-operation which should be made part of the legal framework of our own countries. As for exercising jurisdiction, a number of issues should be considered including the place where the offence was committed, the place of the victim and the ability to conduct investigation. Mr. Suiama was of the opinion that even when the international community has achieved consensus, there are still some areas of conflict (e.g. hate speech) and it is important to consider these areas. He maintained also that the country where the data is located or where the ISP has its headquarters should not be considered the only criteria to define jurisdiction, since there are many international services provided from the US that are used for nationals to commit crimes. The group agreed on the importance of international co-operation/co-ordination and recommended that minimum standards of criminalization must be established and followed to address the issue of dual criminality. In addition, standards for international co-operation in cases of cybercrime should be formulated and established.

III. CONCLUSIONS

After lively discussions, the group reached the following conclusions:

1. The group agreed that all countries may adopt some basic international standards regarding both substantive and procedural criminal law. Recognize that the Convention on Cybercrime can be used as a good reference for minimum standards that may be adopted by the participating countries. It is also necessary to move toward some basic rules regarding the collection and admissibility of evidence from foreign jurisdictions. Three participants wish to include other international conventions (especially human rights treaties) as minimum standards as well;

2. The group also agreed upon the urgent necessity to improve the investigative and judicial mechanisms of international co-operation, in order to cope with a phenomenon that is fundamentally transnational. It was also suggested that adequate procedural laws may be implemented to assure the expedited preservation of evidence also when requested by foreign jurisdictions, while the regular measures are being completed;

3. The group understands that it is necessary to improve also the mechanisms of international co-operation in terms of training and technical aid provided for members of law enforcement agencies. These training programmes may include members from all the institutions related to the criminal justice system;

4. Data espionage is not properly covered by Article 2 of the Convention on Cybercrime and according to the participants an amendment to the text of the treaty should be considered;

5. SPAM is a serious worldwide problem and the group agreed upon the necessity of repressing the diffusion of unsolicited e-mails. The group suggested that spamming may be considered a crime only in cases when the SPAM is used for illegal purposes or when the spammer hides his or her identity;

6. The general principles of substantive law in force in the respective countries may be taken into account in matters of illegal gambling, identity theft, libel, slander and false information committed in cyberspace;

7. Private communications on the Internet should be protected as a civil right. Therefore, the interception of this kind of communication as a method of cybercrime investigation should be considered in a restrictive way, subject to judicial review. Under the same circumstances, ISPs should also retain stored content data, including communication data;

8. The group agreed that the use of remote investigation tools is a very controversial issue but,

considering that sometimes this tool can be the only option available to the investigators, the legal aspects of these methods of investigation should be submitted to an in-depth analysis;

9. The national legislatures should consider including the obligation for retention of traffic data for a minimum period of 180 days, since such time is the minimum reasonable time to identify the point of Internet access;

10. About the requirement of identification of users accessing the Internet through public terminals, the group agreed that although the use of these places differ around the world, it is better to adopt measures to force the owner or the person in charge to identify the users of the terminal. The majority understands that administrative measures are sufficient to reach this aim. One member argued that it would be sufficient to encourage public terminals to voluntarily comply with the recommendation, as a matter of social responsibility;

11. On the issue of mandatory disclosure of encryption keys and passwords by the suspect, the group concluded that such measures may be considered self-incriminating and that it is possible to find a way around these measures; therefore, the group did not support such a legal obligation;

12. Our understanding of jurisdiction as defined in the Convention on Cybercrime is that jurisdiction can be exercised both from the country where the Internet has been accessed as well as where the content is hosted. Moreover, the Convention also suggests the principle of jurisdiction based on nationality, even if the act is not committed in the home country, provided the act is criminalized in both jurisdictions. It is also recommended that the principle of passive personality, i.e. the use of victim's jurisdiction, may also be considered for addition to the Convention;

13. It is important to strengthen the co-operation between local offices of transnational Service Providers and the authorities in order to identify nationals who use remote located services to commit crimes. One participant dissented and argued that even in such cases the countries should use the regular instruments of international co-operation.