ISSN 1020-914X

UNAFEI NEWSLETTER

UNITED NATIONS ASIA AND FAR EAST
INSTITUTE FOR THE PREVENTION OF CRIME
AND THE TREATMENT OF OFFENDERS

No. 127
October 2008

Established
1961

IN THIS ISSUE

Page

UNAFEI IS AN AFFILIATED REGIONAL INSTITUTE OF THE UNITED NATIONS

1-26, HARUMI-CHO, FUCHU, TOKYO 183-0057, JAPAN
TEL: 81-42-333-7021 ◆ FAX: 81-42-333-4656 ◆ E-MAIL: unafei@moj.go.jp
HOME PAGE: http://www.unafei.or.jp/

LETTER FROM THE DIRECTOR

It is my privilege to inform readers of the successful completion of the 140th International Training Course on "The Criminal Justice Response to Cybercrime", which took place from 1 September to 10 October 2008.

In this Course, we welcomed five Japanese and ten overseas participants, and two overseas counsellors: eight from Asia, one from Africa, and three from Latin America. They included police officers, public prosecutors, and other high-ranking public officials.

As this newsletter demonstrates, the Course was extremely productive. It consisted of individual presentations, group workshop and plenary sessions, visits to relevant criminal justice agencies, and presentations by visiting experts, faculty members and ad hoc lecturers.

Despite the tremendous benefits of advancement in Information and Communication Technologies, regrettably, it has also facilitated various types of crimes, whether as the target of crime (e.g., unauthorized access and damage to, or the modification of, computer data or programmes) or as an instrument of crime (e.g., fraud, forgery, child pornography, defamation, infringement of intellectual property). In addition, cyber-attacks on infrastructure can have immediate and serious repercussions for national social and economic systems, as well as profound transnational effects. Thus, in various ways, cybercrime may threaten society as a whole and human rights, including rights to property, privacy, dignity and even life.

Because of the borderless nature of cybercrime, many efforts have been made at various levels for international harmonization or co-operation to tackle the issue. At the international level, organizations such as the United Nations Office on Drugs and Crime (UNODC), the International Criminal Police Organization (Interpol), the Group of Eight (G8), the European Union (EU), the Council of Europe (CE), the Organization of American States (OAS), and the Asia-Pacific Economic Cooperation (APEC) provide the political and technical expertise necessary to foster international co-operation.

Beginning with the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders in 1990, the United Nations has been actively involved in addressing various aspects of computer-related developments. Efforts have included the United Nations Manual on the Prevention and Control of Computer-related Crime, published in 1994, and the United Nations Convention against Transnational Organized Crime (UNTOC), which came into effect in 2003 and indirectly deals with cybercrime when carried out by organized criminal groups. UNAFEI itself assisted with the organization and implementation of a workshop on crimes related to the computer network at the Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders. At the Eleventh UN Congress on Crime Prevention and Criminal Justice a workshop was held on computer-related crime and the Congress adopted the "Bangkok Declaration" which welcomed efforts to enhance and supplement existing co-operation to prevent, investigate and prosecute high-technology and computer-related crime.

In view of the ongoing need for the formulation and implementation of effective measures in the fight against cybercrime, and the importance of such measures as stressed by the various UN instruments, UNAFEI, as a regional institute of the UN Crime Prevention and Criminal Justice

Programme Network, decided to hold this Course.

During the Course, the participants diligently and comprehensively examined the current situation of cybercrime in their respective countries, primarily through a comparative analysis. The participants shared their own experiences and knowledge of the issues, and identified problems and areas in which improvements could be made. After engaging in in-depth discussions with the UNAFEI faculty and visiting experts, the participants were able to put forth effective and practical solutions that could be applied in their respective countries.

I would like to offer my sincere congratulations to all the participants upon their successful completion of the Course, made possible by their strenuous efforts. My heartfelt gratitude goes to the visiting experts and ad hoc lecturers who contributed a great deal to the Course's success. Furthermore, I appreciate the indispensable assistance and co-operation extended to UNAFEI by various agencies and institutions, which helped diversify the programme.

I would like to express my great appreciation to the Japan International Cooperation Agency (JICA) for its immeasurable support throughout the Course. At the same time, a warm tribute must be paid to the Asia Crime Prevention Foundation (ACPF) and its branch organizations for their substantial contributions to our activities. Lastly, I owe my gratitude to all the individuals whose unselfish efforts behind the scenes contributed significantly to the successful realization of this Course.

Upon returning to their home countries, I genuinely believe that, like their predecessors, the strong determination and dedication of the participants will enable them to work towards the improvement of their respective nations' criminal justice systems, and to the benefit of international society as a whole.

Finally, I would like to reiterate my best regards to the participants of the 140th International Training Course. I hope that the experience they gained during the Course proves valuable in their daily work, and that the bonds fostered among the participants, visiting experts and UNAFEI staff will continue to grow for many years to come.

October 2008

相澤恵一

Keiichi Aizawa
Director, UNAFEI

THE 140TH INTERNATIONAL TRAINING COURSE

"THE CRIMINAL JUSTICE RESPONSE TO CYBERCRIME"

Course Rationale

1. The Increasing Threat of Cybercrime and the Necessity to Take Countermeasures

The revolution in information and communication technologies (ICT) is transforming society and human life drastically and fundamentally. ICT, especially computers and computer networks, are now considered indispensable resources for further development; they are seen as tools of management and communication in various social and economic activities.

Despite the tremendous benefits of ICT advancement, regrettably, it has also facilitated various types of crimes, whether as the target of crime (e.g., unauthorized access and damage to, or the modification of, computer data or programmes) or as an instrument of crime (e.g., fraud, forgery, child pornography, defamation, infringement of intellectual property). ICT advances give opportunity not only to mischievous hackers to satisfy their personal interest in intrusive actions, but also to organized criminal groups to profit economically by identity theft, counterfeit credit-card fraud, illicit trafficking etc. ICT can be used for identity-related wrongdoing, such as computer intrusion, phishing and skimming, not only endangering the privacy of individuals but also creating potential for further economic crime. Illegal or harmful material, such as child pornography, as well as websites assisting violent crime, drug crime, economic crime and sex crime, or websites promoting racism, terrorism or suicide, are now easily accessible. Cyber-attacks on infrastructure can have immediate and serious repercussions for national social and economic systems, as well as profound transnational effects. Thus, cybercrime may in various ways threaten society as a whole and human rights, including rights to property, privacy, dignity and even life.

In order to cope with such a situation, some characteristics of cybercrime (which is defined in this course as crimes in which computers or computer networks are the target or the instrument) should be noted. Cybercrime often involves invisible, intangible, volatile and changeable information data with advanced technology and a borderless network; therefore, investigators sometimes face difficulties in tracing it. Internet anonymity may become a licence to lie. At low risk to themselves and without any geographic or time constraints, cybercrime offenders may execute attacks causing instant harm to the general public. Copycat criminals are not uncommon.

These phenomena now pose significant problems in developed countries, and they also have critical implications for developing countries. Cybercrime can now be committed from or through jurisdictions which have at least minimal telecommunications services but have legal frameworks and law enforcement infrastructure too weak to counter cybercrime. Countries where ICT technologies are being initially deployed and maintained may face threats for which they are unprepared. In order to fully utilize ICT for the further development of society, building proper defences against cybercrime is an inevitable challenge.

The threat posed by the proliferation of cybercrime to the sound development of individual nations, as well as to the international community, has been underestimated. However, considering the instant extensive damage that can be caused worldwide by crime facilitated by ICT, a proper and immediate response by criminal justice agencies to cybercrime is indispensable. Nevertheless, since such crimes are relatively new to many countries, not every country has established the necessary legal frameworks. Even if such legal frameworks are effectuated, due to criminal justice

officials' limited knowledge of cybercrime and associated technological problems, difficulties will ensue in the investigation, prosecution and adjudication of these crimes, in particular with the identification of offenders and the collection of evidence. In addition, the complexity of the challenges specific to cybercrime necessitates international co-operation, which ultimately requires countries to be equipped with the necessary legal, procedural and regulatory tools.

Thus, the appropriate stringent control and prevention measures for cybercrime should be introduced as soon as possible. To this end, it is imperative for criminal justice agencies to understand thoroughly the current situation of cybercrime; to establish a proper legal framework to address such crimes; to develop more advanced techniques and tools commensurate with the nature of these crimes; and to enhance international criminal justice co-operation in this regard.

2. International Efforts to Combat Cybercrime

Because of the borderless nature of cybercrime, many efforts have been made at various levels for international harmonization or co-operation to tackle the issue. At the international level, many organizations such as the United Nations Office on Drugs and Crime (UNODC), the International Criminal Police Organization (Interpol), the Group of Eight (G8), the European Union (EU), the Council of Europe (CE), the Organization of American States (OAS) and the Asia-Pacific Economic Cooperation (APEC) provide the political and technical expertise necessary to foster international co-operation.

(i) Efforts by the United Nations

Beginning with the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders in 1990, the United Nations has been actively involved in addressing various aspects of computer-related developments. In 1994, the United Nations Manual on the Prevention and Control of Computer-related Crime was published. In 2000, the United Nations Asia and Far East Institute for the Prevention of Crime and the Treatment of Offenders (UNAFEI) assisted with the organization and implementation of a workshop on crimes related to the computer network at the Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders. The UN General Assembly invited States to take into account the measures to combat computer misuse contained in its resolutions on Combating the Criminal Misuse of Information Technology (55/63 (2000) and 56/121 (2001)). The United Nations Convention against Transnational Organized Crime (UNTOC), which came into effect in 2003, indirectly deals with cybercrime when carried out by organized criminal groups. The Eleventh UN Congress on Crime Prevention and Criminal Justice held a workshop on computer-related crime and adopted the "Bangkok Declaration" which welcomed efforts to enhance and supplement existing co-operation to prevent, investigate and prosecute high-technology and computer-related crime and invited the Commission on Crime Prevention and Criminal Justice to examine the feasibility of providing further assistance in that area under the aegis of the United Nations in partnership with other similarly focused organizations. In 2007, the Sixteenth United Nations Commission on Crime Prevention and Criminal Justice discussed identity-related fraud.

(ii) Other International Efforts

In 1997, the G8 established the Subgroup on High-Tech Crime under the framework of a group of senior experts on transnational organized crime, known as the Lyon Group, and adopted the Ten Principles in the Combat against Computer Crime, aiming to ensure that no such criminal receives safe haven anywhere in the world. The G8 Subgroup on High-Tech Crime established and expanded 24-Hour Contacts for International High-Tech and Computer-Related Crime, a list of computer crime units available to law enforcement agencies 24 hours a day, seven days a week.

The Council of Europe (CE) opened the Convention on Cybercrime (2001) for signature by Member States and selected non-member states in January 2001. The Convention, which took effect in 2004, is the first and currently only binding international instrument on this issue and

serves as a framework for international co-operation between States Parties to this treaty and as a guideline for any country developing comprehensive national legislation against cybercrime. It requires States Parties to harmonize national laws that define substantive offences. These include (i) Offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data/system interference, misuse of devices); (ii) Computer-related forgery, computer-related fraud; (iii) Content-related offences (child pornography); and (iv) Offences related to infringements of copyright. In 2004, the Convention's Additional Protocol, concerning the criminalization of acts of a racist and xenophobic nature committed through a computer system, came into effect. In addition, the Convention requires an important set of procedural powers, including production orders, preservation orders, search and seizure of stored computer data, and real time collection of computer data. There are also provisions to establish a rapid and effective system of international co-operation, including mutual legal assistance, and 24/7 networks and extradition.

In 2002, the Commonwealth Law Ministers adopted "The Model Law on Computer and Computer Related Crime", which shares a common framework with the Convention on Cybercrime. In 2004, the Fifth Meetings of Ministers of Justice or of the Ministers or Attorneys General of the Americas (REMJA V) recommended member states of the Organization of American States (OAS) to evaluate the advisability of implementing the principles of the Convention on Cybercrime (2001), and to consider the possibility of acceding to that Convention. In 2005, the Sixth Asia-Pacific Economic Cooperation (APEC) Ministerial Meeting on the Telecommunications and Information Industry encouraged "all economies to study the Convention on Cybercrime (2001) and to endeavour to enact a comprehensive set of laws relating to cybersecurity and cybercrime that are consistent with international legal instruments, including UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001)." The International Criminal Police Organization (Interpol), which has been providing technical guidance in cybercrime detection, investigation and evidence collection for law enforcement, including development of a 24/7 network, recommended the Convention on Cybercrime (2001) as providing the international legal and procedural standard for fighting cybercrime at the 7th International Conference on Cyber Crime.

In this context, for criminal justice authorities or legislators who wish to explore ways to strengthen legal frameworks against cybercrime in their respective countries, it is advisable to evaluate internationally developed materials such as guidelines, legal and technical manuals and model legislation, especially the Convention on Cybercrime (2001).

With regard to criminalization, this Course will mainly deal with the most common types of cybercrime which are stipulated in the Convention on Cybercrime (2001) and its Additional Protocol, as a starting point for discussion. However, there are many other illegal or harmful activities in which computers and computer networks are used as targets or instruments. These include a range of fraudulent activities using the ICT, such as auction fraud, non-delivery fraud, and significant increases in credit and debit card fraud. This course may discuss such kinds of cybercrime in which ICT is the target or the tool of other crimes.

3. Legal or Practical Issues in Investigation, Prosecution and Adjudication of Cybercrime

Needless to say, strengthening legal procedural tools and the capacity of law enforcement to investigate cybercrime is a critical task in combating cybercrime; however, it is also important that the prosecutors who will bring those cases, and the judges who will hear those cases, understand the current situation and challenges in order to appropriately punish offenders and promote confidence in the safety and security of the online environment.

In the investigation stage, strengthening mechanisms for gathering initial information on cybercrime should be considered. Victims of cybercrime often encounter difficulties in where and how to report the offences. Victims of content-related cybercrime such as child pornography usually have no opportunity to report the offences perpetrated against them. After acquiring initial

information, a timely and appropriate response is indispensable to trace the source or the route of the crime, to identify offenders and to collect evidence, since electronic evidence can be deleted or destroyed more easily than physical documents. To do this effectively, investigators need to be familiar with various types of cybercrime and related technologies and the government is required to take measures to strengthen the capabilities of investigative authorities to combat cybercrime. Without the necessary co-operation from other relevant private sector agents and technical experts, including Internet service providers, it is difficult to preserve, collect and analyse intangible and volatile digital evidence properly and without delay. In such a situation, whether, how, to what extent, and what kind of compulsory measures the investigative authority can use to preserve, collect or analyse stored computer data (traffic data or content data), or computer data in real time, may be the most critical issues. These critical issues include the necessity, target, scope and the method of execution of a warrant for compulsory measures relating to large amounts of computer data, unanticipated data or encrypted data. On the other hand, in collecting digital evidence, due process should be ensured, since such investigations often conflict with the right to privacy and other fundamental human rights. It should be noted that data collection and subsequent retention are charged with the conflicting interests and values of various stakeholders, and it may be advisable to seek a balance among the diverse legitimate interests.

Moreover, cybercrime easily crosses borders of jurisdiction and sovereignty; in such cases, it is crucial for successful investigation to utilize international co-operation, including immediate information sharing and mutual legal assistance among investigative authorities in different jurisdictions. Ordinary bilateral mutual legal assistance is not sufficient to trace cybercrime across many jurisdictions. If a case of cybercrime is serious enough, even extradition should be considered, which may raise other issues such as dual criminality. For international co-operation to function effectively, substantive offences and procedural powers in one jurisdiction should be compatible with those in another. In this context, it is also advisable to assess the provisions of procedural law and international co-operation proposed in the Convention on Cybercrime (2001).

In the prosecution stage, many issues may arise in regard to substantive and/or procedural law, especially when prosecutors try to apply provisions designed for physical goods to the intangible and ephemeral world of digital goods. Prosecutors have to examine the interpretation carefully in deciding whether and whom to prosecute and must frame charges appropriately.

In the trial stage, difficulties in reconciling procedural law and digital evidence may arise. In jurisdictions where there are strict rules governing the admissibility of evidence, or even in jurisdictions where there are no such explicit rules, disputes may arise as to whether or how judges or fact finders can examine intangible data evidence. Cybercrime cases involving large volumes of evidence may also pose new questions for practitioners. Cybercrime offences usually require criminal intent, and the way such intent is proved may vary from jurisdiction to jurisdiction. Since such offences are relatively new to judges, it is advisable to study trends and aggravating or mitigating factors in sentencing in other jurisdictions in order to sentence cyber criminals appropriately.

We will focus on these legal and practical issues relating to cybercrime and explore effective measures to address them in this Training Course.

4. Objectives

This Training Course aims at exploring ways to improve the criminal justice system to combat cybercrime in the respective countries, by examining and analysing the current situation, problems and challenges in regard to the following subtopics:

(1) Current situation and issues in the respective countries of illegal or harmful activities in the field of information and communication technology (ICT), especially concerning the criminalization of cybercrime (crimes in which computers or the computer network are the targets or the instruments) listed below:
   (a) Offences defined in the Convention on Cybercrime (2001) and its Additional Protocol:
      (i) Offences against the confidentiality, integrity and availability of computer data and

systems (illegal access, illegal interception, data/system interference, misuse of devices);
- Computer-related forgery, computer-related fraud;
- Content-related offences (child pornography, racism and xenophobia);
- Offences related to infringements of copyright.

(b) Other offences in which computers or computer networks are the targets or the instruments (e.g. identity-related offences, fraud using the Internet, inducing or assisting violent, drug, economic or sex crimes using e-mails or websites, defamation).
(NB: for the purpose of preparing their individual presentation papers, participants are requested to mention whether offences listed in (a) above are criminalized in their respective countries. In regard to the definition of each offence, please refer to the Convention on Cybercrime (2001) and its Additional Protocol.)

(2) Legal or practical issues and measures for investigation, prosecution and adjudication of cybercrime.
(a) Issues and measures concerning cybercrime investigation:
(i) Initial information gathering (reporting system, cyber patrol, etc.);
(ii) Tracing and identifying criminals (co-operation with other public/private agencies, establishing 24-hour co-operation networks, etc.);
(iii) Preserving and collecting evidence (fair and timely search and seizure of stored computer data (e.g. large amounts of data, unanticipated but related data, encrypted data), preservation, production or recovery of data, real-time collection of traffic data, interception of content data, etc);
(iv) Digital forensic analysis of evidence (specialized units, expert investigators);
(v) International co-operation (mutual legal assistance, joint investigation, 24/7 contact point network, extradition).
(b) Issues and measures concerning cybercrime prosecution (factors deciding whether, where and whom to prosecute, framing appropriate charges, jurisdictional issues).
(c) Issues and measures concerning cybercrime trial, adjudication and sentencing:
(i) Evidential issues (admissibility of the evidence, managing large volumes or encrypted evidence, expert witnesses);
(ii) Proving criminal intent;
(iii) Methods and factors to decide appropriate sanction.
(NB: for the purpose of preparing their individual presentation papers, participants are requested to explain their existing legal regimes and mechanisms to investigate, prosecute and adjudicate cybercrime in their respective countries).

Course Summary

Lectures

In total, seven lectures were presented by visiting experts, six by ad hoc lecturers and six by the professors of UNAFEI. Three distinguished criminal justice practitioners and scholars from abroad served as UNAFEI visiting experts. They lectured on issues relating to the main theme, and contributed significantly to the Course by encouraging discussions after their own lectures and conversing with the participants on informal occasions. Additionally, distinguished senior officials of the Government of Japan, and university professors, delivered ad hoc lectures. The lecturers and lecture topics are listed on pages 9 and 10.

Individual Presentations

During the first two weeks, each Japanese and overseas participant delivered an individual presentation, which introduced the actual situation, problems and future prospects of his/her country. These papers were compiled onto a Compact Disc and distributed to all the participants. The titles of these individual presentation papers are listed on pages 11 and 12.

Group Workshop Sessions

Group Workshop sessions further examined the subtopics of the main theme. In order to conduct each session effectively, the UNAFEI faculty selected individuals to serve as group members for the sub-topics, based on their response to a questionnaire previously distributed. Selected participants served as chairpersons, co-chairpersons, rapporteurs or co-rapporteurs, and visiting experts and faculty members served as advisers. Each group's primary responsibility was to explore and develop their designated topics in the group workshop sessions. The participants, experts and UNAFEI faculty studied the topics and exchanged their views based on information obtained through personal experience, the individual presentations, lectures and so forth. After the group workshop sessions, reports were drafted based on the discussions in their groups. These reports were subsequently presented in the plenary meetings and report-back session, where they were endorsed as the reports of the Course. Brief summaries of the group workshop reports are provided on pages 13 to 14.

Visits and Special Events

Visits to various agencies and institutions in Japan helped the participants obtain a more practical understanding of the Japanese criminal justice system. In addition to the Course's academic agenda, many activities were arranged to provide a greater understanding of Japanese society and culture, with the assistance of various organizations and individuals, including the Asia Crime Prevention Foundation (ACPF). For more detailed descriptions, please refer to pages 15 to 18.

Lecture Topics

Visiting Experts' Lectures

1) Dr. Marco Gerke (Germany)

• Challenges Related to the Fight Against Cybercrime - Challenges for Law Enforcement Agencies

• Substantive Criminal Law Based on the Budapest Convention on Cybercrime

• Procedural Law and International Co-operation Based on the Budapest Convention on Cybercrime

2) Mr. Joel Michael Schwarz (USA)

• Cybercrime Investigations and Prosecutions in the US

• International Co-operation in Combating Cybercrime - An Overview of Multi-lateral Organization Work, and International Co-operation in Practice

3) Mr. Yunsik Jang (Korea)

• The Current Situation and Countermeasures to Cybercrime and Cyber-Terror in the Republic of Korea

UNAFEI Professors' Lectures

1) Mr. Haruhiko Higuchi, *Professor*, UNAFEI

• Challenges of the Koban (Police Box) System in the 21st Century

2) Mr. Junichiro Otani, *Professor*, UNAFEI

• Prosecution in Japan

3) Mr. Jun Oshino, *Professor*, UNAFEI

• The Courts

4) Mr. Ryuji Tatsuya, *Professor*, UNAFEI

• Institutional Corrections in Japan

5) Ms. Tae Sugiyama, *Professor*, UNAFEI

• The Community-Based Treatment of Offenders System in Japan

6) Mr. Takeshi Seto, *Deputy Director*, UNAFEI

• International Co-operation in Criminal Justice

Ad Hoc Lectures

1) Mr. Yasushi Takahashi
Cybercrime Division, National Police Agency, Japan

• Current Situation of Cybercrime and Countermeasures in Japan

2) Mr. Yoshiro Baba
Criminal Affairs Bureau, Ministry of Justice, Japan

• Legal System against Cybercrime in Japan

3) Mr. Yoichi Kumota
Assistant Director, High-Tech Crime Technology Division, National Police Agency, Japan

• Technical Countermeasures against Cybercrime in Japan

4) Mr. Kenji Miyanishi
Director of International Investigative Operations, National Police Agency, Japan

• Interpol and Countermeasures against Cybercrime

5) Mr. Kenichi Shimada
Public Prosecutor, Shizuoka Public Prosecutors Office, Japan

• Legal Issues in the Investigation and Trial of Cybercrime Cases

6) Mr. Toshihisa Hirakawa
High-Tech Crime Control Center, Tokyo Metropolitan Police Department, Japan

• Investigative Methods for Cybercrime

Individual Presentation Topics

Overseas Participants

1) Mr. Mirza Abdullahel Baqui (Bangladesh)
   • The Criminal Justice Response to Cybercrime

2) Mr. Bafi Nlanda (Botswana)
   • The Criminal Justice Response to Cybercrime: The Botswana Perspective

3) Mr. Elcio Ricardo de Carvalho (Brazil)
   • The Criminal Justice Response to Cybercrime

4) Mr. Sergio Gardenghi Suiama (Brazil)
   • Facing Content-Related Offences in Social Networking Services: A Developing Country Perspective

5) Mr. Napoleon Bonaparte (Indonesia)
   • Criminal Justice in Response to Cybercrime in Indonesia

6) Mr. Saleh Ibrahim Mohammed Altawalbeh (Jordan)
   • The Criminal Justice Response to Cybercrime

7) Mr. Jesus Rodriguez Almeida (Mexico)
   • Introduction to Cybercrime Response by the State of Mexico's Security Agency

8) Mr. Syed Abbas Ahsan (Pakistan)
   • Current Situation and Issues of Illegal and Harmful Activities in the Field of Information and Communication Technology in Pakistan

9) Mr. Gilbert Caasi Sosa (Philippines)
   • Country Report on Cybercrimes

10) Mr. Vijith Kumara Malalgoda (Sri Lanka)
    • Information & Communication Technology Law - Sri Lankan Experience in Recognizing Cybercrime

11) Ms. Lam Chun-fa Rita (Hong Kong)
    • Developments and Challenges in Technology Crime Investigation

12) Mr. Santipatn Prommajul (Thailand)
    • The Criminal Justice Response to Cybercrime

Japanese Participants

17) Mr. Hiroyuki Ito
    • Obstruction of Business and Defamation at Internet Auction: A Case Study

18) Mr. Takuya Matsunaga
    • A Fraud Case Involving the Use of *Key Logger*

19) Mr. Yoichi Omura
    • Current Status of Fraud Cases Using the Internet in Japan

20) Mr. Koji Sakamoto
    • The Current Situation and Issues of Sexual Crime on the Internet in Japan

21) Mr. Nozomu Suzuki
    • Investigation and Prosecution of a Case of Basketball Gambling on the Internet

Group Workshop Sessions

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 Ibrahim Mohammed Altawalbeh	(Jordan)
	Mr. Satipatn Prommajul	(Thailand)
	Mr. Koji Sakamoto	(Japan)
	Mr. Nozomu Suzuki	(Japan)
Visiting Experts	Dr. Marco Gerke	(Germany)
Advisers	Deputy Director Takeshi Seto	(UNAFEI)
	Prof. Jun Oshino	(UNAFEI)
	Prof. Junichiro Otani	(UNAFEI)
	Prof. Tae Sugiyama	(UNAFEI)

Report Summary

Group One discussed the above according to 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; and (3) Challenges in combating trans-border cybercrime, including issues of jurisdiction and international co-operation. The group reached the following conclusions. 1. The Council of Europe Convention on Cybercrime can be a good reference for minimum standards that may be adopted by the participating countries, and some basic rules regarding collection and admissibility of evidence from foreign jurisdictions are necessary. 2. Investigative and judicial mechanisms of international co-operation must be improved; adequate procedural laws may be implemented to assure the preservation of evidence when requested. 3. With regard to international co-operation, training and technical aid should be available to law enforcement officials and others. 4. Amendment of Article 2 of the Convention on Cybercrime to properly address the issue of data espionage should be considered. 5. Diffusion of unsolicited emails should be suppressed; in certain circumstances, spamming may be considered a crime. 6. The general principles of substantive law of the respective countries may be taken into account in matters such as illegal gambling, etc. committed in cyberspace. 7. Private online communication should be protected as a civil right; investigative interception of same should be subject to judicial review. 8. While remote investigation is sometimes the only option available to investigators, it is a controversial issue and should be the subject of in-depth analysis. 9. National legislatures should consider a mandatory 180 day retention period of Internet traffic data. 10. Measures to record the identity of users of public terminals are desirable. 11. There should be no mandatory disclosure of encryption keys and passwords. 12. The principle of "passive personality" ought be considered for addition to the Convention on Cybercrime. 13. There was majority but not unanimous agreement on the importance of strengthening co-operation between local offices of transnational service providers and national authorities in order to identify nationals who use remotely located services to commit crimes.

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. Lam Chun-fa Rita	(Hong Kong)
Co-Rapporteurs	Mr. Napoleon Bonaparte	(Indonesia)
	Mr. Yoichi Omura	(Japan)
Members	Mr. Jesus Ameida Rodriguez	(Mexico)
	Mr. Gilbert Cassi Sosa	(Philippines)
	Mr. Hiroyuki Ito	(Japan)
	Mr. Takuya Matsunaga	(Japan)
Visiting Experts	Dr. Marco Gerke	(Germany)
	Mr. Yunsik Jang	(Korea)
Advisers	Prof. Shintaro Naito	(UNAFEI)
	Prof. Ryuiji Tatsuya	(UNAFEI)
	Prof. Tetsuya Sugano	(UNAFEI)
	Prof. Koji Yamada	(UNAFEI)

Report Summary

Group Two discussed the above topic according to 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; and 5. International co-operation in cybercrime investigation.

The group then made the following recommendations. 1. Improve initial information gathering by: i) educating the public about cybercrime; (ii) improving communication with victims, and training officers in report making; and (iii) increasing cyber-patrol facilities. 2. Undercover online investigations should be improved. 3. Data retention by ISPs and telecoms providers should be enforced and available to criminal justice officials in conducting an investigation. 4. Resources must be devoted to capacity building of specialized units. 5. It is advisable to follow the recommendations of the International Review of Criminal Policy (No. 43 & No. 44) - United Nations Manual on the Prevention and Control of Computer-related Crime (1994), art. 198-209. 6. In each country, a main cybercrime unit should assist smaller units in technically demanding investigations. 7. A regular, formal training course on dealing with digital evidence, should be established (and not restricted to specialists). 8. Training activities should be included in international co-operation programmes and efforts. 9. A properly equipped Computer Emergency Team (CERT) is essential for responding promptly to cyber threats, and government and the private sector should co-operate closely on the operation of such teams. 10. In addressing cross-border investigations, the following are suggested: (i) requests for evidence be made under existing MLAT, MLA or Letter Rogatory procedures; (ii) 24/7 points of contact be utilized; (iii) embassies be utilized; (iv) networks of foreign counterparts be utilized. 11. General recommendations regarding international co-operation include: (i) implementing 24/7 points of contact; (ii) sharing information through regional organizations; (iii) co-operation in legal, operational and technical dimensions; (iv) legal frameworks allowing engagement and joint investigation with foreign countries; (v) using the diplomatic channel to contact other countries' private sector entities or ISPs.

Observation Visits

Date	*Agency/Institution*	*Main Persons Concerned*
Sept. 9	Tokyo Probation Office	• Mr. Kazuo Kasahara (Director, Tokyo Probation Office)
	Tokyo District Public Prosecutors Office	• Mr. Shuji Iwamura (Chief Prosecutor)
	Ministry of Justice	• Mr. Hiroshi Ozu (Vice-Minister of Justice)
Sept. 18	Internet Hotline Center	• Mr. Akio Kokubu (Director) Mr. Seiji Yoshikawa (Deputy Director)
	High-Tech Crime Control Center	• Mr. Toshihisa Hirakawa (Leader, Intelligence Section)
Oct. 1	Tokyo District Court	• Mr. Hiroyuki Katsuno (Chief of Criminal Filing and Records Section)
	The Supreme Court	• Mr. Yuki Furuta (Justice)

Group Study Tour

Date	*Location*	*Agency/Institution*	*Main Persons Concerned*
Sept. 24	Kyoto	High-Tech Crime Control Office	• Ms. Masako Koyama (Chief)
Sept. 25	Kobe	Kobe Customs Headquarters	• Mr. Hiroshi Yamamoto (Deputy Director General)
	Hiroshima	Hiroshima Prison	• Mr. Hiroyuki Yoshida (Deputy Warden, Classification Division)
Sept. 26	Hiroshima	6th Regional Coast Guard Headquarters	• Mr. Minoru Kono (Chief of Planning Section, General Affairs Division)

Special Events

Sept. 1 *Welcome Party*

Sept. 4, 5, 8 *Japanese Conversation Classes*

The overseas participants attended three Japanese conversation classes and learned practical Japanese expressions. The *sensei* (teachers) were Ms. Junko Toyoguchi and Ms. Tomoko Toriya of JICE.

Sept. 9 *Courtesy Visit to the Ministry of Justice and Reception by the Vice-Minister of Justice*

After visiting the Ministry of Justice, a reception was held by the Vice-Minister of Justice, Mr. Hiroshi Ozu, at the Ministry of Justice, Tokyo.

Sept. 11 *UNAFEI Olympics*

The UNAFEI Olympic Games were held on the grounds of the Training Institute for Correctional Personnel. The participants competed in such events as racket relay, tug of war and the true or false quiz. Afterwards, the participants enjoyed a social with UNAFEI staff and faculty.

Sept. 17 *TICP Friendship Party*

The participants enjoyed a friendship party hosted by the Training Institute for Correctional Personnel, in Fuchu. The participants enjoyed demonstrations of Japanese games and sports such as *suika wari* and *karate*.

Sept. 20, 21 *Home Visits*

ACPF Fuchu Branch kindly organized dinners for the participants in the homes of their members. The hosts were Mr. Kiyotomo Terashima, Mr. Rinshi Sekiguchi, Ms. Hiroko Maekawa and Ms. Chitose Sashida.

Oct. 3, 4 *ACPF Branches Study Tour*

The participants were invited to visit branches of the ACPF in six locations around Japan. The participants split into groups and visited Aomori, Iwate, Nagano, Nagoya, Osaka and Sapporo. They visited local criminal justice facilities and had an opportunity to do some sightseeing. In addition, each branch held a reception in honour of the participants visiting their region.

Oct. 8 *Visit to Fuchu Daikyu Elementary School*

The participants visited Fuchu Daikyu Elementary School where they had the opportunity to observe a Japanese school, talk to the students and teachers, and take part in traditional Japanese games.

Oct. 8 *Suntory Brewery Visit*

The participants visited the Suntory brewery where they were given a guided tour. Afterwards the Fuchu Rotary Club hosted a very enjoyable party.

Oct. 9 *Farewell Party*

A party was held to bid farewell to all the participants.

Reference Materials

A. United Nations Documents

1. The International Review of Criminal Policy (No. 43 and No. 44): *United Nations Manual on the Prevention and Control of Computer-related Crime* (1994)
2. Combating the Criminal Misuse of Information Technologies (A/RES/55/63) (2000)
3. Crime Related to Computer Networks-Background Paper for the Workshop on Crimes Related to the Computer Network: Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders (A/CONF.187/10) (2000)
4. Background paper for the Workshop on Measures to Combat Computer-related Crime: Eleventh United Nations Congress on Crime Prevention and Criminal Justice (A/CONF.203/14) (2005)

B. Council of Europe Documents

1. Convention on Cybercrime (ETS 185)
2. Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (ETS 189)
3. Explanatory Report to the Convention on Cybercrime
4. Explanatory Report to Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems
5. Guidelines for the Cooperation between Law Enforcement and Internet Service Providers against Cybercrime

C. Group of Eight Documents

1. G8 1997 Communique (Principles and Action Plans to Combat High Tech Crime)
2. Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations (1999)
3. Best Practices for Network Security, Incident Response and Reporting to Law Enforcement (2004)
4. Best Practices for Law Enforcement Interaction with Victim-Companies during a Cybercrime Investigation (2005)

D. Other Related Materials

1. Model Law of Computer and Computer Related Crime (Commonwealth Secretariat, 2002)
2. Resource Materials on Technology-enabled Crime (Gregor Urbas and Kim-Kwang Raymond Choo, Australian Institute of Criminology, 2008)
3. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" Manual (Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice; 2002)
4. "Prosecuting Computer Crimes" Manual (Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice; 2007)

Experts and Participants List

Visiting Experts

Dr. Marco Gerke	Council of Europe Expert/ Lecturer University of Cologne Germany
Mr. Joel Michael Schwarz	Computer Crime and Intellectual Property Section Criminal Division US Department of Justice USA
Mr. Junsik Jang	Professor/Senior Inspector Department of Police Science Korea National Police University Republic of Korea

Overseas Participants

Mr. Mirza Abdullahel Baqui	Superintendent of Police Satkhira Bangladesh
Mr. Bafi Nlanda	Public Prosecutor Directorate of Public Prosecutions Botswana
Mr. Elcio Ricardo de Carvalho	Federal Criminal Expert First Class Technical-Scientific Directorate Federal Police Department Ministry of Justice Brazil
Mr. Sergio Gardenghi Suiama	Federal Prosecutor Cybercrime Division Co-ordinator Cybercrime Division Federal Attorney's Office for the State of Sao Paolo Brazil
Mr. Napoleon Bonaparte	Deputy Director Crime Investigation Department, South Sumatera Police Region Indonesian National Police Indonesia

Mr. Saleh Ibrahim Mohammed Altawalbeh	Head of Operation Division in North Region Public Security Directorate Jordan
Mr. Jesus Rodriguez Almeida	Director of Intelligence State of Mexico Security Agency Mexico
Mr. Syed Abbas Ahsan	Superintendent of Police Islamabad Capital Territory Police Pakistan
Mr. Gilbert Cassi Sosa	Chief Anti-Transnational Crime Division Criminal Investigation and Detection Group Philippine National Police Philippines
Mr. Vijith Kumara Malalgoda	Deputy Solicitor General Criminal Division Attorney General's Department Sri Lanka
Ms. Lam Chun-fa Rita	Senior Computer Forensics Examiner Technology Crime Division Hong Kong Police Force Hong Kong SAR
Mr. Santipatn Prommajul	Deputy Superintendent High Tech Crime Center Royal Thai Police Thailand

Japanese Participants

Mr. Hiroyuki Ito	Public Prosecutor Osaka District Public Prosecutors Office
Mr. Takuya Matsunaga	Public Prosecutor Fukuoka District Public Prosecutors Office Kokura Branch
Mr. Yoichi Omura	Assistant Judge Tokyo District Court
Mr. Koji Sakamoto	Judge Osaka District Court
Mr. Nozomu Suzuki	Public Prosecutor Fukushima District Public Prosecutors Office

INFORMATION ABOUT FORTHCOMING PROGRAMMES

1. The 11th International Training Course on the Criminal Justice Response to Corruption

The 11th International Training Course on the Criminal Justice Response to Corruption will be held from 16 October to 14 November 2008. Twenty overseas participants, including five observers, and four Japanese participants, will attend.

2. The Ninth Country Focused Training Course on the Juvenile Delinquent Treatment System for Kenya

The Ninth Country Focused Training Course on the Juvenile Delinquent Treatment for Kenya will be held from 5 to 27 November 2008. Twelve participants, including one volunteer children's officer, will attend.

3. The Regional Forum on Good Governance for East Asian Countries

The Regional Forum on Good Governance for East Asian Countries will be held on the 10 and 11 December 2008 and will focus on the "Strengthening of Domestic and International Co-operation for Effective Investigation and Prosecution of Corruption". Senior criminal justice officials from 13 East Asian countries, including Japan, and a visiting expert will attend.

4. The 141st International Senior Seminar

The 141st International Senior Seminar will be held from 13 January to 13 February 2009. The theme of the Seminar will be "The Improvement of the Treatment of Offenders Through the Enhancement of Community-Based Alternatives to Incarceration". Approximately 28 government officials from Japan and overseas will attend, as well as visiting experts from Asian and Western countries.

Rationale

The main theme of this course is the improvement of the treatment of offenders through the enhancement of community-based alternatives to incarceration.

It is true that the detention of offenders is one of the most basic measures used by criminal justice systems to secure proper legal procedures in the investigation and trial of criminal offences, and is also important in maintaining justice and security in the community during the execution of a sentence. On the other hand, however, it is insufficient to impose blanket detention on all offenders, for a number of reasons: firstly, in consideration of the humanitarian principle of avoiding restricting prisoners' rights more than is necessary; secondly, to avoid the problem of prison overcrowding; and thirdly, to enhance correctional and community treatment to meet offenders' individual requirements ("Evil communications corrupt good manners").

The United Nations Standard Minimum Rules for Non-Custodial Measures (the Tokyo Rules), which were adopted by the United Nations General Assembly on the basis of a recommendation by the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders in 1990, provide guidelines and basic principles for diversified non-custodial measures. The Tokyo Rules aim at reducing the use of incarceration and rationalizing criminal justice policies by enhancing community-based approaches in order to alleviate problems relating to prison overcrowding and encourage the reintegration of offenders into the community. In response to this situation, "The Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-First Century", adopted by the Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Vienna in 2000, stressed the importance of promoting effective

alternatives to incarceration in order to contain the growth and overcrowding of correctional facilities' populations. As a follow-up, plans of action for the implementation of the Vienna Declaration were adopted by the Commission on Crime Prevention and Criminal Justice in 2002, which includes a paragraph on action on prison overcrowding and alternatives to incarceration. It encourages Member States to prioritize Non-Custodial Measures to imprisonment where possible. It also recommends educating the public on the meaning and effect of alternatives to imprisonment and how they work. Additionally, The Bangkok Declaration: "Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice", adopted by the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok in 2005, also stressed the importance of further developing restorative justice policies, procedures and programmes that include promoting effective alternatives to prosecution, thereby avoiding the possible adverse effects of imprisonment, helping to rehabilitate offenders.

Based on these plans, various alternative measures such as suspension of prosecution, community service, fine, suspended pronouncement of sentence/suspended sentence, probation, parole, etc. have been taken by many countries at both the pre-sentencing and post-sentencing stages.

However, despite the introduction of these measures and policies, the continuous increase of the prison population and subsequent overcrowding is still one of the most pressing problems in criminal justice in many countries. Also, the degree to which community-based alternatives to incarceration of offenders have been adopted varies a great deal from country to country. Sometimes, although officially adopted, community-based alternatives to incarceration do not become functional because of insufficient understanding and support from criminal justice practitioners. Furthermore, the lack of acceleration of community-based alternatives to incarceration can be traced in part to public misunderstanding of the meaning and the effect of such programmes. Therefore, there is a need to educate the public on the importance of community-based alternatives to incarceration.

It is very important to enhance community-based alternatives to incarceration for the purpose not only of reducing the number of offenders who are subject to custodial measures but also to enhance rehabilitation and reintegration into society, to prevent recidivism. Community-based treatment should include guidance, supervision and support for offenders as well as encouragement and help in avoiding conflict and other temptations. Such treatment is practical, considering that the vast majority of offenders will return to the community after completing their sentences. Consequently, community-based alternatives to incarceration are implemented in order to realize effective criminal justice administration, balanced with the necessity of detention.

Objectives

The purpose of this Seminar is to offer participants an opportunity to share experiences and knowledge regarding community-based alternatives to incarceration. In order to achieve this purpose, the Seminar programme will provide an opportunity to clarify the current situations and problems existing in the respective countries in the field of community based alternatives to incarceration. There will also be an opportunity to build participants' knowledge of possible measures to enhance community based alternatives to incarceration at all stages of the criminal justice process. Among the major topics to be studied are the following:

(1) Current situations and problems of community-based alternatives to incarceration which are implemented through supervision and aftercare of offenders at each stage of criminal proceedings:
    - Suspension of prosecution
    - Bail
    - Community service
    - Fine
    - Suspended pronouncement of sentence/suspended sentence
    - Probation

• Parole, etc.

(2) Possible measures to enhance community based alternatives to incarceration:

(a) Measures such as the above mentioned community based alternatives to incarceration;

(b) Other measures to facilitate community based alternatives to incarceration:

• Enhancing training programmes to further develop the ability of staff responsible for the treatment of offenders;

• Enhancing the involvement of private collaborators (volunteers, NGOs, neighbourhood community associations, etc.) and strengthening their expertise;

• Enlightening the general public on crime prevention activity and the treatment of offenders;

• Establishing a co-operative scheme among all parties concerned.

ADMINISTRATIVE NEWS

Overseas Trips by Staff

Director Keiichi Aizawa, Deputy Director Takeshi Seto, Mr. Shintaro Naito (Professor), Mr. Etsuya Iwagami (Staff), and Mr. Ikuo Kosaka (Staff) visited Bangkok, Thailand from 20 to 26 July 2008 as co-hosts of the Second Regional Seminar on Good Governance for Southeast Asian Countries. The focus of the Seminar was "Corruption Control in Public Procurement".

Ms. Tae Sugiyama (Professor) and Mr. Tetsuya Sugano (Professor) visited Kenya from 26 July to 22 August 2008 and 1 August to 5 September 2008 respectively. The purpose of the trip was to visit children's institutions, observe the conditions of the treatment of children and the activities of volunteer children's officers, and exchange ideas with and provide advice to the staff of the Children's Department of the Ministry of Gender, Children and Social Development. The professors also gave lectures at training seminars.

Deputy Director Takeshi Seto and Mr. Junichiro Otani (Professor) visited Costa Rica and Argentina from 16 to 30 August 2008. In Costa Rica they jointly hosted with ILANUD an international training course on Criminal Justice System Reforms in Latin America in which ten countries participated. In Argentina, they held a follow-up seminar focusing on the particular situation in that country.

Director Keiichi Aizawa, Mr. Koji Yamada (Professor) and Mr. Yuichi Shirakawa (Staff) visited Ulan Bator, Mongolia from 25 to 30 August 2008 to attend the 12th ACPF World Conference.

Mr. Shintaro Naito (Professor) visited Singapore from 26 to 30 August 2008 to attend the 13th Annual Conference and General Meeting of the International Association of Prosecutors.

FACULTY AND STAFF OF UNAFEI

Faculty:

Mr. Keiichi Aizawa	Director
Mr. Takeshi Seto	Deputy Director
Mr. Motoo Noguchi	Professor
Mr. Haruhiko Higuchi	Professor
Ms. Tae Sugiyama	Professor, Chief of Information and Library Service Division
Mr. Tetsuya Sugano	Professor, Chief of Research Division
Mr. Jun Oshino	Professor, Chief of Training Division 140th Course Programming Officer
Mr. Ryuji Tatsuya	Professor, 140th Course Deputy Programming Officer
Mr. Koji Yamada	Professor
Mr. Shintaro Naito	Professor
Mr. Junichiro Otani	Professor
Ms. Grace Lord	Linguistic Adviser

Secretariat:

Mr. Sakumi Fujii	Chief of Secretariat
Mr. Hitoshi Nakasuga	Co-Deputy Chief of Secretariat
Mr. Masato Fujiwara	Co-Deputy Chief of Secretariat

General and Financial Affairs Section:

Mr. Masaaki Kojitani	Chief
Mr. Fumihiro Nakayasu	Officer
Mr. Atsushi Takagi	Officer
Ms. Kayoko Ono	Officer

Training and Hostel Management Affairs Section:

Mr. Etsuya Iwakami	Chief
Mr. Yuichi Kitada	Officer, 140th Course Assistant Programming Officer
Mr. Ikuo Kosaka	Officer
Mr. Yuichi Shirakawa	Officer
Ms. Akane Uenishi	Officer

International Research Affairs Section:

Mr. Kenichiro Koiwa	Chief
Ms. Masumi Tomita	Librarian

Secretarial Staff:

Ms. Miki Usuki
Ms. Aiko Ota

Kitchen:

Mr. Yuji Matsumoto Chef

JICA Co-ordinator:

Ms. Yasuko Ono