ISSN 1020-914X

UNAFEI NEWSLETTER

UNAFEI

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

No. 147
June 2015

Established
1961

IN THIS ISSUE

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 160th International Training Course on "The State of Cybercrime: Current Issues and Countermeasures", which took place from 13 May to 17 June 2015. In this Course, we welcomed 7 Japanese participants and 22 overseas participants: 12 from Asia, 3 from Africa, 3 from the Americas, 2 from Europe and 2 from Oceania. The participants included judges, prosecutors, law enforcement officers, and other public officials. As this newsletter demonstrates, the Course was extremely productive. It consisted of lectures by visiting experts, ad hoc lecturers, and faculty members, individual presentations, visits to relevant criminal justice agencies, and group-workshop and plenary sessions.

In 2001, 30 countries, including Japan, signed the Convention on Cybercrime. The Convention aimed to counter cybercrime by harmonizing criminal legislation and establishing closer international cooperation. Nevertheless, criminal justice practitioners from developed and developing countries alike still face numerous challenges in the investigation and prosecution of cybercrime. These challenges include rapidly changing technology, the anonymity of cybercriminals and the borderless nature of cybercrime.

UNAFEI, as one of the institutes of the United Nations Crime Prevention and Criminal Justice Programme Network, held this Course to offer participants an opportunity to clarify and analyse the current situation of cybercrime in each participating country and to explore more effective ways to combat it. Additionally, the participants were able to share experiences, gain knowledge, and build a human network of counterparts.

During the Course, the participants diligently and comprehensively examined the course theme, 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. With the academic and practical input from the visiting experts, ad hoc lecturers and UNAFEI faculty—and the in-depth discussions they had with each other—the participants are now better equipped to cope with the challenges of cybercrime.

I would like to offer my sincere congratulations to all of the participants upon their successful completion of the Course, made possible by their strenuous efforts. My heartfelt gratitude goes out 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 cooperation extended to UNAFEI by various agencies and institutions that helped diversify the Course.

I would also 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 towards the benefit of international society as a whole.

Finally, I would like to reiterate my best regards to the participants of the 160th 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.

June 2015

YAMASHITA, Terutoshi

YAMASHITA, Terutoshi
Director, UNAFEI

THE 160TH INTERNATIONAL TRAINING COURSE

THE STATE OF CYBERCRIME: CURRENT ISSUES AND COUNTERMEASURES

Course Rationale

The spread and development of information and communication technologies (ICT) is transforming society and human life drastically and fundamentally. The Internet not only provides people with access to information from all over the world in an instant but also has become a forum for self-expression, socializing and business, including as a means of settling payments. "Cyberspace", including the Internet, has developed and expanded rapidly, and now it has become an essential element of various social and economic activities. Although the development and expansion of cyberspace has brought great convenience and benefits, it has also produced cybercrime, which causes grave damage.

Cybercrime was defined in this training course as crimes in which computers or computer networks are the target (e.g., unauthorized access and damage to, or the modification of, computer data or programmes) or the instrument used to commit the crime (e.g., fraud, forgery, child pornography, defamation, and infringement of intellectual property). Cybercrime is committed by taking advantage of the characteristics of cyberspace: anonymity, diffusion, lack of traceability, lack of time constraints and lack of restrictions on place; and it can cause grave damage to many people in an instant.

Cybercrime is also borderless, and it will continue to increase as cross-border computer networks have made striking progress by the rapid spread of mobility, such as through smartphones and development of cloud computing. Moreover, cybercriminals exploit computer terminals in developing countries which have insufficient security measures as platforms to commit crimes in the other countries. Therefore, international support for developing countries is one of the greatest concerns throughout the world. In view of the current state of affairs, many efforts have been made at various levels for international harmonization or cooperation to tackle the issue.

a. 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. Through its resolutions on Combating the Criminal Misuse of Information Technology (55/63 (2000) and 56/121 (2001)), the UN General Assembly invited States to take into account measures to combat computer misuse. In December 2010, the First Committee of the United Nations General Assembly established the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. From October 2012 to June 2013, that group discussed norms, rules and principles of responsible behaviour by States, confidence-building measures and the exchange of information, and capacity-building measures regarding cyberspace.

b. Other International Efforts

(i) Convention on Cybercrime

The Convention on Cybercrime, the world's first convention against computer crime, was established and adopted at the Council of Europe (CE) in 2001. After the Convention was adopted at the Committee of Ministers, the signing ceremony was held in Budapest, Hungary in November 2001, and 30 countries, including Japan, signed the Convention at the ceremony.

The purpose of the Convention on Cybercrime is to create an international framework for the prevention and suppression of cross-border cybercrime. The Convention provides that the signatory countries shall establish substantive criminal laws (such as a law criminalizing the production of computer viruses), establish criminal procedure laws (such as a law empowering investigating authorities to execute the protection, search, and seizure of computer data), and cooperate internationally in the extradition of criminals. As of December 2014, 44 countries have ratified or acceded to the Convention.

(ii) Efforts by the G8 Subgroup on High-Tech Crime

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 Principles and Action Plan to combat High-tech Crime, aiming to ensure international cooperation and the improvement of legal systems in the participating countries. 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.

(iii) Efforts by the International Criminal Police Organization (ICPO)

The ICPO established The INTERPOL Global Complex for Innovation in Singapore in September 2014, which emphasizes: innovative research and development for identification of crimes and criminals and enhancing the database capability, capacity building and training for investigators in the field of cybercrime, 24-hour operational support to police. Further, the ICPO has built a framework to support the investigation of cybercrime worldwide.

(iv) International Conferences

In 2011, the London Conference on Cyberspace brought together ministers, senior government officials, industry leaders, and representatives of the Internet technical community and civil society. In all, more than 700 participants from 60 countries took part. In this conference, they identified cybercrime as a significant threat to economic and social well-being, and as one which requires a concrete and urgent international effort, they must work collectively to tackle the threat of cybercrime and ensure there is no safe haven for those who commit cybercrime. Following this conference, the 2012 Budapest Conference on Cyberspace and the 2013 Seoul Conference on Cyberspace were held. The "Seoul Framework for and Commitment to Open and Secure Cyberspace" was issued at the Seoul Conference on Cyberspace.

In order to deter cybercrime and tackle it effectively, it is important that frontline criminal investigators share their knowledge on cybercrime and digital forensics. If investigators do not have such basic knowledge, they will have difficulties tracing cybercrime offenders and collecting and preserving evidence. Moreover, there is a real possibility that they will not be able to recognize the occurrence of cybercrime and the damages that arise from it. They also must understand the necessity of due process, as cybercrime investigations are often confronted with issues such as the right of privacy. Additionally, investigators must be familiar with possible measures of international cooperation and with its procedures because informa-

tion sharing and mutual legal assistance are indispensable in view of the cross-jurisdictional nature of cybercrime.

Cybercrime causes various problems during the prosecution and trial stages. Prosecutors must properly charge cybercrime after careful evaluation and analysis of digital evidence. To do so, they must have adequate knowledge of the characteristics of cybercrime. Prosecutors must also prove their cases in court by making effective use of digital evidence. Likewise, judges have to determine the facts of the case with a proper understanding of digital evidence, and they must determine the appropriate sentencing by considering the damages caused by cybercrime. Often these damages are significant, but they are hard to detect.

It is not necessarily for criminal justice officials to have high levels of expert knowledge or advanced technology. There is no doubt that the training for the experts who specialize in the field of cybercrime is extremely important and an urgent matter for the every country. At the same time, many criminal justice officials must have basic knowledge and use appropriate measures to tackle cybercrime in general as cybercrime is no longer a rare crime but a common and daily crime which is rampant in society. Criminal justice officials who have basic knowledge of cybercrime can seek assistance from experts at every stage of the criminal justice system, and that is the best way to tackle cybercrime.

Therefore, the aim of this training course was that participants would gain the basic knowledge and techniques necessary for their daily duties and that they would learn to recognize the threats and characteristics of cybercrime, which will ultimately improve the investigation, prosecution and adjudication of cybercrime. Moreover, they would be able to establish an effective multinational network of criminal justice professionals through this international training course.

Objectives of the Course

The purpose of this training course was to offer participants an opportunity to share experiences and knowledge regarding measures for tackling cybercrime. In order to achieve this purpose, the training course provided an opportunity to clarify the current situations and problems existing in the participating countries in the field of measures against cybercrime. The participants also built their knowledge of possible ways to enhance measures for tackling cybercrime at all stages of the criminal justice process. Among the major topics studied were the following:

Key Topics of the Course

The following are key topics that were addressed during the Course:

1. The characteristics of cybercrime around the world.
    1) Types of cybercrime and modus operandi
    2) Damages caused by cybercrime

2. Basic knowledge of computer networks
    1) Basic elements of storage devices and computer networks
    2) Basic elements of security systems
    3) Basic techniques for unauthorized computer access and hacking

3. Issues in the investigation, prosecution and adjudication of cybercrime

1) Initial information gathering
   (a) Cyberpatrols
   (b) Reporting systems (establishment of hotline call centers etc.)

2) Tracing and identifying criminals, preserving and collecting evidence
   (a) Tracing and identifying by IP address and other measures
   (b) Fair and timely search, seizure and preservation of digital evidence
   (c) Real-time collection of traffic data, interception of content data
   (d) Technical analysis of digital data

3) Prosecution
   (a) Appropriate evaluation of digital evidence
   (b) Identifying criminal acts and proper selection of cybercrime charges

4) Adjudication
   (a) Issues concerning the law of evidence
   (b) Clear presentation of digital evidence
   (c) Legal elements necessary to obtain conviction

4. International cooperation
   1) International assistance in investigation and joint investigation
   2) Extradition
   3) Establishment of 24/7 contact point and utilization

5. Cooperation between the public and private sectors
   1) Cooperation with Internet Service Providers
   2) Technical assistance for investigation by experts

6. Capacity building
   1) Employment and training of experts who are highly specialized in the field of cybercrime
   2) Training system for criminal justice officials

Each participant was required to submit an Individual Presentation Paper regarding the above-mentioned topics as they apply to his or her country, and to explain and discuss these topics in his or her individual presentation.

Course Summary

Lectures

In total, the participants attended 41 lectures, including 10 presented by the visiting experts, 5 by ad hoc lecturers and 4 by the faculty of UNAFEI. Four distinguished criminal justice practitioners served as UNAFEI's visiting experts. They lectured on issues relating to the main theme of the Course and contributed significantly beyond their lectures by encouraging discussions after their lectures, participating in the discussions of other programmes, and conversing with the participants on informal occasions. Additionally, the ad hoc lectures were delivered by officials from the National Police Agency of Japan, the Supreme Public Prosecutor's Office, and from private sector IT companies. The lecturers and lecture topics are listed on pages 8 to 10.

Individual Presentations

During the first three weeks, all participants delivered individual presentations which introduced the situation, problems and future prospects of the participants' countries. These papers were compiled onto a USB memory stick and distributed to all the participants. The titles of these individual presentation papers are listed on pages 11 to 13.

Group Workshop Sessions

Group workshop sessions provided the participants with the opportunity to further examine the sub-topics 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 responses to a previously distributed questionnaire. Selected participants served as chairpersons, co-chairpersons, rapporteurs or co-rapporteurs, 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 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 report-back session, where they were endorsed as the reports of the Course. Brief summaries of the group workshop reports are provided on pages 14 to 16.

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 17 to 19.

Lecture Topics

Visiting Experts' Lectures

1) Dr. Kim-Kwang Raymond CHOO

   • The Cyberthreat Landscape

   • Contemporary Digital Forensic Investigations

2) Mr. Fernando FERNANDEZ LAZARO

   • Current Cybercrime Situation and INTERPOL's Role & Efforts Combating Cybercrime

   • Best Practice of Joint International Cybercrime Investigation

   • Cybercrime trend: malware

3) Mr. HONDA Yuki

   • Current Cybercrime Situation and INTERPOL's Role & Efforts Combating Cybercrime

   • Best Practice of Joint International Cybercrime Investigation

   • Basic OSINT (Open Source Intelligence)

   • Basic Log Analysis

4) Prof. Dr. Marco GERCKE

   • International legal framework against cybercrime including the Convention on Cybercrime

   • Future Challenges on the Legislation against Cybercrime and Countermeasures

   • Exercise of the mock trial for Cybercrime

UNAFEI Professors' Lectures

1) Mr. MORINAGA Taro, Deputy Director, UNAFEI

   • Basics of Japanese Criminal Procedure

2) Mr. MORIYA Kazuhiko, *Professor*, UNAFEI

• Flow of Criminal Justice Procedure in Japan

3) Mr. KAYA Tomonobu, *Professor*, UNAFEI

• The Criminal Justice System in Japan: Japanese Police

4) Mr. HIROSE Yusuke, *Professor*, UNAFEI

• Japan's Legislative Response to Cybercrime

5) Mr. YUKAWA Tsuyoshi, *Professor*, UNAFEI

• International Assistance in Investigation

Ad Hoc Lectures

1) Mr. KIMURA Kimiya
Superintendent, Assistant Director, Cybercrime Division, National Expert For Cybercrime Investigation, National Police Agency

• Countermeasures against Cybercrime

Mr. TANAKA Ryuji
Section Chief/Chief Inspector, Cybercrime Division, National Police Agency

• Basic Strategy for Cyber Crime in Japan

2) Mr. SUZUKI Humihito
Network Security Specialist, NI Staff Incorporated

• The Fundamentals of Cybersecurity

3) Mr. NAKANISHI Motohiro
Information-Technology Promotion Agency (IPA), IT Security Center, Technology Headquarters

• 10 major Security Threats—Threat Trends and Countermeasures

4) Mr. SUGIURA Kazuhiko
Senior Vice President, AOS Legal Tech Inc.

• Digital Forensic Technology in Recent Years

5) Mr. YAMAGUCHI Takaaki
Public Prosecutor, The Public Prosecution Reform Promotion Office, The Supreme Public Prosecutors Office

• Investigation and Prosecution of Cybercrime in Japan (Case Studies)

Individual Presentation Topics

Overseas Participants

1) Mr. Kunlay TENZIN (Bhutan)

   • The State of Cybercrime in Bhutan

2) Mr. Werton Magalhaes COSTA (Brazil)

   • The State of Cybercrime: Current Issues and Countermeasures

3) Mr. CHAY Chandaravan (Cambodia)

   • The Current Situation: Issues and Countermeasure

4) Mr. DIABATE Djakaridja (Cote d'Ivoire)

   • The State of Cybercrime: Current Issues and Countermeasures

5) Mr. Joash Odhiambo DACHE (Kenya)

   • The State of Cybercrime: Current Issues and Countermeasures

6) Mr. Thurain Aung (Myanmar)

   • Myanmar's Current Issues and Countermeasures Relating to Cybercrime

7) Mr. Arjun Prasad KOIRALA (Nepal)

   • The State of Cybercrime: Current Issues and Countermeasures

8) Mr. Ramesh Prasad GYAWALI (Nepal)

   • The State of Cybercrime: Current Issues and Countermeasures

9) Mr. Emil Oscar GONZALEZ Pinto (Panama)

   • "The State of Cybercrime" Current Issues and Countermeasures

10) Ms. Judith Del Socorro GOMEZ SERRANO (Panama)

   • The State of Cybercrime: Current Issues and Countermeasures in Panama

11) Mr. Vincent AGUSAVE (Papua New Guinea)

   • The State of Cybercrime: Current Issues and Countermeasures

12) Ms. Irene Cayetano CENA (Philippines)

• Legislation & Criminal Justice Procedure of Cybercrime in the Philippines

13) Ms. Karla Torres CABEL (Philippines)

• Combating Cybercrime in the Philippines

14) Mr. Faatasi PULEIATA (Samoa)

• Cybercrime—Current Issues and Countermeasures

15) Mr. JEAN BAPTISTE Jeffery Alexis (Seychelles)

• Countermeasures Cybercrime
• Action Plan for Combating Cybercrime in Seychelles

16) Mr. Safarbek NURALIEV (Tajikistan)

• Cybercrime and the Fight against Cybercrime in the Republic of Tajikistan

17) Mr. Wasawat CHAWALITTHAMRONG (Thailand)

• Dangers of Internet Use

18) Mr. Thongchai ITTHINITIKUL (Thailand)

• Prosecuting Computer-Related Crimes in Thailand

19) Mr. Ihor SEKHIN Sergeyovich (Ukraine)

• The State of Cybercrime: Current Issues and Countermeasures

20) Ms. Tetiana PAVLIUKOVETS (Ukraine)

• Cybercrimes: Privacy versus Security during Evidence Preservation and Collection

21) Ms. LAI Thi Thu Ha (Viet Nam)

• Cybercrime in Vietnam: Situation and Some Recommendations for Solutions

22) Ms. NGUYEN Thi Khanh (Viet Nam)

• Issues on Cross-National Tracing and Identification of Criminals and Internal Cooperation in Vietnam

Japanese Participants

23) Mr. HOSHI Takashi

• Investigation of Cybercrime: an Extortion Case with Sexual Intimidation Using Unlawfully Created Electromagnetic Records through the "LINE" Application

24) Ms. KAWABATA Yuko

• Cybercrime in Japan

25) Mr. SATO Hiroyuki

• Laws & Regulations Concerning Cyber Crimes in Japan

26) Mr. SATO Takeru

• Examples of Cybercrime by Individuals and Its Prevention

27) Mr. TOYAMA Katsuya

• Current Situation and Countermeasures against Cyber-Crime (Drug Cases)

28) Mr. UEHARA Taku

• Japan Coast Guard and Cybercrime at Sea

29) Ms. URAOKA Naoko

• A Cybercrime Case in Japan

Group Workshop Sessions

Group 1

EFFECTIVE CYBERCRIME LEGISLATION FROM THE PERSPECTIVE OF ENFORCEMENT PRACTICES

Chairperson	Mr. Werton Magalhaes COSTA	(Brazil)
Co-Chairperson	Mr. Emil GONZALEZ	(Panama)
Rapporteur	Mr. Joash DACHE	(Kenya)
Co-Rapporteur	Ms. Yuko KAWABATA	(Japan)
Members	Mr. Djakaridja DIABATE	(Cote d'Ivoire)
	Mr. Ramesh Prasad GYAWALI	(Nepal)
	Mr. Vincent AGUSAVE	(Papua New Guinea)
	Mr. Jeffery JEAN BAPTISTE	(Seychelles)
	Mr. Ihor SEKHIN	(Ukraine)
	Mr. Hiroyuki SATO	(Japan)
Adviser	Prof. Yusuke HIROSE	(UNAFEI)
	Prof. Tsuyoshi YUKAWA	(UNAFEI)

Report Summary

Focusing on the development of cybercrime legislation, Group 1 used the Convention on Cybercrime (the Budapest Convention) as a basis for discussion and formulation of its recommendations. The group reported that four of the nine participating countries have adopted the Convention and encouraged all states to ratify the Convention as it is the current and foremost global framework on cybercrime.

In considering how long internet service providers should be required to preserve data, the group noted the difference between data preservation (suspicion of crime) and retention (no suspicion of crime). The group members concluded that legislation should require the retention of data for one year; a warrant should be required for data preservation, and the group agreed with the Convention's 90-day preservation period, which can be extended.

The group agreed that domestic legislation must provide for the admissibility of digital evidence. Because this issue is not addressed in the Convention, the group recommended borrowing strategies from regional cybercrime approaches. Conditions for admitting digital evidence should (1) require a chain of custody to guarantee authenticity, (2) maintain victim privacy, and (3) ensure that digital evidence is subjected to forensic examination.

Regarding Internet anonymity, the group agreed that privacy and freedom of expression must be protected. Thus, in line with the Council of Europe's Committee of Ministers' Declaration on Freedom of Communication on the Internet (2003), the group supports Internet anonymity and noted that a prohibition against such anonymity would be difficult to enforce. The group members also considered whether Internet users should be forced to disclose encryption keys during criminal prosecutions and unanimously concluded that users should not be required to do so. The burden of proof is on the prosecution, and the right to remain silent should not be abridged in cybercrime cases. However, law enforcement should be permitted to use advanced investigation techniques that mitigate the problems posed by data encryption.

In addition to its recommendations above, the group members identified numerous enforcement challenges and proposed measures to address them. The challenges identified were: (1) lack of specialized cybercrime laws in most jurisdictions, (2) lack of adequate sanctions to deter cybercrime, (3) the Convention has not been universally adopted, (4) lack of public–private sector coordination, (5) lack of specialized personnel, (6) prohibitive costs of cybercrime investigation and enforcement, and (7) lack of international cooperation frameworks that utilize mutual legal assistance treaties.

Group 2

MEASURES FOR EFFECTIVE INVESTIGATION, PROSECUTION AND ADJUDICATION OF CYBERCRIME CASES

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

Report Summary

Group 2 considered the investigation, prosecution and adjudication of cybercrime cases by engaging in an intensive review of the current practices in each of the participating countries and by identifying challenges to overcome and approaches and measures to improve current practices. In summarizing their discussions, the group focused on effective measures for: (1) generating cybercrime leads, (2) identifying criminals and collecting evidence, and (3) prosecution and adjudication.

A majority of the group members reported that their countries do not conduct cyberpatrolling; members whose countries do conduct cyberpatrolling reported that the private sector is often reluctant to voluntarily submit data records to investigators due to customer-privacy concerns. The group concluded that all countries should adopt laws requiring service providers to furnish necessary information to authorities. All members agreed that it is critical for investigators who receive or generate leads on cybercrime to have sufficient technical skills.

When identifying criminals and collecting evidence of cybercrime, the group agreed that obtaining information such as IP addresses and SIM cards is necessary but not sufficient evidence. IP addresses are often only the beginning of the investigation because perpetrators use proxy servers, TOR onion routers and applications to immediately erase access logs. Requiring registration of SIM cards and the use of cybercrime experts, international cooperation and traditional investigation methods are also necessary to trace cybercriminals.

Regarding prosecution and adjudication, common challenges include document authentication and chain of custody issues; the inadequacy of existing criminal procedure laws at handling cybercrime evidence; and delays in the prosecution of cybercrime cases due to the need for expert witnesses. Solutions to these problems include the adoption of specialized cybercrime laws and procedures, access to forensic laboratories, specialized training for criminal justice professionals and collaboration between prosecutors and expert witnesses to present the cybercrime evidence clearly and simply in court.

The group concluded that there are four key elements to proper investigation, prosecution and adjudication of cybercrime: (1) capacity building of relevant criminal justice professionals; (2) improving public awareness of cybercrime, which involves recognizing and reporting cybercrime to the relevant governmental contact point; (3) encouraging public–private partnerships to collect evidence and share investigation techniques; and (4) enhanced international cooperation coupled with the harmonization of legislation on cybercrime. In addition to the recommendations above, many others were detailed in the group workshop report, which will be published in a forthcoming issue of UNAFEI's Resource Material Series.

Group 3

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

Chairperson	Ms. Tetiana PAVLIUKOVETS	(Ukraine)
Co-Chairperson	Mr. Takeru SATO	(Japan)
Rapporteur	Ms. Irene Cayetano CENA	(Philippines)
Co-Rapporteur	Ms. Thi Khanh NGUYEN	(Viet Nam)
	Mr. Kunlay TENZIN	(Bhutan)
Members	Mr. Thurain AUNG	(Myanmar)
	Mr. Wasawat CHAWALITTHAMRONG	(Thailand)
	Mr. Katsuya TOYAMA	(Japan)
	Mr. Taku UEHARA	(Japan)
Advisers	Prof. Ayuko WATANABE	(UNAFEI)
	Prof. Tsuyoshi YUKAWA	(UNAFEI)

Report Summary

Addressing the topic of suppression and prevention of cybercrime, Group 3 discussed the following issues: (1) establishment of special organizations or units against cybercrime and measures of capacity building for criminal justice practitioners, (2) facilitating international, regional and domestic cooperation among cybercrime agencies, and (3) facilitating public–private partnerships against cybercrime.

Most of the group members agreed that forensic laboratories and other specialized cybercrime units are necessary to handle the complexity of cybercrime cases, but some group members expressed concerns over the organization and administration of such units, as well as conflicts that may result from the overlapping functions of other governmental agencies. Regarding capacity building, the group members agreed that two levels of training should be offered. First, all cyber-practitioners, including police officers and other first responders, should be trained on basic knowledge for handling cybercrime cases and to preserve evidence of cybercrime so that it will be admissible in court. Second, specialized training and certification is necessary for experts who conduct cybercrime investigations.

To coordinate the suppression of cybercrime, the group recommended the establishment of a 24/7 point of contact on the international level that operates in line with the Convention on Cybercrime (the Budapest Convention). In addition to accepting reports of cybercrime from governments and the general public, the centre could share cybercrime intelligence reports and other relevant information. All members of the group agreed that greater cooperation between investigative agencies and digital forensic laboratories is necessary, but there was no consensus on the need for the expertise of private institutions. The debate focused on the perception that private institutions offer the advantage of technical expertise but raised concerns over chain of custody issues involved in relying on a third party analysis of potential cybercrime evidence.

The group agreed that public–private partnerships are essential to the suppression and prevention of cybercrime, and recommended a broad cooperation strategy involving internet service providers (ISPs), telecommunications companies (TELCOs), cooperation with universities and research groups, and enhanced public awareness of cybercrime. The group's recommendations included, among others: (1) requiring international regulation for all ISPs and a strict policy of regulatory permitting to ensure compliance; (2) requiring ISPs to preserve traffic data for at least 90 days with the possibility of extending the preservation requirement; (3) requiring TELCOs to register SIM cards to prevent criminals from concealing their identities; (4) the creation of CERT or CSIRT in each country in cooperation with the private sector. The group concluded that although cybercrime will persist, governments, the private sector and citizens must work together to suppress cybercrime.

Observation Visits

Date	***Agency/Institution***	***Main Persons Concerned***
20 May	Ministry of Justice	• Ms. KAMIKAWA Yoko (Minister of Justice)
26 May	Internet Hotline Centre	• Ms. ITO Yoko (Deputy Head)
29 May	Yokohama District Court	• Ms. HASHIMOTO Tomoko (Senior Officer)
5 Jun.	Metropolitan Police Department Network Crime Investigation Advisory Section	• Mr. HIRAKAWA Toshihisa (Section Chief)

Group Study Tours

Date	***Location***	***Agency/Institution***	***Main Persons Concerned***
10 Jun.	Hiroshima	6th Regional Headquarters' Operations Command Center	• Mr. NISHIMURA Noriaki (Commander)
11 Jun.	Kyoto	Kyoto District Public Prosecutors Office	• Mr. OTANI Kodai (Commander)
12 Jun.	Kyoto	Kyoto Prefectural Police	

Special Events

13 May — *Welcome Party*

15, 18, 19 May — *Japanese Conversation Classes*

The overseas participants attended three Japanese conversation classes and learned practical Japanese expressions. The *sensei* (teachers) were Ms. KOIKE Keiko and Ms. NAGAI Yae from EP Academy.

20 May — *Courtesy Call to the Minister of Justice*
and
Reception by the Vice-Minister of Justice

At the conclusion of their courtesy visit to the Minister of Justice, Ms. KAMIKAWA Yoko, a reception was held for the participants by the Vice-Minister of Justice, Mr. INADA Nobuo, at the Danwa-shitsu lounge on the 20th floor of the ministry building, overlooking Hibiya Park.

22 May — *UNAFEI International Table Tennis Tournament*

The UNAFEI Table Tennis Tournament was held in the auditorium. Mixed teams of international participants, Japanese participants and UNAFEI faculty and staff were formed, and competed against each other. All participants, faculty and staff celebrated later in Lounge B.

23 May — *Grand Sumo Tournament Visit and ACPF Kisei Branch Party*

Following a tour of Ryogoku, including a visit to the Edo-Tokyo Museum, the participants attended the Grand Sumo Tournament at the Ryogoku Kokugikan in Tokyo. They later enjoyed a party hosted by the Kisei Branch of the ACPF held at the Daiichi Ryogoku Hotel.

29 May — *Yokohama Dinner Cruise*

The participants enjoyed a sunset cruise and dinner aboard the *Marine Rouge*, hosted by the ACPF Yokohama branch.

3 Jun. — *The Way of Tea (Tea Ceremony)*

The participants participated in a "*cha-no-yu*" or "*sado*", a formal Japanese tea ceremony, kindly hosted by Soroptimist International Tokyo, Fuchu.

17 Jun. — *Farewell Party*

A party was held to bid farewell to the participants.

Reference Materials

UNAFEI 160TH INTERNATIONAL TRAINING COURSE
LIST OF REFERENCE MATERIALS

A. International Telecommunications Union

A-1 Understanding Cybercrime: Phenomena, Challenges and Legal Response (Prof. Dr. Marco Gercke, 2014)

B. United Nations

B-1 UN Manual on the Prevention and Control of Computer-related Crime (1994)
B-2 Combating the Criminal Misuse of Information Technologies (General Assembly Resolution 55/63, 2001)
B-3 Working Paper for the 12th UN Congress (2010)
B-4 12th UN Congress on Crime Prevention and Criminal Justice (General Assembly Resolution 65/230, 2011)
B-5 Background Paper for the Workshop 3 of the 13th UN Congress (2015)
B-6 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
B-7 UN Convention against Transnational Organized Crime (2004)

C. Council of Europe

C-1 Convention on Cybercrime (2001)
C-2 Explanatory Report of Convention on Cybercrime
C-3 Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (2003)
C-4 Explanatory Report of the Additional Protocol (2-3)
C-5 Guidelines for the Cooperation between Law Enforcement and Internet Service Providers against Cybercrime (2008)
C-6 T-CY (Cybercrime Convention Committee) Guidance Notes (2014)

D. Other

D-1 Commonwealth Model Law on Computer and Computer Related Crime (2002)
D-2 African Union Convention on Cyber Security and Personal Data Protection (2011)
D-3 Materials related Dr. Kim-Kwang Raymond Choo (1-23, Data only)

1 IT standards and guides do not adequately prepare IT practitioners to appear as expert witnesses: An Australian perspective
2 The cyber threat landscape: Challenges and future research directions
3 Cloud computing and its implications for cybercrime investigations in Australia
4 Bridging the Air Gap: Inaudible Data Exfiltration by Insiders
5 Forensic Analysis of Windows Thumbcache files
6 Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users
7 Online child exploitation: Challenges and future research directions
8 Impacts of increasing volume of digital forensic data: A survey and future research challenges
9 Distributed filesystem forensics: XtreemFS as a case study
10 Building the next generation of cyber security professionals

11 Should there be a new body of law for cyber space?
12 iOS anti-forensics: How can we securely conceal, delete and insert data?
13 Windows event forensic process
14 The Oxford handbook of organized crime
15 Data reduction and data mining framework for digital forensic evidence: Storage, intelligence, review and archive
16 Enforcing file system permissions on Android external storage
17 Remote Programmatic vCloud Forensics
18 Mobile Cloud Storage Users
19 A survey of information security incident handling in the cloud
20 Exfiltrating data from Android devices
21 Cyber security readiness in the South Australian Government
22 A generic process to identify vulnerabilities and design weaknesses in iOS healthcare apps
23 Cloud Attack and Risk Assessment Taxonomy

E. Legislation of Japan

E-1 Penal Code
E-2-1 Code of Criminal Procedure (Part 1 and Part 2)
E-2-2 Code of Criminal procedure (Part 3)
E-3 Act on Prohibition of Unauthorized Computer Access
E-4 Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children
E-5 Copyright Act
E-6 Unfair Competition Prevention Act

Expert and Participant List

Visiting Experts

Dr. Kim-Kwang Raymond CHOO	Senior Lecturer University of South Australia Australia
Mr. Fernando FERNANDEZ LAZARO	Coordinator Digital Forensics Laboratory, INTERPOL Digital Crime Centre, INTERPOL Global Complex for Innovation (IGCI) Singapore
Mr. HONDA Yuki	Digital Crime Officer Cyber Fusion Centre, Digital Crime Investigative Support Sub Directorate, INTERPOL Digital Crime Centre, INTERPOL Global Complex for Innovation (IGCI) Japan
Prof. Dr. Marco GERCKE	Director Cybercrime Research Institute Germany

Overseas Participants

Mr. Kunlay TENZIN	Legal Officer Legal Division, Crime and Operations, Royal Bhutan Police Bhutan
Mr. Werton Magalhaes COSTA	Federal Prosecutor Centre Federal Prosecutor Office in the State of Paraiba, Federal Public Prosecution Service in Brazil Brazil

Mr. CHAY Chandaravan	Judge Civil and Criminal Division, Court of Appeal Cambodia
Mr. DIABATE Djakaridja	Judge of Investigation Court of Justice of Yopougon/Abidjan, Ministry of Justice, Human Rights and Public Liberties Cote d'Ivoire
Mr. Joash Odhiambo DACHE	Secretary/CEO Kenya Law Reform Commission Kenya
Mr. Thurain Aung	Senior Investigator (Staff Officer) Nay Pyi Taw Region Division, Seconded to Financial Intelligence Unit, Bureau of Special Investigation Myanmar
Mr. Arjun Prasad KOIRALA	District Judge Lalitpur District Court Nepal
Mr. Ramesh Prasad GYAWALI	District Judge Bajhang District Court Nepal
Mr. Emil Oscar GONZALEZ Pinto	Lawyer Legal Assessor Department, National Police Panama
Ms. Judith Del Socorro GOMEZ SERRANO	District Attorney Public Ministry Panama
Mr. Vincent AGUSAVE	Solicitor in Charge-Goroka Public Solicitor's Office, PNG Government Papua New Guinea

Ms. Irene Cayetano CENA	Chief, Cyber Security Section Anti-Cybercrime Group, Philippine National Police Philippines
Ms. Karla Torres CABEL	Prosecution Attorney II National Prosecution Service, Department of Justice Philippines
Mr. Faatasi PULEIATA	Deputy Registrar of Court Civil & Criminal Courts, Ministry of Justice and Courts Administration Samoa
Mr. JEAN BAPTISTE Jeffery Alexis	Assistant Superintendent Criminal Investigation Division, Seychelles Police Force Seychelles
Mr. Safarbek NURALIEV	Judge Ismoili Somoni District Court of Dushanbe City Tajikistan
Mr. Wasawat CHAWALITTHAMRONG	Head of Technology and Cyber Crime Sector 1 Department of Special Investigation/Bureau of Technology and Cyber Crime, Ministry of Justice Thailand
Mr. Thongchai ITTHINITIKUL	Divisional Public Prosecutor Executive Director's Office of Criminal Litigation 10, Office of the Attorney General Thailand
Mr. Ihor SEKHIN Sergeyovich	Prosecutor Department of Criminal Investigations Supervision, Prosecutor's Office of Transcarpathian Region Ukraine

Ms. Tetiana PAVLIUKOVETS	Prosecutor, Head of Department Department of Criminal Investigations Supervision, Prosecutor's Office of Rivne Region Ukraine
Ms. LAI Thi Thu Ha	Senior Procurator-Assistant, Manager of Division for Scientific Management Institute for Procuratorial Science, Supreme People's Procuracy Viet Nam
Ms. NGUYEN Thi Khanh	Lecturer International Law Department, The University of Prosecution, Supreme People's Procuracy Viet Nam

INFORMATION ABOUT FORTHCOMING PROGRAMMES

1. The Joint Study on the Legal Systems of Japan and Viet Nam 2015 RTI – SPP Exchange Programme Japan Session

From 21 to 27 July 2014, UNAFEI will host The Joint Study on the Legal Systems of Japan and Viet Nam 2015 RTI – SPP Exchange Programme Japan Session in Tokyo, Japan. The theme of the Course is "Current issues of crime and prosecutorial practice in Viet Nam and Japan" and "white paper on crime".

2. The 161st International Training Programme (Group and Region Focus)

From 19 August to 18 September 2015, UNAFEI will host the 161st International Training Course in Tokyo, Japan. The theme of the Course is "Staff Training for Correctional Leadership". Government officials from across Southeast Asia, including Japan, and visiting experts and lecturers will attend.

3. The Seminar on Promoting Community-based Treatment in the ASEAN Region

From 29 September to 1 October 2015, UNAFEI, along with the Rehabilitation Bureau of the Japanese Ministry of Justice, the Department of Probation of Thailand and the Thailand Institute of Justice, will co-host the Seminar on Promoting Community-Based Treatment in the ASEAN Region in Tokyo, Japan. The seminar aims to share strategies for community engagement in the field of community-based treatment of offenders. Government officials and volunteer probation officers across Southeast Asia, including Japan, will attend.

4. The 18th UNAFEI UNCAC Training Programme (Group and Region Focus)

From 14 October to 18 November 2015, UNAFEI will host the 18th UNAFEI UNCAC Training Programme in Tokyo, Japan. Government officials from across Southeast Asia, including Japan, and visiting experts and lecturers will attend.

5. The Ninth Regional Seminar on Good Governance for Southeast Asian Countries

From 24 to 26 November 2015, UNAFEI will host the Ninth Good Governance Seminar in Jakarta, Indonesia. The theme of the Seminar will address "Current Issues in the Investigation, Prosecution and Prevention of Corruption". Government officials from across Southeast Asia, including Japan, and visiting experts and lecturers will attend.

6. Training Programme (Country Focused) on Legal Technical Assistance for Viet Nam

From 2 to 16 December 2015, UNAFEI will host the Training Course on Legal Technical Assistance for Vietnam, in Tokyo, Japan.

ADMINISTRATIVE NEWS

Faculty Changes

Mr. IWASHITA Shinichiro, formerly a professor of UNAFEI, was transferred to the Kumamoto District Public Prosecutors Office on 1 April 2015.

Mr. YUKAWA Tsuyoshi, a public prosecutor of the Sendai District Public Prosecutors Office, was appointed as a professor of UNAFEI on 1 April 2015.

Ms. MIO Yukako, formerly a professor of UNAFEI, was transferred to the Tokyo District Public Prosecutors Office on 1 April 2015.

Ms. WATANABE Ayuko, formerly a public prosecutor of the Tokyo District Public Prosecutors Office, was appointed as a professor of UNAFEI on 1 April 2015.

Ms. TASHIRO Akiko, formerly a professor of UNAFEI, was transferred to the Rehabilitation Bureau on 1 May 2015.

Mr. MINOURA Satoshi, formerly the Chief of the General Affairs and Planning Section, Rehabilitation Bureau, was appointed as a professor of UNAFEI on 1 April 2015.

Overseas Trips by Staff

Professor NAGAI Toru and Professor AKASHI Fumiko visited Phnom Penh, Cambodia, Vientiane, Lao PDR, Hanoi, Viet Nam and Manila, Philippines from 27 February to 11 March 2015 to research the criminal justice systems of the aforementioned countries.

Professor YOSHIMURA Koji visited Yangon, Myanmar from 23 February to March 7 2015 to attend the 4th Asian Conference of Correctional Facilities Architects and Planners (ACCFA) and to research the criminal justice system in Myanmar and to discuss the "Myanmar Country Programme" with related organizations.

Deputy Director MORINAGA Taro visited Bangkok, Thailand and Yangon, Myanmar from 2 to 7 March 2015 to research the criminal justice systems in Myanmar and to discuss the "Myanmar Country Programme" with related organizations.

Professor TASHIRO Akiko, Professor NAGAI Toru, and Professor AKASHI Fumiko visited Bangkok, Thailand from 22 to 28 March 2015 to attend the Seminar on Promoting Community-based Treatment in the ASEAN Region.

Professor MORIYA Kazuhiko visited Jakarta, Indonesia from 23 to 27 March 2015 to research anti-corruption efforts in Southeast Asia.

Director YAMASHITA Terutoshi, Professor TASHIRO Akiko, Professor NAGAI Toru and Professor AKASHI Fumiko visited Doha, Qatar from 12 to 19 April 2015 to attend the 13th United Nations Congress on Crime Prevention and Criminal Justice (Congress).

Professor HIROSE Yusuke visited Hong Kong from 11 to 13 May 2015 to attend The 6th Independent Commission Against Corruption (ICAC) Symposium.

Director YAMASHITA Terutoshi and Professor NAGAI Toru visited Vienna, Austria from 18 to 22 May 2015 to attend the 24th Session of the Commission on Crime Prevention and Criminal Justice.

Professor MINOURA Satoshi and AKASHI Fumiko visited Tagaytay, Philippines from 20 to 21 May 2015 to attend the ASEAN Plus Three Forum on Probation and Community-Based Rehabilitation.

Director YAMASHITA Terutoshi visited Bangkok, Thailand from 4 to 5 June 2015 to attend the AsianSIL Inter-Sessional Regional Conference 2015.

Professor HIROSE Yusuke visited Bangkok, Thailand on 11 June 2015 to attend the Thailand Institute of Justice (TIJ) Seminar on Criminal Justice Human Resources.

FACULTY AND STAFF OF UNAFEI

Faculty:

Mr. YAMASHITA Terutoshi	Director
Mr. MORINAGA Taro	Deputy Director
Mr. MORIYA Kazuhiko	Professor 160th Course Programming Officer Chief of Training Division
Ms. WATANABE Ayuko	Professor 160th Course Deputy Programming Officer
Mr. YUKAWA Tsuyoshi	Professor
Mr. HIROSE Yusuke	Professor
Mr. YOSHIMURA Koji	Professor
Mr. NAGAI Toru	Professor Chief of Research Division
Mr. MINOURA Satoshi	Professor
Ms. AKASHI Fumiko	Professor Chief of Information and Public Relations
Mr. KAYA Tomonobu	Professor
Mr. Thomas L. Schmid	Linguistic Adviser

Secretariat:

Mr. ANDO Hiromitsu	Chief of Secretariat
Mr. SHOJIMA Naoki	Chief of General and Financial Affairs Section
Mr. ITO Jin	Chief of Training and Hostel Management Affairs Section

General and Financial Affairs Section:

Mr. MIYAGAWA Wataru	Senior Officer
Ms. EMA Ayako	Officer
Ms. ODA Michie	Officer

Training and Hostel Management Affairs Section:

Mr. TOYODA Yasushi	Senior Officer
Ms. SATO Marie	Senior Officer
Mr. OZAWA Yoichi	Officer
Mr. ENDO Yuki	Officer 160th Course Assistant Programming Officer

International Research Affairs Section:

Ms. HANDO Mayumi	Senior Officer
Ms. IWAKATA Naoko	Librarian

Secretarial Staff:

Ms. YAMADA Hisayo	Officer

Kitchen:

Ms. ODAGIRI Maki	Chef

JICA Coordinators for the 160th International Training Course:

Ms. KITA Chizuko	JICA
Ms. FUKUDA Noriko	JICA