



ISPAC
*International Scientific and Professional
Advisory Council
of the United Nations
Crime Prevention and Criminal
Justice Programme*



International Conference on
CYBERCRIME: Global Phenomenon and Its Challenges

at the initiative of
International Scientific and Professional Advisory Council of the United Nations
Crime Prevention and Criminal Justice Programme-ISPAC
Centro Nazionale di Prevenzione e Difesa Sociale-CNPDS
Courmayeur Foundation

in cooperation with
United Nations Office on Drugs and Crime-UNODC, Vienna
Korean Institute of Criminology - KIC, Seoul

Courmayeur Mont Blanc, Italy, 2-4 December 2011
Hôtel Pavillon

FONDAZIONE CRT

The development of new information and communication technologies (ICTs), including the use of computers and databases, have deeply changed the way our societies operate. Government agencies and companies rely on networks and store sensitive information electronically. Individuals use Internet for all sorts of activities from e-shopping to banking or maintaining contacts through social web-based networks. At the same time, this worldwide proliferation of ICTs has given rise to increasing forms of cyber-crime, which pose threats not only to the confidentiality, integrity, or availability of computer systems, but also to the security of critical infrastructure. Computer systems, the Internet, databases etc. have become tools of crime, constituting both an opportunity to facilitate the commission of traditional crimes such as fraud or extortion, and a vehicle for new types of crimes, which emerge in parallel to the development of new technologies. Cybercrime, or the criminal use of ICTs, has in fact penetrated into everyday life in many forms. Further, cybercrime, which is not constrained by national boundaries, often relies on governance failures in the criminal justice system (law enforcement, prosecution, judiciary, etc.), to thrive and operate with virtual impunity.

In recent years, the international community has become more aware of the need to further understand and begin to tackle this new transnational crime. This is expressed in the increasingly important mandates the United Nations, including the United Nations Office on Drugs and Crime (UNODC), has received from its Member States and governing bodies.

The 11th UN Congress on Crime Prevention and Criminal Justice, held in Bangkok, Thailand in 2005, recognized the seriousness of cybercrime, and a workshop was held on computer-related crimes. The Bangkok Declaration on Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, endorsed by General Assembly resolution 60/177 of December 2005, welcomed the efforts to enhance and supplement existing cooperation to prevent, investigate and prosecute high-technology and computer-related crime.

In 2010, the 12th UN Congress on Crime Prevention and Criminal Justice, held in Salvador de Bahia, Brazil, which had a strong focus on cybercrime, resulted in two very concrete outcomes. The Salvador Declaration recommended that the United Nations Office on Drugs and Crime (UNODC) provide technical assistance and training to States, upon request, to improve national legislation and build the capacity of national authorities in order to deal with cybercrime. In addition, the Salvador Declaration requested UNODC to convene an intergovernmental expert group to carry out a comprehensive study on the problem of cybercrime and responses to it by Member States, the international community and the private sector. The first meeting of this open-ended intergovernmental expert group took place from 17-21 January 2011 and, among other things,

the group endorsed the topics, methodology and timeline for the study. Both mandates were subsequently echoed by the Commission on Crime Prevention and Criminal Justice (Crime Commission), the Economic and Social Council and the General Assembly in resolution 65/230.

In April 2011, the Crime Commission adopted two resolutions relating to UNODC's work on cybercrime, underscoring the importance of the mandates of the Salvador Declaration: resolution 20/7 on the promotion of activities relating to combating cybercrime, including technical assistance and capacity-building which requested UNODC to continue to provide, upon request, technical assistance and training to States, based on national needs, especially with regard to the prevention, detection, investigation and prosecution of cybercrime in all its forms; and draft resolution I (currently at ECOSOC for endorsement) on "Prevention, protection and international cooperation against the use of new information technologies to abuse and/or exploit children".

It's clear that, although many steps have been taken, there is still the need for improved capacity-building, technical assistance, mutual legal assistance and international cooperation to combat cybercrime. Effective prevention and prosecution of cybercrime offences, first of all, require public awareness and coordinated criminal investigation. Technical assistance and training tools must be provided to enhance the capacity of developing countries to combat cybercrime. This will enable them to not only share knowledge and information to properly detect, investigate and prosecute cybercrime, but also to overcome the digital divide between developing countries and developed countries in this field.

Indeed, it is of concern that, given the inconsistent legal frameworks and lack of capacity, many countries are potential grey zones from which cyber criminals could operate and target the rest of the world with de facto impunity. Such trends of seeking "safe harbours" can already be witnessed. It is therefore essential to improve the capacities in those countries that are least developed in this regard.

Combating cybercrime is especially challenged by problems of jurisdiction that arise at both the national and international levels. The traditional forms of jurisdiction are based on the concept of boundaries, and laws are based on "territorial sovereignty". Because cyberspace has no physical boundaries, criminals can change their locations from one country to another within seconds in the cyber-world, irrespective of their physical location. Consequently, all States must also be able to use and contribute to international cooperation mechanisms. This is especially important for developing countries as they are often technologically less able to combat cybercrime, and thus especially vulnerable to being used as platforms from which to stage cybercrime.

In light of the above, it is essential that UN PNI members have the opportunity to discuss the global challenge of cybercrime and its countermeasures as a theme of 2011 ISPAC annual meeting. Through this meeting, members will discuss several topics. Session I of the conference will be devoted to find the right balance between security and civil liberties in the fight against cybercrime, debating topics under the light of Human Rights in the Technology Era. Privacy, freedom of expression and other fundamental rights will be examined by experts, academics and other institutions calling the attention of all countries worldwide. Session II will review technology development in particular, and Members will be able to examine specific case studies, such as data crimes, network crimes, access crimes and other crimes. In Session III Speakers will examine National Enforcement and Investigation practices against Cybercrime. The lack of formal policies and procedures as well as difficulties in sharing information will be considered as main obstacles to international cooperation. PNI research institutes will aim to call for more cooperative tasks at the regional and international levels.

PROGRAMME

Day 1
Friday 2 December
3 p.m.

Opening Session

Welcoming Remarks

- LODOVICO PASSERIN d'ENTRÈVES, *Courmayeur Foundation*
- FABRIZIA DERRIARD, *Mayor of Courmayeur*
- LIVIA POMODORO, *President, Court of Milan; CNPDS/ISPAC Chairman*
- KIM IL-SU, *President, Korean Institute of Criminology - KIC*

3.30 p.m.

Keynote Address

JOHN SANDAGE, *Director, Division for Treaty Affairs and Officer-in-Charge, Organized Crime Branch, United Nations Office on Drugs and Crime - UNODC*

4 p.m.

SESSION I

SECURITY AND CIVIL LIBERTIES IN THE FIGHT AGAINST CYBERCRIME

Chair and Introduction

ULRICH SIEBER, *Director and Head, Criminal Law Section, Max-Planck Institute*

- **Balancing Liberty and Security Fighting Cybercrime: Challenges for the Networked Society**
EMILIO VIANO, *Professor, Department of Justice, Law and Society, American University & Washington College of Law, Washington DC*

5 p.m.

Coffee Break

- **Fundamental legal principles for a balanced approach**
GIOVANNI BUTTARELLI, *Assistant European Data Protection Supervisor, EDPS, Brussels*
- **BEN HAYES, Statewatch - Monitoring the State and Civil Liberties in Europe, London, UK**

6.30 p.m.

Discussion

Day 2
Saturday 3 December
9 a.m.

SESSION II CASE STUDIES IN CYBERCRIMINALITY

Chair

JOON OH JANG, *Senior Research Fellow, Director of International Center for Criminal Justice, Korean Institute of Criminology - KIC*

- United against cybercrime: The UNODC/ITU cybercrime capacity building initiative
GILLIAN MURRAY, *Chief, Focal Point for Cybercrime, Conference Support Section, Division for Treaty Affairs UNODC*
CARLA LICCIARDELLO, *Project Officer on Cybersecurity, International Telecommunication Union - ITU*
- Exploring the International Market for Stolen Data and Malware
THOMAS HOLT, *Associate Professor, School of Criminal Justice Michigan State University, USA*
- Patterns of Cyber Victimization
K. JAISHANKAR *Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Executive Director, Centre for Cyber Victim Counselling, India*

Coffee Break

11 a.m.

SESSION II Continue

Chair

DUNCAN CHAPPELL, *Professor of Criminal Law, Faculty of Law, University of Sydney*

- Organised Cybercrime: Myth or Reality, Malignant or Benign?
ROB McCUSKER, *Director of Centre for Fraud and Financial Crime, University of Teesside Middlesbrough, UK*
- The Perspective of Europol on Cybercrime ROBERTO

FERNANDEZ ALONSO, *Europol Cybercrime Center,
The Netherlands*

12.30 p.m.

Discussion

1 p.m.

Lunch

3 p.m.

**SESSION III
NATIONAL ENFORCEMENT AND INVESTIGATION
AGAINST CYBERCRIME**

Chair

LUIS ARROYO ZAPATERO, *Director, Instituto de de Derecho
Penal Europeo e Internacional, Ciudad Real, España*

- China New Criminal Legislation on Cybercrime in the Common Internet
PI YONG, *Professor School of Law, Wuhan University, China*
- WONSANG LEE, *Associate Research Fellow, Korean Institute of Criminology, South Korea*
- Cyber Criminal Law; Perspectives, Policies and Legislation in Iran
BATOUL PAKZAD, *Associate Professor, Ph.D of Criminal Law and Criminology, Legal Consultant, Ministry of Justice, I.R. of Iran*
GHASSEM GHASSEMI, *Lawyer and Lecturer at Law, Islamic Azad University, Teheran, I.R. of Iran*

5.30 p.m.

Discussion

Day 3

Sunday 4 December

9 a.m.

**SESSION IV
NEW NATIONAL AND INTERNATIONAL LEGAL
RESPONSES TO CYBERCRIME**

Chair

GILLIAN MURRAY, *Chief, Focal Point for Cybercrime,
Conference Support Section, Division for Treaty Affairs
UNODC*

- The Budapest Convention 10 years on: Lessons learnt
ALEXANDER SEGER, *Secretary Cybercrime*

Convention Committee and Head of Data Protection and Cybercrime Division, Council of Europe, Strasbourg

- Potential new global legal mechanisms on combating cybercrime and global cyberattacks
STEIN SCHJOLBERG, Judge, Co-chair of the EastWest Institute (EWI) Cybercrime Legal Working Group, Oslo
- Current trends in the harmonization of Cybercrime legislation
MARCO GERCKE, Director, Cybercrime Research Institute, Köln University, Germany
- Cyberselfdefense against Cybercrime
MIGUEL ONTIVEROS ALONSO, Director of the National Institute for Criminal Science of Mexico, Mexico (OAS)

General Discussion

11 a.m.

Closing Remarks and Recommendations

11.30 a.m.

STEFANO MANACORDA, Professor of Criminal Law, University of Naples II, Italy; Collège de France, Paris; Deputy Chair ISPAC Board

Conference Venue
Conference Hall, Hôtel Pavillon
Via Regionale, 62 - 11013 Courmayeur (AO)

Official languages
English and Italian with simultaneous interpretation

Conference Secretariat
Fondazione Centro nazionale di prevenzione e difesa sociale-CNPDS
Palazzo Comunale delle Scienze Sociali
3, Piazza Castello - 20121 Milano MI
Phone: +39 02 86.46.07.14 - Fax: +39 02 72.00.84.31
E-mail: cnps.ispac@cnps.it - Home page: www.cnps.it
Home page: <http://ispac.cnps.org>