United Nations A/CONF.213/IE/7

Twelfth United Nations Congress on Crime Prevention and Criminal Justice

Salvador, Brazil, 12-19 April 2010

Distr.: General
23 March 2010

Original: English

Items 8 of the provisional agenda*

Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime

Background documents** received from individual experts***

A CYBERSPACE TREATY - A UNITED NATIONS CONVENTION OR PROTOCOL ON CYBERSECURITY AND CYBERCRIME

Prepared by

Stein Schjolberg

* A/CONF.213/1.

** Distribution is limited to the quantities and languages in which the paper is made available to the United Nations Office on Drugs and Crime.

*** The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

A Cyberspace Treaty - A United Nations Convention or Protocol on Cybersecurity and Cybercrime

Ancillary Meeting Tuesday April 13, 2010, 1630-1800, Room 4
Background paper

By JUDGE STEIN SCHJOLBERG, Norway [1]

1. Introduction

Cyberspace, as the fifth common space – after land, sea, air and outer space, is in great need for coordination, cooperation and legal measures among all nations. Deterrence against cyberthreats may best be achieved through a global United Nations framework. A Cyberspace Treaty, including cybersecurity and cybercrime, should be the framework for peace and security in cyberspace.

The rapid growth of cyberspace has created new opportunities for criminals in perpetrating crime, or to exploit vulnerabilities and attack countries' critical information infrastructure. The costs associated with cybercrime and cyberattacks are significant – in terms of lost revenues, loss of sensitive data, and damage to equipment. The future growth and potential of the online information society are in danger from growing cyberthreats. Cyberthreats are global problems and they need a global harmonization, involving all stakeholders.

The progressive developments of cyberthreats against sovereign States, such as massive and coordinated attacks against critical information infrastructures, will necessitate a global response. Regional and bilateral agreements may not be sufficient. International Law is necessary to make the global community able to deter the urgent and increasing cyberthreats.

In order to reach for a common understanding of cybersecurity and cybercrime among countries at all stages of economic development, a United Nations Cyberspace Treaty should be established that includes solutions aimed at addressing the global challenges.

Cyberspace is one of the great legal frontiers of our time. From 2000 to 2009, the Internet has expanded at an average rate of 380 % on a global level, and currently an estimated

---

[1] Judge Stein Schjolberg is an international expert on global harmonization of cybercrime legislations. He has served as an expert for several international institutions and organizations since 1980. He was in 2007-2008 the Chairman of the High-level Experts Group (HLEG) at the International Telecommunication Union (ITU) in Geneva. See www.cybercrimelaw.net

1,7 billion people are "on the Net."[2] The increase in Asia has been 545% and in Africa 1,392%.

Cybersecurity and cybercrime, and terrorists use of the Internet, are cyberthreats of vital concerns, involving all stakeholders. A global framework is necessary for harmonizing security measures against risks and threats. This may also provide for essential architecture in developing national and international solutions. A global agreement may also reduce cybersecurity digital divide for developing countries.

The United Nations International Law Commission should consider a draft code of a Cyberspace Treaty – A Convention or a Protocol on Cybersecurity and Cybercrime. Peace and security of cyberspace should be a part of the progressive development of international law.

I recommend that the International Law Commission, due to the urgency of the global challenges, establish a working group to handle this topic. This group may undertake preliminary work or help to define the scope and direction.

2. A United Nations Cyberspace Treaty – A Convention or Protocol on Cybersecurity and Cybercrime

The International Law Commission adopted at its forty-eight session in 1996 *The Draft Code of Crimes against Peace and Security of Mankind*, and submitted it to the United Nations General Assembly. Crimes against the peace and security of mankind were then established as crimes under international law, whether or not they were punishable under national law.

Serious crimes against peace and security in cyberspace should be established as crimes under international law through a Cyberspace Treaty on the United Nations level whether or not they were punishable under national law.

The International Telecommunication Union (ITU) launched in May 2007 the Global Cybercrime Agenda (GCA) for a framework where the international response to growing challenges of cybersecurity could be coordinated. In order to assist the ITU in developing strategic proposals, a global High-Level Experts Group (HLEG) was established in October 2007. This global experts group of almost 100 persons delivered the Chairman's Report in August 2008 with recommendations, including cyber crime legislations. The Global Strategic Report was delivered in November 2008, including strategies in five work areas: Legal measures, Technical and procedural measures, Organizational structures, Capacity building, and International cooperation. Both reports were based on broad agreements in the HLEG.

As a follow-up of the HLEG reports, a paper on a Global Protocol on Cybersecurity and Cybercrime[3] was presented at the Internet Governance Forum (IGF) in Sharm El Sheikh, Egypt, in November 2009.

---

[2] See World Internet Usage and Population Statistics, http://www.internetworldstats.com/stats.htm (September 2009).

[3] See www.cybercrimelaw.net

The criminal conducts in cyberspace are global and a global harmonization of cybercrime legislation covering new conducts should be established in a Cyberspace Treaty. The Council of Europe Convention on Cybercrime (2001) is based on criminal cyber conducts in the late 1990s and do not necessary be suitable for the 2010s.

3. Substantive criminal law and procedural law in a Cyberspace Treaty

In order to establish criminal offences in Cyberspace, provisions must be enacted with as much clarity and specificity as possible, and not rely on vague interpretations in the existing laws. When cybercrime laws are adopted, perpetrators will be convicted for their explicit acts and not by existing provisions stretched in the interpretations, or by provisions enacted for other purposes covering only incidental or peripheral acts.

3.1. The Council of Europe Convention on Cybercrime is an example of a regional initiative on legal measures that may be used as a guideline or as a reference. The basic standards and principles in this convention may be implemented in a Cyberspace Treaty, considering the countries reservations and declarations. Application of some provisions in this convention may also prejudice countries sovereignty and national security. Articles 2-9 on substantive criminal law in the Convention covers illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud and offences related to child pornography. Many countries, especially in Asia, do not have traditions on copyright legislations such as covered by Article 10 on Offences related to infringements of copyright and related rights. That makes it not naturally to include this principle in a global Protocol for recommendations of measures to be implemented.

Many member countries have ratified or signed to the Convention. With regard to the exceptions, it must be emphasized that Russia will not make a signature to the Convention due to the existence of Article 32: Trans-border access to stored computer data with consent or where publicly available.

The HLEG recommendations and proposals may also be used as a guideline or as a reference for substantive criminal law and procedural law. The discussions at the HLEG meetings and the recommendations have revealed that to most other global regions it still is a European convention. The HLEG were in broad agreement on the following:

> *«Considering the Council of Europe´s Convention on Cybercrime as an example of legal measures realized as a regional initiative, countries should complete its ratification, or consider the possibility of acceding to the Convention on Cybercrime. Other countries should, or may want to, use the Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contain, in accordance with their own legal system and practice.*
>
> *It is very important to implement at least Articles 2-9 in the substantive criminal law section, and to establish the procedural tools necessary to investigate and prosecute such crimes as described in Articles 14-22 in the section on procedural law.»*

It is in other words necessary within a global framework to recommend the accepted standards and principles, with certain important exceptions. Some countries do not accept all principles, and must be respected for their opinions.

3.2. Terrorism in cyberspace consists of both cybercrime and terrorism. Terrorist attacks in cyberspace are a category of cybercrime and a criminal misuse of information technologies. The developments have blurred the differences between cybercrime and cyberterrorism. Terrorism has been used to describe criminal conducts long before the computer communication and network technology was introduced. International organizations have been involved in the prevention of such acts for a long period, but the global society has not yet been able to agree upon a universal definition on terrorism. In the final conference on preparing for the establishment of an international criminal court,[4] other serious crimes such as terrorism were discussed, but the conference regretted that no generally acceptable definition could be agreed upon.

We are already today facing urgent growing problems of terrorist use of the Internet, and massive and coordinated cyber attacks against critical information infrastructure of a country. These developments must be discussed in a process for a global Cyberspace Treaty.

In Europe a Council of Europe treaty *The European Convention on the Suppression of Terrorism* was adopted in 1977 as a multilateral treaty. The treaty was in 2005 supplemented by the Council of Europe Convention on the Prevention of Terrorism.

According to the Convention on the Prevention of Terrorism, Articles 5-7, the parties to the Convention are required to adopt certain preparatory conducts that have a potential to lead to terrorist acts, as criminal offences.[5]

Public provocation to commit a terrorist offence is a criminal offence if the distribution of a message to the public, "whether or not directly advocating terrorist offences, causes a danger that one or more such offences may be committed" (Article 5). Presenting a terrorist offence as necessary and justified is a criminal offence. A specific intent is required to incite the commission of a terrorist offence. The provocation must in addition be committed unlawfully and intentionally.

Recruitment for terrorism is also a criminal offence if a person is solicited "to commit or participate in a commission of a terrorist offence, or to join an association or group, for the purpose of contributing to the commission of one or more terrorist offences by the association or the group" (Article 6). The recruitment for terrorism may be carried out through the use of Internet, but it is required that the recruiter successfully approach the person. The recruitment must be unlawfully and intentionally.

Training for terrorism is a criminal offence if instructions are provided for "making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques" (Article 7). The purpose must be to execute the terrorist offence or contribute to it. The trainer must have knowledge of that skills or "know-how" and intended to be used for the carrying out of the terrorist offence or for a contribution to it. The training must be unlawfully and intentionally.

Member countries should complete their ratification of the Council of Europe Convention on the Prevention of Terrorism of 2005. Other countries should, or may want to, use the

---

[4] Final Act of the United Nations diplomatic conference of plenipotentiaries on the establishment of an International Criminal Court, Rome July 17, 1998 (U.N. Doc. A/CONF.183/10)

[5] See http://conventions.coe.int

Convention as a guideline, or as a reference for developing their internal legislation, by implementing the standards and principles it contains, in accordance with their own legal system and practice. It is very important to implement at least Articles 5-7.

3.3. Cyber attacks may include the use of botnets that is designed or intended to destroy or seriously disrupt critical information infrastructure of vital importance to a country. These conducts are global problems and need a global solution.

3.4. Phishing may be carried out through the use of botnets. Botnets may include thousands of compromised computers, and are produced and offered on the marked to criminals for sale or lease also with the intent of cyber attacks. It is estimated that at least 80% of phishing incidents are carried out through botnets. The individual access is normally considered as illegal access to computer systems and illegally obtaining information

Another method is sending of e-mail messages, falsely claiming or pretending to be from a legitimate organization or company. The victim may also be lured to counterfeit or fake Web sites that look identical to the legitimate web sites maintained by banks, insurance company, or a government agency. The e-mails or websites are designed to impersonate well known institutions, very often using spam techniques in order to appear to be legal. Company logos and identification information, web site text and graphics are copied, thus making the conducts possible criminal conducts as forgeries or frauds.

The emails may appear to be from the "billing center" or "account department". The text may often contain a warning that if the consumer did not respond, the account would be cancelled. A link in the e-mail may take the victim to what appeared to be the Billing Center, with a logo and live links to real company web sites. The victim may then be lured to provide the phisher with "updated" personal and financial information, that later will be used to fraudulently obtain money, goods or services. Such cases may cost Internet service providers a millions dollar to detect and combat the phishing scheme.

The perpetrator may also purchase, sell or transfer the illegally obtained information to other criminals. The trafficking of stolen personal or financial information could be provided to third parties through a web site or a closed web forum and will use it to obtain money, credit goods and services. In such cases, the perpetrators openly engage in the sale of information. It may be a criminal offence, especially if the information is illegally obtained access codes. In other cases it may not be covered by criminal codes.

3.5. Preparatory acts. Criminal laws on cybercrime may also cover preparatory conducts to traditional cybercrime provisions, by establishing the acts as independent separate statutes.

In China, the Penal Code section 22 on preparatory crime, make the following acts a criminal offence:

- Preparation of tools to commit a crime
- Creation of conditions to commit a crime

In Sweden, an amendment of 23 chapter 2 BrB on preparatory acts was adopted on July 1, 2001, in conjunction with other amendments in the Penal Code. It was especially emphasized that the introduction of a specific Article on preparatory acts was directed not only at ordinary crimes, but also at the problems with computer virus and other

computer programs that solely was created for the purpose to obtain illegal access to data or other computer crime. The Article includes:

> *"any involvement with something that is especially suitable to be used as a tool for a crime"*

A provision on preparatory acts may be found in the Convention on Cybercrime Article 6, but may also be as follows:

> *"The production, obtaining, possession, sale or otherwise making available for another, computer programs and data especially suitable as a tool for criminal conducts in a computer system or network, when committed intentionally, shall be punished as a preparatory act to criminal offences."*

Another alternative may be expanding the traditional concept of "attempting to commit an offence" to include all categories of intentional preparatory acts.

3.6. Identity theft is fundamentally, the misuse of personal information belonging to another to commit fraud. The theft or identity infringement of the information itself does not ordinarily constitute a criminal offence. A great number of people around the world suffer the financial and emotional trauma of identity theft.

Some countries use the term "identity theft" when perpetrators obtains, often thousands of credit and debit card numbers, social security numbers, and other personal identification information. The new Penal Code in Norway (2009) avoids the term "theft", using a substitution such as "identity infringement".

The crime itself was known before computers were around, but through the use of information and communication technology, it has turned into a very nasty business.

In most countries, no legislation exists covering the phishing by itself or as identity theft and a global cyberspace treaty is needed.

One exception is the United States, where federal legislation and almost all states have adopted laws on identity theft that may also be applied against criminal conducts through computer systems.

The main section is US Penal Code § 1028. This section criminalizes eight categories of conduct involving fraudulent identification documents or the unlawful use of identification information. § 1028 (a)(7) was adopted in 1998, amended in 2004 and reads as follows:

> *"Whoever, in a circumstance described in subsection (c) of this section-*
>
> *(7) knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable, shall be punished as provided in subsection (b) of this section.*

The term "means of identification" is defined as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual. The section will apply to both online and manual crime cases, and may be a model law for other countries now facing special laws on identity theft. Aggravated Identity Theft was established in § 1028A as a new offense in 2004. § 1028A adds an additional two-year

term of imprisonment whenever a perpetrator knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person during and in relation to any felony violation of certain federal offenses.

In Europe, the new Norwegian Penal Code (2009) has in § 202 a provision on Identity Infringements that reads as follows:

> *"With a fine or imprisonment not exceeding 2 years shall whoever be punished, that without authority possesses of a means of identity of another, or acts with the identity of another or with an identity that easily may be confused with the identity of another person, with the intent of*
>
> *a) procuring an economic benefit for oneself or for another person, or*
>
> *b) causing a loss of property or inconvenience to another person."*

3.7. Crime in social networks and virtual worlds. Social networks services are building online communities of individuals that shares common interests or activities, or interchange information with friends. The most important global social networking are Facebook, MySpace, and Twitter with several hundred million users. Social networks are also used by criminals, mostly for identity thefts and fraud.

Online games[6] are like a mirror of human beings behaviors where players are allowed to build virtual objects with defined economic values. Virtual currency supports commerce that offers virtual objects for sale. Exchanging the virtual currency to real-world currency is also established.

3.8. Procedural law. The standards and principles on procedural law in the Council of Europe Convention on Cybercrime (2001) Articles 14-25 are commonly accepted as necessary measures for an efficient investigation[7] and prosecution of criminal conducts in cyberspace, both nationally and in a global perspective.

Adopting procedural laws necessary to establish powers and procedures for the prosecution of criminal conducts in cyberspace are essential for a global investigation and prosecution of cybercrime. But such powers and procedures are also necessary for the prosecution of other criminal offences committed by means of a computer system, and should apply on the collection of evidence in electronic form of all criminal offences. (Article 14)

International coordination and cooperation are necessary in prosecuting cybercrime and require innovation by international organizations and governments. The Council of Europe Convention on Cybercrime Articles 23-25 address basic requirements for international cooperation in cybercrime cases.

3.8.1. The real-time collection and recording of traffic data, interception of content data, data retention, and the use of key-loggers, are among challenges that constitute discussions today. A special problem has been caused by Voice over Internet Protocol (VoIP). The old methods of recording vocal human voices are no longer possible. In most countries, no procedural legislation exists covering all these new powers and procedures

---

[6] See Marco Gercke: ITU Global Strategic Report 1.6.2.4, page 37 (2008)

[7] See Marc Goodman: ITU Global Strategy Report 1.8, page 51 (2008). This chapter contains a detailed and comprehensive presentation of the challenges for law enforcement

in cyberspace. VoIP and other new technologies may be a challenge for law enforcement in the future. It is important that law enforcement, government, the VoIP industry and ICT community consider ways to work together to ensure that law enforcement has the tools it needs to protect the public from criminal activity.

Given the ever changing nature of ICTs, it is challenging for law enforcement in most parts of the world to keep up with criminals in their constant efforts to exploit technology for personal and illegal gains. With this in mind, it is critical that the police work closely with government and other elements of the criminal justice system, Interpol and other international organizations, the public at large, the private sector and non-governmental organizations to ensure the most comprehensive approach to addressing the problem.

3.8.2. Cloud computing are means to provide remote computer services in cyberspace. Users have no knowledge of, or expertise in, or control over, the technology infrastructure in the "cloud" that support them. Cloud computing do not allow users to physically possess the storage of their data, and the user leave the responsibility of data storage and control to the provider.

The "cloud" may be the ultimate category of globalization, since it could cover many borders and regions. The users could be offered selected "availability zones" around the world. That may create great concern with regard to multi-jurisdictional crime scenarios for the investigation and prosecution of criminal acts, and a global harmonization of procedural laws should be developed through a cyberspace treaty. These problems may only be solved through a global Cyberspace Treaty that includes necessary jurisdictional provisions under international law, whether or not they are possible to prosecute under national law.

3.8.3. Data retention refers to the storage of Internet traffic and transaction data, usually of telecommunications, emails, and websites visited. The purpose for data retention is traffic data analysis and mass surveillance of data, in order to avoid problems of getting access to traffic data before they are deleted.

The European Union adopted in 2006 a *Directive on the retention of data*.[8] The data must be available to law enforcement for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State. The Directive requires that communications providers must retain, for a period of between six months and two years, necessary data as specified in the Directive in order:

- to trace and identify the source of a communication
- to trace and identify the destination of a communication
- to identify the date, time and duration of a communication
- to identify the type of communication
- to identify the communication device
- to identify the location of mobile communication equipment

---

[8] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

The implementation of a data retention approach is one approach to avoid the difficulties of getting access to traffic data before they are deleted, and countries should carefully consider adopting such procedural legislation.

4. An International Criminal Court

A criminal prosecution of international law need an international criminal court for the proceedings of the criminal cases.

The International Criminal Court (ICC)[9] that was established in 1998 is the first ever permanent, treaty based, fully independent international criminal court established to promote the rule of law and ensure that the gravest international crimes do not go unpunished. The Court do not replace national courts, the jurisdiction is only complementary to the national criminal jurisdictions. It will investigate and prosecute if a State, party to the Rome Statute[10] that entered into force in 2002, is unwilling or unable to prosecute. Anyone, who commits any of the crimes under the Statute, will be liable for prosecution by the Court.

A State is unwilling whenever it appears to be a lack of genuine will to investigate or prosecute the crime. A State is unable whenever it appears to be a total or substantial collapse of its judicial system, or by some reason is unable to obtain the accused or the necessary evidence and testimony or otherwise unable to carry out its proceedings due to its unavailability.

The jurisdiction of the International Criminal Court is limited to States that becomes Parties to the Rome Statute. The maximum term of imprisonment is 30 years, and also a life sentence may be imposed.

In the final diplomatic conference in Rome serious crimes such as terrorism crimes were discussed, but the conference regretted that no generally acceptable definition could be agreed upon. The conference recognized that terrorist acts are serious crimes of concern to the international community, and recommended that a review conference pursuant to the article 123 of the Statute of the International Criminal Court consider such crimes with the view of their inclusion in the list within the jurisdiction of the Court. The review conference is held in Kampala, Uganda, in April-May 2010.

Massive and coordinated cyber attacks against critical information infrastructures may also qualify as a "serious crime", even if it may not be considered as terrorism. Expanding the jurisdiction should also include other serious crimes in cyberspace.

---

[9] See www.icc-cpi.int

[10] See http://untreaty.un.org/cod/icc/index.html

5. The International Law Commission (ILC)

I have on January 29, 2010 sent a following letter to the Secretary of the United Nations International Law Commission [11] titled: A United Nations Convention or Protocol on Cybersecurity and Cybercrime.

The main parts of this letter is as follows:

«In order to reach for a global agreement on cybersecurity and cybercrime among countries at all stages of economic development, the International Law Commission should consider a draft code of a Convention or a Protocol. Peace and security of cyberspace should be a part of the progressive development of international law.

It is now in my opinion, necessary to make the International Law Commission aware of the need for a global response to the urgent cyberthreats and cyberattacks. These are new developments in international law and pressing concerns of the international community as a whole.

...

In addition, the progressive developments of cyberthreats and transnational cyber attacks against sovereign States, such as massive and coordinated attacks against critical information infrastructures, will necessitate an urgent response for a global legal framework.

A global10 cybersecurity framework is necessary for harmonizing international security measures to protect information and communication technology. This may also prevent such threats and attacks in cyberspace and provide for essential architecture in developing national and international solutions. A global agreement on cybersecurity and cybercrime may also reduce the cybersecurity digital divide for developing countries.

I recommend that the Commission due to the urgency of the global challenges establish a working group to handle this topic. This group may undertake preliminary work or help to define the scope and direction.»

[11] See www.un.org/law/ilc

APPENDIX

Biography of Stein Schjolberg

Stein Schjolberg is the Chief judge of Moss tingrett Court in Norway. He was appointed as a judge in 1984 and a Chief judge since 1994. Until 1984 he served as a prosecutor and an Ass. Commissioner of Police in Oslo.

Judge Schjolberg is an international expert on cybercrime, and one of the founders of the harmonization of national criminal law on computer crime. He was a Fulbright Scholar at Stanford Research Institute (SRI International) in 1981-82. He has published widely on computer crime and cybercrime law. Judge Schjolberg has served as an expert on cybercrime for several international institutions.

He was in 2007-2008 appointed as Chairman of the global High-Level Experts Group (HLEG) on Cybersecurity and Cybercrime at the International Telecommunication Union (ITU) in Geneva. The Chairmans´s Report was published in August 2008 and the Global Strategic Report on Cybersecurity and Cybercrime in November 2008.

Some of Judge Schjolberg's recent international presentations on cybercrime includes:

- *EastWest Institute Worldwide Cybersecurity Conference, Brussels, (2010)*
- *Internet Governance Forum (IGF), Sharm El Sheikh, Egypt (2009)*
- *World Bank Seminars, Ankara and Istanbul, Turkey (2009)*
- *European Network Forensic and Security Conference, Heerlen, The Netherlands (2008)*
- *International Conference on Forensic Issues, Riga, Latvia (2008)*
- *XVth World Congress of Criminology, Barcelona, Spain (2008)*
- *The 7th Interpol International Conference on Cyber Crime, New Dehli, India, (2007)*
- *ITU Asian-Pacific Regional Workshop on Cybersecurity and Critical Information Infrastructure Protection, Hanoi, Vietnam, 2007,*
- *Digital PhishNet 2007 Conference, Berlin, Germany, 2007,*
- *The International Telecommunication Union (ITU), Geneva, Switzerland, 2007, 2006 and 2005,*
- *NATO Advanced Research Workshop on Cyberterrorism, Sofia, Bulgaria (2006),*
- *Council of Europe Conference, Strasbourg, France (2006),*
- *The International Criminal Law Network, The Hague, The Netherlands (2005),*
- *The 11th United Nations Crime Conference, Bangkok, Thailand (2005).*
- *Council of Europe Conference, Strasbourg, France (2004)*
- *Council of Europe Conference, Sinaia, Romania (2003)*
- *OECD Cybercrime Workshop, Oslo Norway (2003)*
- *The 13th World Congress of Criminology, Rio de Janeiro, Brazil (2003)*
- *The 5th Interpol International Conference on Computer crime, Seoul, Korea (2003)*
- *Conference on International Cooperation to Combat Cyber Crime and terrorism, Stanford University, USA (1999)*

For more information see his websites www.cybercrimelaw.net